

Web Application Security Assessment Report

OWASP Juice Shop – Vulnerability
Analysis

Prepared by: Murtaza Sukhsarwala

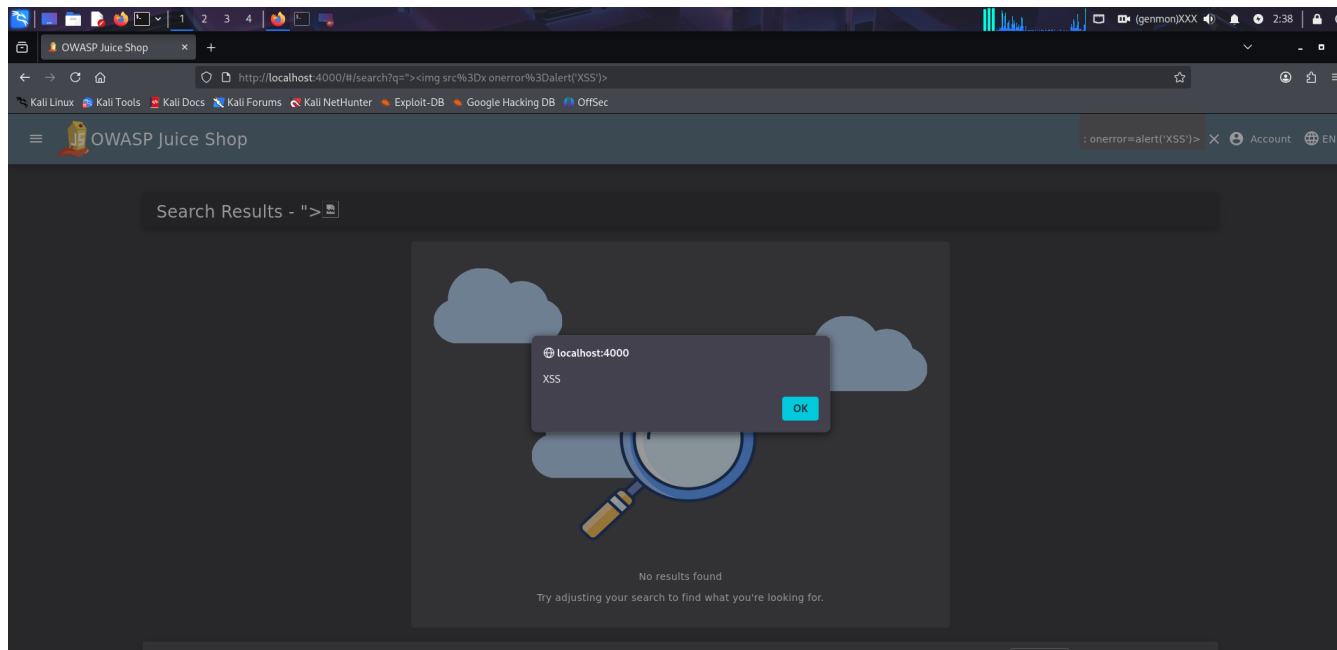
Scope & Tools Used

- - 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:
- `"/>`
- Impact:
 - - Allows execution of arbitrary JavaScript
 - - Can lead to session hijacking and phishing attacks
- Recommendations:
 - - Sanitize and validate input
 - - Encode output
 - - Add strong CSP

The screenshot shows the ZAP (Zed Attack Proxy) web interface. At the top, there's a menu bar with options like File, Edit, View, Analyse, Report, Tools, Import, Export, Online, and Help. Below the menu is a toolbar with various icons for navigation and analysis. The main content area displays a 'Welcome to ZAP' message, stating that ZAP is an easy-to-use integrated penetration testing tool for finding vulnerabilities in web applications. It also mentions that if you're new to ZAP, it's best to start with one of the options below. On the left side, there's a sidebar with three main sections: 'Sites', 'Contexts', and 'Alerts'. The 'Alerts' section is expanded, showing a list of alerts. The alerts are categorized by severity (Critical, High, Medium, Low, Info) and include details like the alert name, count, and a brief description. For example, 'Content Security Policy (CSP) Header Not Set' is a High severity alert. The bottom status bar shows 'Alerts 0 5 4 3 Main Proxy: localhost:8080' and 'Current Status' with various icons representing different alert types and the proxy's operational status.

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- ✓ A06: Vulnerable & Outdated Components – Confirmed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.