HCL SOFTWARE | AppScan on Cloud

Compliance Security Report

Application Name: DAST-Demo

Report Name: DAST-Demo

Report created at: Sunday, April 2, 2023

Notes: Sample report for demo scan.

Summary of security issues

Critical severity issues:	4
High severity issues:	12
Medium severity issues:	67
Informational severity issues:	16
Total security issues:	**99**

The Payment Card Industry Data Security Standard (PCI) Version 3.2.1

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 3.2.1 has replaced PCI DSS version 3.2 and is effective as of May 2018. The PCI DSS version 3.2 may not be used for PCI DSS compliance after December 31, 2018.

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

The information provided does not constitute legal advice. The results of a vulnerability assessment will demonstrate potential vulnerabilities in your application that should be corrected in order to reduce the likelihood that your information will be compromised. As legal advice must be tailored to the specific application of each law, and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent counsel. HCL customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

Violated Section

Sections	Number of Issues
Requirement 2 - Do not use vendor-supplied defaults for system passwords and other security parameters.	27
Requirement 2.1 - Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.)	27
Requirement 2.2.2 - Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	27
Requirement 2.2.4 - Configure system security parameters to prevent misuse.	27
Requirement 2.2.5 - Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems.	28
Requirement 2.3 - Encrypt all non-console administrative access using strong cryptography.	3
Requirement 2.6 - This section applies to web applications that are used by hosting providers for hosting purposes – Hosting providers must protect each entity’s hosted environment and data.	86
Requirement 4 - Encrypt transmission of cardholder data across open, public networks.	3
Requirement 4.1 - Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.	1
Requirement 6 - Develop and maintain secure systems and applications.	99
Requirement 6.1 - Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.	0
Requirement 6.2 - Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release. Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1	28
Requirement 6.3 - Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party.	97
Requirement 6.3.1 - Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	4
Requirement 6.4.4 - Removal of test data and accounts from system components before the system becomes active / goes into production.	4
Requirement 6.5 - Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	97
Requirement 6.5.1 - Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath	10

injection flaws as well as other injection flaws.	
Requirement 6.5.2 - Buffer overflow	2
Requirement 6.5.3 - Insecure cryptographic storage	41
Requirement 6.5.4 - Insecure communications	3
Requirement 6.5.5 - Improper error handling	0
Requirement 6.5.7 - Cross site scripting (XSS)	9
Requirement 6.5.8 - Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	6
Requirement 6.5.9 - Cross site request forgery (CSRF)	4
Requirement 6.5.10 - Broken authentication and session management Note: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement	1
Requirement 6.6 - For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	0
Requirement 7 - Restrict access to data by business need-to-know	86
Requirement 7.1 - Limit access to system components and cardholder data to only those individuals whose job requires such access.	28
Requirement 7.1.2 - Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	2
Requirement 8.2 - In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • 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.	64
Requirement 8.2.1 - Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	22
Requirement 8.7 - All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	72

Section Violation by Issue

Location	Issue Type	Sections
https://demo.testfire.net/bank/showTransactions	SQL Injection	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.1, Requirement 7, Requirement 8.7
https://demo.testfire.net/bank/showTransactions	SQL Injection	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.1, Requirement 7, Requirement 8.7
https://demo.testfire.net/doLogin	SQL Injection	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.1, Requirement 7, Requirement 8.7
https://demo.testfire.net/doLogin	SQL Injection	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.1, Requirement 7, Requirement 8.7
https://demo.testfire.net/bank/showAccount	Integer Overflow	Requirement 6, Requirement

		6.3, Requirement 6.5, Requirement 6.5.2, Requirement 7
https://demo.testfire.net/bank/doTransfer	Integer Overflow	Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.2, Requirement 7
https://demo.testfire.net/bank/customize.jsp	Phishing Through URL Redirection	Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.8
https://demo.testfire.net/sendFeedback	Reflected Cross Site Scripting	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.7, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/bank/customize.jsp	Reflected Cross Site Scripting	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.7, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/bank/queryxpath.jsp	Reflected Cross Site Scripting	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.7, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/sendFeedback	Reflected Cross Site Scripting	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.7, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/search.jsp	Reflected Cross Site Scripting	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.7, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/index.jsp	Reflected Cross Site Scripting	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.7, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/util/serverStatusCheckService.jsp	Reflected Cross Site Scripting	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.7, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/bank/queryxpath.jsp	Reflected Cross Site Scripting	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.7, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7

https://demo.testfire.net/bank/customize.jsp	Reflected Cross Site Scripting	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.7, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/login.jsp	Autocomplete HTML Attribute Not Disabled for Password Field	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/apply.jsp	Autocomplete HTML Attribute Not Disabled for Password Field	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/admin/admin.jsp	Autocomplete HTML Attribute Not Disabled for Password Field	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/showTransactions	Body Parameters Accepted in Query	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/doTransfer	Body Parameters Accepted in Query	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/admin/admin.jsp	Body Parameters Accepted in Query	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7

https://demo.testfire.net/search.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/subscribe.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/index.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/showAccount	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/feedback.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/status_check.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/login.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/transfer.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/customize.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/util/serverStatusCheckService.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/transaction.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7

https://demo.testfire.net/bank/queryxpath.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/main.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/apply.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/swagger/properties.json	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/survey_questions.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/admin/admin.jsp	Cacheable SSL Page Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/showAccount	Credit Card Number Pattern Found (Visa)	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/transfer.jsp	Credit Card Number Pattern Found (Visa)	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/main.jsp	Credit Card Number Pattern Found (Visa)	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7

https://demo.testfire.net/bank/doTransfer	Credit Card Number Pattern Found (Visa)	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/showTransactions	Cross-Site Request Forgery	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.9, Requirement 7.1
https://demo.testfire.net/bank/doTransfer	Cross-Site Request Forgery	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.9, Requirement 7.1
https://demo.testfire.net/bank/customize.jsp	Cross-Site Request Forgery	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.9, Requirement 7.1
https://demo.testfire.net/admin/admin.jsp	Cross-Site Request Forgery	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.9, Requirement 7.1
https://demo.testfire.net/bank/showTransactions	Database Error Pattern Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.1, Requirement 7, Requirement 8.7
https://demo.testfire.net/bank/showTransactions	Database Error Pattern Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.1, Requirement 7, Requirement 8.7
https://demo.testfire.net/bank/showTransactions	Database Error Pattern Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.1, Requirement 7, Requirement 8.7
https://demo.testfire.net/doLogin	Database Error Pattern Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.1, Requirement 7, Requirement 8.7
https://demo.testfire.net/doLogin	Database Error Pattern Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.1, Requirement 7, Requirement 8.7
https://demo.testfire.net/doLogin	Database Error Pattern Found	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.1, Requirement 7, Requirement 8.7
https://demo.testfire.net/	Direct Access to Administration Pages	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 7, Requirement 7.1, Requirement

		7.1.2, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/	Encryption Not Enforced	Requirement 2.3, Requirement 2.6, Requirement 4, Requirement 4.1, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 6.5.4, Requirement 7, Requirement 8.2.1
https://demo.testfire.net/bank/queryxpath.jsp	Host Header Injection	Requirement 6, Requirement 6.3, Requirement 6.5
https://demo.testfire.net/doLogin	Inadequate Account Lockout	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 7, Requirement 7.1, Requirement 7.1.2, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/	Insecure "OPTIONS" HTTP Method Enabled	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 7
https://demo.testfire.net/	Insecure "OPTIONS" HTTP Method Enabled	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 7
https://demo.testfire.net/search.jsp	Link Injection (facilitates Cross-Site Request Forgery)	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/index.jsp	Link Injection (facilitates Cross-Site Request Forgery)	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/sendFeedback	Link Injection (facilitates Cross-Site Request Forgery)	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/util/serverStatusCheckService.jsp	Link Injection (facilitates Cross-Site Request Forgery)	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/bank/customize.jsp	Link Injection (facilitates Cross-Site Request Forgery)	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement

		7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/bank/queryxpath.jsp	Link Injection (facilitates Cross-Site Request Forgery)	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/	Missing "Content-Security-Policy" header	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/	Missing HttpOnly Attribute in Session Cookie	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/	Missing or insecure "X-Content-Type-Options" header	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/	Missing or insecure Cross-Frame Scripting Defence	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/	Missing or insecure HTTP Strict-Transport-Security Header	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/	Missing Secure Attribute in Encrypted Session (SSL) Cookie	Requirement 2.3, Requirement 2.6, Requirement 4, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 6.5.4, Requirement 7, Requirement 8.2, Requirement 8.2.1
https://demo.testfire.net/	Missing Secure Attribute in Encrypted Session (SSL) Cookie	Requirement 2.3, Requirement 2.6, Requirement 4, Requirement 6, Requirement 6.3, Requirement 6.5,

		Requirement 6.5.3, Requirement 6.5.4, Requirement 7, Requirement 8.2, Requirement 8.2.1
https://demo.testfire.net/bank/main.jsp	Older TLS Version is Supported	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/search.jsp	Phishing Through Frames	Requirement 6, Requirement 6.3, Requirement 6.5
https://demo.testfire.net/index.jsp	Phishing Through Frames	Requirement 6, Requirement 6.3, Requirement 6.5
https://demo.testfire.net/sendFeedback	Phishing Through Frames	Requirement 6, Requirement 6.3, Requirement 6.5
https://demo.testfire.net/sendFeedback	Phishing Through Frames	Requirement 6, Requirement 6.3, Requirement 6.5
https://demo.testfire.net/util/serverStatusCheckService.jsp	Phishing Through Frames	Requirement 6, Requirement 6.3, Requirement 6.5
https://demo.testfire.net/bank/customize.jsp	Phishing Through Frames	Requirement 6, Requirement 6.3, Requirement 6.5
https://demo.testfire.net/bank/queryxpath.jsp	Phishing Through Frames	Requirement 6, Requirement 6.3, Requirement 6.5
https://demo.testfire.net/doLogin	Session Identifier Not Updated	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.10, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/bank/main.jsp	SHA-1 cipher suites were detected	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 7, Requirement 7.1, Requirement 8.2, Requirement 8.2.1, Requirement 8.7
https://demo.testfire.net/bank/main.jsp	Unnecessary Http Response Headers found in the Application	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/showAccount	Application Error	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 7
https://demo.testfire.net/bank/showTransactions	Application Error	Requirement 2.6, Requirement

		6, Requirement 6.3, Requirement 6.5, Requirement 7
https://demo.testfire.net/bank/showTransactions	Application Error	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 7
https://demo.testfire.net/bank/doTransfer	Application Error	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 7
https://demo.testfire.net/bank/doTransfer	Application Error	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 7
https://demo.testfire.net/swagger/swagger-ui-bundle.js	Client-Side (JavaScript) Cookie References	Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.5, Requirement 7
https://demo.testfire.net/doSubscribe	Email Address Pattern Found	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js	Email Address Pattern Found	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/swagger/properties.json	Email Address Pattern Found	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/swagger/swagger-ui-bundle.js	Email Address Pattern Found	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/bank/showAccount	HTML Comments Sensitive Information Disclosure	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.3.1, Requirement 6.4.4, Requirement 6.5, Requirement 6.5.3, Requirement 6.5.8,

		Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/login.jsp	HTML Comments Sensitive Information Disclosure	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.3.1, Requirement 6.4.4, Requirement 6.5, Requirement 6.5.3, Requirement 6.5.8, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/admin/admin.jsp	HTML Comments Sensitive Information Disclosure	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.3.1, Requirement 6.4.4, Requirement 6.5, Requirement 6.5.3, Requirement 6.5.8, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/admin/admin.jsp	HTML Comments Sensitive Information Disclosure	Requirement 2.6, Requirement 6, Requirement 6.3, Requirement 6.3.1, Requirement 6.4.4, Requirement 6.5, Requirement 6.5.3, Requirement 6.5.8, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/	Missing "Referrer policy" Security Header	Requirement 2, Requirement 2.1, Requirement 2.2.2, Requirement 2.2.4, Requirement 2.2.5, Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.3, Requirement 7, Requirement 8.2, Requirement 8.7
https://demo.testfire.net/feedback.jsp	Possible Server Path Disclosure Pattern Found	Requirement 2.6, Requirement 6, Requirement 6.2, Requirement 6.3, Requirement 6.5, Requirement 6.5.8, Requirement 7

Detailed Security Issues by Sections

M Requirement 2 - Do not use vendor-supplied defaults for system passwords and other security parameters. 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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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:	74

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

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

Severity	Location
Medium	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
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:	693

Severity	Location
Medium	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
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 -	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 2.1 - Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.) 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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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:	74

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

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

Severity	Location
Medium	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
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:	693

Severity	Location
Medium	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
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 -	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 - Enable only necessary services, protocols, daemons, etc., as required for the function of the system. 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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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:	74

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

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

Severity	Location
Medium	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
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:	693

Severity	Location
Medium	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
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 -	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 - Configure system security parameters 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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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:	74

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

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

Severity	Location
Medium	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
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:	693

Severity	Location
Medium	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
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 -	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 2.2.5 - Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems. 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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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:	74

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

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

Severity	Location
Medium	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
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:	693

Severity	Location
Medium	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
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 -	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 2.3 - Encrypt all non-console administrative access using strong cryptography. 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:	319

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/

C Requirement 2.6 - This section applies to web applications that are used by hosting providers for hosting purposes – Hosting providers must protect each entity's hosted environment and data. 86

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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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/search.jsp
Medium	https://demo.testfire.net/subscribe.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/feedback.jsp
Medium	https://demo.testfire.net/status_check.jsp
Medium	https://demo.testfire.net/login.jsp
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/swagger/properties.json
Medium	https://demo.testfire.net/survey_questions.jsp
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 -	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:	319

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

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

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

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:	693

Severity	Location
Medium	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
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 -	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

M Requirement 4 - Encrypt transmission of cardholder data across 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:	319

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/

M Requirement 4.1 - Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use. 1

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:	319

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

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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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/search.jsp
Medium	https://demo.testfire.net/subscribe.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/feedback.jsp
Medium	https://demo.testfire.net/status_check.jsp
Medium	https://demo.testfire.net/login.jsp
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/swagger/properties.json
Medium	https://demo.testfire.net/survey_questions.jsp
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 -	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:	319

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:	74

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

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

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

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:	693

Severity	Location
Medium	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
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 -	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

Requirement 6.1 - Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities. 0

M Requirement 6.2 - Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release. Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1 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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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:	74

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

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

Severity	Location
Medium	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
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:	693

Severity	Location
Medium	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
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 -	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 6.3 - Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party. 97

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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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/search.jsp
Medium	https://demo.testfire.net/subscribe.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/feedback.jsp
Medium	https://demo.testfire.net/status_check.jsp
Medium	https://demo.testfire.net/login.jsp
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/swagger/properties.json
Medium	https://demo.testfire.net/survey_questions.jsp
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 -	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:	319

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:	74

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

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

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

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:	693

Severity	Location
Medium	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
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 -	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 -	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 -	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 6.3.1 - Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers. 4

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

I Requirement 6.4.4 - Removal of test data and accounts from system components before the system becomes active / goes into production. 4

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 6.5 - Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements. 97

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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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/search.jsp
Medium	https://demo.testfire.net/subscribe.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/feedback.jsp
Medium	https://demo.testfire.net/status_check.jsp
Medium	https://demo.testfire.net/login.jsp
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/swagger/properties.json
Medium	https://demo.testfire.net/survey_questions.jsp
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 -	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:	319

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:	74

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

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

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

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:	693

Severity	Location
Medium	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
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 -	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 -	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 -	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 6.5.1 - Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection 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 6.5.2 - Buffer overflow 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 6.5.3 - Insecure cryptographic storage 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/search.jsp
Medium	https://demo.testfire.net/subscribe.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/feedback.jsp
Medium	https://demo.testfire.net/status_check.jsp
Medium	https://demo.testfire.net/login.jsp
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/swagger/properties.json
Medium	https://demo.testfire.net/survey_questions.jsp
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 -	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:	319

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

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

Severity	Location
Medium	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
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:	693

Severity	Location
Medium	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
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 -	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 6.5.4 - Insecure communications 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:	319

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/

Requirement 6.5.5 - Improper error handling 0

H Requirement 6.5.7 - Cross site scripting (XSS) 9

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

H Requirement 6.5.8 - Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). 6

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 -	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

M Requirement 6.5.9 - Cross site request forgery (CSRF) 4

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

M Requirement 6.5.10 - Broken authentication and session management Note: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement 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

Requirement 6.6 - For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic. 0

C Requirement 7 - Restrict access to data by business need-to-know 86

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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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/search.jsp
Medium	https://demo.testfire.net/subscribe.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/feedback.jsp
Medium	https://demo.testfire.net/status_check.jsp
Medium	https://demo.testfire.net/login.jsp
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/swagger/properties.json
Medium	https://demo.testfire.net/survey_questions.jsp
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 -	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:	319

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:	74

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

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

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

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:	693

Severity	Location
Medium	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
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 -	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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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 7.1.2 - Restrict access to privileged user IDs to 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

H Requirement 8.2 - In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • 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. 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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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/search.jsp
Medium	https://demo.testfire.net/subscribe.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/feedback.jsp
Medium	https://demo.testfire.net/status_check.jsp
Medium	https://demo.testfire.net/login.jsp
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/swagger/properties.json
Medium	https://demo.testfire.net/survey_questions.jsp
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 -	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 "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

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

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

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:	693

Severity	Location
Medium	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
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 -	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 8.2.1 - Using strong cryptography, render all authentication credentials (such as passwords/phrases) 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:	319

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

C Requirement 8.7 - All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes). 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/login.jsp
Medium	https://demo.testfire.net/bank/apply.jsp
Medium	https://demo.testfire.net/admin/admin.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/search.jsp
Medium	https://demo.testfire.net/subscribe.jsp
Medium	https://demo.testfire.net/index.jsp
Medium	https://demo.testfire.net/bank/showAccount
Medium	https://demo.testfire.net/feedback.jsp
Medium	https://demo.testfire.net/status_check.jsp
Medium	https://demo.testfire.net/login.jsp
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/swagger/properties.json
Medium	https://demo.testfire.net/survey_questions.jsp
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 -	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 "Content-Security-Policy" header
Risk:	
Cause:	Insecure web application programming or configuration
Threat Classification:	Information Leakage
CWE:	1032

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

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

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:	693

Severity	Location
Medium	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
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 -	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/