Web Application Report

Prepared for: Future Interns

Prepared by: K. Gautham Naga Ravi

Date: 24 August 2025

Objective

This report provides a detailed security assessment of the sample web application. The assessment focused on identifying vulnerabilities that could be exploited by malicious actors and providing mitigation strategies to improve the overall security posture of the application.

Scope

The scope of this engagement was limited to testing the publicly available modules of the web application. Manual testing and automated scanning (Burp Suite, OWASP ZAP) were used. Findings are mapped against the OWASP Top 10 vulnerabilities.

Identified Vulnerabilities

SQL Injection

Description: The application fails to sanitize user input in the login form, allowing attackers to bypass authentication or extract sensitive data.

Impact: High – Database exposure, authentication bypass.

Mitigation: Use parameterized queries (prepared statements), implement input validation and WAF rules.

Cross-Site Scripting (XSS)

Description: Reflected XSS vulnerability found in the search bar, enabling attackers to inject malicious JavaScript.

Impact: Medium – Session hijacking, phishing attacks.

Mitigation: Implement output encoding, use Content Security Policy (CSP), and sanitize user input.

Broken Authentication

Description: Weak password policy and lack of account lockout on multiple failed attempts.

Impact: High – Brute force attacks, account takeover.

Mitigation: Enforce strong password policy, implement account lockout, use MFA.

Insecure Direct Object Reference (IDOR)

Description: User IDs in URLs can be manipulated to access other users' profiles without authorization.

Impact: High – Data exposure, privacy violation.

Mitigation: Implement proper access control checks, avoid exposing direct identifiers.

Security Misconfiguration

Description: Directory listing enabled on /uploads, exposing sensitive files.

Impact: Medium – Information disclosure, file leakage.

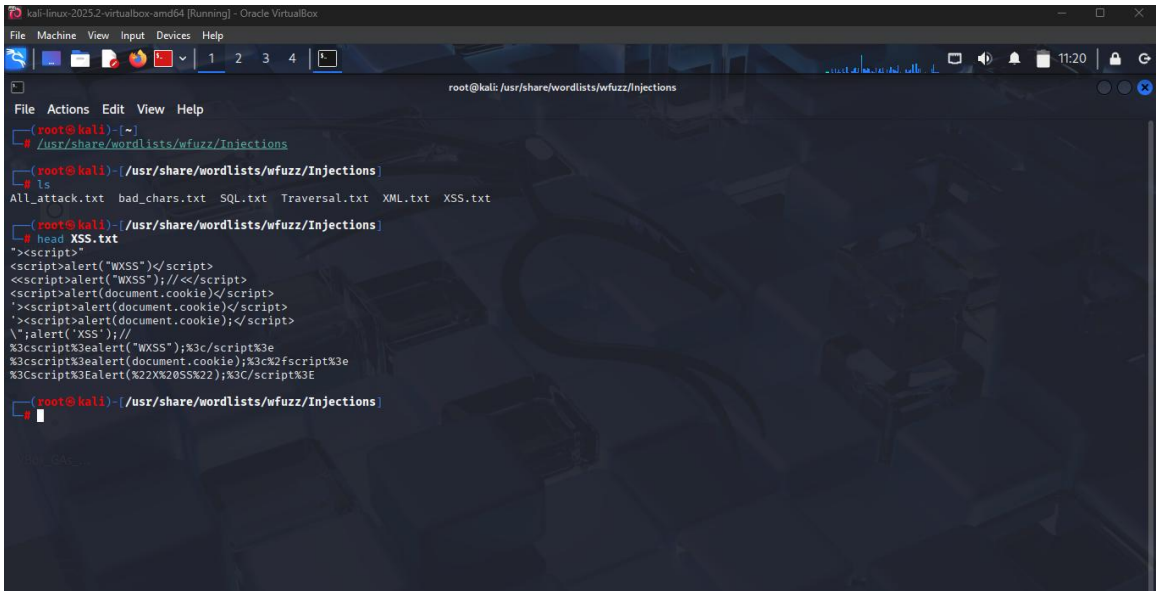
Mitigation: Disable directory listing, apply least privilege on server directories.

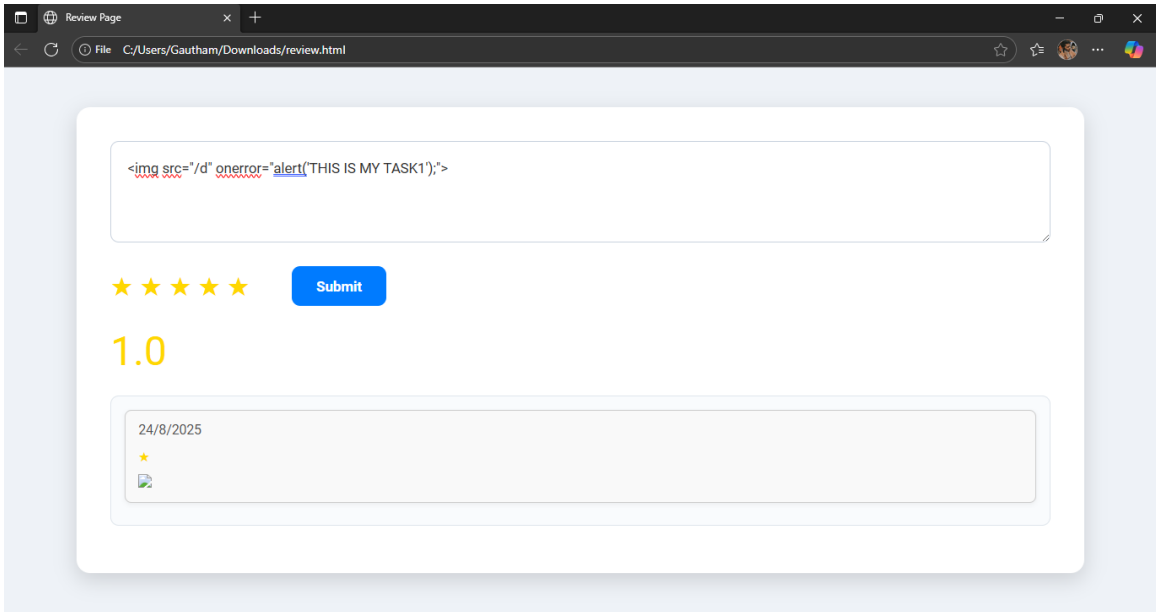
OWASP Top 10 Mapping

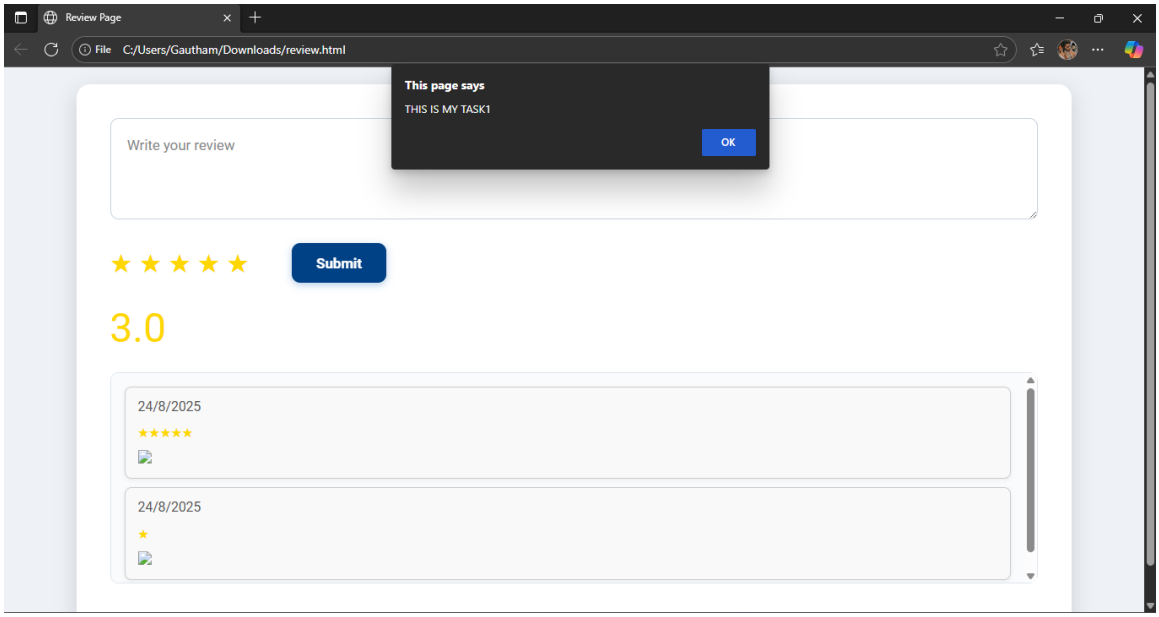
Vulnerability	OWASP Top 10 Category
SQL Injection	A03:2021 – Injection
XSS	A03:2021 – Injection
Broken Authentication	A07:2021 – Identification & Authentication Failures
IDOR	A01:2021 – Broken Access Control
Security Misconfiguration	A05:2021 – Security Misconfiguration
Data Exposure	A02:2021-Cryptographic failures
Insecure Design	A04:2021-Insecure Design
Known Vulnerabilities	A06:2021-Vulnerable and Outdated Components
CVE /CVSS	A08:2021-Software and Data Integrity failures
Login Failures	A09:2021-Security Logging and Monitoring Failures
SSRF	A10:2021- Server Side Request Forgery

Screen Shots

Screenshots of Xss attack







Conclusion

The identified vulnerabilities pose significant risks to the web application if not addressed promptly. It is strongly recommended to prioritize remediation efforts based on the severity of each issue and re-test the application post-fix deployment.