Web Application Penetration Test Report

Project: Future Interns Task 1
By: Brittany Brinson
Date: July 29, 2025

Summary

A penetration test was performed on the OWASP Juice Shop web application to identify security flaws. Using Burp Suite, OWASP ZAP, and manual testing, five vulnerabilities were confirmed, including high-risk issues such as SQL Injection, Cross-Site Scripting (XSS), and Authentication Bypass.

Vulnerability Overview

Vulnerability	Risk	Method Used	Impact	Mitigation
SQL Injection	High	Burp Suite + manual payload ' OR 1=1--	Database manipulation, auth bypass	Parameterized queries, input validation
Cross-Site Scripting (XSS)	High	<script>alert('XSS')</script>	Script execution in browser	Input sanitization, CSP
Authentication Bypass	High	High Burp Suite brute force attack	Admin account compromise	Strong passwords, account lockout
Missing CSP Header	Med	OWASP ZAP scan	Increased XSS risk	Add CSP header

Tools Used

-Kali Linux
-OWASP ZAP
-Burp Suite
-SQLMap
-Browser DevTools

Conclusion

The test revealed exploitable vulnerabilities that could lead to data breaches, account takeover, and code execution. Remediation should focus first on SQL Injection, XSS, and Authentication Bypass.