

Web Application Security Assessment Report

Prepared for: Client Project
Performed by: Murtaza
Target: OWASP Juice Shop (localhost:4000)

Executive Summary

A comprehensive security assessment was conducted on OWASP Juice Shop to evaluate its security posture. Testing revealed several vulnerabilities including Reflected XSS, SQL Injection risk, and multiple security misconfigurations. This report provides proof-of-concept evidence, risk ratings, and recommended security improvements.

Scope of Assessment

Assessment Items	Details
Target	OWASP Juice Shop (localhost:4000)
Tools Used	OWASP ZAP, Browser Testing, Kali Linux
Focus Areas	Injection flaws, Authentication, Security headers, Components

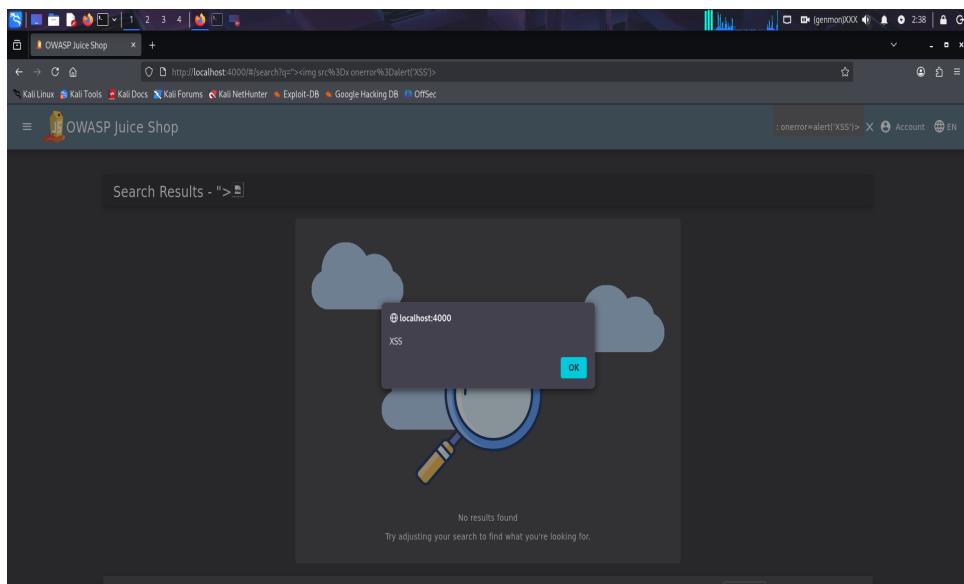
Finding 1: Reflected Cross-Site Scripting (XSS)

A Reflected XSS vulnerability exists in the search parameter. JavaScript injection was executed using the payload below:

Payload Used: "/>

Impact: High – Allows attackers to execute arbitrary JavaScript.

Recommendation: Encode output, sanitize input, implement CSP.



Finding 2: SQL Injection Risk – Login Page

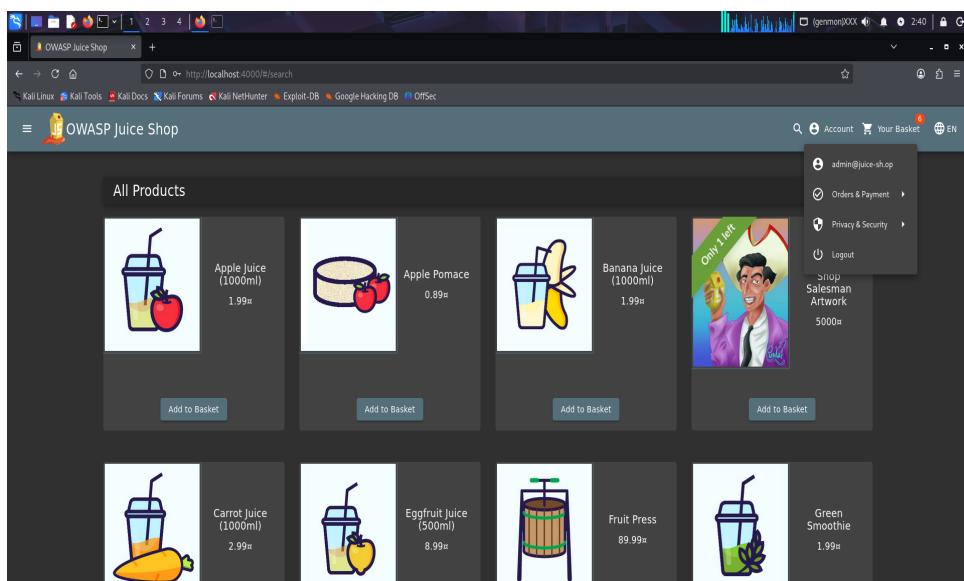
The login form was tested for SQL Injection. If the backend fails to use parameterized queries, attackers may bypass authentication.

Test Payloads:

```
' OR '1='1' --  
admin' --  
' OR 1=1--
```

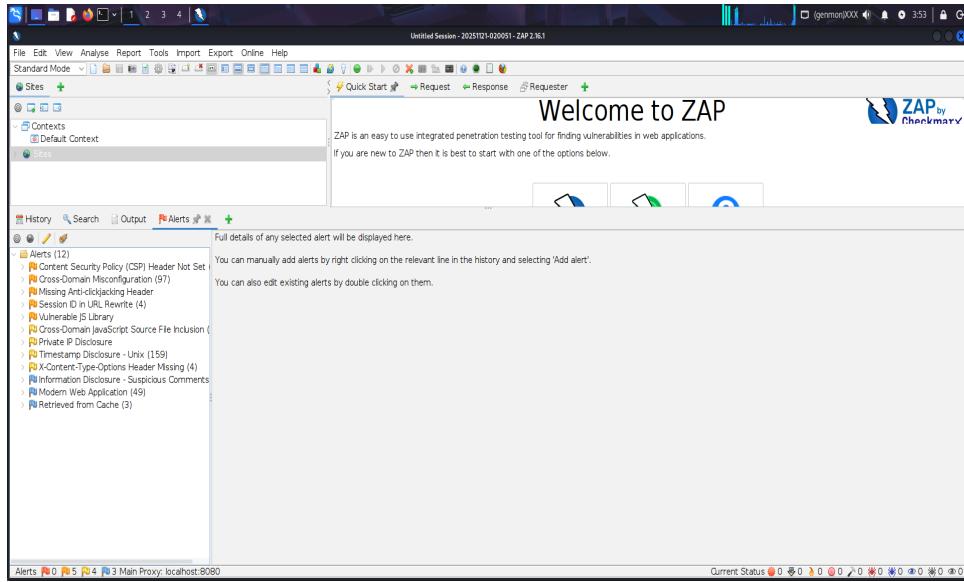
Impact: Critical – Authentication bypass, data exposure.

Recommendation: Use parameterized queries, validate input, hide DB errors.



ZAP Automated Scan Summary

- Missing Content Security Policy
- Cross-Domain Misconfiguration
- Session ID in URL
- Vulnerable JavaScript Library
- Timestamp Disclosure
- Suspicious Comments



OWASP Top 10 Mapping

OWASP Category	Status
A01: Broken Access Control	Not Observed
A02: Cryptographic Failures	Not Observed
A03: Injection	XSS & SQL Injection Risk
A04: Insecure Design	CSP Missing
A05: Security Misconfiguration	Confirmed
A06: Vulnerable Components	Confirmed
A07: Auth Failures	Possible Risk
A08: Integrity Failures	Not Observed
A09: Logging Failures	Not Tested
A10: SSRF	Not Observed

Conclusion

The assessment identified serious vulnerabilities affecting data integrity, confidentiality, and overall application security. Immediate remediation is advised to enhance the application's security posture.