Penetration Testing Report

Target: OWASP Juice Shop

Client: Future Interns – Cybersecurity Internship 2025

Intern: Christian Dolce

Date: July 02, 2025

Project Folder: /Task_1_Identity_Access

1. Executive Summary

The OWASP Juice Shop application was subjected to a vulnerability assessment using manual and automated testing techniques. The goal was to uncover application security weaknesses and assess the impact of various exploits such as Cross-Site Scripting (XSS) and SQL Injection (SQLi). Multiple vulnerabilities were found, including Reflected XSS, Stored XSS, and SQL Injection login bypass. These issues demonstrate a lack of input validation and poor output encoding, leading to potential threats to user confidentiality and application integrity.

2. Scope and Objectives

The scope of this engagement was limited to the OWASP Juice Shop web application hosted locally on port 3000. The objective was to identify and validate vulnerabilities related to identity and access management through web application testing tools such as Burp Suite and manual testing techniques.

3. Methodology

The testing methodology followed the OWASP Testing Guide and included:
- Reconnaissance and enumeration
- Manual input manipulation
- Proxy-based interception and tampering
- Review of HTTP requests and responses
- Cross-referencing with OWASP Top 10 vulnerabilities

4. Vulnerability Findings

4.1 Reflected Cross-Site Scripting (XSS)

Severity: Medium

Category: A03 – Injection

Affected URL: /#/search?q=<img src=x onerror=alert(1)>

Description:
User-supplied input is reflected directly in the response without proper encoding. This allows an attacker to craft malicious links that execute scripts when clicked by a user.

Recommendation:
Implement context-aware output encoding and sanitize user input.

4.2 SQL Injection – Login Bypass

Severity: High

Category: A03 – Injection

Affected Endpoint: POST /rest/user/login

Description:
SQL Injection was discovered in the login functionality. Using `' OR 1=1--` in the email field bypassed authentication controls and allowed login without valid credentials.

Recommendation:
Use parameterized queries and apply strict input validation.

4.3 Stored Cross-Site Scripting (XSS)

Severity: High

Category: A03 – Injection

Affected Endpoint: POST /api/Feedbacks

Render Location: /#/about

Description:
Feedback input submitted by a user is stored and rendered on the About Us page without sanitization. A payload such as `<img src=x onerror=alert('Stored XSS')>` triggers script execution for viewers.

Recommendation:
Sanitize stored input and implement output encoding using tools like DOMPurify.

5. Conclusion

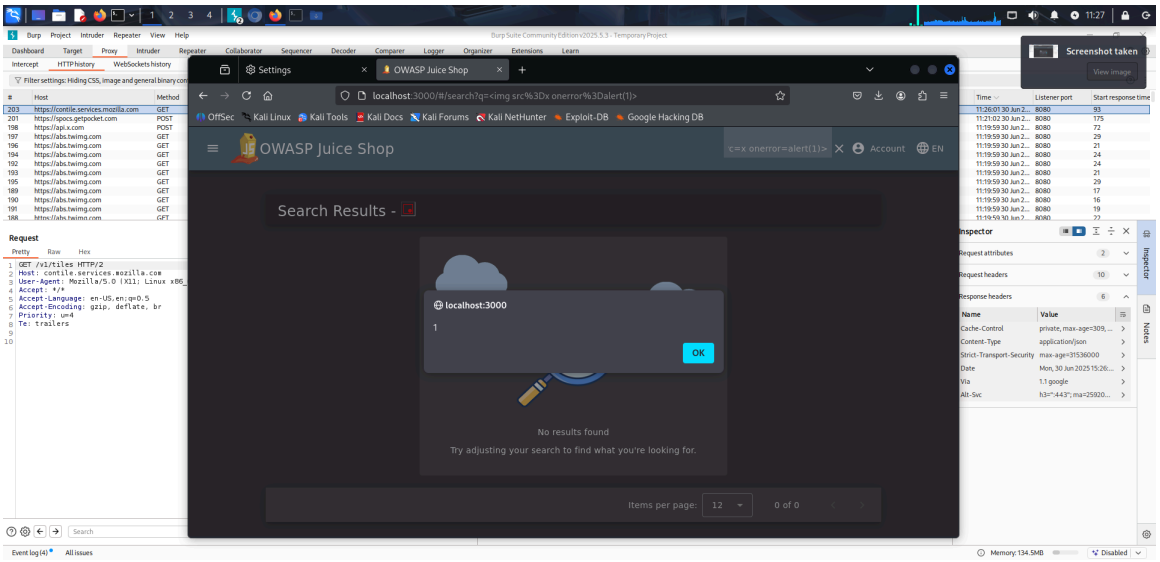
This assessment identified critical and high-severity vulnerabilities in the OWASP Juice Shop application. By exploiting weak input validation and poor output handling, attackers could bypass authentication and execute malicious scripts. Adopting secure coding practices and applying the recommended mitigations will significantly improve the application's security posture.

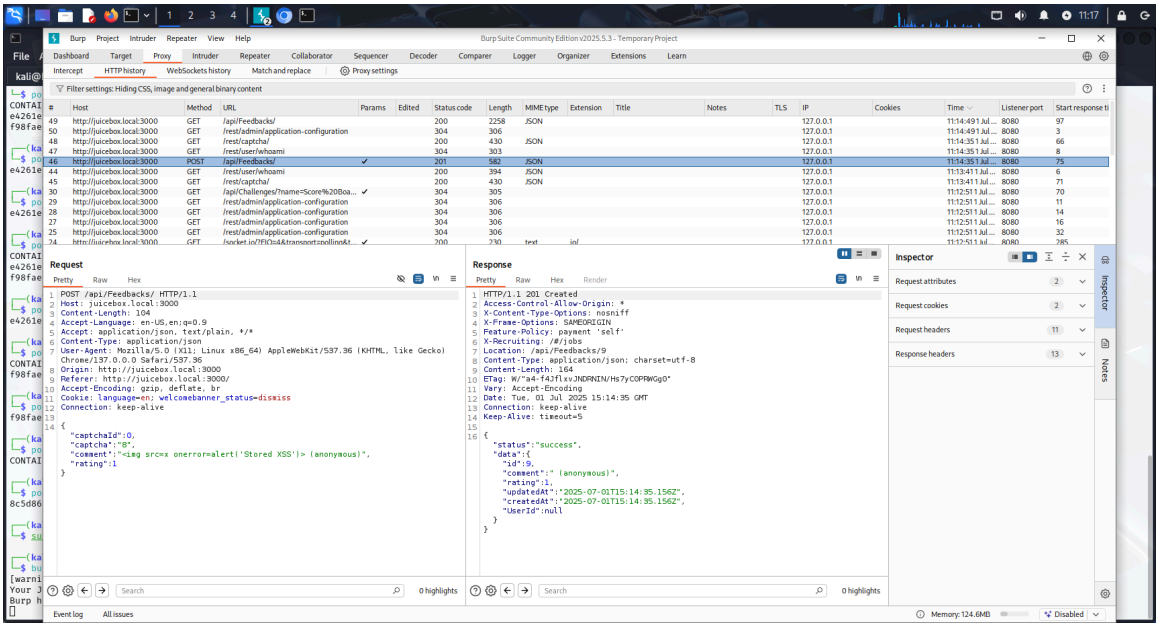
6. Appendix

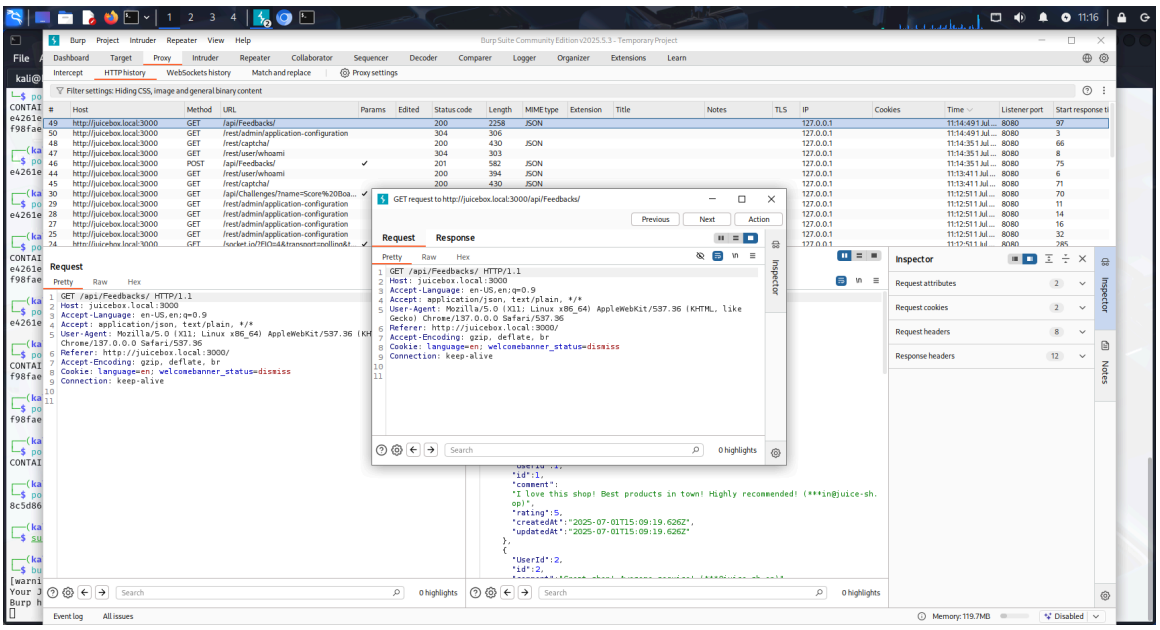
Tools Used:
- Burp Suite Community Edition
- Firefox (with proxy setup)

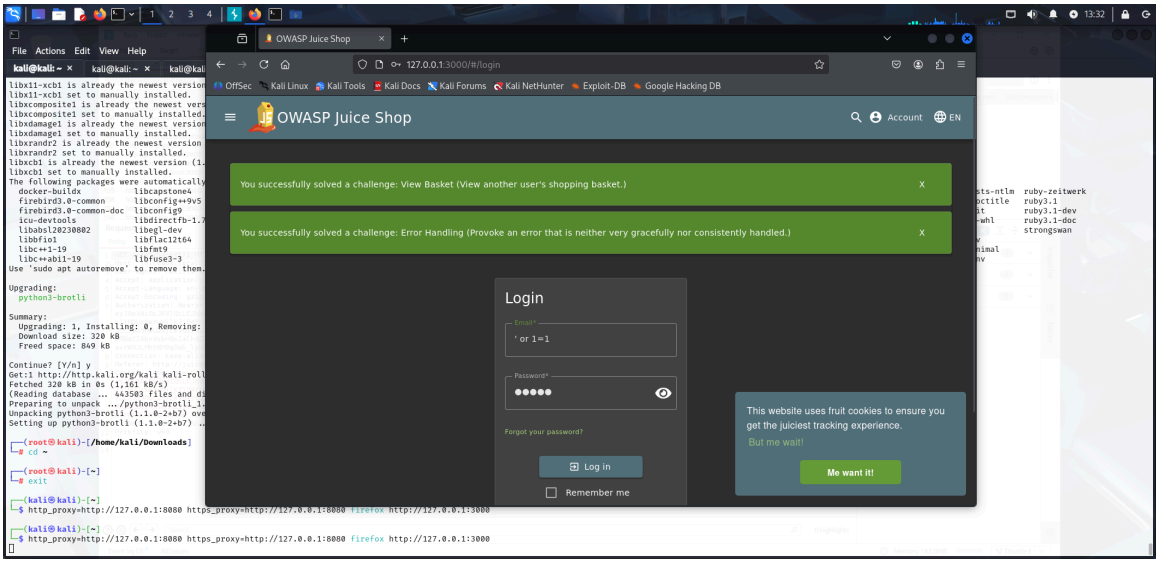
- Podman/Docker
- Linux (Kali)

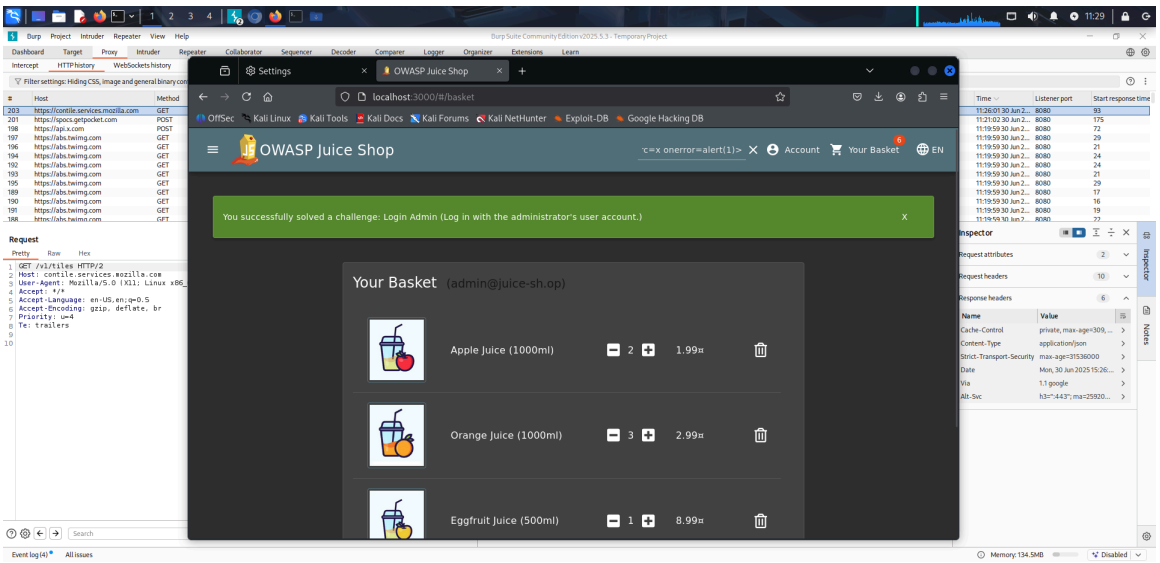
Artifacts:
- Screenshots: xss_search_alert.png, sqli_login_success.png, stored_xss_about_us.png

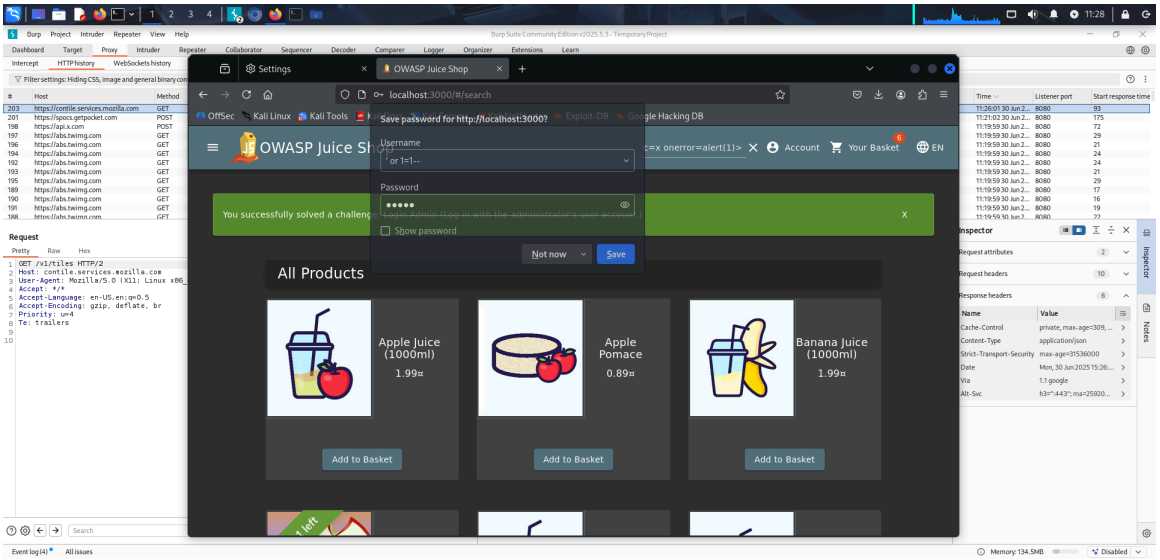







OWASP Juice Shop
You successfully solved a challenge: View Basket (View another user's shopping basket.)
You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)
Login
' or 1=1
Log in
Remember me
This website uses fruit cookies to ensure you get the juiciest tracking experience.
Me want it!


OWASP Juice Shop
You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)
Your Basket (admin@juice-sh.op)
Apple Juice (1000ml)
Orange Juice (1000ml)
Eggfruit Juice (500ml)


Settings
OWASP Juice Shop
localhost:3000/#/search
Save password for http://localhost:3000?
Username
' or 1=1--
Password
Show password
Not now
Save
OWASP Juice Shop
Account
Your Basket
EN
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Banana Juice (1000ml)
1.99¤
Add to Basket
Add to Basket
Add to Basket