Cyber Security Penetration Testing Report

Target Application: OWASP Juice Shop

Internship Program: Future Intern

Date: December 19, 2025

Report Prepared By: Insha Ur Rehman

---

1. Executive Summary

A security assessment was performed on the OWASP Juice Shop web application. The testing focused on identifying vulnerabilities listed in the OWASP Top 10. During the audit, multiple critical issues were discovered, including SQL Injection, IDOR, and Cross-Site Scripting (XSS). These vulnerabilities allow unauthorized access to sensitive data and administrative control.

Tools Used:

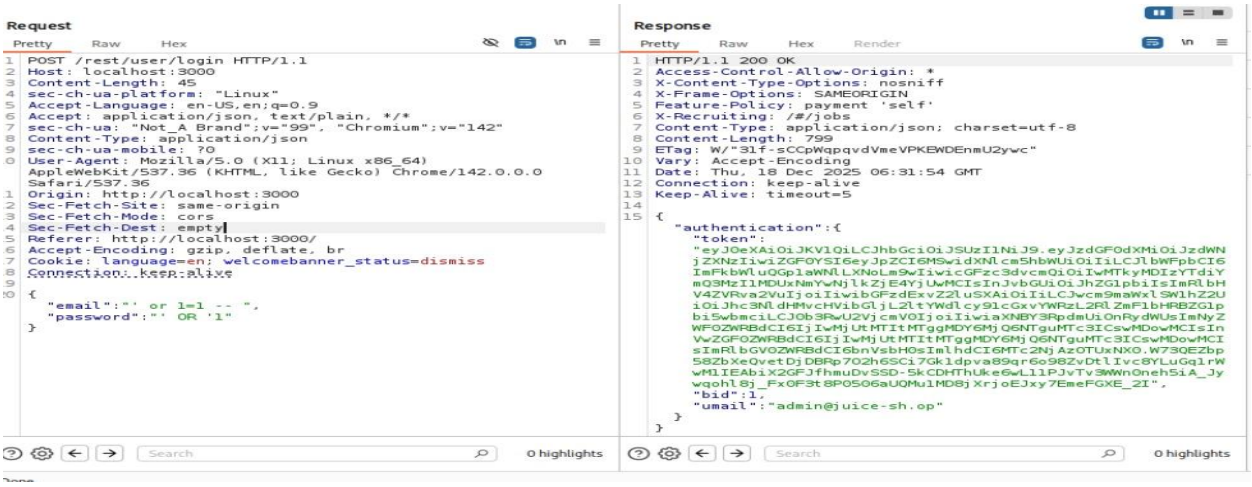
- Kali linux (Operating System)
- Burpsuit (Web Security testing)
- Nikto (Vulnaribility Scanner)
- Curl (Code Analyzer)
- Gobuster (Directory Busting)

2. Vulnerability Assessment Findings

2.1 SQL Injection (Admin Login Bypass)

- **Vulnerability:** SQL Injection (SQLi)
- **Severity: Critical**
- **Description:** The login page fails to sanitize user input, allowing an attacker to bypass authentication.
- **Steps to Reproduce:** Injected the payload ' OR 1=1 -- into the email field.

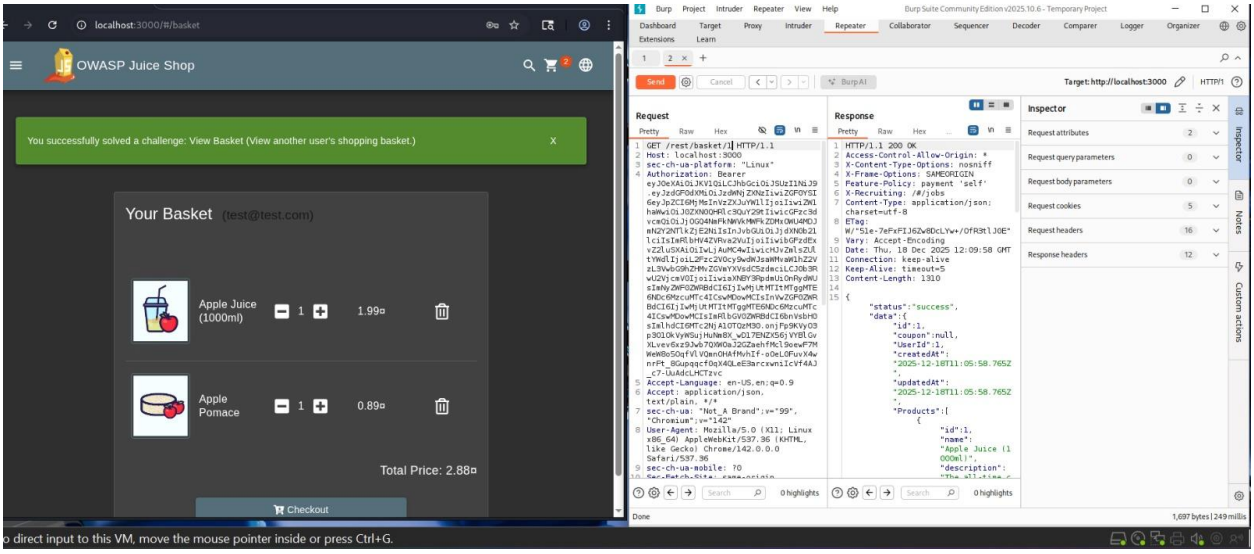
- **Impact:** Full access to the Admin account without a password.



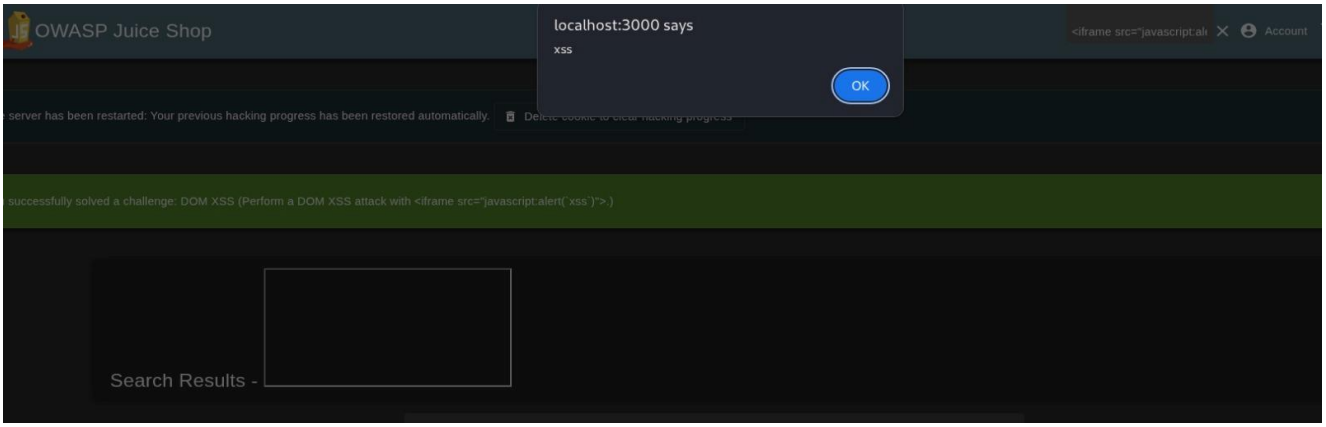
-

2.2 Insecure Direct Object Reference (IDOR)

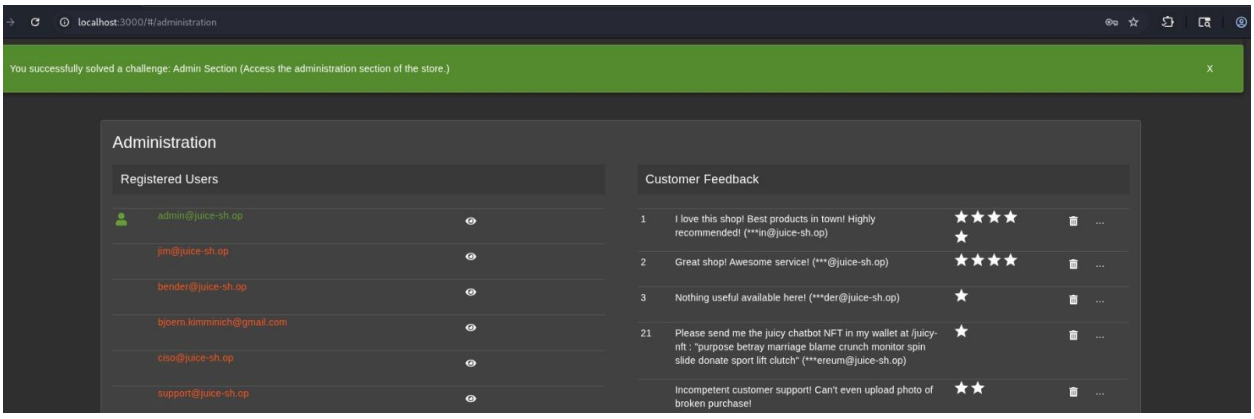
- **Vulnerability:** IDOR
- **Severity: High**
- **Description:** By changing the basket ID in the URL/Request, a user can view other customers' private shopping carts.
- **Steps to Reproduce:** Intercepted the /rest/basket/ request and changed the ID number.
- **Impact:** Violation of user privacy and exposure of purchase history.



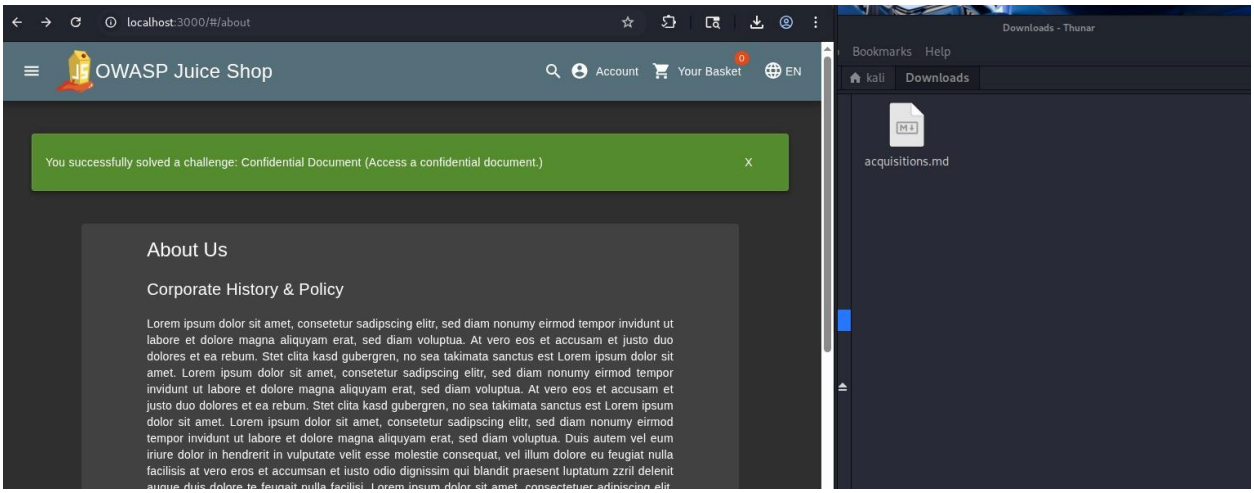
2.3 DOM-based Cross-Site Scripting (XSS)

- **Vulnerability:** XSS
- **Severity: High**
- **Description:** The application executes unsanitized JavaScript code entered into the search bar.
- **Steps to Reproduce:** Entered <iframe src="javascript:alert('xss')"> into the search field.
- **Impact:** Attacker can steal user session cookies.
- 

2.4 Broken Access Control (Admin Panel)

- **Vulnerability:** Unauthorized Admin Access
- **Severity: High**
- **Description:** The administration panel is accessible via a hidden URL path.
- **Steps to Reproduce:** Manually navigated to /#/administration.
- **Impact:** Attacker can view all user emails and delete customer feedback.
- 

2.5 Sensitive Data Exposure (Confidential Files)

- **Vulnerability:** Improper File Access
- **Severity: Medium**
- **Description:** Confidential company documents are exposed in the public directory.
- **Steps to Reproduce:** Accessed acquisitions.md through the directory structure.
- **Impact:** Leakage of internal company information.
- 

---

3. Remediation Summary

1. **Input Filtering:** Use parameterized queries to prevent SQL Injection.
2. **Authorization:** Implement server-side checks to ensure users can only access their own data (IDOR fix).
3. **Encoding:** Use output encoding to prevent XSS.
4. **Access Control:** Restrict the /administration path to specific IP addresses or roles only.