

# WEB APPLICATION SECURITY ASSESSMENT REPORT

**Target Application:** OWASP Juice Shop

**Assessment Type:** Vulnerability Assessment & Penetration Testing (VAPT)

**Standards:** OWASP Top 10 (2021)

**Testing Approach:** Black-Box

Prepared by: Gangadhar J

## 1. Executive Summary

This document presents the findings of a security assessment conducted on the OWASP Juice Shop web application. The objective of this engagement was to identify security weaknesses that could be exploited by attackers. The assessment revealed multiple high and medium severity vulnerabilities that could result in unauthorized access, data leakage, and application compromise.

## 2. Scope and Methodology

The scope of this assessment was limited to the OWASP Juice Shop web application hosted in a controlled environment. A black-box testing methodology was adopted, simulating an external attacker with no prior knowledge of the system. Automated scanning and manual exploitation techniques were used.

## 3. Vulnerability Findings

Vulnerability	OWASP Category	Severity	Impact
SQL Injection	A03 – Injection	High	Authentication Bypass, Data Breach
Cross-Site Scripting (XSS)	A07 – XSS	High	Session Hijacking
Broken Authentication	A02 – Auth Failures	Medium	Account Takeover
Security Misconfiguration	A05 – Misconfiguration	Medium	Unauthorized Access
Sensitive Data Exposure	A02	Low	Information Disclosure

## 4. Detailed Vulnerability Analysis

### SQL Injection

The login functionality was found vulnerable to SQL Injection, allowing attackers to bypass authentication controls by manipulating backend SQL queries.

**Remediation:** Use parameterized queries and enforce strict input validation.

### Cross-Site Scripting (XSS)

The application does not properly sanitize user input, allowing execution of malicious JavaScript code in users' browsers.

**Remediation:** Implement output encoding and Content Security Policy (CSP).

## 5. OWASP Top 10 Mapping

OWASP Category	Status
A01 – Broken Access Control	Vulnerable
A02 – Auth Failures	Vulnerable
A03 – Injection	Vulnerable
A05 – Security Misconfiguration	Vulnerable
A07 – XSS	Vulnerable

## 6. Conclusion & Recommendations

The assessment indicates that the application is vulnerable to multiple critical security issues. Immediate remediation is recommended, followed by periodic security assessments and secure development practices









