Web Application Security Assessment Report

OWASP Juice Shop – Vulnerability Analysis

Prepared by: Murtaza Sukhsarwala

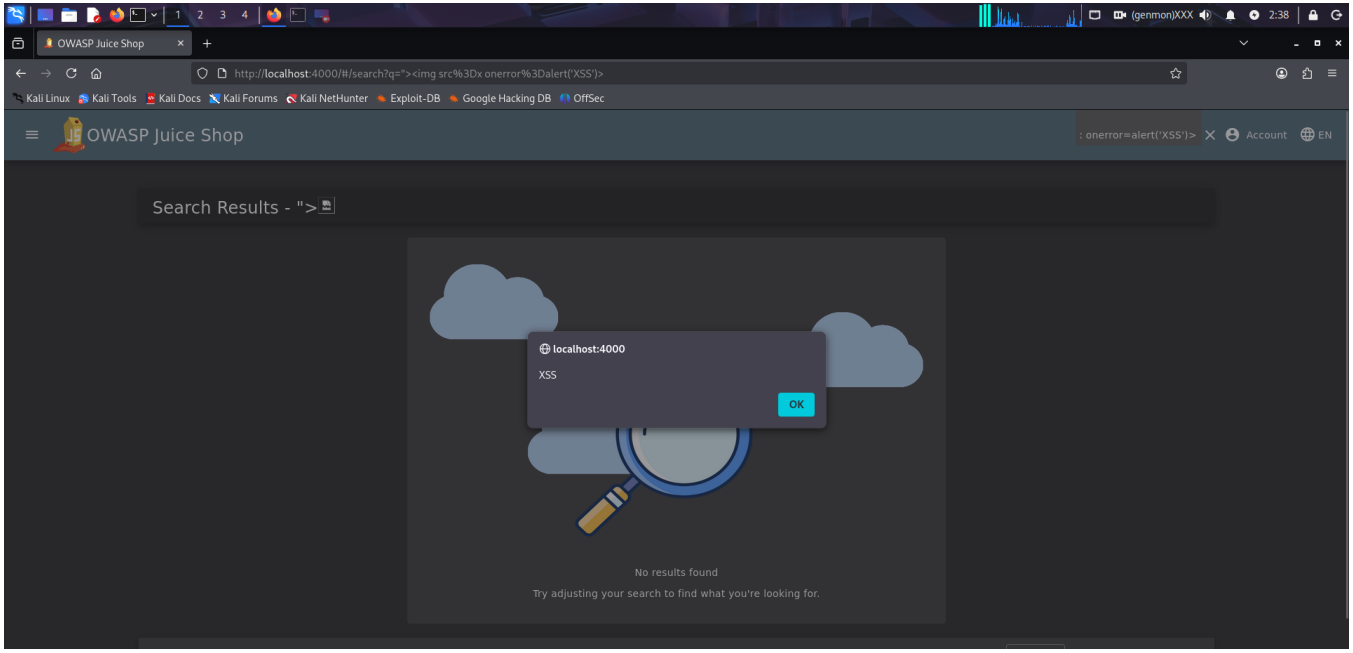
Scope & Tools Used

- - Target: OWASP Juice Shop (localhost:4000)
- - Tools: OWASP ZAP, Browser, Kali Linux
- - Tests: XSS, Security Headers, Misconfigurations

ZAP Scan Summary

- Key Findings from ZAP Scan:
- - Missing CSP Header (Medium)
- - Cross-Domain Misconfiguration (Medium)
- - Session ID in URL Rewrite (Medium)
- - Vulnerable JS Library (Medium)
- - Timestamp Disclosure (Low)
- - Suspicious Comments (Informational)

Reflected XSS – Proof of Concept



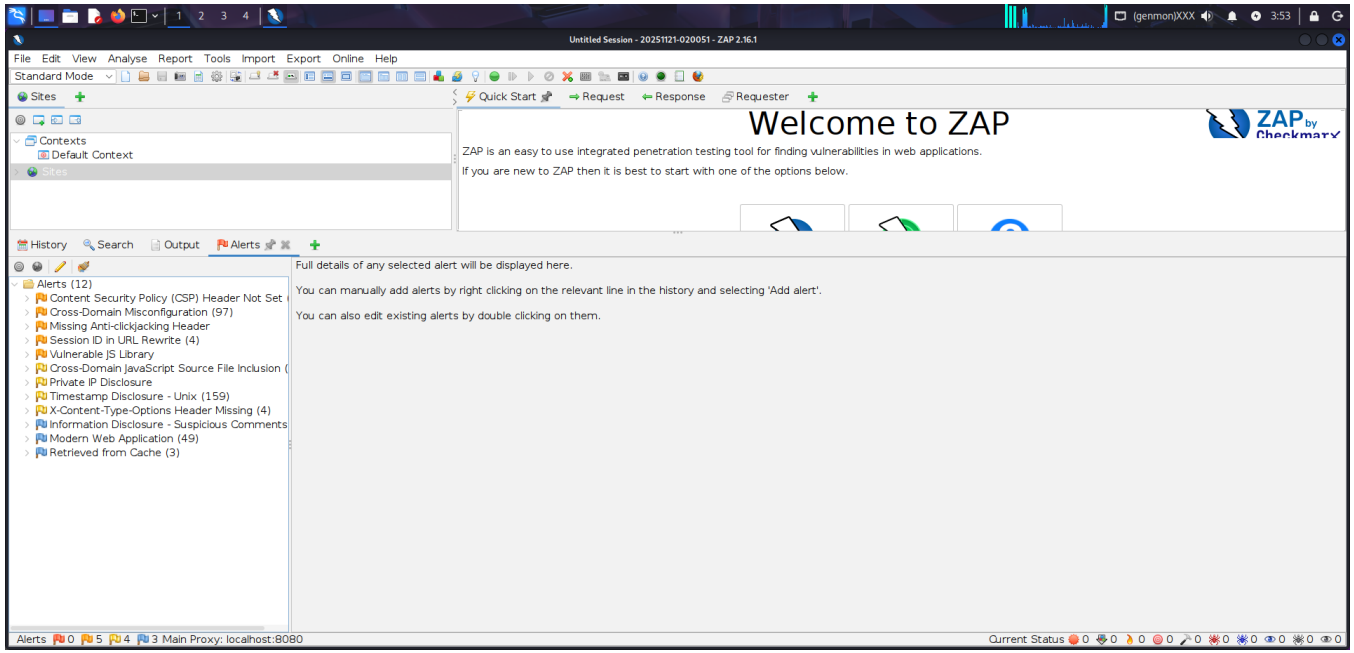
Reflected XSS – Explanation

- Payload used:
- "/><img src=x onerror=alert('XSS')>

- Impact:
- - Allows execution of arbitrary JavaScript
- - Can lead to session hijacking and phishing attacks

- Recommendations:
- - Sanitize and validate input
- - Encode output
- - Add strong CSP

ZAP Alerts Overview



OWASP Top 10 Mapping Checklist

- ✓ A01: Broken Access Control – Not Observed
- ✓ A02: Cryptographic Failures – Not Observed
- ✓ A03: Injection – Reflected XSS Confirmed
- ✓ A04: Insecure Design – Possible (Missing CSP)
- ✓ A05: Security Misconfiguration – Confirmed
- ✓ A06: Vulnerable & Outdated Components – Confirmed
- ✓ A07: Identification & Authentication Failures – Not Observed
- ✓ A08: Software & Data Integrity Failures – Not Observed
- ✓ A09: Security Logging & Monitoring Failures – Not Tested
- ✓ A10: SSRF – Not Observed

Conclusion

- The test revealed multiple vulnerabilities including XSS and misconfigurations.
- Implementing secure headers, validating inputs, and updating components is recommended.