Cyber Security Internship Report

Task 1: Web Application Security Testing

Author: Waggari Misganu Ebsa
Internship Submitted to: Future Intern
Target Application: OWASP Juice Shop
Submission: September 2025

Contents

Executive Summary

This report presents the findings from a web application vulnerability assessment conducted on OWASP Juice Shop. The primary objective was to identify common security flaws, analyze their potential impact, and recommend remediation strategies. The vulnerabilities discovered during testing include SQL Injection, Authentication Flaws, and potential Cross-Site Scripting (XSS). These map directly to the OWASP Top 10 categories and represent real-world risks such as unauthorized access, data leakage, and malicious script execution.

Implementing the suggested mitigations—such as parameterized queries, enforcing strong authentication controls, and applying Content Security Policies—will significantly strengthen the security posture of the application.

1. Introduction

Purpose

The purpose of this internship project was to perform an ethical hacking assessment on a test web application (OWASP Juice Shop), simulating real-world penetration testing engagements. The exercise aimed to provide hands-on experience in identifying vulnerabilities aligned with the OWASP Top 10 and documenting them in a professional security report.

Scope

- Target: OWASP Juice Shop (demo instance)
- Tools: Web browser (manual testing), OWASP resources
- Standards: OWASP Top 10 2021

2. Environment Setup & Exploration

Environment:

- Application deployed at: https://demo.owasp-juice.shop
- Accessed using a standard web browser
- Manual testing approach focusing on core web functions

Exploration Activities:

- Login and authentication workflows
- Input fields (login form, search, comment forms)
- Error messages and responses to crafted payloads

3. Vulnerability Findings

3.1 SQL Injection

- **Description:** Injection attempt using `' OR 1=1–` in the login form.
- **Outcome:** Successful login without valid credentials (authentication bypass).
- **Impact:** Unauthorized access to user accounts.
- **Mitigation:** Use parameterized queries, validate and sanitize inputs.

3.2 Cross-Site Scripting (XSS)

- **Description:** Injected `<script>alert("XSS")</script>` into form input.
- **Outcome:** Input was accepted but alert did not execute; indicates potential stored/reflected XSS filtered at frontend.
- **Impact:** Possible risk of script execution if bypassed.
- **Mitigation:** Sanitize inputs, encode outputs, enforce Content Security Policy (CSP).

3.3 Authentication Flaw (Weak Credentials)

- **Description:** Login attempt with breached credentials (admin@juice-sh.op / admin123).
- **Outcome:** Login succeeded with weak credentials.
- **Impact:** Exploitable authentication weakness; risk of account takeover.
- **Mitigation:** Enforce strong password policies, implement account lockout, enable MFA.

4. Mapping to OWASP Top 10

Vulnerability	OWASP Top 10 Category	Description	Status
SQL Injection	A03:2021 – Injection	Login bypass via crafted SQL payload	Confirmed
Cross-Site Scripting	A07:2021 – Identification & Authn. Failures*	Input accepted, potential for XSS	Potential / Observed
Authentication Flaw	A07:2021 – Identification & Authentication Failures	Weak credentials accepted	Confirmed

5. Impact Analysis & Risk Rating

Vulnerability	Impact Level	Likelihood	Overall Risk	Description
SQL Injection	Critical	High	High	Full authentication bypass possible
Cross-Site Scripting	Medium	Medium	Medium	Malicious script execution possible if filters bypassed
Authentication Flaw	High	High	High	Weak/default credentials enable unauthorized access

6. Remediation & Recommendations

Vulnerability	Recommended Fixes	Priority
SQL Injection	Implement prepared statements; strict input validation	High
Cross-Site Scripting	Sanitize inputs, encode outputs, implement CSP	Medium
Authentication Flaw	Strong password policies, MFA, account lockout after failed attempts	High

7. Conclusion

The assessment of OWASP Juice Shop revealed several vulnerabilities that align with OWASP Top 10 risks. The confirmed flaws (SQL Injection and Authentication Weaknesses) pose serious threats to confidentiality and integrity if left unresolved. Addressing these vulnerabilities promptly will significantly reduce exposure to exploitation and enhance the security of the application. The exercise provided practical experience in vulnerability assessment and remediation planning.

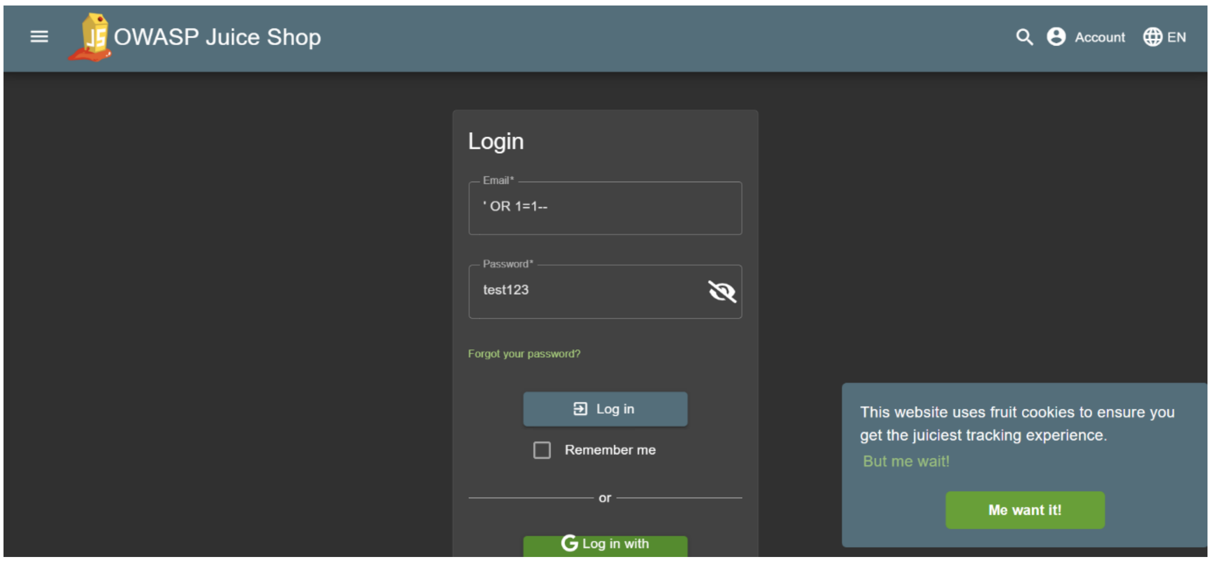
8. Appendices

A. Tools Used

- Web browser (manual testing)
- OWASP Juice Shop demo instance

B. Evidence

- Screenshots of login bypass (SQL Injection)


OWASP Juice Shop

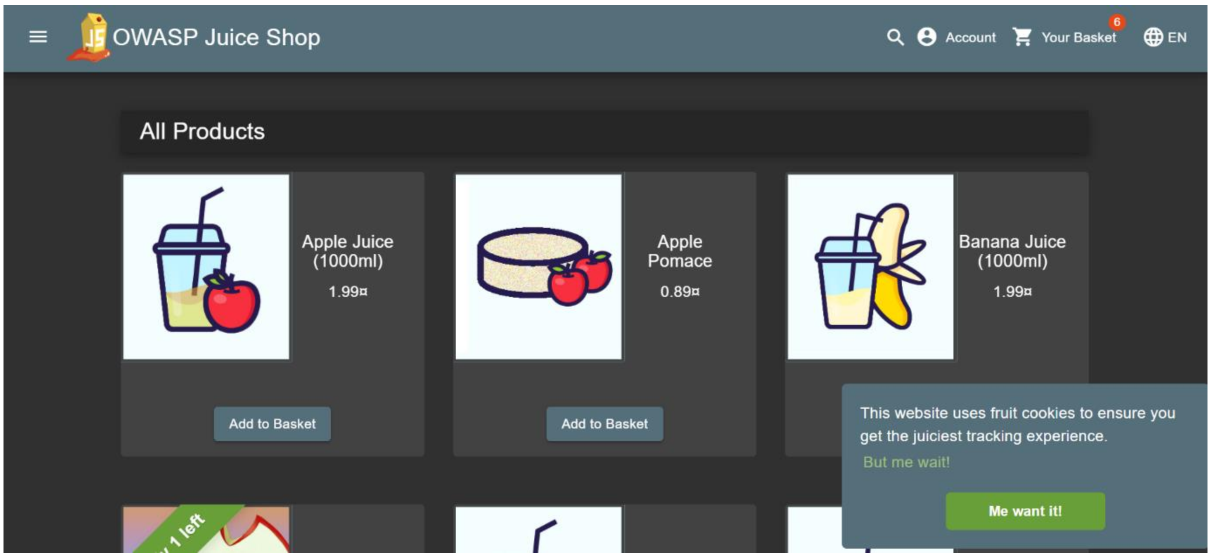
Login

Email*: ' OR 1=1--

Password*: test123

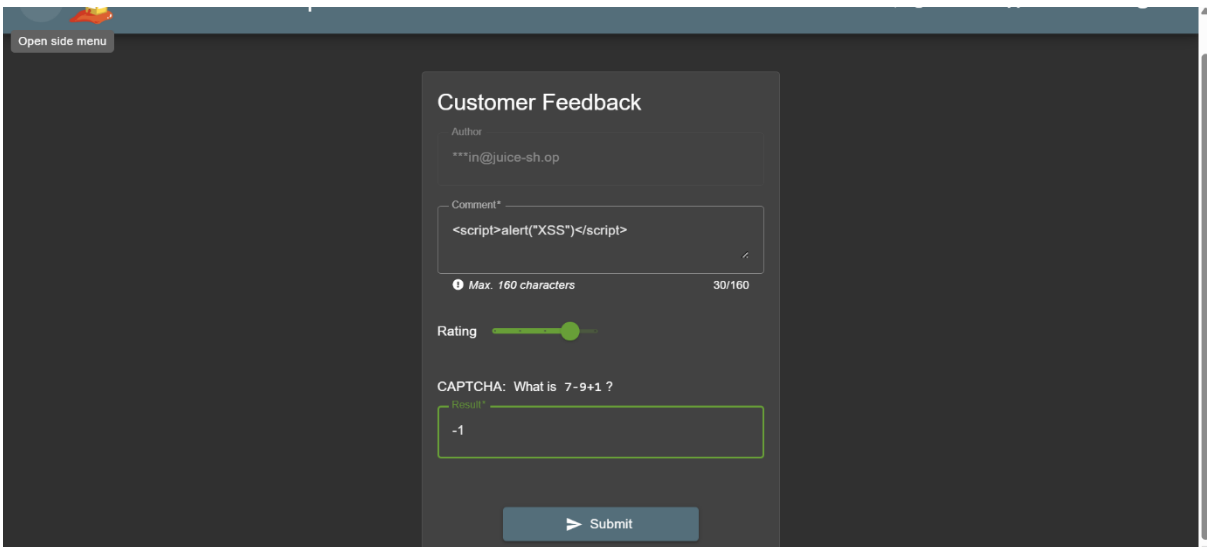
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

- Screenshot of weak credentials login



This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!

- Screenshot of XSS payload input form



Customer Feedback

Author
***in@juice-sh.op

Comment*
<script>alert("XSS")</script>

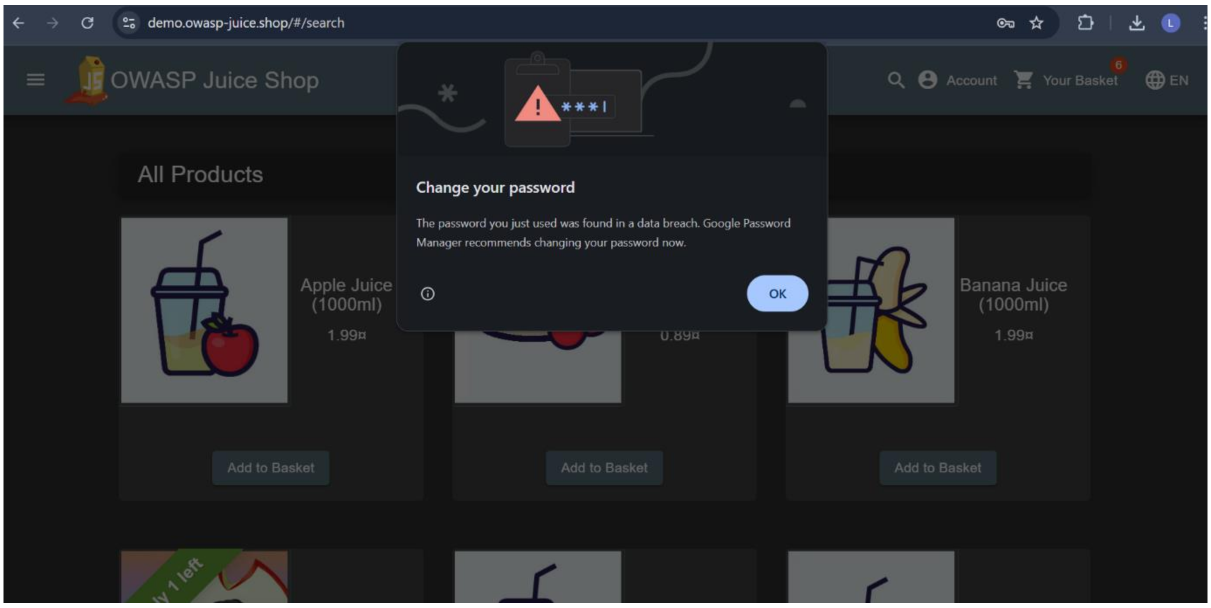
Max. 160 characters 30/160

Rating

CAPTCHA: What is 7-9+1 ?

Result*
-1

- Screenshot of Authentication flaw


demo.owasp-juice.shop/#/search

Change your password

The password you just used was found in a data breach. Google Password Manager recommends changing your password now.

9. References

1, OWASP Top 10 Web Application Security Risks (2021): https://owasp.org/Top10/

2, OWASP Juice Shop Project: https://owasp.org/www-project-juice-shop/

3, SQL Injection Prevention Cheat Sheet: https://owasp.org/www-community/attacks/SQL_Injection

4, XSS Prevention Cheat Sheet: https://owasp.org/www-community/xss-prevention