FUTURE_CS_01 - Web Application Penetration Testing Report

FUTURE_CS_01 - Web Application Penetration Testing Report

Intern Name: Sabarish V

Date: 3 June 2025

Task: Security Assessment of Web Applications

Target: OWASP Juice Shop (Demo Instance)

Tools Used: Browser Developer Tools, Manual Payloads

---

1. Objective

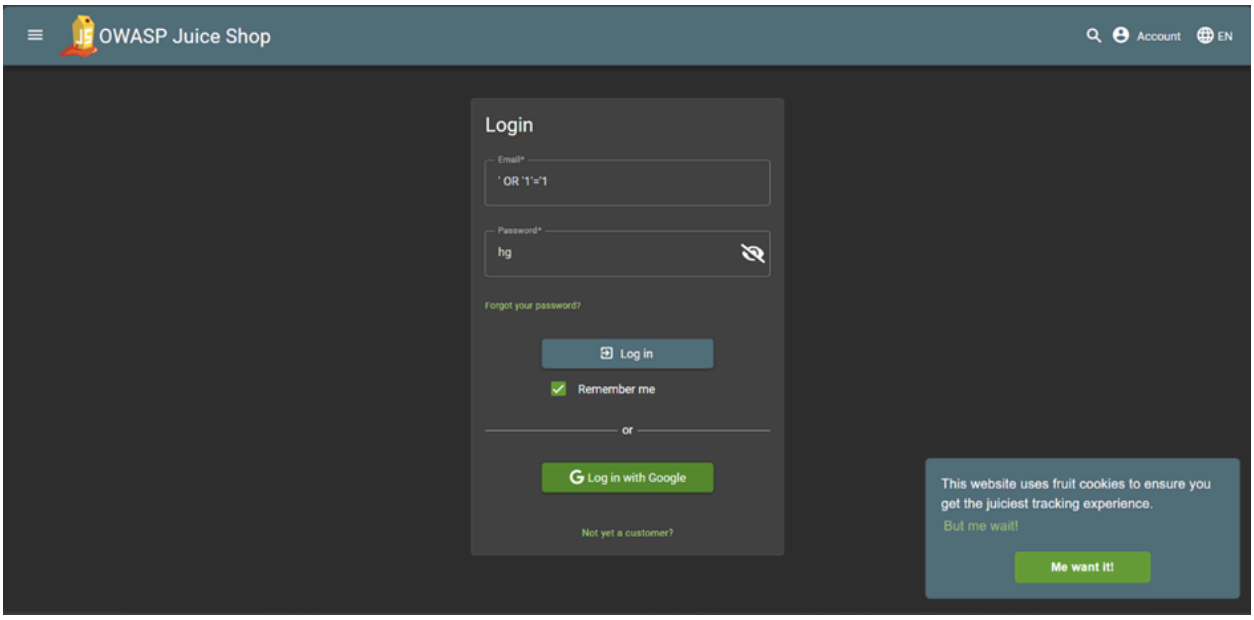
This report evaluates the security of OWASP Juice Shop, a purposely vulnerable application, through simulated attacks including SQL Injection, Cross-Site Scripting (XSS), and authentication testing.

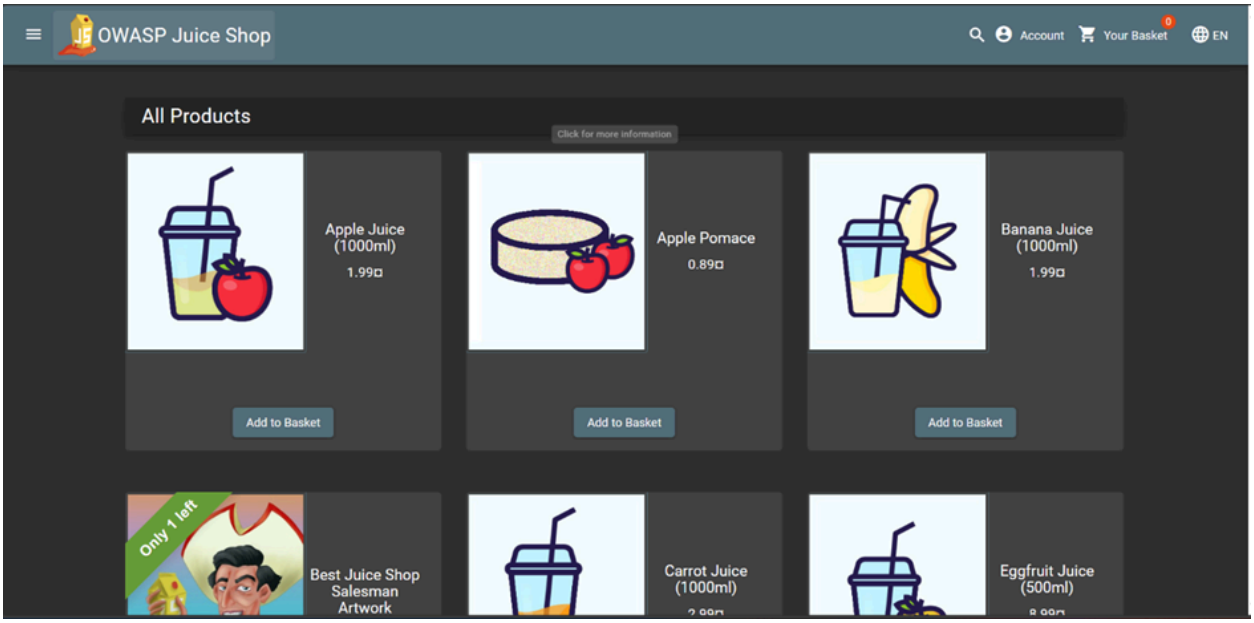
---

2. Key Vulnerability Tests

2.1 SQL Injection

- **Payload:** `' OR '1'='1`
- **Result:** Successfully bypassed login.

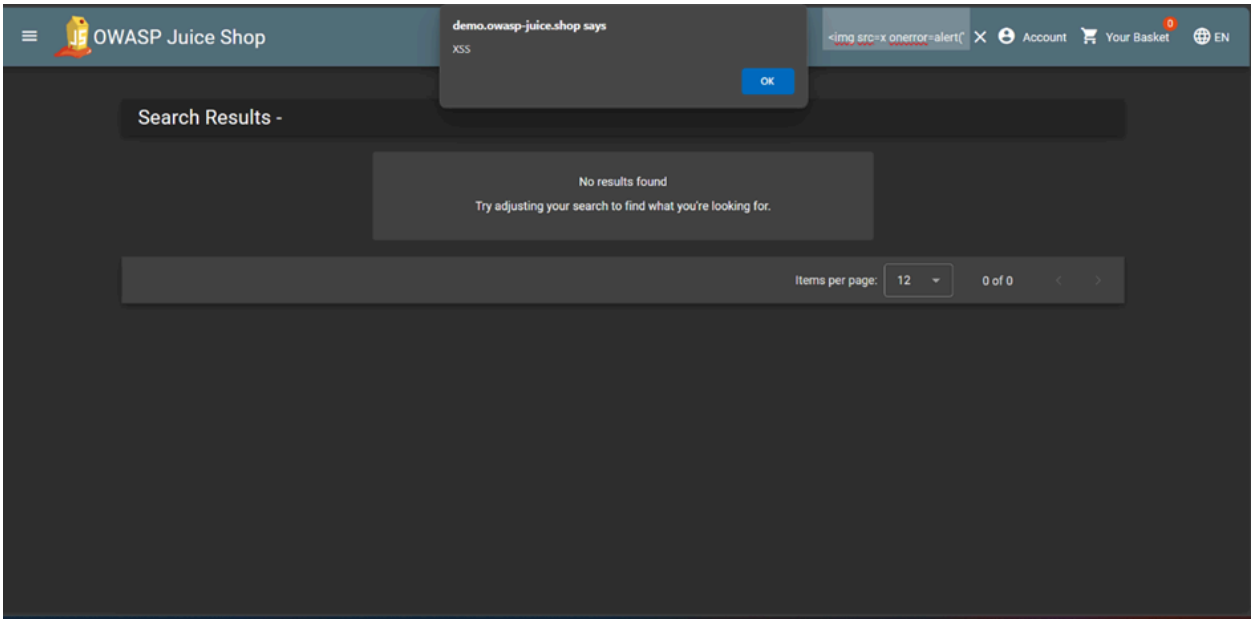




- **Fix:** Use parameterized queries or ORMs.

2.2 Cross-Site Scripting (XSS)

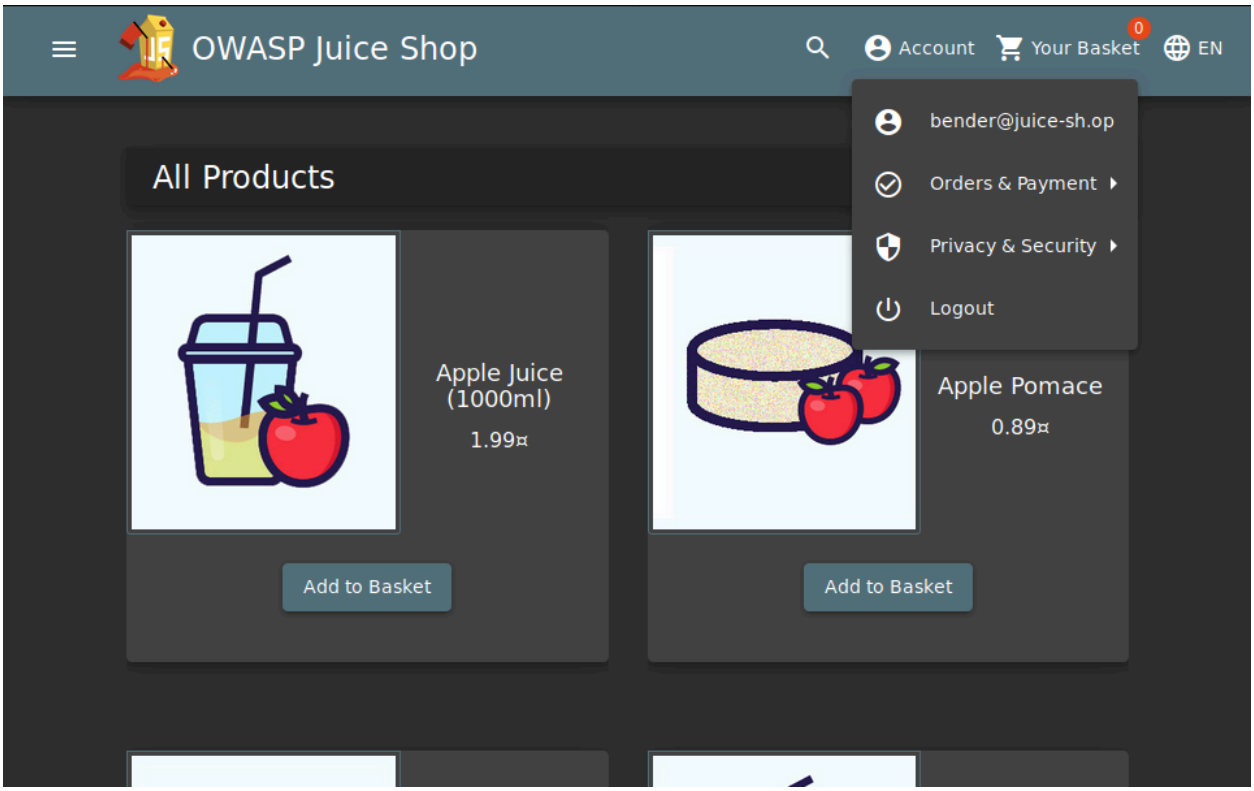
- **Payload:** `<img src=x onerror=alert('XSS')>`
- **Result:** Alert triggered successfully.



- **Fix:** Implement input/output sanitization and encoding.

2.3 Authentication Flaws

- **Methods:** Tested weak credentials and session tampering.
- **Result:** No vulnerabilities detected.



- **Fix:** Continue enforcing strong passwords and session validation.

3. Tools & Techniques

- OWASP Juice Shop (Demo)
- Browser Network & Console Tools
- Manual payload testing

4. Conclusion

Successfully exploited SQL injection and XSS vulnerabilities. Authentication mechanisms proved robust. Recommend implementing proper input validation and secure coding practices for remediation.

5. References

- OWASP Juice Shop

- SQL Injection
- XSS Attacks