# Executive Summary

Target Application: OWASP Juice Shop (https://demo.owasp-juice.shop) Assessment Date: June 24, 2025

Assessed By: Mushab

Tools Used: Burp Suite, OWASP ZAP, SQLMap

Total Vulnerabilities Identified: 3 Risk Levels: 1 High, 2 Medium Overall Risk Rating: High

Testing Approach: Manual and Automated (Burp Suite, ZAP, SQLMap)

# Vulnerabilities Identified

* 1. Reflected Cross-Site Scripting (XSS)

s

* + - Location: Contact Page (/#/contact)
    - Payload Used: <script>alert('XSS')</script>
    - Tool Used: Burp Suite (Repeater)
    - Impact: Executes JavaScript in user's browser, allowing for session hijacking or redirection.
    - Severity: High
    - Recommendation: Sanitize user input and implement output encoding to prevent script execution.
  1. SQL Injection (Search Endpoint)
     + Location: /rest/products/search?q=apple
     + Tool Used: SQLMap
     + Payload: ' OR '1'='1
     + Impact: Allows attacker to extract database content.
     + Severity: Medium
     + Recommendation: Use parameterized queries and input validation to prevent SQL injection.
  2. Weak Authentication Handling
     + Observation: Unlimited login attempts without lockout or CAPTCHA.
     + Tool Used: Burp Suite (Repeater)
     + Impact: Vulnerable to brute-force attacks.
     + Severity: Medium
     + Recommendation: Implement rate limiting, CAPTCHA, and account lockout mechanisms.