**Task 1 — Web Application Security Testing (OWASP Juice Shop)**
**Author:** Armaan Singh — Intern at Future Interns (CIN: FIT/SEP25/CS4007)
**Date:** 21 September 2025

# 1. Executive Summary

This report documents a hands-on web application security assessment performed on the OWASP Juice Shop application. The goal was to identify common web vulnerabilities (authentication, input validation, CSRF) and provide remediation recommendations. Tools used: Burp Suite (Community), OWASP ZAP, browser DevTools and screen recording. Confirmed issues:

**SQL Injection (Login bypass)** using payload `admin' or 1=1--`

**Reflected XSS (Search)** — JS execution that revealed cookie content via `prompt(document.cookie)`

**CSRF** — token validation logic depends only on token presence (weak validation)

# 2. Scope & Target

- **Target:** OWASP Juice Shop (public instance)
- **Scope:**Authentication, input validation, session handling, CSRF token validation
- **Test type:** Non-destructive, educational testing on Juice Shop intentionally vulnerable app

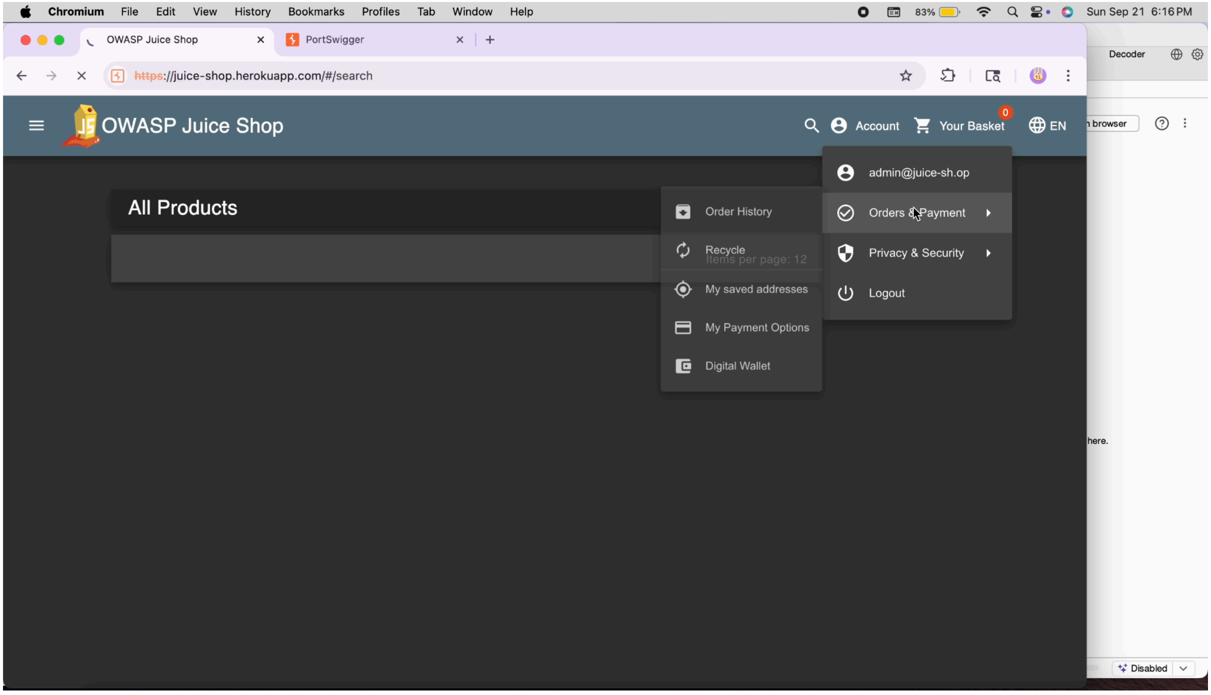
# 4. Findings (Detailed)

## Finding 1 — SQL Injection (Login Bypass)

- **Location / Endpoint:** Juice Shop Login page (`/#/login`)
- **Payload used (Email field and Password field : admin' or 1=1--**
-

**Steps to reproduce:**

1. Open Juice Shop → Click **Login**.
2. In **Email** field paste: **admin' or 1=1--**
3. In **Password** field fill same payload and click **Login**.
4. Observe successful login without valid credentials.



- **Impact (Severity: High):**

  **Authentication bypass allows an attacker to access user accounts without credentials — enabling account takeover, data disclosure, and possible privilege escalation. In production systems this can lead to full application compromise.**

**Recommendation / Mitigation:**

- **Use parameterized queries / prepared statements.**
- **Perform strict server-side input validation.**
- **Apply least-privilege to DB accounts; avoid building dynamic SQL from user input.**
- **Add WAF rules and rate-limiting to detect/reduce automated injection attempts.**
- **Log & alert on suspicious authentication behavior.**