Cyber Security Task 1 – Web Application Security Testing

Overview

This task focuses on performing basic web application security testing against a deliberately vulnerable application to understand common security flaws, their impact, and mitigation techniques. The objective is to simulate a real-world penetration testing scenario using industry-standard tools and align the findings with the OWASP Top 10 framework.

Test Application

OWASP Juice Shop
OWASP Juice Shop is an intentionally insecure web application designed for security training and awareness. It contains numerous vulnerabilities commonly found in real-world applications, making it ideal for hands-on learning and testing.

Tools Used

- **OWASP ZAP (Zed Attack Proxy):** Used for automated and manual vulnerability scanning, intercepting requests, and analyzing responses.
- **Burp Suite:** Used to intercept HTTP traffic, manipulate requests, test input validation, and confirm exploitation of vulnerabilities.

Both tools were used in combination to ensure accurate identification and validation of security issues.

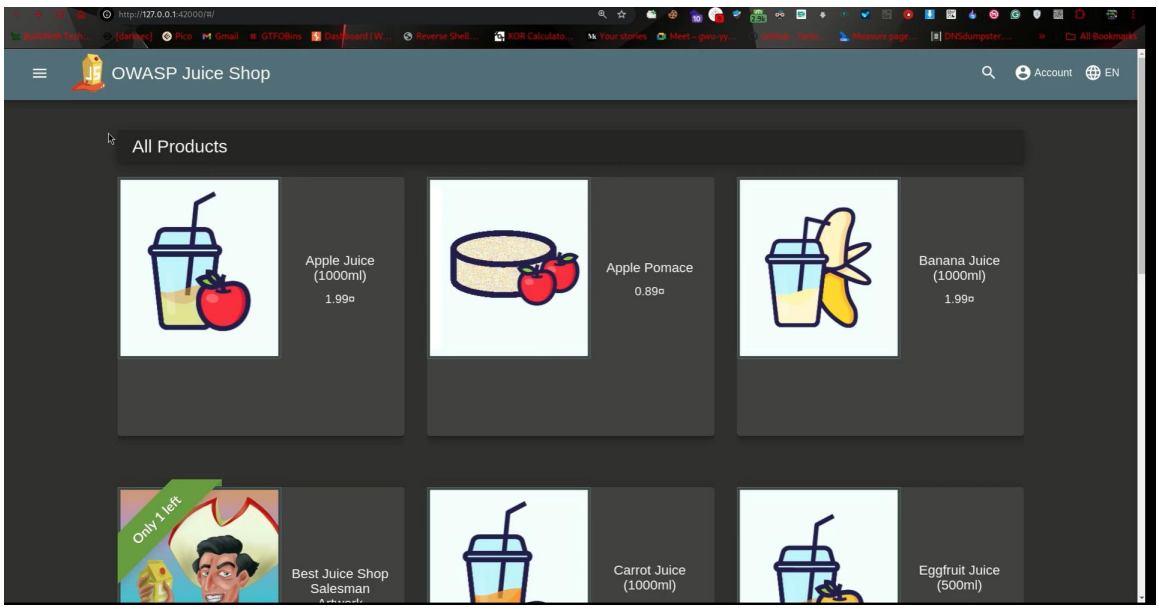
Identified Vulnerabilities

1. SQL Injection

Description: The login page accepts malicious SQL input, allowing attackers to manipulate backend database queries.

Affected Component: Login Authentication Mechanism

Screenshot Title: OWASP Juice Shop SQL Injection Login page



Impact: High

OWASP Category: A03 – Injection

Details:
By injecting crafted SQL statements into the login input fields, authentication controls can be bypassed. This may allow unauthorized access to user accounts or administrative functions.

Potential Risks:

- Unauthorized access to sensitive data
- Account takeover
- Data modification or deletion
- Full database compromise in severe cases

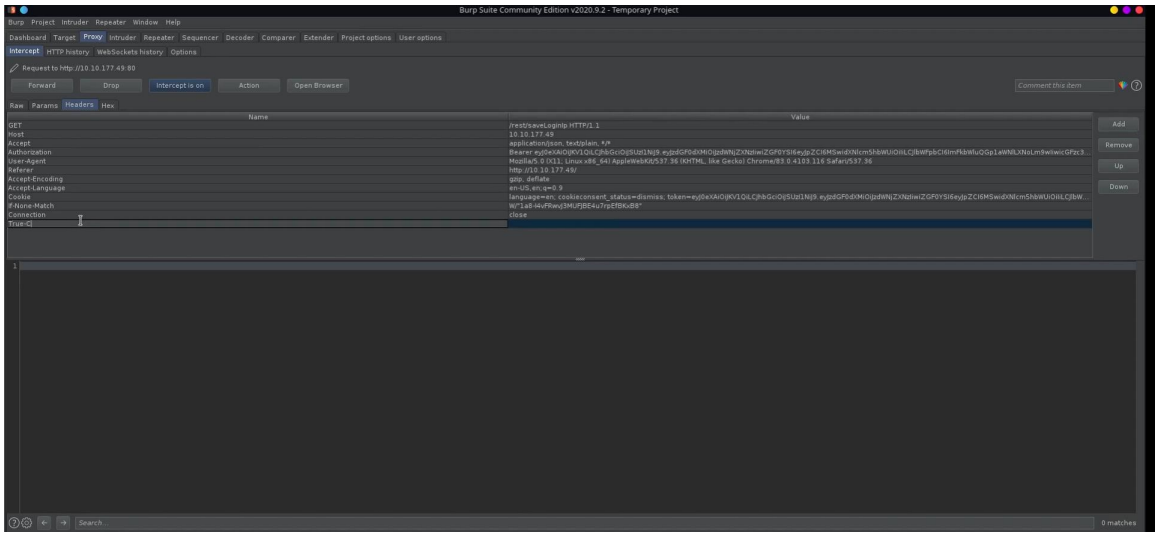
---

2. Cross-Site Scripting (XSS)

Description: Malicious scripts were successfully injected into the search field and reflected back to the user.

Affected Component: Search Functionality

Screenshot Title: OWASP Juice Shop Reflected XSS search



Impact: Medium

OWASP Category: A07 – Cross-Site Scripting (XSS)

Details:
The application fails to properly sanitize user input before rendering it in the browser. This allows attackers to execute arbitrary JavaScript in a victim's browser.

Potential Risks:

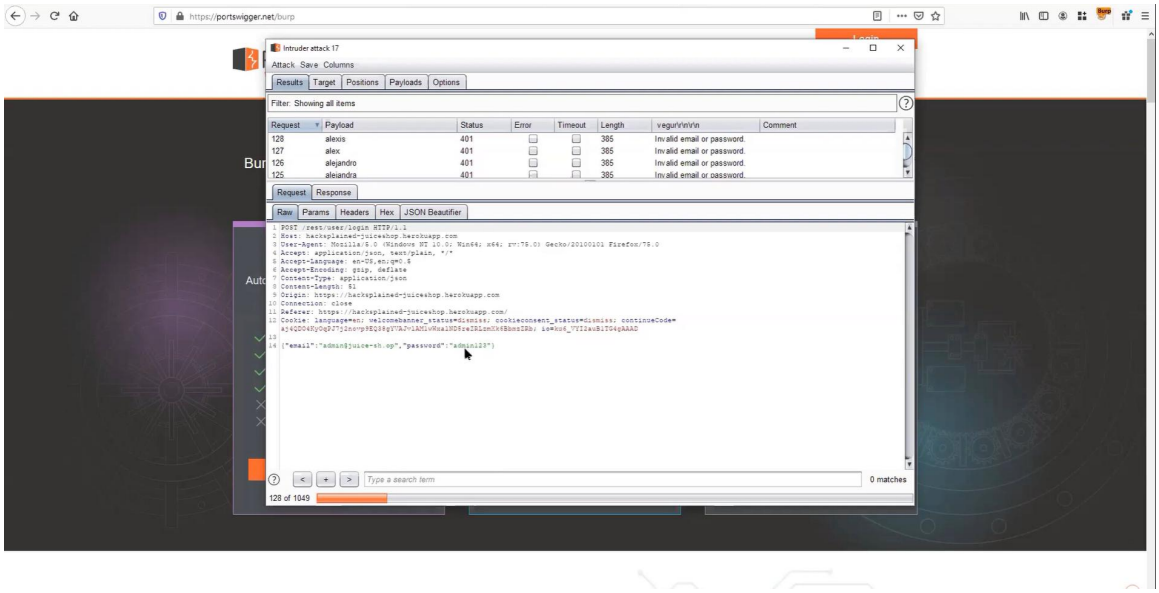
- Session hijacking
- Theft of cookies or authentication tokens
- Defacement of web pages
- Phishing attacks targeting end users

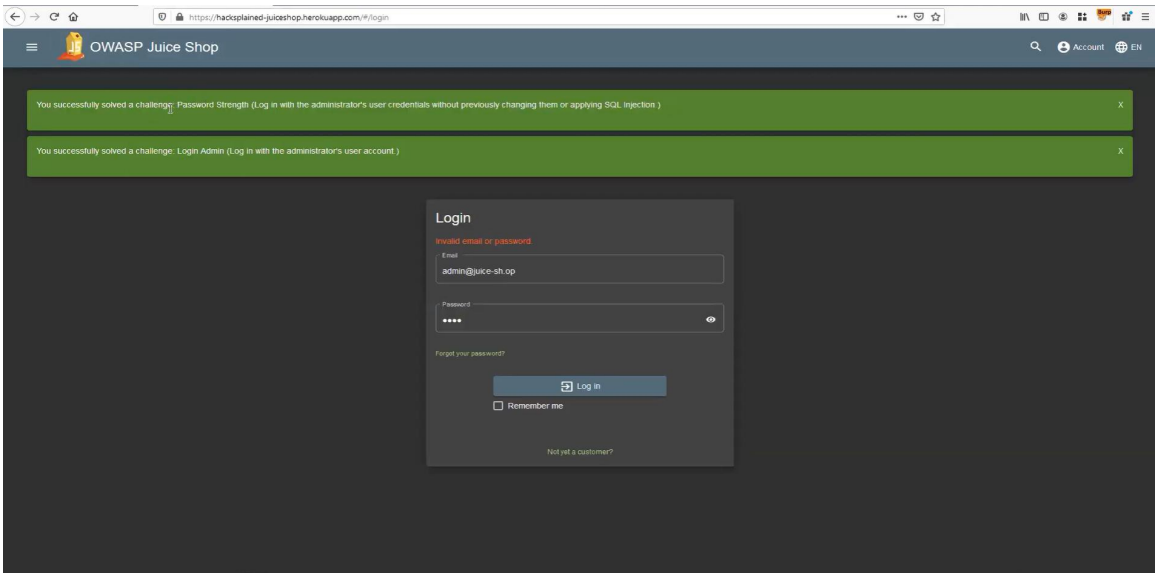
3. Broken Authentication

Description: The application allows the use of weak passwords during login.

Affected Component: Authentication and Password Policy

Screenshot Title: OWASP Juice Shop Weak Password Login





Impact: High

OWASP Category: A02 – Broken Authentication

Details:
Weak password enforcement increases the likelihood of successful brute-force or credential-stuffing attacks. Attackers can gain access using commonly used or easily guessable passwords.

Potential Risks:

- Unauthorized account access
- Privilege escalation
- Compromise of user data
- Increased attack surface for further exploitation

Mitigation Steps (Short)

- Use prepared statements and parameterized queries to prevent SQL Injection.
- Validate, sanitize, and encode all user input to protect against XSS attacks.
- Enforce strong password policies, implement account lockout mechanisms, and enable Multi-Factor Authentication (MFA).

OWASP Top 10 Mapping

- **A02 – Broken Authentication**
- **A03 – Injection**
- **A07 – Cross-Site Scripting (XSS)**

This mapping ensures that the identified vulnerabilities align with globally recognized security standards.

Conclusion

This assessment successfully identified multiple common web application vulnerabilities using OWASP ZAP and Burp Suite. The findings demonstrate how improper input handling, weak authentication controls, and insufficient validation can expose applications to serious security risks. This report simulates a real-world client security assessment and highlights the importance of secure coding practices, regular security testing, and adherence to OWASP Top 10 guidelines.