AppScan 360°

HCL AppScan Report

Report Type: Compliance Security Report

Scan Name: Sample Report [mode=demo]

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:	55
Low severity issues:	12
Informational severity issues:	16
Total security issues:	**99**

The Payment Card Industry Data Security Standard (PCI) Version 4.0

Summary

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data.

PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personal information or other data elements (for example, cardholder name). PCI DSS does not supersede local or regional laws, government regulations, or other legal requirements.

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data.

“System components” include network devices, servers, computing devices, and applications. Examples of system components include but are not limited to the following: Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or web redirection servers) the CDE.

Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.

Network components including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.

Server types including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).

Applications including all purchased and custom applications, including internal and external (for example, Internet) applications. Any other component or device located within or connected to the CDE.

Covered Entities

PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

PCI DSS requirements apply to organizations and environments where account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted. Some PCI DSS requirements may also be applicable to organizations that have outsourced their payment operations or management of their CDE1. Additionally, organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the account data is protected by the third party per the applicable PCI DSS requirements.

Compliance Penalties

If a merchant or service provider does not comply with the security requirements or fails to rectify a security issue, the card companies may fine the acquiring member, or impose restrictions on the merchant or its agent.

Compliance Required By

PCI DSS version 4.0 has replaced PCI DSS version 3.2.1 and is effective as of April 2024. The PCI DSS version 3.2.1 may not be used for PCI DSS compliance after March 31, 2024.

Regulators

The PCI Security Standards Council, and its founding members including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International.

For more information on the PCI Data Security Standard, please visit:

https://www.pcisecuritystandards.org./index.htm

For more information on securing web applications, please visit https://www.hcltechsw.com/products/appscan

Violated Section

Sections	Number of Issues
Requirement 2 - Apply secure configurations to all system components	27
Requirement 2.2.2 - If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. If the vendor default account(s) will not be used, the account is removed or disabled.	27
Requirement 2.2.4 - Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	28
Requirement 2.2.6 - System security parameters are configured to prevent misuse.	27
Requirement 4 - Protect cardholder data with strong cryptography during transmission over open, public networks	3
Requirement 5 - Protect all systems and networks from malicious software	1
Requirement 6 - Develop and maintain secure systems and applications.	99
Requirement 6.2.1 - Bespoke and custom software are developed securely	99
Requirement 6.2.4.1 - Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws.	10
Requirement 6.2.4.2 - Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.	2
Requirement 6.2.4.3 - Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.	41
Requirement 6.2.4.4 - Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).	16
Requirement 6.2.4.5 - Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms.	7
Requirement 6.3 - Security vulnerabilities are identified and addressed	99
Requirement 6.3.2 - An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	1
Requirement 6.3.3 - All system components are protected from known vulnerabilities by installing applicable security patches/updates.	28
Requirement 6.4 - Public-facing web applications are protected against attacks.	99
Requirement 6.5.6 - Test data and test accounts are removed from system components before the system goes into production.	11
Requirement 7 - Restrict access to system components and cardholder data by business need to know.	84
Requirement 7.1 - Limit access to system components and cardholder data to only those individuals whose job requires such access.	28
Requirement 7.2.2 - Access is assigned to users, including privileged users, based on: Job classification and function and least privileges necessary to perform job responsibilities.	2
Requirement 7.2.6 - All user access to query repositories of stored cardholder data is restricted as follows: Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. Only the responsible administrator(s) can directly access or query repositories of stored CHD.	72
Requirement 8.2.8 - If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	1
Requirement 8.3.1 - All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: Something you know, such as a password or passphrase. Something you have, such as a token device or smart card. Something you are, such as a biometric element	64
Requirement 8.3.2 - Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	22
Requirement 8.6.2 - Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.	0
Requirement 11.4 - External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.	99

Section Violation by Issue

Location	Issue Type	Sections
https://demo.testfire.net/bank/showTransactions	SQL Injection	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 11.4
https://demo.testfire.net/bank/showTransactions	SQL Injection	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 11.4
https://demo.testfire.net/doLogin	SQL Injection	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 11.4
https://demo.testfire.net/doLogin	SQL Injection	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 11.4
https://demo.testfire.net/bank/showAccount	Integer Overflow	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.2, Requirement 6.3, Requirement 6.4, Requirement 6.5.6, Requirement 7, Requirement 11.4
https://demo.testfire.net/bank/doTransfer	Integer Overflow	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.2, Requirement 6.3, Requirement 6.4, Requirement 6.5.6, Requirement 7, Requirement 11.4
https://demo.testfire.net/bank/customize.jsp	Phishing Through URL Redirection	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.5, Requirement 6.3, Requirement 6.4, Requirement 11.4
https://demo.testfire.net/sendFeedback	Reflected Cross Site Scripting	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/bank/customize.jsp	Reflected Cross Site Scripting	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/bank/queryxpath.jsp	Reflected Cross Site Scripting	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/sendFeedback	Reflected Cross Site Scripting	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4

https://demo.testfire.net/search.jsp	Reflected Cross Site Scripting	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/index.jsp	Reflected Cross Site Scripting	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/util/serverStatusCheckService.jsp	Reflected Cross Site Scripting	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/bank/queryxpath.jsp	Reflected Cross Site Scripting	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/bank/customize.jsp	Reflected Cross Site Scripting	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/bank/apply.jsp	Autocomplete HTML Attribute Not Disabled for Password Field	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/admin/admin.jsp	Autocomplete HTML Attribute Not Disabled for Password Field	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/showTransactions	Body Parameters Accepted in Query	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4

https://demo.testfire.net/bank/doTransfer	Body Parameters Accepted in Query	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/admin/admin.jsp	Body Parameters Accepted in Query	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/showAccount	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/transfer.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/customize.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/util/serverStatusCheckService.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/transaction.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/queryxpath.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/main.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/apply.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/admin/admin.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4

https://demo.testfire.net/bank/showAccount	Credit Card Number Pattern Found (Visa)	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/transfer.jsp	Credit Card Number Pattern Found (Visa)	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/main.jsp	Credit Card Number Pattern Found (Visa)	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/doTransfer	Credit Card Number Pattern Found (Visa)	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/showTransactions	Cross-Site Request Forgery	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7.1, Requirement 11.4
https://demo.testfire.net/bank/doTransfer	Cross-Site Request Forgery	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7.1, Requirement 11.4
https://demo.testfire.net/bank/customize.jsp	Cross-Site Request Forgery	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7.1, Requirement 11.4
https://demo.testfire.net/admin/admin.jsp	Cross-Site Request Forgery	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7.1, Requirement 11.4
https://demo.testfire.net/bank/showTransactions	Database Error Pattern Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 11.4
https://demo.testfire.net/bank/showTransactions	Database Error Pattern Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 11.4
https://demo.testfire.net/bank/showTransactions	Database Error Pattern Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 11.4

https://demo.testfire.net/doLogin	Database Error Pattern Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 11.4
https://demo.testfire.net/doLogin	Database Error Pattern Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 11.4
https://demo.testfire.net/doLogin	Database Error Pattern Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 11.4
https://demo.testfire.net/	Direct Access to Administration Pages	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.2, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/	Encryption Not Enforced	Requirement 4, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/bank/queryxpath.jsp	Host Header Injection	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 11.4
https://demo.testfire.net/doLogin	Inadequate Account Lockout	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.2, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/	Insecure "OPTIONS" HTTP Method Enabled	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 11.4
https://demo.testfire.net/	Insecure "OPTIONS" HTTP Method Enabled	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 11.4
https://demo.testfire.net/search.jsp	Link Injection (facilitates Cross-Site Request Forgery)	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/index.jsp	Link Injection (facilitates Cross-Site Request Forgery)	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4

https://demo.testfire.net/sendFeedback	Link Injection (facilitates Cross-Site Request Forgery)	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/util/serverStatusCheckService.jsp	Link Injection (facilitates Cross-Site Request Forgery)	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/bank/customize.jsp	Link Injection (facilitates Cross-Site Request Forgery)	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/bank/queryxpath.jsp	Link Injection (facilitates Cross-Site Request Forgery)	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/	Missing HttpOnly Attribute in Session Cookie	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/	Missing or insecure Cross-Frame Scripting Defence	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/	Missing Secure Attribute in Encrypted Session (SSL) Cookie	Requirement 4, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/	Missing Secure Attribute in Encrypted Session (SSL) Cookie	Requirement 4, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.2.4.4, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/bank/main.jsp	Older TLS Version is Supported	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/search.jsp	Phishing Through Frames	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 11.4

https://demo.testfire.net/index.jsp	Phishing Through Frames	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 11.4
https://demo.testfire.net/sendFeedback	Phishing Through Frames	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 11.4
https://demo.testfire.net/sendFeedback	Phishing Through Frames	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 11.4
https://demo.testfire.net/util/serverStatusCheckService.jsp	Phishing Through Frames	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 11.4
https://demo.testfire.net/bank/customize.jsp	Phishing Through Frames	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 11.4
https://demo.testfire.net/bank/queryxpath.jsp	Phishing Through Frames	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 11.4
https://demo.testfire.net/doLogin	Session Identifier Not Updated	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.5, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.2.8, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/bank/main.jsp	SHA-1 cipher suites were detected	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 8.3.2, Requirement 11.4
https://demo.testfire.net/bank/main.jsp	Unnecessary Http Response Headers found in the Application	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/login.jsp	Autocomplete HTML Attribute Not Disabled for Password Field	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.1, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/subscribe.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/search.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4

https://demo.testfire.net/index.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/feedback.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/status_check.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/login.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/swagger/properties.json	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/survey_questions.jsp	Cacheable SSL Page Found	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/	Missing "Content-Security-Policy" header	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/	Missing or insecure "X-Content-Type-Options" header	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/	Missing or insecure HTTP Strict-Transport-Security Header	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/showAccount	Application Error	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 6.5.6, Requirement 7, Requirement 11.4

https://demo.testfire.net/bank/showTransactions	Application Error	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 6.5.6, Requirement 7, Requirement 11.4
https://demo.testfire.net/bank/showTransactions	Application Error	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 6.5.6, Requirement 7, Requirement 11.4
https://demo.testfire.net/bank/doTransfer	Application Error	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 6.5.6, Requirement 7, Requirement 11.4
https://demo.testfire.net/bank/doTransfer	Application Error	Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 6.5.6, Requirement 7, Requirement 11.4
https://demo.testfire.net/swagger/swagger-ui-bundle.js	Client-Side (JavaScript) Cookie References	Requirement 2.2.4, Requirement 6, Requirement 6.2.1, Requirement 6.3, Requirement 6.4, Requirement 7, Requirement 11.4
https://demo.testfire.net/doSubscribe	Email Address Pattern Found	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js	Email Address Pattern Found	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/swagger/properties.json	Email Address Pattern Found	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/swagger/swagger-ui-bundle.js	Email Address Pattern Found	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/bank/showAccount	HTML Comments Sensitive Information Disclosure	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.2.4.5, Requirement 6.3, Requirement 6.4, Requirement 6.5.6, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4

https://demo.testfire.net/login.jsp	HTML Comments Sensitive Information Disclosure	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.2.4.5, Requirement 6.3, Requirement 6.4, Requirement 6.5.6, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/admin/admin.jsp	HTML Comments Sensitive Information Disclosure	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.2.4.5, Requirement 6.3, Requirement 6.4, Requirement 6.5.6, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/admin/admin.jsp	HTML Comments Sensitive Information Disclosure	Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.2.4.5, Requirement 6.3, Requirement 6.4, Requirement 6.5.6, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/	Missing "Referrer policy" Security Header	Requirement 2, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.6, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.3, Requirement 6.3, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 7.2.6, Requirement 8.3.1, Requirement 11.4
https://demo.testfire.net/feedback.jsp	Possible Server Path Disclosure Pattern Found	Requirement 5, Requirement 6, Requirement 6.2.1, Requirement 6.2.4.5, Requirement 6.3, Requirement 6.3.2, Requirement 6.3.3, Requirement 6.4, Requirement 7, Requirement 11.4

Detailed Security Issues by Sections

M Requirement 2 - Apply secure configurations to all system components 27

DAST -	**Autocomplete HTML Attribute Not Disabled for Password Field**
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Insecure "OPTIONS" HTTP Method Enabled
Risk:	It is possible to upload, modify or delete web pages, scripts and files on the web server
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Content Spoofing
CWE:	749

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

M Requirement 2.2.2 - If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. If the vendor default account(s) will not be used, the account is removed or disabled. 27

DAST -	Autocomplete HTML Attribute Not Disabled for Password Field
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Insecure "OPTIONS" HTTP Method Enabled
Risk:	It is possible to upload, modify or delete web pages, scripts and files on the web server
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Content Spoofing
CWE:	749

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

M Requirement 2.2.4 - Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled. 28

DAST -	Autocomplete HTML Attribute Not Disabled for Password Field
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Insecure "OPTIONS" HTTP Method Enabled
Risk:	It is possible to upload, modify or delete web pages, scripts and files on the web server
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Content Spoofing
CWE:	749

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Client-Side (JavaScript) Cookie References
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Cause:	Cookies are created at the client side
Threat Classification:	Information Leakage
CWE:	602

Severity	Location
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

M Requirement 2.2.6 - System security parameters are configured to prevent misuse. 27

DAST -	Autocomplete HTML Attribute Not Disabled for Password Field
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Insecure "OPTIONS" HTTP Method Enabled
Risk:	It is possible to upload, modify or delete web pages, scripts and files on the web server
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Content Spoofing
CWE:	749

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

M Requirement 4 - Protect cardholder data with strong cryptography during transmission over open, public networks 3

DAST -	Encryption Not Enforced
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Cause:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Threat Classification:	Information Leakage
CWE:	311

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing Secure Attribute in Encrypted Session (SSL) Cookie
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Cause:	The web application sends non-secure cookies over SSL
Threat Classification:	Information Leakage
CWE:	614

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

I Requirement 5 - Protect all systems and networks from malicious software 1

DAST -	Possible Server Path Disclosure Pattern Found
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
Cause:	Latest patches or hotfixes for 3rd. party products were not installed
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/feedback.jsp

C Requirement 6 - Develop and maintain secure systems and applications. 99

DAST -	SQL Injection
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	89

Severity	Location
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/doLogin
Critical	https://demo.testfire.net/doLogin

DAST -	Integer Overflow
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Integer Overflows
CWE:	190

Severity	Location
High	https://demo.testfire.net/bank/showAccount
High	https://demo.testfire.net/bank/doTransfer

DAST -	Phishing Through URL Redirection
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The web application performs a redirection to an external site
Threat Classification:	URL Redirector Abuse
CWE:	601

Severity	Location
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Reflected Cross Site Scripting
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
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Cross-site Scripting
CWE:	79

Severity	Location
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/bank/customize.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/search.jsp
High	https://demo.testfire.net/index.jsp
High	https://demo.testfire.net/util/serverStatusCheckService.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Autocomplete HTML Attribute Not Disabled for Password Field
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Cacheable SSL Page Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Sensitive information might have been cached by your browser
Threat Classification:	Information Leakage
CWE:	525

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/transaction.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/subscribe.jsp
Low	https://demo.testfire.net/search.jsp
Low	https://demo.testfire.net/index.jsp
Low	https://demo.testfire.net/feedback.jsp
Low	https://demo.testfire.net/status_check.jsp
Low	https://demo.testfire.net/login.jsp
Low	https://demo.testfire.net/swagger/properties.json
Low	https://demo.testfire.net/survey_questions.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Cross-Site Request Forgery
Risk:	It may be possible to force an end-user to execute unwanted actions on a web application in which they're currently authenticated.
Cause:	Insufficient authentication method was used by the application
Threat Classification:	Cross-site Request Forgery
CWE:	352

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Database Error Pattern Found
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	209

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Encryption Not Enforced
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Cause:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Threat Classification:	Information Leakage
CWE:	311

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Host Header Injection
Risk:	
Cause:	The web application performs a redirection to an external site
Threat Classification:	Abuse of Functionality
CWE:	644

Severity	Location
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Insecure "OPTIONS" HTTP Method Enabled
Risk:	It is possible to upload, modify or delete web pages, scripts and files on the web server
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Content Spoofing
CWE:	749

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Link Injection (facilitates Cross-Site Request Forgery)
Risk:	
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	74

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Missing HttpOnly Attribute in Session Cookie
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
Cause:	The web application sets session cookies without the HttpOnly attribute
Threat Classification:	Information Leakage
CWE:	653

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing Secure Attribute in Encrypted Session (SSL) Cookie
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Cause:	The web application sends non-secure cookies over SSL
Threat Classification:	Information Leakage
CWE:	614

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Phishing Through Frames
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	79

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Application Error
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Information Leakage
CWE:	550

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/doTransfer
Informational	https://demo.testfire.net/bank/doTransfer

DAST -	Client-Side (JavaScript) Cookie References
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Cause:	Cookies are created at the client side
Threat Classification:	Information Leakage
CWE:	602

Severity	Location
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	HTML Comments Sensitive Information Disclosure
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Debugging information was left by the programmer in web pages
Threat Classification:	Information Leakage
CWE:	615

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/login.jsp
Informational	https://demo.testfire.net/admin/admin.jsp
Informational	https://demo.testfire.net/admin/admin.jsp

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

DAST -	Possible Server Path Disclosure Pattern Found
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
Cause:	Latest patches or hotfixes for 3rd. party products were not installed
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/feedback.jsp

C Requirement 6.2.1 - Bespoke and custom software are developed securely 99

DAST -	SQL Injection
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	89

Severity	Location
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/doLogin
Critical	https://demo.testfire.net/doLogin

DAST -	Integer Overflow
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Integer Overflows
CWE:	190

Severity	Location
High	https://demo.testfire.net/bank/showAccount
High	https://demo.testfire.net/bank/doTransfer

DAST -	Phishing Through URL Redirection
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The web application performs a redirection to an external site
Threat Classification:	URL Redirector Abuse
CWE:	601

Severity	Location
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Reflected Cross Site Scripting
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
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Cross-site Scripting
CWE:	79

Severity	Location
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/bank/customize.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/search.jsp
High	https://demo.testfire.net/index.jsp
High	https://demo.testfire.net/util/serverStatusCheckService.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Autocomplete HTML Attribute Not Disabled for Password Field
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Cacheable SSL Page Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Sensitive information might have been cached by your browser
Threat Classification:	Information Leakage
CWE:	525

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/transaction.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/subscribe.jsp
Low	https://demo.testfire.net/search.jsp
Low	https://demo.testfire.net/index.jsp
Low	https://demo.testfire.net/feedback.jsp
Low	https://demo.testfire.net/status_check.jsp
Low	https://demo.testfire.net/login.jsp
Low	https://demo.testfire.net/swagger/properties.json
Low	https://demo.testfire.net/survey_questions.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Cross-Site Request Forgery
Risk:	It may be possible to force an end-user to execute unwanted actions on a web application in which they're currently authenticated.
Cause:	Insufficient authentication method was used by the application
Threat Classification:	Cross-site Request Forgery
CWE:	352

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Database Error Pattern Found
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	209

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Encryption Not Enforced
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Cause:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Threat Classification:	Information Leakage
CWE:	311

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Host Header Injection
Risk:	
Cause:	The web application performs a redirection to an external site
Threat Classification:	Abuse of Functionality
CWE:	644

Severity	Location
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Insecure "OPTIONS" HTTP Method Enabled
Risk:	It is possible to upload, modify or delete web pages, scripts and files on the web server
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Content Spoofing
CWE:	749

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Link Injection (facilitates Cross-Site Request Forgery)
Risk:	
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	74

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Missing HttpOnly Attribute in Session Cookie
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
Cause:	The web application sets session cookies without the HttpOnly attribute
Threat Classification:	Information Leakage
CWE:	653

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing Secure Attribute in Encrypted Session (SSL) Cookie
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Cause:	The web application sends non-secure cookies over SSL
Threat Classification:	Information Leakage
CWE:	614

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Phishing Through Frames
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	79

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Application Error
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Information Leakage
CWE:	550

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/doTransfer
Informational	https://demo.testfire.net/bank/doTransfer

DAST -	Client-Side (JavaScript) Cookie References
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Cause:	Cookies are created at the client side
Threat Classification:	Information Leakage
CWE:	602

Severity	Location
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	HTML Comments Sensitive Information Disclosure
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Debugging information was left by the programmer in web pages
Threat Classification:	Information Leakage
CWE:	615

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/login.jsp
Informational	https://demo.testfire.net/admin/admin.jsp
Informational	https://demo.testfire.net/admin/admin.jsp

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

DAST -	Possible Server Path Disclosure Pattern Found
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
Cause:	Latest patches or hotfixes for 3rd. party products were not installed
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/feedback.jsp

C Requirement 6.2.4.1 - Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. 10

DAST -	SQL Injection
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	89

Severity	Location
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/doLogin
Critical	https://demo.testfire.net/doLogin

DAST -	Database Error Pattern Found
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	209

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin

H Requirement 6.2.4.2 - Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. 2

DAST -	Integer Overflow
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Integer Overflows
CWE:	190

Severity	Location
High	https://demo.testfire.net/bank/showAccount
High	https://demo.testfire.net/bank/doTransfer

M Requirement 6.2.4.3 - Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. 41

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Cacheable SSL Page Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Sensitive information might have been cached by your browser
Threat Classification:	Information Leakage
CWE:	525

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/transaction.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/subscribe.jsp
Low	https://demo.testfire.net/search.jsp
Low	https://demo.testfire.net/index.jsp
Low	https://demo.testfire.net/feedback.jsp
Low	https://demo.testfire.net/status_check.jsp
Low	https://demo.testfire.net/login.jsp
Low	https://demo.testfire.net/swagger/properties.json
Low	https://demo.testfire.net/survey_questions.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Encryption Not Enforced
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Cause:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Threat Classification:	Information Leakage
CWE:	311

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing Secure Attribute in Encrypted Session (SSL) Cookie
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Cause:	The web application sends non-secure cookies over SSL
Threat Classification:	Information Leakage
CWE:	614

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	HTML Comments Sensitive Information Disclosure
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Debugging information was left by the programmer in web pages
Threat Classification:	Information Leakage
CWE:	615

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/login.jsp
Informational	https://demo.testfire.net/admin/admin.jsp
Informational	https://demo.testfire.net/admin/admin.jsp

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

H Requirement 6.2.4.4 - Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). 16

DAST -	Reflected Cross Site Scripting
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
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Cross-site Scripting
CWE:	79

Severity	Location
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/bank/customize.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/search.jsp
High	https://demo.testfire.net/index.jsp
High	https://demo.testfire.net/util/serverStatusCheckService.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Cross-Site Request Forgery
Risk:	It may be possible to force an end-user to execute unwanted actions on a web application in which they're currently authenticated.
Cause:	Insufficient authentication method was used by the application
Threat Classification:	Cross-site Request Forgery
CWE:	352

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Encryption Not Enforced
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Cause:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Threat Classification:	Information Leakage
CWE:	311

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing Secure Attribute in Encrypted Session (SSL) Cookie
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Cause:	The web application sends non-secure cookies over SSL
Threat Classification:	Information Leakage
CWE:	614

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

H Requirement 6.2.4.5 - Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. 7

DAST -	Phishing Through URL Redirection
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The web application performs a redirection to an external site
Threat Classification:	URL Redirector Abuse
CWE:	601

Severity	Location
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	HTML Comments Sensitive Information Disclosure
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Debugging information was left by the programmer in web pages
Threat Classification:	Information Leakage
CWE:	615

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/login.jsp
Informational	https://demo.testfire.net/admin/admin.jsp
Informational	https://demo.testfire.net/admin/admin.jsp

DAST -	Possible Server Path Disclosure Pattern Found
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
Cause:	Latest patches or hotfixes for 3rd. party products were not installed
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/feedback.jsp

C Requirement 6.3 - Security vulnerabilities are identified and addressed 99

DAST -	SQL Injection
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	89

Severity	Location
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/doLogin
Critical	https://demo.testfire.net/doLogin

DAST -	Integer Overflow
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Integer Overflows
CWE:	190

Severity	Location
High	https://demo.testfire.net/bank/showAccount
High	https://demo.testfire.net/bank/doTransfer

DAST -	Phishing Through URL Redirection
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The web application performs a redirection to an external site
Threat Classification:	URL Redirector Abuse
CWE:	601

Severity	Location
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Reflected Cross Site Scripting
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
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Cross-site Scripting
CWE:	79

Severity	Location
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/bank/customize.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/search.jsp
High	https://demo.testfire.net/index.jsp
High	https://demo.testfire.net/util/serverStatusCheckService.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Autocomplete HTML Attribute Not Disabled for Password Field
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Cacheable SSL Page Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Sensitive information might have been cached by your browser
Threat Classification:	Information Leakage
CWE:	525

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/transaction.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/subscribe.jsp
Low	https://demo.testfire.net/search.jsp
Low	https://demo.testfire.net/index.jsp
Low	https://demo.testfire.net/feedback.jsp
Low	https://demo.testfire.net/status_check.jsp
Low	https://demo.testfire.net/login.jsp
Low	https://demo.testfire.net/swagger/properties.json
Low	https://demo.testfire.net/survey_questions.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Cross-Site Request Forgery
Risk:	It may be possible to force an end-user to execute unwanted actions on a web application in which they're currently authenticated.
Cause:	Insufficient authentication method was used by the application
Threat Classification:	Cross-site Request Forgery
CWE:	352

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Database Error Pattern Found
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	209

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Encryption Not Enforced
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Cause:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Threat Classification:	Information Leakage
CWE:	311

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Host Header Injection
Risk:	
Cause:	The web application performs a redirection to an external site
Threat Classification:	Abuse of Functionality
CWE:	644

Severity	Location
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Insecure "OPTIONS" HTTP Method Enabled
Risk:	It is possible to upload, modify or delete web pages, scripts and files on the web server
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Content Spoofing
CWE:	749

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Link Injection (facilitates Cross-Site Request Forgery)
Risk:	
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	74

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Missing HttpOnly Attribute in Session Cookie
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
Cause:	The web application sets session cookies without the HttpOnly attribute
Threat Classification:	Information Leakage
CWE:	653

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing Secure Attribute in Encrypted Session (SSL) Cookie
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Cause:	The web application sends non-secure cookies over SSL
Threat Classification:	Information Leakage
CWE:	614

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Phishing Through Frames
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	79

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Application Error
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Information Leakage
CWE:	550

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/doTransfer
Informational	https://demo.testfire.net/bank/doTransfer

DAST -	Client-Side (JavaScript) Cookie References
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Cause:	Cookies are created at the client side
Threat Classification:	Information Leakage
CWE:	602

Severity	Location
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	HTML Comments Sensitive Information Disclosure
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Debugging information was left by the programmer in web pages
Threat Classification:	Information Leakage
CWE:	615

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/login.jsp
Informational	https://demo.testfire.net/admin/admin.jsp
Informational	https://demo.testfire.net/admin/admin.jsp

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

DAST -	Possible Server Path Disclosure Pattern Found
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
Cause:	Latest patches or hotfixes for 3rd. party products were not installed
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/feedback.jsp

I Requirement 6.3.2 - An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management. 1

DAST -	Possible Server Path Disclosure Pattern Found
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
Cause:	Latest patches or hotfixes for 3rd. party products were not installed
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/feedback.jsp

M Requirement 6.3.3 - All system components are protected from known vulnerabilities by installing applicable security patches/updates. 28

DAST -	Autocomplete HTML Attribute Not Disabled for Password Field
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Insecure "OPTIONS" HTTP Method Enabled
Risk:	It is possible to upload, modify or delete web pages, scripts and files on the web server
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Content Spoofing
CWE:	749

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

DAST -	Possible Server Path Disclosure Pattern Found
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
Cause:	Latest patches or hotfixes for 3rd. party products were not installed
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/feedback.jsp

C Requirement 6.4 - Public-facing web applications are protected against attacks. 99

DAST -	SQL Injection
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	89

Severity	Location
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/doLogin
Critical	https://demo.testfire.net/doLogin

DAST -	Integer Overflow
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Integer Overflows
CWE:	190

Severity	Location
High	https://demo.testfire.net/bank/showAccount
High	https://demo.testfire.net/bank/doTransfer

DAST -	Phishing Through URL Redirection
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The web application performs a redirection to an external site
Threat Classification:	URL Redirector Abuse
CWE:	601

Severity	Location
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Reflected Cross Site Scripting
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
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Cross-site Scripting
CWE:	79

Severity	Location
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/bank/customize.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/search.jsp
High	https://demo.testfire.net/index.jsp
High	https://demo.testfire.net/util/serverStatusCheckService.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Autocomplete HTML Attribute Not Disabled for Password Field
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Cacheable SSL Page Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Sensitive information might have been cached by your browser
Threat Classification:	Information Leakage
CWE:	525

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/transaction.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/subscribe.jsp
Low	https://demo.testfire.net/search.jsp
Low	https://demo.testfire.net/index.jsp
Low	https://demo.testfire.net/feedback.jsp
Low	https://demo.testfire.net/status_check.jsp
Low	https://demo.testfire.net/login.jsp
Low	https://demo.testfire.net/swagger/properties.json
Low	https://demo.testfire.net/survey_questions.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Cross-Site Request Forgery
Risk:	It may be possible to force an end-user to execute unwanted actions on a web application in which they're currently authenticated.
Cause:	Insufficient authentication method was used by the application
Threat Classification:	Cross-site Request Forgery
CWE:	352

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Database Error Pattern Found
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	209

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Encryption Not Enforced
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Cause:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Threat Classification:	Information Leakage
CWE:	311

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Host Header Injection
Risk:	
Cause:	The web application performs a redirection to an external site
Threat Classification:	Abuse of Functionality
CWE:	644

Severity	Location
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Insecure "OPTIONS" HTTP Method Enabled
Risk:	It is possible to upload, modify or delete web pages, scripts and files on the web server
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Content Spoofing
CWE:	749

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Link Injection (facilitates Cross-Site Request Forgery)
Risk:	
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	74

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Missing HttpOnly Attribute in Session Cookie
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
Cause:	The web application sets session cookies without the HttpOnly attribute
Threat Classification:	Information Leakage
CWE:	653

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing Secure Attribute in Encrypted Session (SSL) Cookie
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Cause:	The web application sends non-secure cookies over SSL
Threat Classification:	Information Leakage
CWE:	614

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Phishing Through Frames
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	79

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Application Error
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Information Leakage
CWE:	550

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/doTransfer
Informational	https://demo.testfire.net/bank/doTransfer

DAST -	Client-Side (JavaScript) Cookie References
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Cause:	Cookies are created at the client side
Threat Classification:	Information Leakage
CWE:	602

Severity	Location
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	HTML Comments Sensitive Information Disclosure
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Debugging information was left by the programmer in web pages
Threat Classification:	Information Leakage
CWE:	615

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/login.jsp
Informational	https://demo.testfire.net/admin/admin.jsp
Informational	https://demo.testfire.net/admin/admin.jsp

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

DAST -	Possible Server Path Disclosure Pattern Found
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
Cause:	Latest patches or hotfixes for 3rd. party products were not installed
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/feedback.jsp

H Requirement 6.5.6 - Test data and test accounts are removed from system components before the system goes into production. 11

DAST -	Integer Overflow
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Integer Overflows
CWE:	190

Severity	Location
High	https://demo.testfire.net/bank/showAccount
High	https://demo.testfire.net/bank/doTransfer

DAST -	Application Error
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Information Leakage
CWE:	550

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/doTransfer
Informational	https://demo.testfire.net/bank/doTransfer

DAST -	HTML Comments Sensitive Information Disclosure
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Debugging information was left by the programmer in web pages
Threat Classification:	Information Leakage
CWE:	615

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/login.jsp
Informational	https://demo.testfire.net/admin/admin.jsp
Informational	https://demo.testfire.net/admin/admin.jsp

C Requirement 7 - Restrict access to system components and cardholder data by business need to know. 84

DAST -	SQL Injection
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	89

Severity	Location
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/doLogin
Critical	https://demo.testfire.net/doLogin

DAST -	Integer Overflow
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Integer Overflows
CWE:	190

Severity	Location
High	https://demo.testfire.net/bank/showAccount
High	https://demo.testfire.net/bank/doTransfer

DAST -	Reflected Cross Site Scripting
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
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Cross-site Scripting
CWE:	79

Severity	Location
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/bank/customize.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/search.jsp
High	https://demo.testfire.net/index.jsp
High	https://demo.testfire.net/util/serverStatusCheckService.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Autocomplete HTML Attribute Not Disabled for Password Field
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Cacheable SSL Page Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Sensitive information might have been cached by your browser
Threat Classification:	Information Leakage
CWE:	525

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/transaction.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/subscribe.jsp
Low	https://demo.testfire.net/search.jsp
Low	https://demo.testfire.net/index.jsp
Low	https://demo.testfire.net/feedback.jsp
Low	https://demo.testfire.net/status_check.jsp
Low	https://demo.testfire.net/login.jsp
Low	https://demo.testfire.net/swagger/properties.json
Low	https://demo.testfire.net/survey_questions.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Database Error Pattern Found
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	209

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Encryption Not Enforced
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Cause:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Threat Classification:	Information Leakage
CWE:	311

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Link Injection (facilitates Cross-Site Request Forgery)
Risk:	
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	74

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Missing HttpOnly Attribute in Session Cookie
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
Cause:	The web application sets session cookies without the HttpOnly attribute
Threat Classification:	Information Leakage
CWE:	653

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing Secure Attribute in Encrypted Session (SSL) Cookie
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Cause:	The web application sends non-secure cookies over SSL
Threat Classification:	Information Leakage
CWE:	614

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Application Error
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Information Leakage
CWE:	550

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/doTransfer
Informational	https://demo.testfire.net/bank/doTransfer

DAST -	Client-Side (JavaScript) Cookie References
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Cause:	Cookies are created at the client side
Threat Classification:	Information Leakage
CWE:	602

Severity	Location
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	HTML Comments Sensitive Information Disclosure
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Debugging information was left by the programmer in web pages
Threat Classification:	Information Leakage
CWE:	615

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/login.jsp
Informational	https://demo.testfire.net/admin/admin.jsp
Informational	https://demo.testfire.net/admin/admin.jsp

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

DAST -	Possible Server Path Disclosure Pattern Found
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
Cause:	Latest patches or hotfixes for 3rd. party products were not installed
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/feedback.jsp

H Requirement 7.1 - Limit access to system components and cardholder data to only those individuals whose job requires such access. 28

DAST -	Reflected Cross Site Scripting
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
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Cross-site Scripting
CWE:	79

Severity	Location
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/bank/customize.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/search.jsp
High	https://demo.testfire.net/index.jsp
High	https://demo.testfire.net/util/serverStatusCheckService.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Autocomplete HTML Attribute Not Disabled for Password Field
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Cross-Site Request Forgery
Risk:	It may be possible to force an end-user to execute unwanted actions on a web application in which they're currently authenticated.
Cause:	Insufficient authentication method was used by the application
Threat Classification:	Cross-site Request Forgery
CWE:	352

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Link Injection (facilitates Cross-Site Request Forgery)
Risk:	
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	74

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Missing HttpOnly Attribute in Session Cookie
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
Cause:	The web application sets session cookies without the HttpOnly attribute
Threat Classification:	Information Leakage
CWE:	653

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

M Requirement 7.2.2 - Access is assigned to users, including privileged users, based on: Job classification and function and least privileges necessary to perform job responsibilities. 2

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

C Requirement 7.2.6 - All user access to query repositories of stored cardholder data is restricted as follows: Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. Only the responsible administrator(s) can directly access or query repositories of stored CHD. 72

DAST -	SQL Injection
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	89

Severity	Location
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/doLogin
Critical	https://demo.testfire.net/doLogin

DAST -	Reflected Cross Site Scripting
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
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Cross-site Scripting
CWE:	79

Severity	Location
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/bank/customize.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/search.jsp
High	https://demo.testfire.net/index.jsp
High	https://demo.testfire.net/util/serverStatusCheckService.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Autocomplete HTML Attribute Not Disabled for Password Field
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Cacheable SSL Page Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Sensitive information might have been cached by your browser
Threat Classification:	Information Leakage
CWE:	525

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/transaction.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/subscribe.jsp
Low	https://demo.testfire.net/search.jsp
Low	https://demo.testfire.net/index.jsp
Low	https://demo.testfire.net/feedback.jsp
Low	https://demo.testfire.net/status_check.jsp
Low	https://demo.testfire.net/login.jsp
Low	https://demo.testfire.net/swagger/properties.json
Low	https://demo.testfire.net/survey_questions.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Database Error Pattern Found
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	209

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Link Injection (facilitates Cross-Site Request Forgery)
Risk:	
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	74

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Missing HttpOnly Attribute in Session Cookie
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
Cause:	The web application sets session cookies without the HttpOnly attribute
Threat Classification:	Information Leakage
CWE:	653

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	HTML Comments Sensitive Information Disclosure
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Debugging information was left by the programmer in web pages
Threat Classification:	Information Leakage
CWE:	615

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/login.jsp
Informational	https://demo.testfire.net/admin/admin.jsp
Informational	https://demo.testfire.net/admin/admin.jsp

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

M Requirement 8.2.8 - If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session. 1

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

H Requirement 8.3.1 - All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: Something you know, such as a password or passphrase. Something you have, such as a token device or smart card. Something you are, such as a biometric element 64

DAST -	Reflected Cross Site Scripting
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
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Cross-site Scripting
CWE:	79

Severity	Location
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/bank/customize.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/search.jsp
High	https://demo.testfire.net/index.jsp
High	https://demo.testfire.net/util/serverStatusCheckService.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Autocomplete HTML Attribute Not Disabled for Password Field
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Cacheable SSL Page Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Sensitive information might have been cached by your browser
Threat Classification:	Information Leakage
CWE:	525

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/transaction.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/subscribe.jsp
Low	https://demo.testfire.net/search.jsp
Low	https://demo.testfire.net/index.jsp
Low	https://demo.testfire.net/feedback.jsp
Low	https://demo.testfire.net/status_check.jsp
Low	https://demo.testfire.net/login.jsp
Low	https://demo.testfire.net/swagger/properties.json
Low	https://demo.testfire.net/survey_questions.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Link Injection (facilitates Cross-Site Request Forgery)
Risk:	
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	74

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Missing HttpOnly Attribute in Session Cookie
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
Cause:	The web application sets session cookies without the HttpOnly attribute
Threat Classification:	Information Leakage
CWE:	653

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing Secure Attribute in Encrypted Session (SSL) Cookie
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Cause:	The web application sends non-secure cookies over SSL
Threat Classification:	Information Leakage
CWE:	614

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	HTML Comments Sensitive Information Disclosure
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Debugging information was left by the programmer in web pages
Threat Classification:	Information Leakage
CWE:	615

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/login.jsp
Informational	https://demo.testfire.net/admin/admin.jsp
Informational	https://demo.testfire.net/admin/admin.jsp

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

H Requirement 8.3.2 - Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components. 22

DAST -	Reflected Cross Site Scripting
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
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Cross-site Scripting
CWE:	79

Severity	Location
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/bank/customize.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/search.jsp
High	https://demo.testfire.net/index.jsp
High	https://demo.testfire.net/util/serverStatusCheckService.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Encryption Not Enforced
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Cause:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Threat Classification:	Information Leakage
CWE:	311

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Link Injection (facilitates Cross-Site Request Forgery)
Risk:	
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	74

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Missing HttpOnly Attribute in Session Cookie
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
Cause:	The web application sets session cookies without the HttpOnly attribute
Threat Classification:	Information Leakage
CWE:	653

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing Secure Attribute in Encrypted Session (SSL) Cookie
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Cause:	The web application sends non-secure cookies over SSL
Threat Classification:	Information Leakage
CWE:	614

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

Requirement 8.6.2 - Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code. 0

C Requirement 11.4 - External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected. 99

DAST -	SQL Injection
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	89

Severity	Location
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/bank/showTransactions
Critical	https://demo.testfire.net/doLogin
Critical	https://demo.testfire.net/doLogin

DAST -	Integer Overflow
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Integer Overflows
CWE:	190

Severity	Location
High	https://demo.testfire.net/bank/showAccount
High	https://demo.testfire.net/bank/doTransfer

DAST -	Phishing Through URL Redirection
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The web application performs a redirection to an external site
Threat Classification:	URL Redirector Abuse
CWE:	601

Severity	Location
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Reflected Cross Site Scripting
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
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Cross-site Scripting
CWE:	79

Severity	Location
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/bank/customize.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/sendFeedback
High	https://demo.testfire.net/search.jsp
High	https://demo.testfire.net/index.jsp
High	https://demo.testfire.net/util/serverStatusCheckService.jsp
High	https://demo.testfire.net/bank/queryxpath.jsp
High	https://demo.testfire.net/bank/customize.jsp

DAST -	Autocomplete HTML Attribute Not Disabled for Password Field
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	522

Severity	Location
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/login.jsp

DAST -	Body Parameters Accepted in Query
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Cacheable SSL Page Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Sensitive information might have been cached by your browser
Threat Classification:	Information Leakage
CWE:	525

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/transaction.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.jsp
Low	https://demo.testfire.net/subscribe.jsp
Low	https://demo.testfire.net/search.jsp
Low	https://demo.testfire.net/index.jsp
Low	https://demo.testfire.net/feedback.jsp
Low	https://demo.testfire.net/status_check.jsp
Low	https://demo.testfire.net/login.jsp
Low	https://demo.testfire.net/swagger/properties.json
Low	https://demo.testfire.net/survey_questions.jsp

DAST -	Credit Card Number Pattern Found (Visa)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/bank/transfer.jsp
Medium	https://demo.testfire.net/bank/main.jsp
Medium	https://demo.testfire.net/bank/doTransfer

DAST -	Cross-Site Request Forgery
Risk:	It may be possible to force an end-user to execute unwanted actions on a web application in which they're currently authenticated.
Cause:	Insufficient authentication method was used by the application
Threat Classification:	Cross-site Request Forgery
CWE:	352

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/doTransfer
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/admin/admin.jsp

DAST -	Database Error Pattern Found
Risk:	It is possible to view, modify or delete database entries and tables
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	SQL Injection
CWE:	209

Severity	Location
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/bank/showTransactions
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin
Medium	https://demo.testfire.net/doLogin

DAST -	Direct Access to Administration Pages
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Predictable Resource Location
CWE:	306

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Encryption Not Enforced
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Cause:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Threat Classification:	Information Leakage
CWE:	311

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Host Header Injection
Risk:	
Cause:	The web application performs a redirection to an external site
Threat Classification:	Abuse of Functionality
CWE:	644

Severity	Location
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Inadequate Account Lockout
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Cause:	Insecure web application programming or configuration
Threat Classification:	Brute Force
CWE:	307

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	Insecure "OPTIONS" HTTP Method Enabled
Risk:	It is possible to upload, modify or delete web pages, scripts and files on the web server
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Content Spoofing
CWE:	749

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Link Injection (facilitates Cross-Site Request Forgery)
Risk:	
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	74

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Missing HttpOnly Attribute in Session Cookie
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
Cause:	The web application sets session cookies without the HttpOnly attribute
Threat Classification:	Information Leakage
CWE:	653

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing or insecure Cross-Frame Scripting Defence
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1021

Severity	Location
Medium	https://demo.testfire.net/

DAST -	Missing Secure Attribute in Encrypted Session (SSL) Cookie
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Cause:	The web application sends non-secure cookies over SSL
Threat Classification:	Information Leakage
CWE:	614

Severity	Location
Medium	https://demo.testfire.net/
Medium	https://demo.testfire.net/

DAST -	Older TLS Version is Supported
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Phishing Through Frames
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Sanitation of hazardous characters was not performed correctly on user input
Threat Classification:	Content Spoofing
CWE:	79

Severity	Location
Medium	https://demo.testfire.net/search.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/sendFeedback
Medium	https://demo.testfire.net/util/serverStatusCheckService.jsp
Medium	https://demo.testfire.net/bank/customize.jsp
Medium	https://demo.testfire.net/bank/queryxpath.jsp

DAST -	Session Identifier Not Updated
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
Cause:	Insecure web application programming or configuration
Threat Classification:	Session Fixation
CWE:	304

Severity	Location
Medium	https://demo.testfire.net/doLogin

DAST -	SHA-1 cipher suites were detected
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
Cause:	The web server or application server are configured in an insecure way
Threat Classification:	Server Misconfiguration
CWE:	327

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Unnecessary Http Response Headers found in the Application
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Medium	https://demo.testfire.net/bank/main.jsp

DAST -	Missing "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure "X-Content-Type-Options" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Missing or insecure HTTP Strict-Transport-Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Low	https://demo.testfire.net/

DAST -	Application Error
Risk:	It is possible to gather sensitive debugging information
Cause:	
Threat Classification:	Information Leakage
CWE:	550

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/showTransactions
Informational	https://demo.testfire.net/bank/doTransfer
Informational	https://demo.testfire.net/bank/doTransfer

DAST -	Client-Side (JavaScript) Cookie References
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Cause:	Cookies are created at the client side
Threat Classification:	Information Leakage
CWE:	602

Severity	Location
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	Email Address Pattern Found
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	359

Severity	Location
Informational	https://demo.testfire.net/doSubscribe
Informational	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Informational	https://demo.testfire.net/swagger/properties.json
Informational	https://demo.testfire.net/swagger/swagger-ui-bundle.js

DAST -	HTML Comments Sensitive Information Disclosure
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Debugging information was left by the programmer in web pages
Threat Classification:	Information Leakage
CWE:	615

Severity	Location
Informational	https://demo.testfire.net/bank/showAccount
Informational	https://demo.testfire.net/login.jsp
Informational	https://demo.testfire.net/admin/admin.jsp
Informational	https://demo.testfire.net/admin/admin.jsp

DAST -	Missing "Referrer policy" Security Header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/

DAST -	Possible Server Path Disclosure Pattern Found
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
Cause:	Latest patches or hotfixes for 3rd. party products were not installed
Threat Classification:	Information Leakage
CWE:	200

Severity	Location
Informational	https://demo.testfire.net/feedback.jsp