Web Application Vulnerability Assessment Report-By Dilliraj S

1. Introduction

This report presents the findings of a vulnerability assessment conducted on intentionally vulnerable web applications, namely OWASP Juice Shop and DVWA. The purpose was to identify common web application vulnerabilities, simulate real-world attacks, and recommend remediation steps using ethical hacking techniques.

2. Test Environment Setup

The applications were deployed locally using Docker . The tools utilized for scanning and analysis include OWASP ZAP and Burp Suite (Community Edition)

3. Summary of Findings

1. OWASP Top 10 Mapping – ZAP Scan Report

Vulnerability Detected	OWASP Category	Description	Risk Level
Content Security Policy Header Not Set	A05: Security Misconfiguration	Missing CSP allows XSS and injection attacks.	Medium
Cross-Domain Misconfiguration	A05: Security Misconfiguration	Allows resources to be loaded from potentially malicious origins.	Medium
Hidden File Found	A05: Security Misconfiguration	Sensitive files exposed that may reveal configuration or credentials.	Medium
Missing Anti-clickjacking Header	A05: Security Misconfiguration	Can be embedded in iframes, enabling clickjacking attacks.	Medium

Session ID in URL Rewrite	A07: Identification & Auth Failures	Session IDs in URLs can be leaked via logs or referrers.	Medium
Vulnerable JavaScript Library	A06: Vulnerable & Outdated Components	Outdated JS libraries with known vulnerabilities.	Medium
Cross-Domain JS Source File Inclusion	A08: Software/Data Integrity Failures	Risk of including tampered JS files from third-party domains.	Low
Private IP Disclosure	A01: Broken Access Control	Internal IPs revealed can help attackers pivot inside networks.	Low
Timestamp Disclosure - Unix	A09: Logging & Monitoring Failures	Server timestamp leaks useful for recon or timing attacks.	Low
X-Content-Type-Options Header Missing	A05: Security Misconfiguration	May allow MIME type sniffing leading to script execution.	Low
Information Disclosure - Suspicious Comments	A09: Logging & Monitoring Failures	Developer comments in source code could expose logic or secrets.	Informational

2.OWASP Top 10 Vulnerability Mapping-Burp Suite report

Vulnerability	Risk	Tool	OWASP Mapping
SQL Injection	High	Burp Suite	A03: Injection
XSS (Cross-site Scripting)	High	Burp Suite / ZAP	A03: Injection
Session ID in URL	Medium	ZAP	A07: Authentication Failures
Missing Security Headers	Medium	ZAP	A05: Security Misconfiguration

Outdated JavaScript Library	Medium	ZAP	A06: Vulnerable Components

4. Detailed Findings

SQL Injection

Description: The login form is vulnerable to SQL injection, allowing attackers to bypass authentication.

Risk Level: High

OWASP Mapping: A03: Injection

Remediation: Use prepared statements and parameterized queries.

Cross-site Scripting (XSS)

Description: Input fields do not sanitize user input, enabling injection of malicious JavaScript.

Risk Level: High

OWASP Mapping: A03: Injection

Remediation: Implement input validation and output encoding.

Session ID in URL

Description: Session IDs are exposed in URLs, which can be leaked via logs or referrer headers.

Risk Level: Medium

OWASP Mapping: A07: Authentication Failures

Remediation: Use cookies for session tracking and enforce HTTPS.

Missing Security Headers

Description: Security headers like Content-Security-Policy and X-Frame-Options are not set.

Risk Level: Medium

OWASP Mapping: A05: Security Misconfiguration

Remediation: Configure web server to include recommended security headers.

Outdated JavaScript Library

Description: The application uses an outdated JS library with known vulnerabilities.

Risk Level: Medium

OWASP Mapping: A06: Vulnerable Components

Remediation: Update to the latest stable version of the library.

5. Conclusion

The assessment identified multiple vulnerabilities, including high-risk SQL Injection and XSS flaws. All issues have been documented with recommended remediation steps. Securing the application will involve addressing these issues according to best practices and the OWASP Top 10 guidelines.