Penetration Testing Report – Task 1

Intern Name: Samia Noor

Intern ID:1wTo1MNEC9keeyVGFsmK

Internship Program: Intern Intelligence

Internship Task: Task 1 – Penetration Testing Report

Platform: TryHackMe (Web-based Kali Linux)

Date: July 18, 2025

Objective

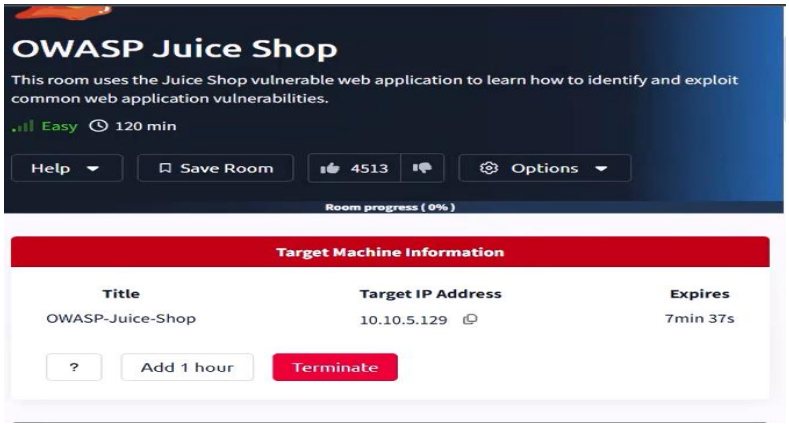
To identify and exploit vulnerabilities in a deliberately insecure web application (OWASP Juice Shop) using Cross-Site Scripting (XSS) and SQL Injection techniques.

Tools Used

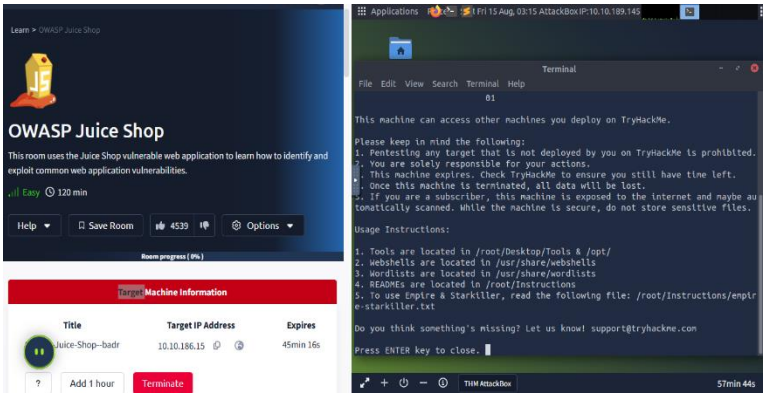
- TryHackMe OWASP Juice Shop Room
- Web-based Kali Linux (Firefox Browser)

Step-by-Step Process

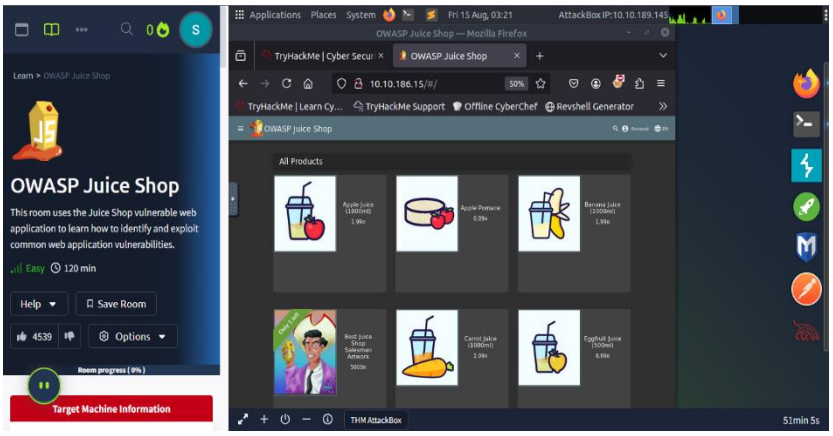
Step 1: Access the Vulnerable Application Opened TryHackMe and joined the 'OWASP Juice Shop' room. Copied the target IP address provided in the room.



Step 2: Start Kali Linux Environment Launched the web-based Kali Linux machine on TryHackMe. Opened Firefox browser inside Kali Linux.

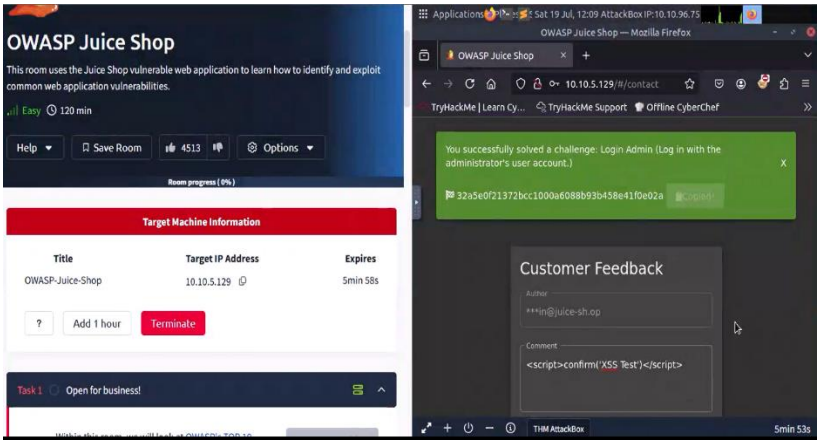


Step 3: Open Target in Browser Pasted the target IP into Firefox. Verified that OWASP Juice Shop loaded successfully.

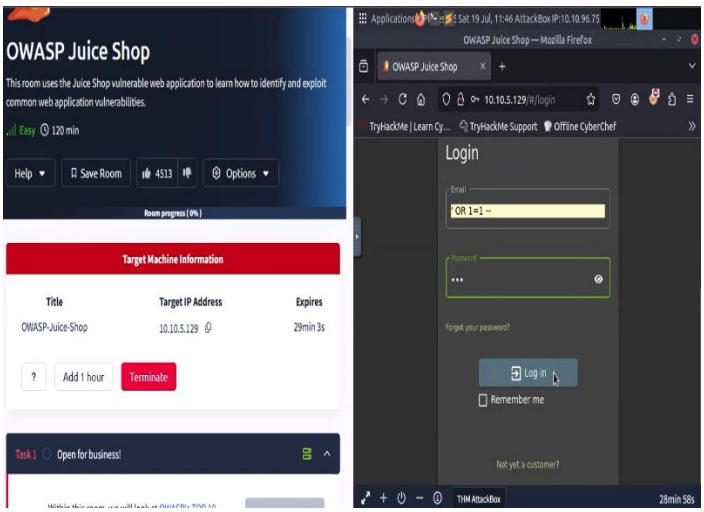


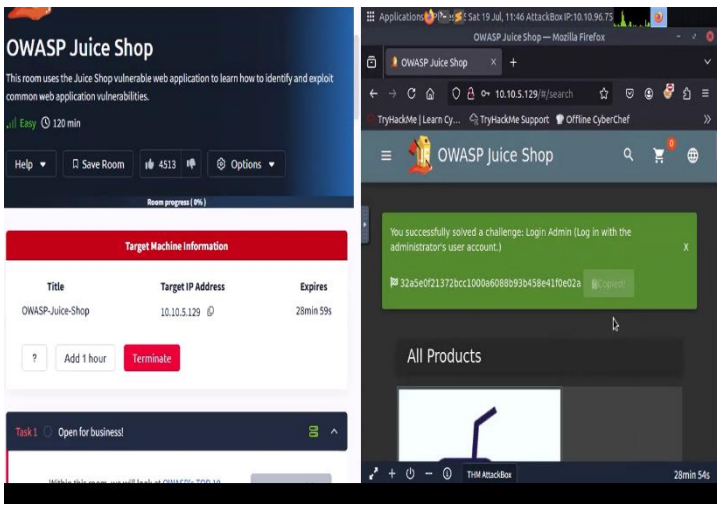
Step 4: Perform XSS Attack Located the search bar and feedback form. Injected:

Observed alert popup confirming vulnerability.



Step 5: Perform SQL Injection Located the login form. Entered: ' OR '1'='1 Successfully bypassed authentication and logged in.





Findings

- Vulnerabilities found: Reflected XSS, SQL Injection
- Impact: XSS allows malicious scripts to run in browser; SQL Injection bypasses authentication.

Recommendations

- Implement input sanitization and output encoding.
- Use parameterized SQL queries.
- Enable Web Application Firewall (WAF).