TECHDEFENCELABS

Your Trusted Cyber Security Partner

A CERT-In Empanelled Information Security Organisation

No:- 3(15)/2004-CERT-In

Document Authorization, Revision History, and Control

Document Preparation	
Document Title	Web Application Vulnerability Assessment & Penetration Testing Report
Evaluated Organization	Xponentia Capital Partners LLP
Document ID	TDL-XCPL-WB-06/25/0549
Report Version	v1.0
Web Application Name	Xponentia
Type of Audit	Black Box Web Application VAPT Audit
Type of Audit Report	First Audit Report
Assessment Period	27-Jun-2025
Report Prepared by	Mokksh Parekh
Reviewed by	Heet Kakadiya
Approved by	Pavan Saxena
Released by	Pavan Saxena
Date of Release	30-Jun-2025

Document Change History		
Version	Date	Remarks / Reason of Change
v1.0	30-Jun-2025	First Audit Report

Document Distribution List			
Name	Organization	Designation	Email Id
Pavan Saxena	TechDefence Labs	Team - Lead	pavan@techdefence.com
Harsh Chauhan	TechDefence Labs	Security Analyst	harsh.chauhan@techdefence.com
Jaimin Doshi	TechDefence Labs	Business - Manager	jaimin.doshi@techdefence.com
Shilpa Jadhav	Xponentia Capital Partners LLP	VP Operations	shilpa@xponentia.in

Confidentiality and Disclaimer

This report is prepared exclusively for the management of **Xponentia Capital Partners LLP** and is intended solely for internal use. TechDefence Labs Solutions Limited disclaims any liability to third parties for the unauthorized use or distribution of this document or its contents. The findings, information, data, advice, and recommendations are based on the cooperation of **Xponentia Capital Partners LLP** and the data provided during the assessment period. Any limitations due to environment constraints, access restrictions, or insufficient information may have impacted the thoroughness of our analysis and could result in unidentified vulnerabilities.

The report assesses the initial security controls implemented by **Xponentia Capital Partners LLP**, specifically focusing on the security of the defined domain and systems in-scope. TechDefence Labs highlights areas for potential improvement; however, the responsibility for implementing and maintaining robust security measures lies with the management of **Xponentia Capital Partners LLP**. The information provided in this document reflects the state of the security environment at the time of preparation and is not an exhaustive evaluation.

9th Floor, Abhishree Adroit,
Near Mansi Circle, Vastrapur,
Ahmedabad-380015.

Table of Contents

1. Assessment Details

Xponentia Capital Partners LLP engaged TechDefence Labs to assess the security of its Web Application. The evaluation focused on identifying Web Application-level vulnerabilities, testing security mechanisms, and resilience against unauthorized access. The assessment followed industry standards, including OWASP Security Top 10, SANS Institute's Top 25 and Penetration Testing Execution Standard (PTES).

1.1 Engagement Scope

The following web application provided by **Xponentia Capital Partners LLP** have been identified as in-scope for this security assessment, as defined and specified by **Xponentia Capital Partners LLP**:

In Scope of Assessment	
Web Application Name	Xponentia
Web Application URL	https://www.xponentia.in/
Version of Web Application	N/A
Audit Type	Black Box
Testing Environment Configuration	Production
User Roles Configured for Testing	N/A

Out of the Scope of Assessment			
Sr. No	**Application Function Name**	**Application Function URL**	**Reason**
N/A	N/A	N/A	N/A

1.2 Scope Exclusions

1. Server testing on which the Web Application is hosted is outside the scope of this assessment.
2. The source code review of the Web Application is not included in the scope of this assessment.
3. Any API gateways connected to the Web Application but not owned by Xponentia Capital Partners LLP are outside the scope of this assessment.
4. For production environments provided during testing, vulnerabilities or test cases that may cause damage, or downtime will be excluded from the security audit.
5. Any Web Application endpoints or functions explicitly listed as "Out of Scope" for the assessment will not be tested.

1.3 VAPT Assessment Timeline

Events	Dates
Initial Security Assessment Start Date	27-Jun-2025
Initial Security Assessment End Date	27-Jun-2025
Initial Security Assessment Reports Shared Date	30-Jun-2025

1.4 Project Team

Below are the TechDefence Labs Auditing team members who played a key role in this engagement:

Name	Designation	Email-ID	Qualifications/ Certifications	Has the resource been listed on CERT-In's published Snapshot? (Yes/No)
Pavan Saxena	Team Lead - VAPT	pavan@techdefence.com	BCA (ISC)2 - CC, AZ-900, CEHv12, eJPT-v2, CAP, CNSP, CAPen, KLCP, ISO-27001: Lead Auditor	No
Khushi Bhatt	Security Analyst	khushi@techdefence.com	Msc.IT (IMS) & CS, CAP, CEHv12	No

2. VAPT Audit Methodology and Standards

2.1 Phases of the Assessment

- **Pre-engagement Phase:** This is the stage where the logistics and the rules of engagement of the test are discussed.
- **Reconnaissance/ Discovery Phase:** To simulate a cyber-attack on a Web Application, the penetration tester needs access to information about the target. They gather this information in the reconnaissance stage.
- **Vulnerability Analysis:** This phase consists of testing the Web Application for known vulnerabilities. Using an automated and manual approach for uncovering new and hidden vulnerabilities in the Web Application.
- **Exploitation and Post Exploitation:** The goal here is establishing access to a system using the loopholes uncovered in the earlier phases of Pen testing. The penetration tester tries to identify an entry point and then look for assets that can be accessed through that.
- **Reporting and Recommendations:** All the previous penetration testing phases contribute to this phase where a VAPT report is created and shared with the client.
- **Remediation and Rescan:** Once the vulnerabilities are fixed, we would carry out the round of rescans to identify any security loopholes that might have been left unattended.

2.2 Standards and Methodologies

- **OWASP Security Top 10:** is a list of the most critical security risks related to Web Application. It highlights common vulnerabilities that can lead to data breaches, unauthorized access, and other security incidents, helping organizations prioritize Web Application security measures.

- **SANS Institute's Top 25:** The SANS Top 25 is a list of the most critical software vulnerabilities, identified by the SANS Institute, which pose significant risks to applications and systems. It serves as a guide for developers and security professionals to prioritize and address common vulnerabilities to improve overall security posture.

- **Penetration Testing Execution Standard (PTES):** The Penetration Testing Execution Standard (PTES) provides a structured methodology for conducting comprehensive penetration testing. It includes seven essential phases—planning, information gathering, threat modelling, vulnerability analysis, exploitation, post-exploitation, and reporting—ensuring thorough coverage of vulnerabilities and helping organizations enhance their security posture through systematic testing and analysis.

2.3 Vulnerability Metrics

This section outlines the CVSS Scoring System used to calculate the severity of vulnerabilities, determined using leading security practices and TechDefence Labs' experience in similar projects. Each vulnerability is assigned a qualitative impact factor—Critical, High, Medium, Low, or Informational to help **Xponentia Capital Partners LLP** prioritize remediation efforts effectively and enhance their risk management strategy.

Risk Exposure	CVSS Score	Description
Critical	**9.0 – 10.0**	Exploitation of such vulnerabilities can lead to unauthorized access to sensitive information, data manipulation, and service disruptions, severely impacting Confidentiality, Integrity, and Availability (CIA) of the data, operations, business continuity and security posture.
High	**7.0 – 8.9**	Exploitation can lead to significant system or data compromise, with the potential for unauthorized access or privilege escalation. Prompt action is needed to mitigate risks before they escalate.
Medium	**4.0 – 6.9**	Exploitation may result in localized impact or reduced security but does not immediately threaten the overall system. These should be addressed in a timely manner to prevent potential exploitation.
Low	**0.1 – 3.9**	Exploitation has a minimal impact on system security and generally requires specific conditions. These can be addressed after higher-priority issues are resolved.
Informational	**0**	Findings that do not pose a direct risk but suggest improvements or optimizations to security practices. These should be reviewed for the best practices and continuous improvement.

Risk Factors: Risk is assessed based on two primary factors: Likelihood and Impact.

- **Likelihood:** This factor measures the probability of a vulnerability being exploited. Ratings are determined by the attack difficulty, the availability of tools, the skill level of potential attackers, and the environment.
- **Impact:** This factor evaluates the potential consequences of a vulnerability on operations, including its effect on confidentiality, integrity, and availability of systems/data, as well as any reputational or financial damage.

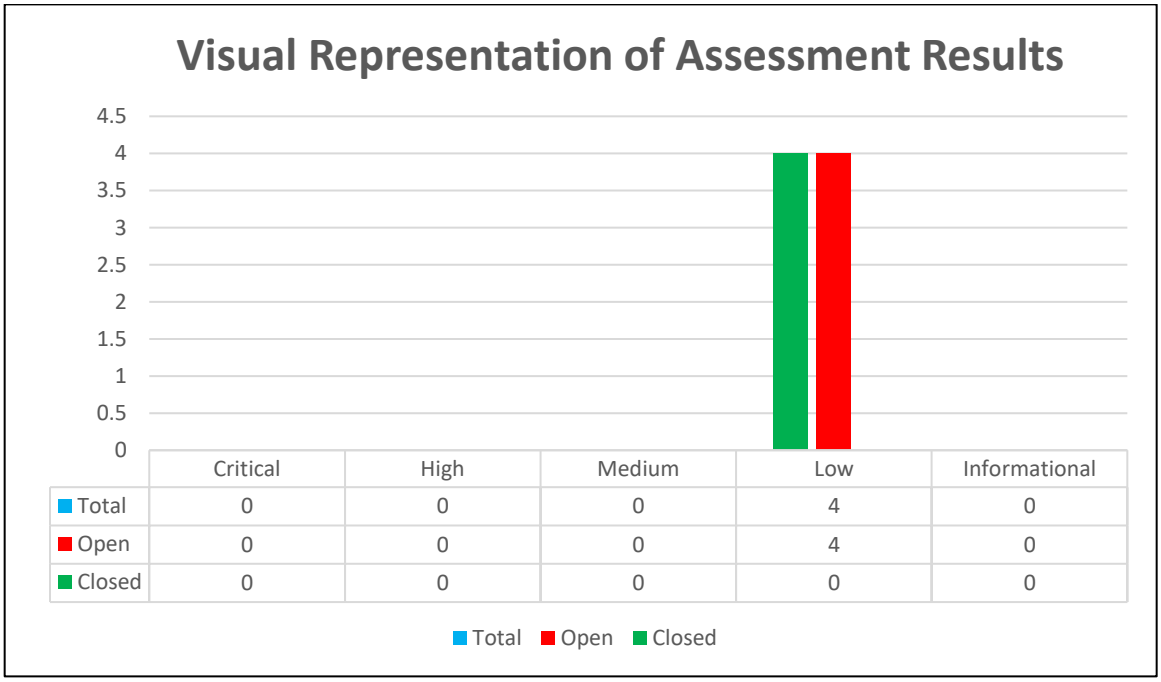
2.4 Tools used during the assessment

Sr. No	Name of Tool /Software used	Version of the tool /Software used	Open Source /Licensed
01	Burp Suite Professional	v2025.4.1	Licensed

3. Executive Summary

The following section provides an Executive Summary of the vulnerabilities identified during this Security Audit. Detailed recommendations for each observation are outlined in Section 4 of this report.

3.1 Visual Representation of Assessment Results



	Critical	High	Medium	Low	Informational
Total	0	0	0	4	0
Open	0	0	0	4	0
Closed	0	0	0	0	0

3.2 Vulnerability Overview Table

The table below outlines the vulnerabilities discovered during the assessment, along with their associated risk severity. It provides an evaluation of both the potential impact and the likelihood of each vulnerability occurring.

ID	Vulnerable URL	Vulnerability Name	CVE/CWE	Severity	Status
TDL-001	https://www.xponentia.in/	Clickjacking	CWE-1021	Low	Open
TDL-002	https://www.xponentia.in/	Missing security headers	CWE-693	Low	Open
TDL-003	https://static.viamagus.com/static/sitebuilder/js/jquery.validate.js https://static.viamagus.com/static/sitebuilder/js/jquery.js	Vulnerable & Outdated Components	CWE-1395	Low	Open
TDL-004	https://www.xponentia.in/register/afd	Server Name and Version Disclosure	CWE-200	Low	Open

4. Detailed Vulnerability Observations

TDL-001 - Clickjacking – {Low} {Open}

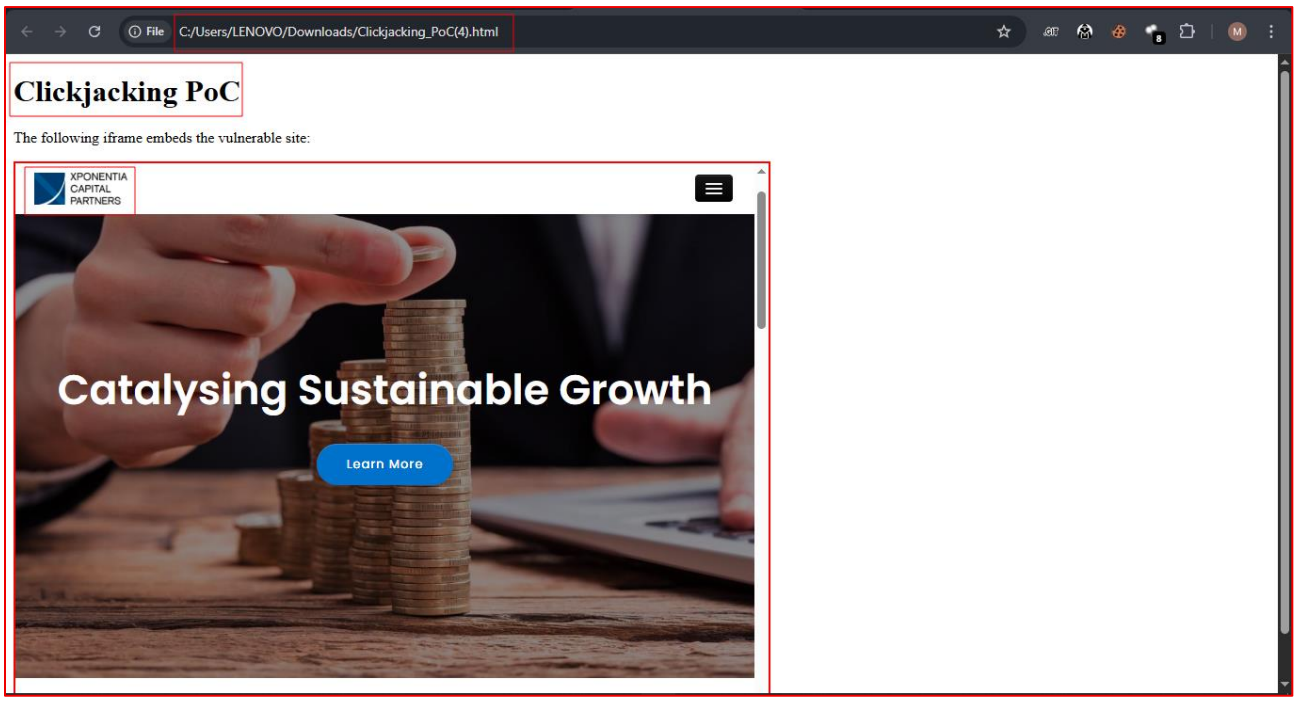
Vulnerable URLs	https://www.xponentia.in/
Vulnerable Parameter	N/A
Payload	N/A
Vulnerability Class	A05:2021 – Security Misconfiguration
CVSS Score 3.1	**Security Misconfiguration**
CWE-ID	**CWE-1021**
Vulnerability Explanation:	Clickjacking is a UI redressing attack where a malicious site embeds a legitimate web page inside an invisible iframe, tricking users into clicking elements (like buttons or links) they didn't intend to interact with. This exploits user trust and lack of frame protection mechanisms, allowing attackers to hijack clicks and perform unauthorized actions on behalf of users.
Vulnerability Impact:	If successful, clickjacking can lead to unauthorized transactions, data exposure, or permission changes—especially if the target site includes sensitive functions (e.g., banking, settings updates). Attackers can trick users into clicking "Allow," "Buy," or "Delete" buttons, resulting in privilege escalation or loss of control.
Remediation	Deploy the X-Frame-Options header with the "DENY" or "SAMEORIGIN" directive to prevent embedding of your site in iframes. Use Content Security Policy (CSP) to define allowable sources and locations for content.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Steps to Reproduce & Proof of Concept:

1. Copy the target URL.
2. Use the following HTML code:

```
<!DOCTYPE html>
<html>
<head>
 <title>Clickjacking PoC</title>
 <style>
  iframe {
   width: 800px;
   height: 600px;
   border: 2px solid red;
  }
 </style>
</head>
<body>
 <h1>Clickjacking PoC</h1>
 <p>The following iframe embeds the vulnerable site:</p>
 <iframe src="https://www.xponentia.in/home.html#" allowfullscreen></iframe>
</body>
</html>
```

3. Save it as clickjack.html and open in a browser.

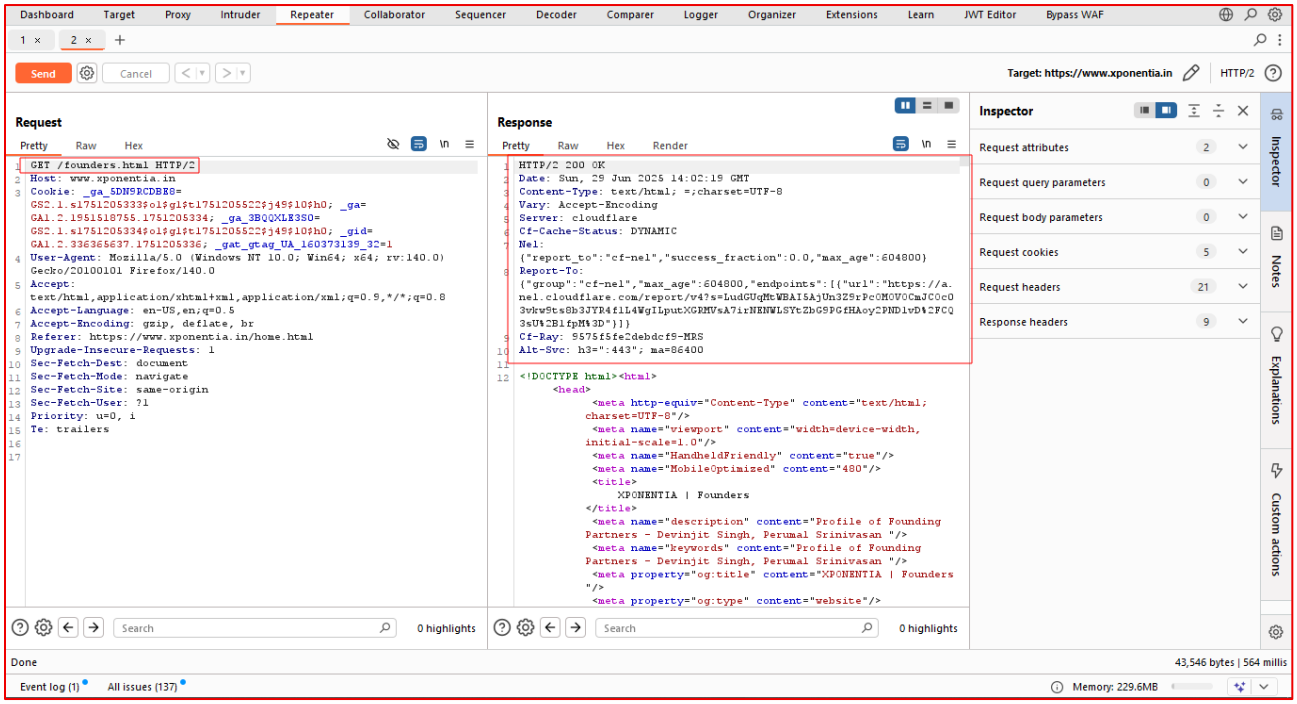

File
C:/Users/LENOVO/Downloads/Clickjacking_PoC(4).html
Clickjacking PoC
The following iframe embeds the vulnerable site:
XPONENTIA CAPITAL PARTNERS
Catalysing Sustainable Growth
Learn More

TDL-002 – Missing Security Headers – {Low} {Open}

Vulnerable URLs	https://www.xponentia.in/*
Vulnerable Parameter	N/A
Payload	N/A
Vulnerability Class	A05:2021 – Security Misconfiguration
CVSS Score 3.1	**Security Misconfiguration**
CWE-ID	**CWE-200**
Vulnerability Explanation:	Missing security headers occurs when essential HTTP response headers, such as Content-Security-Policy, X-Content-Type-Options, or Strict-Transport-Security, are not implemented or configured properly. These headers play a critical role in protecting web applications against common vulnerabilities like cross-site scripting (XSS), clickjacking, and MIME-type sniffing. Without these headers, the application is more susceptible to attacks, potentially exposing sensitive user data or compromising functionality.
Vulnerability Impact:	The absence of security headers increases the risk of various attacks. For example, without Content-Security-Policy, attackers can inject malicious scripts (XSS). Without X-Frame-Options, the site becomes vulnerable to clickjacking, which can trick users into performing unintended actions. A missing Strict-Transport-Security header allows attackers to execute man-in-the-middle attacks by downgrading secure HTTPS connections to HTTP, exposing sensitive information. Collectively, these issues undermine user trust and the application's security posture.
Remediation	Implement the following security headers in web server configuration or application code: 1. Content-Security-Policy (CSP): Prevents XSS and data injection attacks. 2. X-Frame-Options: Prevents clickjacking (e.g., DENY or SAMEORIGIN). 3. X-Content-Type-Options: Stops MIME-type sniffing (nosniff). 4. Referrer-Policy: Controls referrer info (e.g., no-referrer-when-downgrade). 5. Strict-Transport-Security (HSTS): Enforces HTTPS (max-age=31536000; includeSubDomains). 6. Permissions-Policy: Restricts use of powerful browser features like camera, mic, etc.
Reference	https://docs.patchstack.com/faq-troubleshooting/technical/how-to-add-security-headers-with-patchstack/

Steps to Reproduce & Proof of Concept:

1. Visit the targeted URL.
2. Meanwhile capture request in burpsuite, send the request to repeater tab.
3. Observe the response headers.

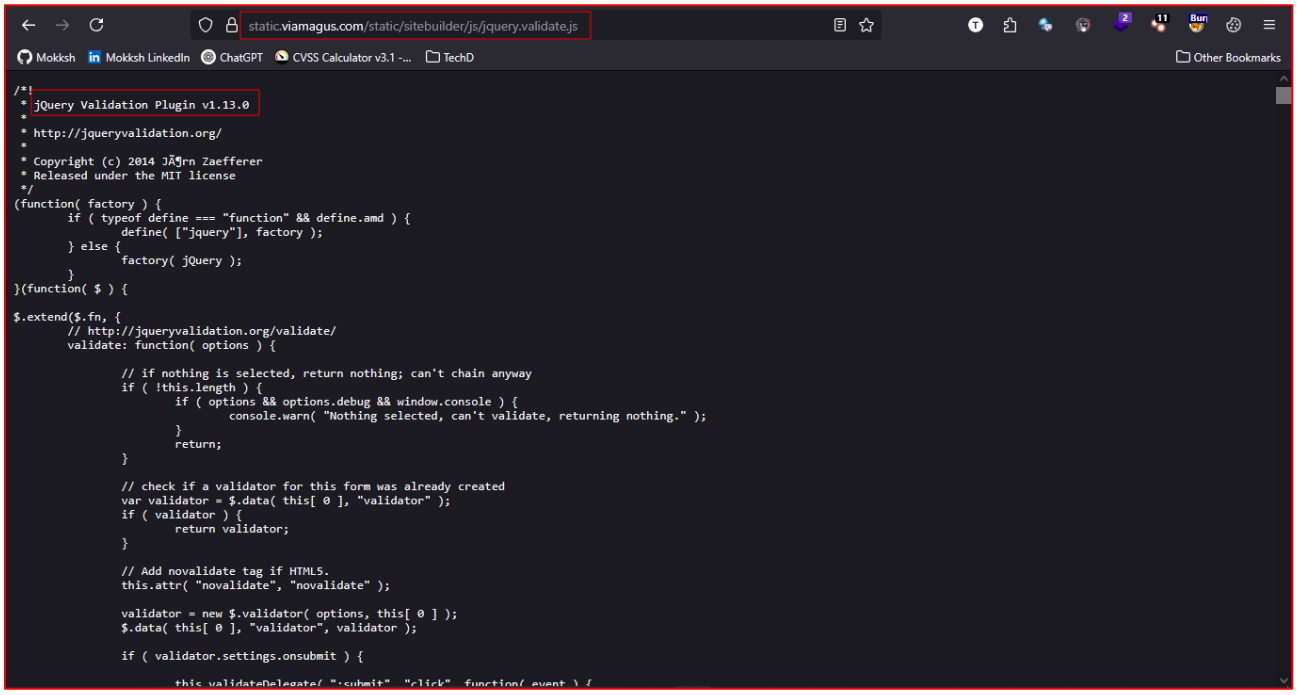


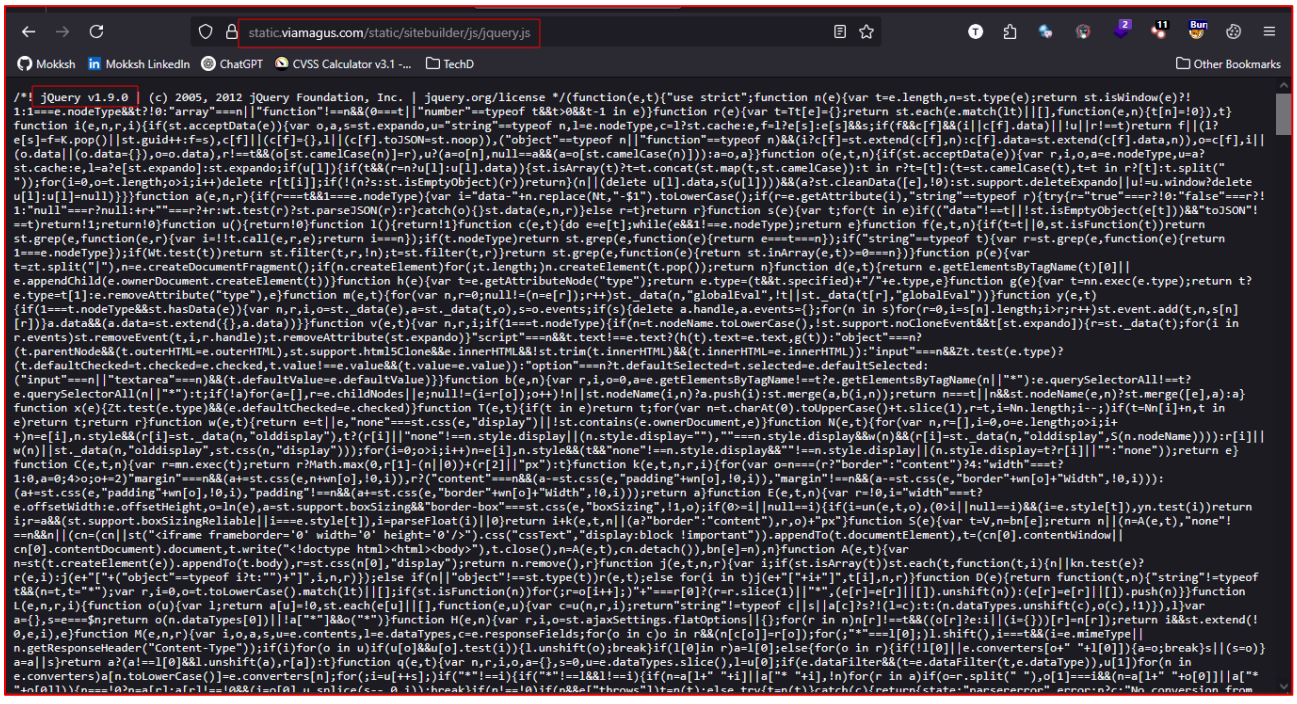
TDL-003 – Vulnerable & Outdated Components – {Low} {Open}

Vulnerable URLs	https://static.viamagus.com/static/sitebuilder/js/jquery.validate.js https://static.viamagus.com/static/sitebuilder/js/jquery.js
Vulnerable Parameter	N/A
Payload	N/A
Vulnerability Class	A05:2021 – Security Misconfiguration
CVSS Score 3.1	**Security Misconfiguration**
CWE-ID	**CWE-200**
Vulnerability Explanation:	This refers to the use of outdated or vulnerable third-party libraries, frameworks, or software components within an application. These components may contain known security flaws that can be exploited.
Vulnerability Impact:	Using outdated components increases the risk of exploitation through known vulnerabilities, potentially leading to data breaches, system compromise, or other security incidents.
Remediation	- Keep all software, libraries, and components up to date with the latest security patches and updates. - Use automated tools to scan for vulnerable and outdated components regularly. - Implement a robust dependency management process to ensure that all components are reviewed and updated as necessary.
Reference	https://cwe.mitre.org/data/definitions/1395.html

Steps to Reproduce & Proof of Concept:

1. Visit the targeted URL.



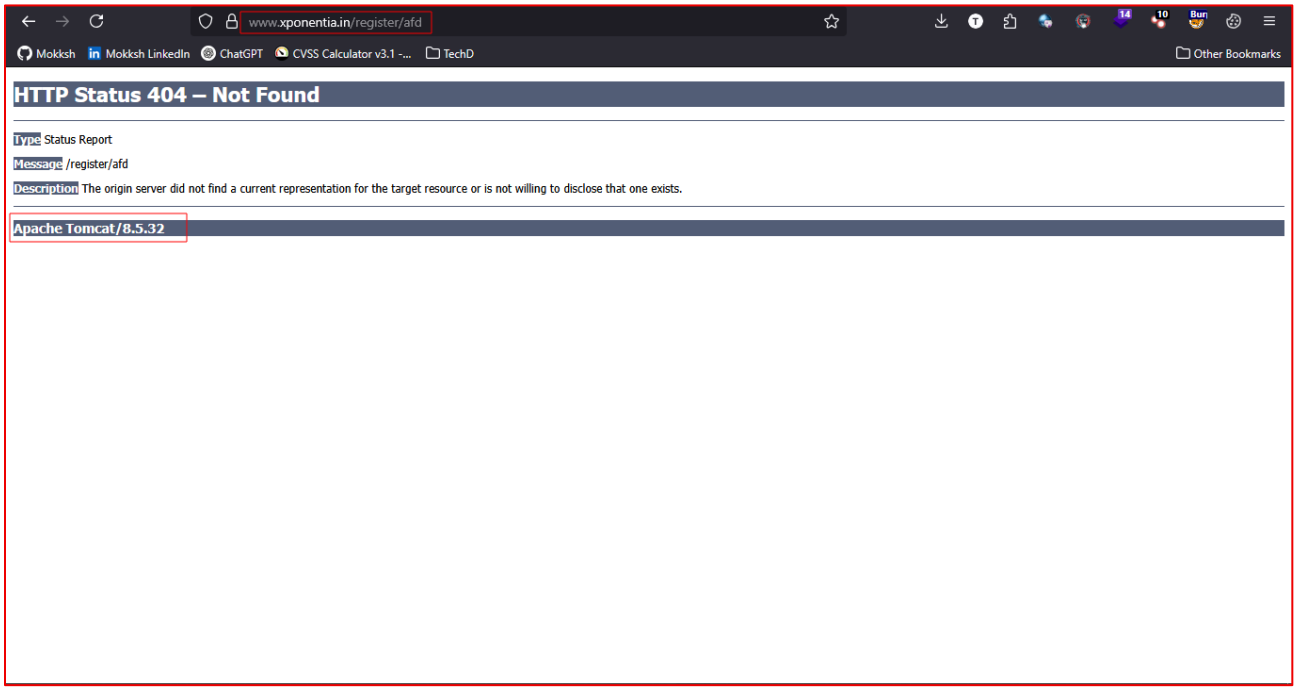


TDL-004 - Server Name and Version Disclosure – {Low} {Open}

Vulnerable URLs	https://www.xponentia.in/register/afd
Vulnerable Parameter	N/A
Payload	N/A
Vulnerability Class	A05:2021 – Security Misconfiguration
CVSS Score 3.1	**Security Misconfiguration**
CWE-ID	**CWE-200**
Vulnerability Explanation:	Server headers expose software names and versions, aiding attackers in fingerprinting.
Vulnerability Impact:	Revealing server details facilitates fingerprinting and targeted attacks using known vulnerabilities.
Remediation	Suppress server details in HTTP headers and error messages.
Reference	https://www.thesmartscanner.com/vulnerability-list/server-version-disclosure

Steps to Reproduce & Proof of Concept:

1. Visit the targeted URL.



Disclaimer and Precautions for Patch Implementation

Before initiating any patching, updates, or remediation work based on the vulnerabilities identified in the following report, please ensure the following precautions are in place:

- **Backups:** Confirm that comprehensive backups of the systems, code, and relevant data are created prior to making any changes. This ensures that you can restore the environment if needed.
- **Rollback Plan:** Have a clear rollback plan ready in case the patching or remediation leads to unexpected issues. This plan should outline steps to return the system to its previous state with minimal downtime.
- **Testing in UAT Environment:** Prior to implementing any hotfixes, service packs, or patches in the production environment, ensure thorough testing is conducted in a User Acceptance Testing (UAT) environment. This step helps verify that the fixes do not cause unforeseen issues or downtime.
- **Third-Party Links Disclaimer:** The following report includes third-party links to resources for vulnerability remediation. Please note that TechDefence Labs does not assume responsibility for the accuracy, availability, or content of these external sites, as they may change overtime.
- **Vulnerability Report Limitations:** The vulnerabilities listed in this report are based on security scans and tests conducted on the specified date using a non-intrusive approach within the tested environment. Please be aware that new vulnerabilities may be discovered after the report is generated. Additionally, certain vulnerabilities that could lead to system instability or downtime were not assessed in this report. The assessment was conducted within the timeline constraints of the audit, which may have excluded some potential test cases.
- **Ongoing Security:** This Vulnerability Assessment and Penetration Testing (VAPT) report should not be construed as an assertion of absolute security for the system or applications. Security is an ongoing process, and the system's security posture can evolve over time. The penetration tester does not accept responsibility for new risks that may arise after the assessment period due to changes in the target system or other unforeseen factors.

Appendices

As a CERT-IN empanelled organization, we have received communication stating that all CERT-IN empanelled organizations are required to submit audit-related data (including Cyber Audits, IS Audits, Regulatory audits, and VAPT audits) to CERT-IN starting from this fiscal year 2024. We will be sharing this VAPT Audit Reports or related details with CERT-IN. According to CERT-IN regulations, a period of 90 days is provided for the remediation/patching process from the release date of the audit reports. Therefore, we kindly request you to address all mentioned vulnerabilities within the 90-day timeframe and to inform us for the follow-up audit.