Terasoft

STQC and CERT-IN Empaneled Test Laboratory

Investor Portal Application Security Assessment & Penetration Testing

Client Name: “Facilon Services Private Ltd”

INITIAL Technical Report

Report ID - TTPL/Certin/PR/25/09/webapp/PN/S034/v1.0

Report Version No.: 1.0

Date: 25/09/2025

1. Document Control

1.1 Company Confidential

This document contains confidential company information and is submitted in confidence to the customer for their own internal use.

1.2 Proprietary Information

The content of this document should be considered proprietary information and should not be disclosed outside of Terasoft.

Document History			
Issue No.	Date of Issue	Issued by	Description
0.1	25/09/2025	Terasoft Pen Test Team	First Draft
0.2	25/09/2025	Terasoft Pen Test Team	Quality Assurance
1.0	25/09/2025	Terasoft Pen Test Team	Initial Report Release

Document Distribution List	
Client Name	Facilon Services Private Ltd
Function Owner	Facilon Services Private Ltd
SPOC (Special Person of Contact)	Rajiv Shah

S. No	Name of Tool/Software used	Version of the tool /Software used	Open Source/Licensed
1	Burp Suite Professional	2025.1.2	Licensed
2	SQLmap	1.8.2	Open Source
3	Nmap	7.94	Open Source
4	Dirbuster	--	Open Source
5	Nikto	--	Open Source

1.3 Internal Team

The following members from the Terasoft's Pen Test team participated in the testing, reviewed documentation, and/or contributed to this report.

Rashmi Jalindre – Technical Director

Table of Contents

2. Executive Summary

TERASOFT Pen Test team was engaged by **Facilon Services Private Ltd.** to conduct a penetration testing of **Facilon web application** during the period **18th Sept 2025** to **25th Sept 2025**.

The penetration test provides insight into the resilience of its systems to withstand attacks from unauthorized users and the potential for valid users to abuse their privileges and access.

The prime objective of this security exercise was to test **Facilon web application** for vulnerabilities in their systems and applications that could allow access to internal private networks, systems or gain unauthorized access to sensitive or confidential information.

The security assessment discovered **4 vulnerabilities** in the target penetration test. These vulnerabilities may have the following negative business impact.

2.0 Risk Ratings

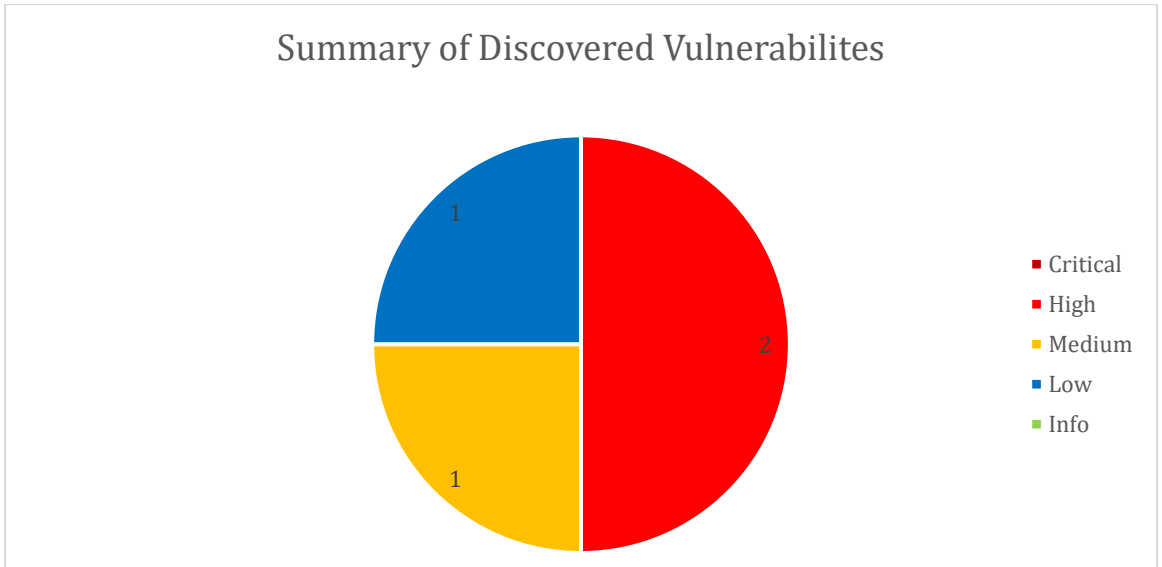
The risk rating for each finding in this report is based on the Impact and Exploit vector of the vulnerability. Here's a guide to interpreting the risk rating:

Risk Rating	Explanation
CRITICAL	Vulnerability was discovered that has been rated as critical. It is recommended that corrective actions are implemented urgently. This category of risk should be monitored closely by management.
HIGH	Vulnerability was discovered that has been rated as important. It is recommended that corrective actions must be implemented within a short term.
MEDIUM	Vulnerability was discovered that has been rated as of medium criticality. It is recommended that corrective actions should be part of on-going security maintenance of the system.
LOW	Vulnerability was discovered that has been rated as of low criticality. Owner should consider whether to apply corrective measures as part of routine maintenance tasks or to accept the risk.
INFO	A finding was discovered that has been rated as of informational value which should be addressed in order to meet industry best practice.

2.1 Summary of Findings

The graph below shows a summary of the number of findings found for each risk level during the penetration testing.

0 Critical, 2 High, 1 Medium, 1 Low risk findings were noted and should be addressed as a priority.



2.2 Details of Vulnerabilities

Vulnerability ID	Vulnerability Name	Severity	Status
Facilon – Q3 - 2025 – 001	Insecure Direct Object Reference (IDOR)	High	Open
Facilon – Q3 - 2025 - 002	Insecure Session Management	High	Open
Facilon – Q3 - 2025 - 003	No rate Limit on OTP	Medium	Open
Facilon – Q3 - 2025 - 004	Missing Security Headers	Low	Open

3. Penetration Test Goals and Objectives

As part of our information security program the Terasoft Pen Test team evaluated the protection of its people, process, data, systems and networks to ensure that controls are in place.

The objectives of this assessment are highlighted below:

- To identify technical as well as logical vulnerabilities/weaknesses in the application and provide recommendations for risk mitigation.
- To discover whether an attacker can leverage flaws in the application to compromise the confidentiality, integrity and availability of the information.
- To help management & development team to understand their current application security postures in order to develop an action plan to minimize the threat of attack or misuse.

4. Description of Scope

The scope of penetration testing included below components and the Terasoft Pen Test team located in the Terasoft office of Ahmednagar, India conducted the pen testing. Testing was conducted from **18th Sept 2025** to **25th Sept 2025.**

The following constitutes the scope of the **Facilon Web Application** penetration test; this includes any system(s) used to provide any security feature such as authentication or encryption:

Application/ Server Name	Application/ Server Type	URL/IP Address
Facilon	Web Application	URL: https://demo.facilonservices.com/demo/investor/home/

5. Penetration Test Approach

Terasoft's penetration testing team took the following approach:

5.1 Phase 1 – Project Planning and Initiation

Prior to commencement of the Penetration Test Terasoft conducted a kick-off meeting with business unit to commence the assessment and finalize the proposal document containing in-scope components, rules of engagement ("RoE") etc.

The proposal document included a draft engagement plan and overall schedule, and tasks planned for the assessment.

The proposal document included points of contact, in-scope components, people engaged and pen testing activities, and guidelines.

5.2 Phase 2 – Penetration Testing Services

Terasoft's team performed penetration testing based on the following three activities.

5.2.1 Activity 1: Intelligence Gathering

This step consisted of gathering information about the in-scope components. The team will gather information about infrastructure, process, applications, people etc. to evaluate attack surface.

5.2.2 Activity 2: Vulnerability Detection

Terasoft's team performed vulnerability identification, which included:

- Vulnerability Identification – Active vulnerability analysis on the in-scope components.
- Confirmation & Manual Testing – Review and analysis to remove false positives. Manual testing will be performed to identify flaws not easily identifiable with automated tools.

Specifically, Terasoft's team:

- Performed initial scanning with automated vulnerability identification and analysis tools to identify target areas for manual testing
- Performed manual testing to identify security weaknesses based on the security standards such as OWASP Top 10 (2017 and 2021) vulnerabilities
- Performed automated scanning with and analyzed results manually to eliminate false positives
- Performed verification and manual penetration testing of identified potential vulnerabilities
- Performed manual testing for vulnerability discovery and exploitation in conjunction with automatic vulnerability scanning
- Correlated discovered vulnerabilities to discover additional threats posed by an aggregate of vulnerabilities

5.2.3 Activity 3: Penetration Testing

Terasoft's team performed vulnerability exploitation based on agreement with business unit, including:

- Communicating the exploitation strategy with the brand and obtaining confirmation before performing the actual exploitation steps on the target systems
- Performing controlled vulnerability exploitation using automated and manual techniques

5.3 Phase 3 – Reporting

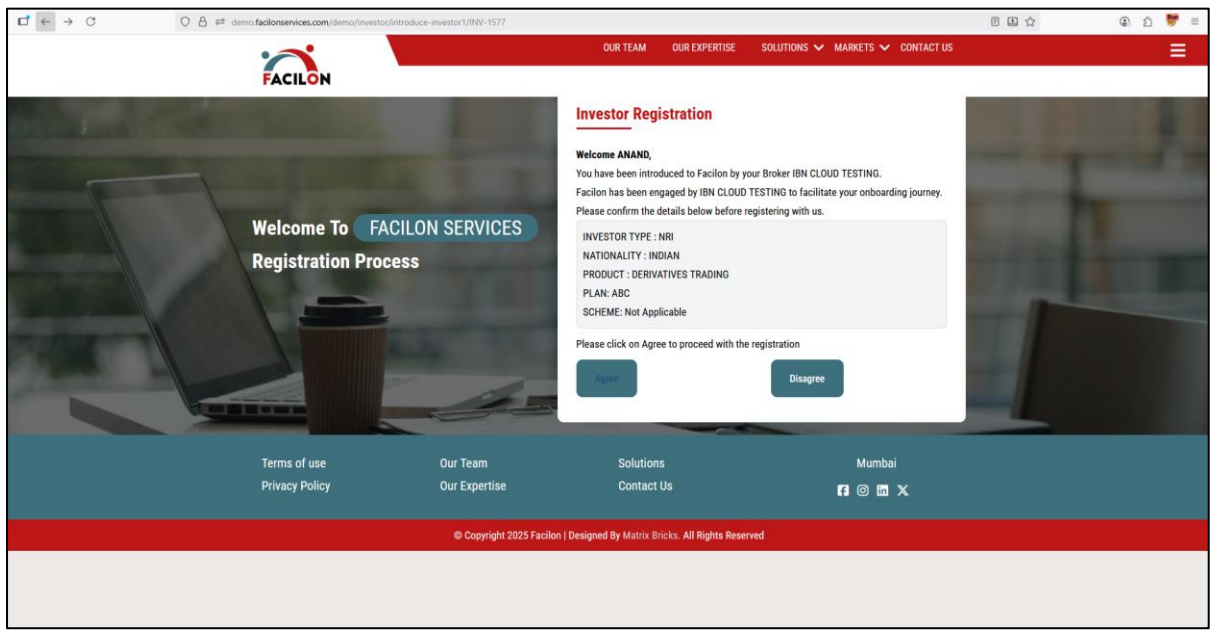
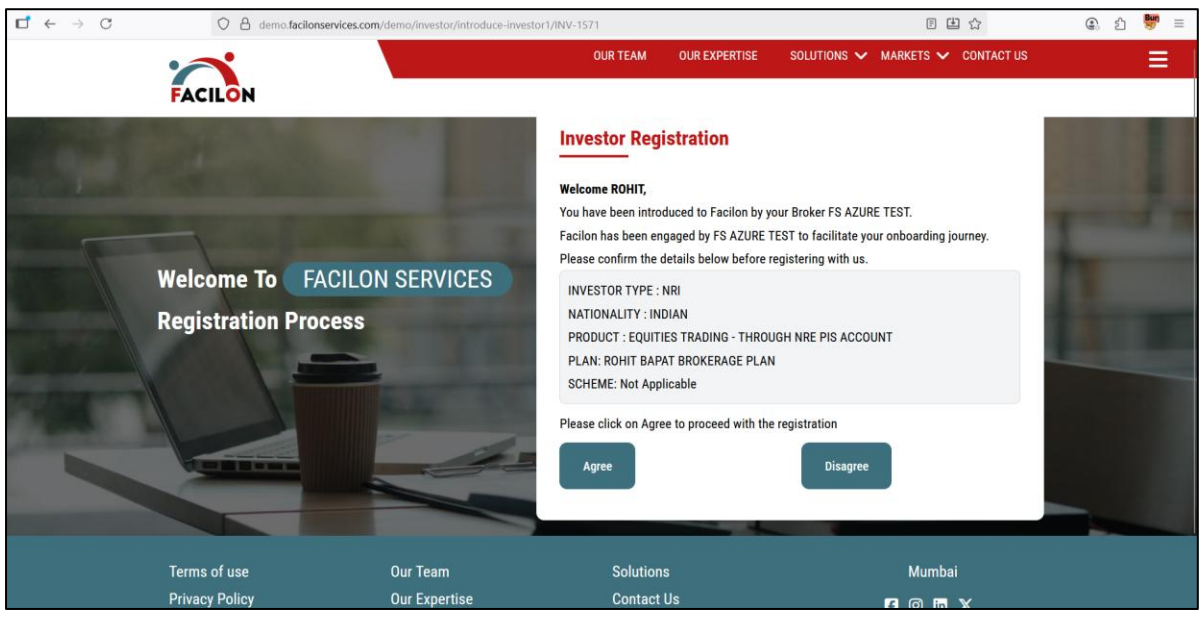
This document report was created and shared in draft form with brand, before finalization.

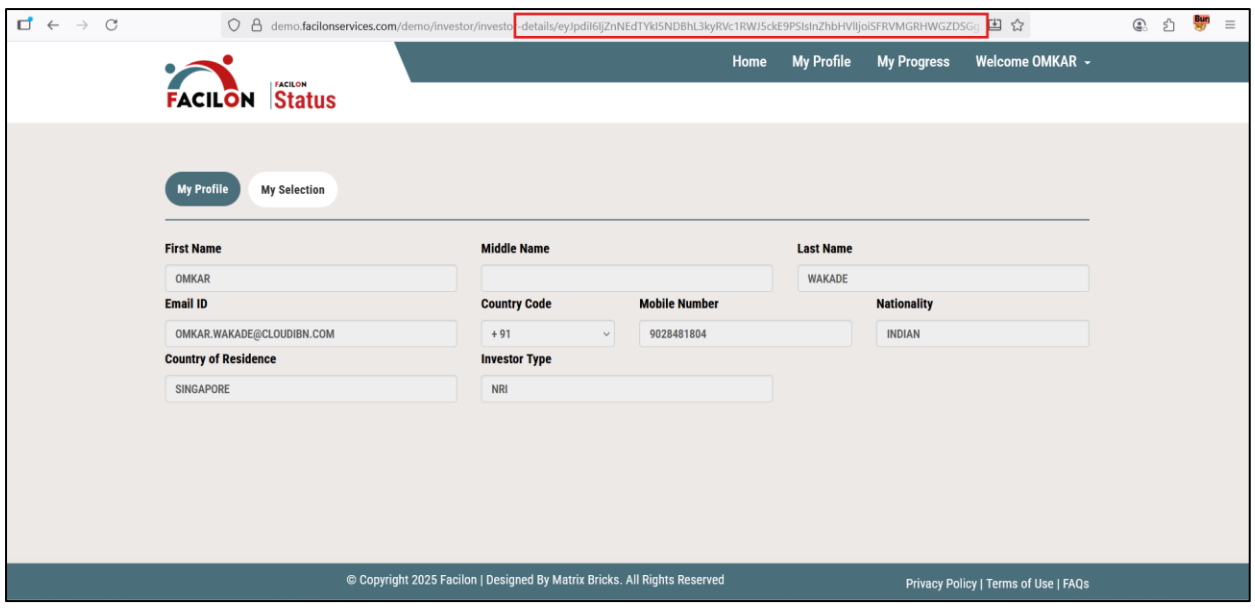
5.4 Phase 4 – Retesting

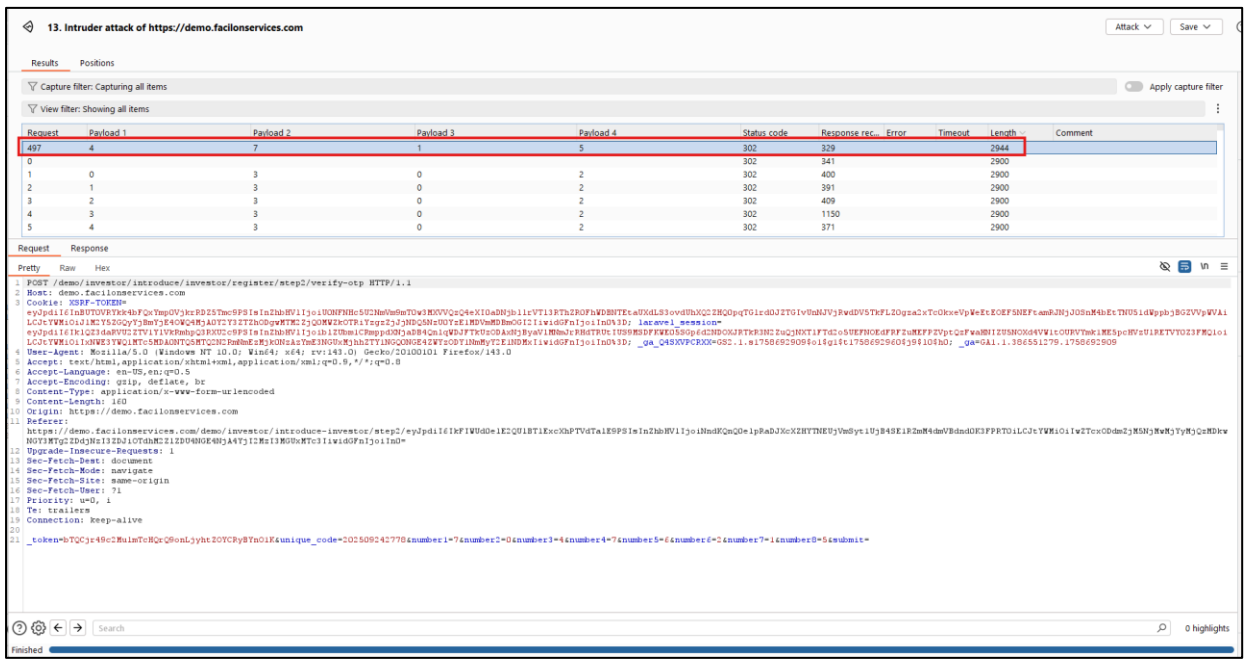
Terasoft's pen test team will provide remediation support and perform retesting of vulnerabilities upon request from brand or remediation team.

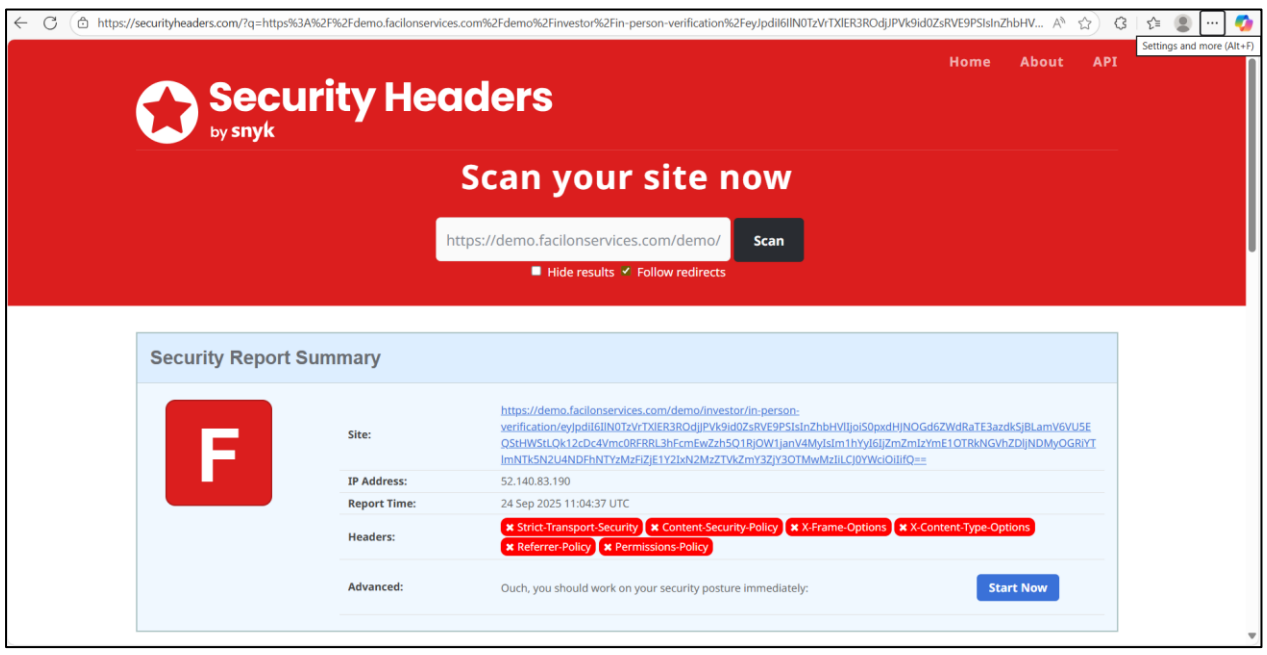
6. Security Assessment Findings

This section documents the detailed findings that were noted and documented during the testing. These findings are assigned a rating that corresponds to the exposure associated with each.

Facilon – Q3 - 2025 - 001	**Insecure Direct Object Reference (IDOR)**	**High**
Finding Description:	IDOR happens when a website or app lets users access something (like a file, profile, or record) by using a number or ID, but doesn't check if the user should really access it. An attacker can change the ID in the URL or request to see or modify other people's data.  
CWE ID:	284	
Step to Reproduce:	1) Go to Introduce-investor page 2) Change investor number in URL.	
Security Impact:	An Attacker can get details of any other user by changing only Investor Number.	
Affected Areas:	https://demo.facilonservices.com/demo/investor/introduce-investor1/INV-1571	
Recommendations:	• Always check on the server if the user is allowed to access the resource. • Don't use simple sequential IDs; use random or hashed IDs.	
References:	https://cwe.mitre.org/data/definitions/284.html	

Facilon – Q3 - 2025 - 002	Insecure Session Management	High
Finding Description:	The web application is exposing session identifiers (session cookies) in the URL. This means that after logging out, if someone revisits the URL containing the session ID, they can reuse the session to access the account without proper authentication. 
CWE ID:	614
Step to Reproduce:	1) Login with Investor. 2) Now click on log out. 3) After successful log out revisit the last page.
Security Impact:	• Account takeover or unauthorized access. • Sensitive user data can be accessed by attackers.
Affected Areas:	https://demo.facilonservices.com/demo/investor/investor-details/eyJpdiI6IjZnNEdTYkI5NDBhL3kyRVc1RWJ5ckE9PSIsInZhbHVlIjoiSFRVMGRHWGZDSGg3Wm0zckVkWnluQVBXdjJjNkJ0MHhJcEZoWkoyei9DSmpTajU0YW4wUHg0Q3BtVndraVN6WiIsIm1hYyI6IjA4MGQxZGE3ZWYxYjZiMDE5YjI0MWRlYzdiODU1MDMyN2U4YzQ1NzUyMzIzZGUxYWIwMWUxMGI4NGE2ZmIyNDgiLCJ0YWciOiIifQ==
Recommendations:	• Never include session IDs in URLs; use secure cookies instead. • Invalidate sessions properly on logout. • Regenerate session IDs after login to prevent fixation.
References:	https://cwe.mitre.org/data/definitions/614.html

Facilon – Q3 - 2025 - 003	No rate Limit on OTP	Medium
Finding Description:	The application allows unlimited attempts to request or verify OTPs without restricting the number of attempts or applying a cooldown period. This can let attackers repeatedly try OTPs to gain unauthorized access or overwhelm the system. 
CWE ID:	307
Step to Reproduce:	1) Complete Registration of Investor. 2) Now at Email and Mobile verification page capture the request with burp suite. 3) Start Brute force attacking using Intruder. 4) Observe changes in Content length of correct otp and wrong otp.
Security Impact:	Brute-force attacks on user accounts.
Affected Areas:	https://demo.facilonservices.com/demo/investor/introduce/investor/register/step2/verify-otp
Recommendations:	• Implement rate limiting for OTP requests and verification attempts. • Apply account lockouts or temporary delays after multiple failed attempts.
References:	https://cwe.mitre.org/data/definitions/307.html

Facilon – Q3 - 2025 - 004	Missing Security Headers	Low
Finding Description:	Missing security headers vulnerability occurs when a web application does not include HTTP response headers that are designed to enhance browser security. 
CWE ID:	693
Step to Reproduce:	1) Go to securityheaders.com 2) Enter URL and search for security headers.
Security Impact:	Missing security headers increase the risk of attacks like clickjacking, and MIME sniffing. They can lead to data exposure, insecure content rendering, and reduced browser protection, making the application more vulnerable to client-side exploits.
Affected Areas:	https://fportalvapt.powerappsportals.com/
Recommendations:	• Set Essential Security Headers
References:	https://cwe.mitre.org/data/definitions/693.html

Conclusion

On analysing the reported vulnerabilities that have been identified during this testing exercise, it appears that most of them might have crept in at different phases of the deployment and software development cycle.

These findings underscore the need for vigorously applying a culture of security upon the entire length and breadth of the SDLC model that is being applied for developing the application. This would mean a continuous process of strengthening the threat model, risk identification and mitigation processes at each stage of the application development lifecycle.

While it is certain that fixing the vulnerabilities identified in this exercise would greatly reduce the risk exposure of the application, it must be appreciated that the concept of total security is complex.

To achieve a strong defense, in-depth capability and technical solutions must be implemented at various layers (network, physical etc.) and these must be supplemented with strong and verifiable policies, processes and procedures.

7. Terasoft Pen Test Methodology

Terasoft Pen Test Methodology includes the following phases:

Phase 1. Information Gathering - Performing reconnaissance against a target to gather as much information as possible to be utilized when penetrating the target during the vulnerability mapping and exploitation phases. The more information we can gather during this phase, the more vectors of attack we may be able to use in the future.

Phase 2. Enumeration - Map the in-scope targets, this could be called Information Gathering 2.0 as the objectives are similar but more focused. Here our goal is to identify any: IP addresses, Web servers, DNS servers, Proxies, usernames, file shares, URLs, Links, services, versions, open ports, authentication mechanisms and anything else that allows us to research and formulate an attack on the target(s).

Phase 3. Vulnerability Mapping – Utilizing all the information we have gathered we can now run vulnerability scanners, application scanners, and fuzzers. Using this data, we can research exploits and weaknesses and map them to our targets. We utilize sites like exploit-db and packetstormsecurity to download and load exploits and tools we feel will allow us to gain access to systems.

Phase 4. Exploitation - This phase shows the resilience of the target against actual attacks. Here we attempt to circumvent security controls and gain access to vulnerable systems and applications that reside within the scope of the test. The focus is to identify the main entry point into the organization and identify high value target assets.

8. Appendix: Core References

- **OWASP -** https://www.owasp.org/index.php/The_Owasp_Code_Review_Top_9
- **OWASP Web Top10 -** https://owasp.org/www-project-top-ten/
- **OWASP Mobile Top 10 -** https://owasp.org/www-project-mobile-top-10/
- **OWASP Desktop Top 10 -** https://owasp.org/www-project-desktop-app-security-top-10/
- **WASC -** http://projects.webappsec.org/f/WASC-TC-v2_0.pdf
- **MSDN-** http://msdn.microsoft.com/en-us/library/ff649268.aspx
- **MSDN-** http://msdn.microsoft.com/en-us/library/ff648637.aspx#c21618429_006
- **SANS -** http://www.sans.org/top25-software-errors/
- **CERT -** https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices
- **Best Practices -** https://safecode.org/uncategorized/best-practices/