Security Assessment Report — Web Application Security Testing

Target: OWASP Juice Shop (Test Environment)
Prepared by: SK. Lathi Funnisa Begam — Cyber Security Intern, Future Interns
Date: 2025-11-04

Table of Contents

Executive Summary

This report presents the results of a security assessment against a lab instance of OWASP Juice Shop. Testing used OWASP ZAP for automated scanning and Burp Suite for manual verification. The assessment focused on common web vulnerabilities and mapping to OWASP Top 10.

Scope & Methodology

Scope: Non-production Juice Shop instance. **Methodology:** Reconnaissance, automated scanning (ZAP), manual testing (Burp), verification.

Findings (Detailed)

Finding 1: SQL Injection (Reflected)

Endpoint: /api/search or /api/
Severity: High
OWASP Mapping: A03: Injection
Description: Search/login endpoints accepted input that was not parameterized.
Proof of Concept:

```
GET /api/search?q=1' OR '1'='1
```

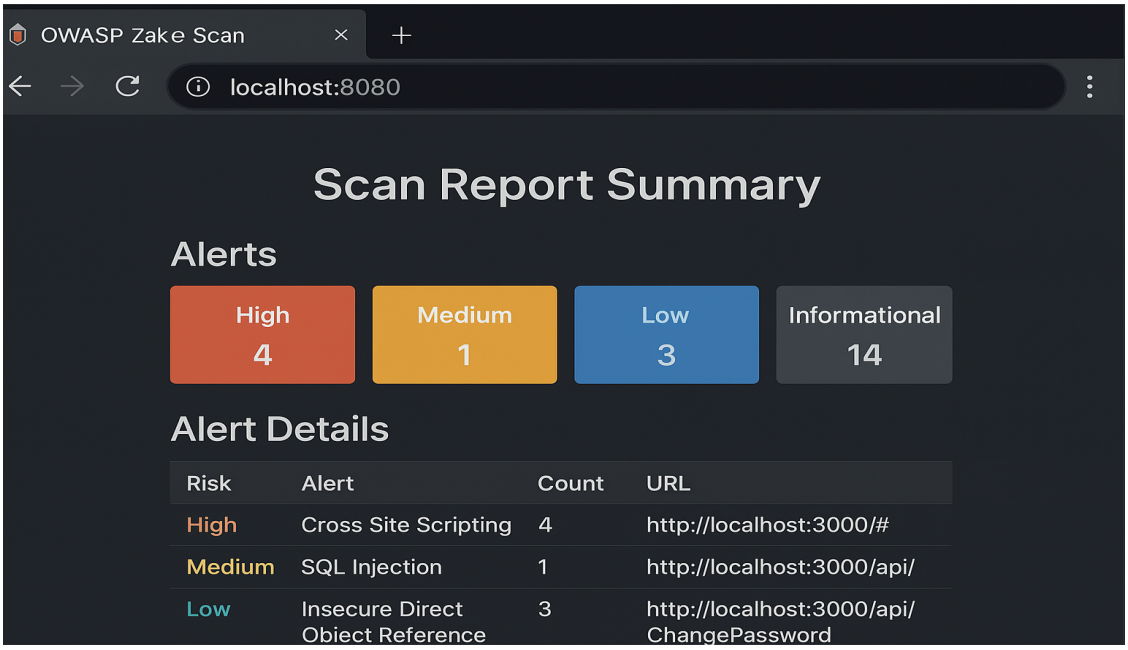


Figure: Evidence for SQL Injection (Reflected)
Impact: Data exposure or auth bypass.
Remediation: Use prepared statements, validate inputs, limit DB privileges.

Finding 2: Stored Cross-Site Scripting (XSS)

Endpoint: /feedback
Severity: High
OWASP Mapping: A07: XSS
Description: User feedback rendered without proper output encoding.
Proof of Concept:
`Submit alert('xss') in feedback.`

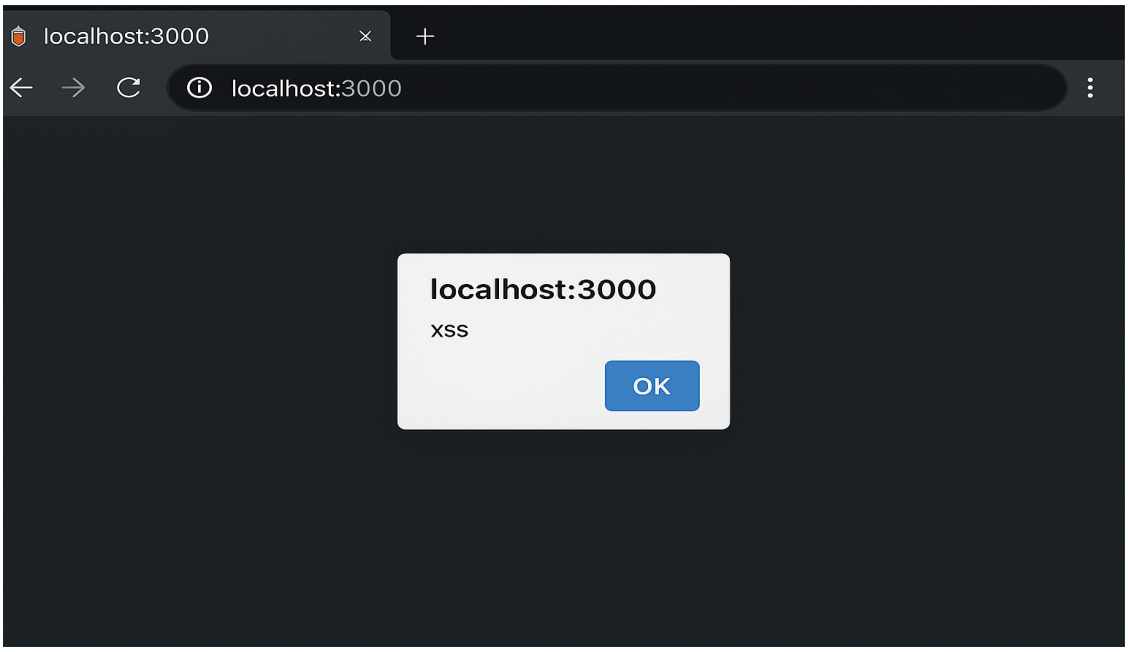


Figure: Evidence for Stored Cross-Site Scripting (XSS)
Impact: Cookie theft, account takeover.
Remediation: Output encode, CSP, input validation.

Finding 3: Cross-Site Request Forgery (CSRF)

Endpoint: /user/change-password
Severity: Medium
OWASP Mapping: A08: CSRF
Description: Sensitive actions lacked anti-CSRF tokens.
Proof of Concept:
`Auto-submitting form to /user/change-password.`

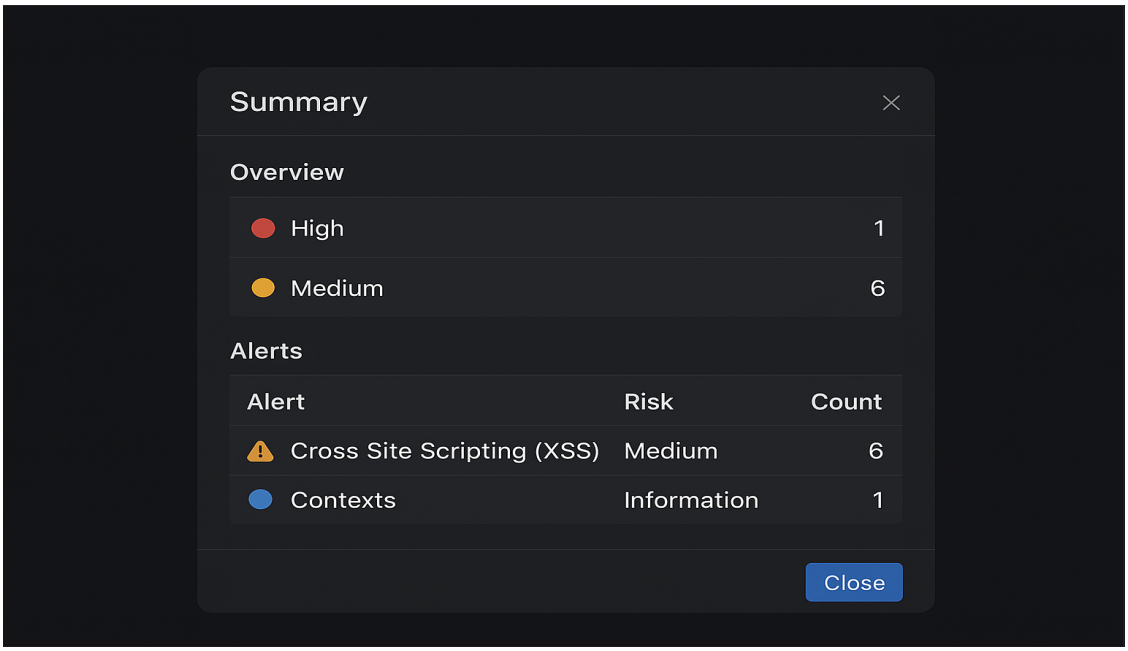


Figure: Evidence for Cross-Site Request Forgery (CSRF)
Impact: Forced password change / account compromise.
Remediation: Implement CSRF tokens, SameSite cookies.

Finding 4: Insecure Direct Object Reference (IDOR) / Broken Access Control

Endpoint: /api/orders/{id}
Severity: High
OWASP Mapping: A01: Broken Access Control
Description: API returned resources by ID without verifying ownership.
Proof of Concept:

```
Access /api/orders/1002 while logged in as another user.
```

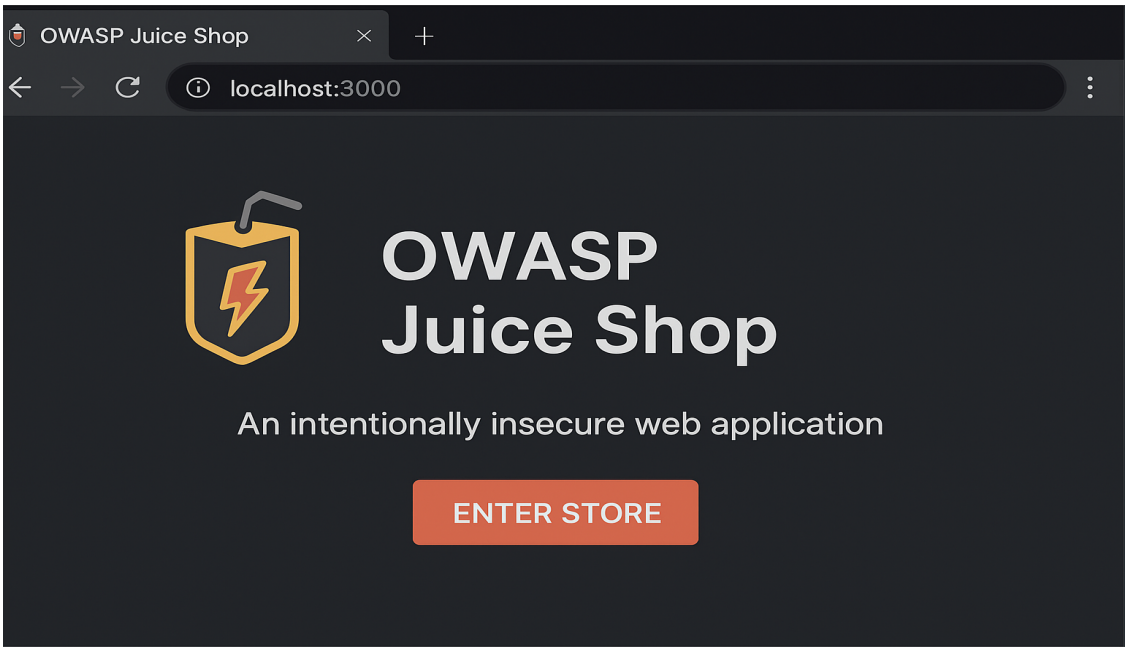
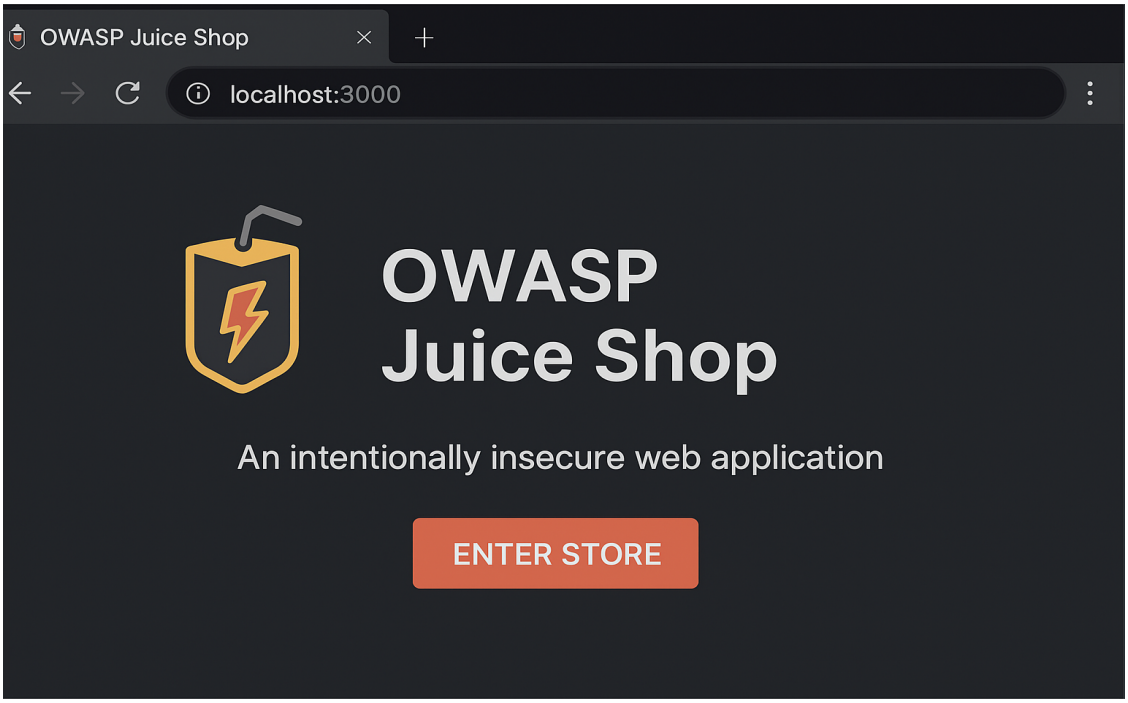


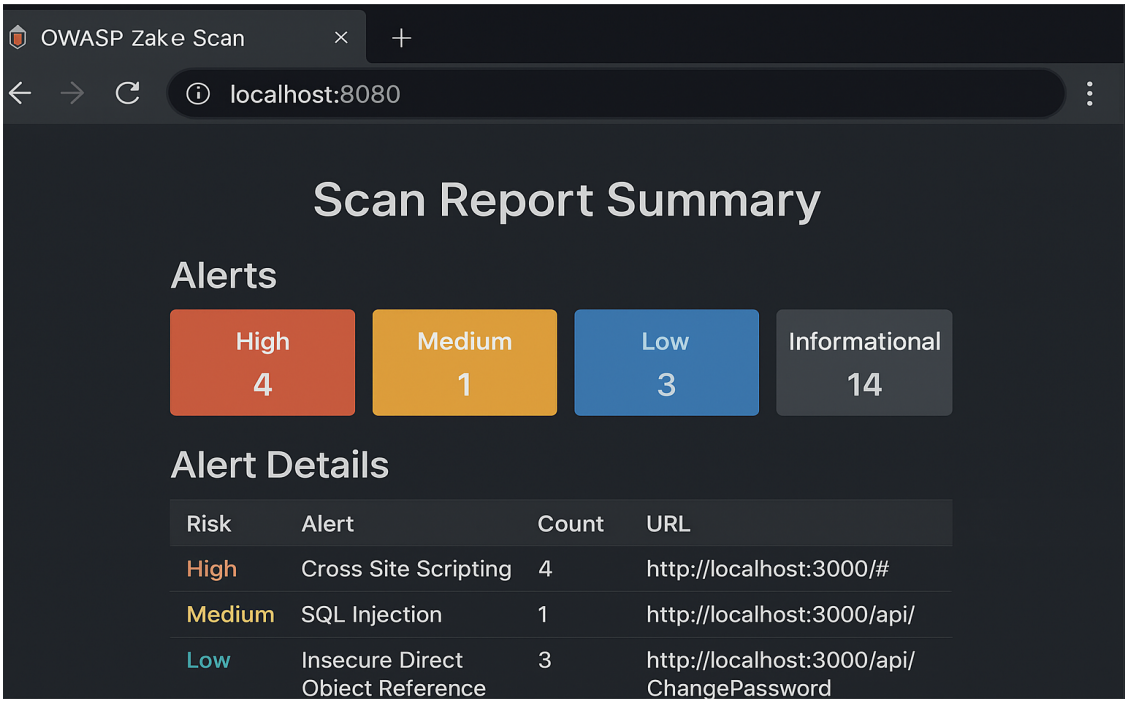
Figure: Evidence for Insecure Direct Object Reference (IDOR) / Broken Access Control
Impact: Exposure of PII and business data.
Remediation: Enforce server-side authorization and indirect references.

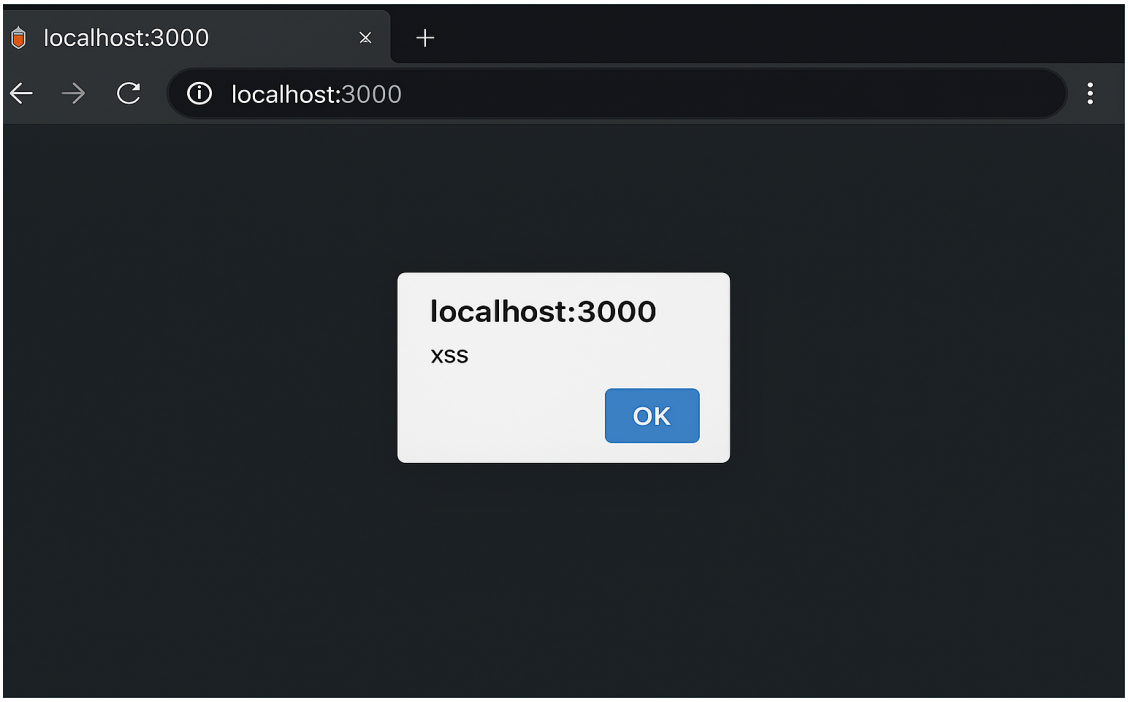
OWASP Top 10 (2021) — Mapping & Checklist

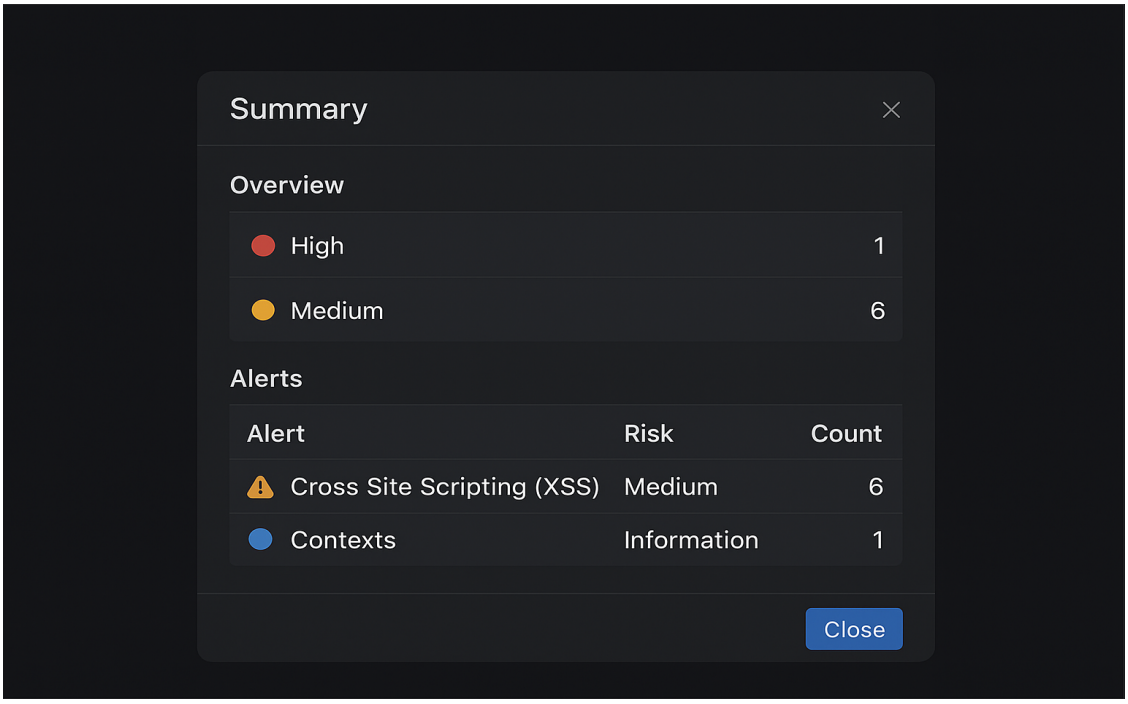
OWASP Top 10 (2021)	Covered / Notes
A01: Broken Access Control	Finding 4 (IDOR) — enforce authorization.
A02: Cryptographic Failures	Not in scope.
A03: Injection	Finding 1 (SQLi) — parameterize queries.
A04: Insecure Design	Recommended in remediation.
A05: Security Misconfiguration	Remove defaults; secure headers.
A06: Vulnerable & Outdated Components	Inventory and update components.
A07: Identification & Authentication Failures	Use strong passwords and MFA.
A08: Software & Data Integrity Failures	Finding 3 (CSRF) — add protections.
A09: Security Logging & Monitoring Failures	Central logging and alerting recommended.
A10: SSRF	Not observed in this assessment.

Screenshots & Evidence (Full Size)






localhost:3000
localhost:3000
localhost:3000
xss
OK


Summary
Overview
High 1
Medium 6
Alerts
Alert Risk Count
Cross Site Scripting (XSS) Medium 6
Contexts Information 1
Close

Conclusion & Recommendations

High-risk issues (SQLi, Stored XSS, IDOR) should be remediated as a priority. Follow remediation steps and re-scan. Implement secure coding practices and monitoring.

Recommendations:

- Remediate high-risk findings immediately.
- Use prepared statements and input validation.
- Implement server-side authorization and indirect references.
- Add anti-CSRF tokens and SameSite cookie flags.
- Enable central logging with alerting.

Appendix: Tool Reports & Logs

- Attach OWASP ZAP report (zap_report.html)
- Attach Burp Suite report (burp_report.xml or PDF)
- Attach Nikto or other scan outputs