XSS Exploitation Drill – OWASP Juice Shop  
 20/052025  
John Alexander Londono Gomez

**Scenario Description**

A reflected Cross-Site Scripting (XSS) vulnerability is exploited in the Juice Shop login form. The incident response team must detect, analyze, and contain the issue.

**Trigger**

User reports suspicious behavior and popup alerts from the login page at http://localhost:3000.

**Objectives**

Test detection capability for XSS vulnerabilities

Coordinate response via Slack and Teams

Practice incident documentation and escalation

**Step-by-Step Actions**

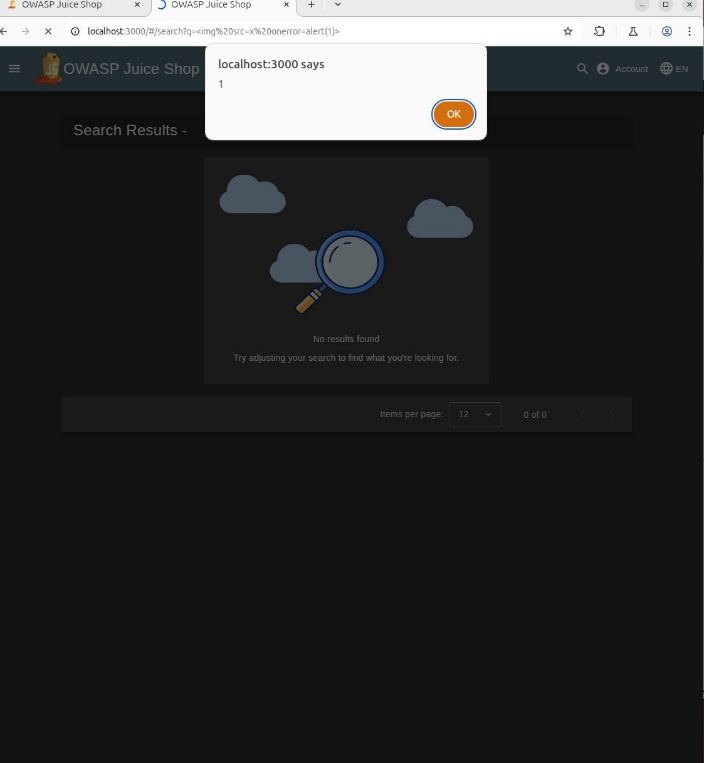
| **Step** | **Action** | **Responsible** | **Tool** |
| --- | --- | --- | --- |
| 1 | Reproduce the XSS via "><script>alert(1)</script> | Analyst | Browser, Burp Suite |
| 2 | Capture evidence (screenshot + HTTP request) | Analyst | Burp Suite |
| 3 | Notify team in [#incidents](https://juice-shop.slack.com/archives/C08TFL4REA3) Slack channel | Analyst | Slack |
| 4 | Start Evergreen Teams call via [Crisis-Updates](https://teams.live.com/meet/9391338353402?p=m0bkOgZspsQV5m4w2i&eventType=community) | Incident Lead | Teams |
| 5 | Disable login page temporarily | Developer | VM Console |
| 6 | Fix input sanitization & test fix | Developer | Juice Shop Source |
| 7 | Document lessons learned | All | Word / Confluence |

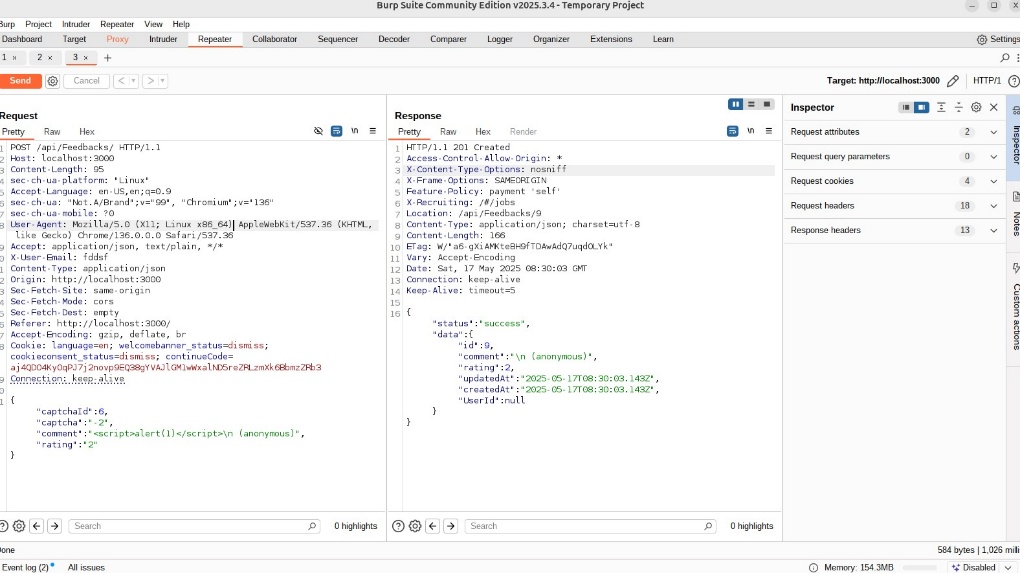
**Output**

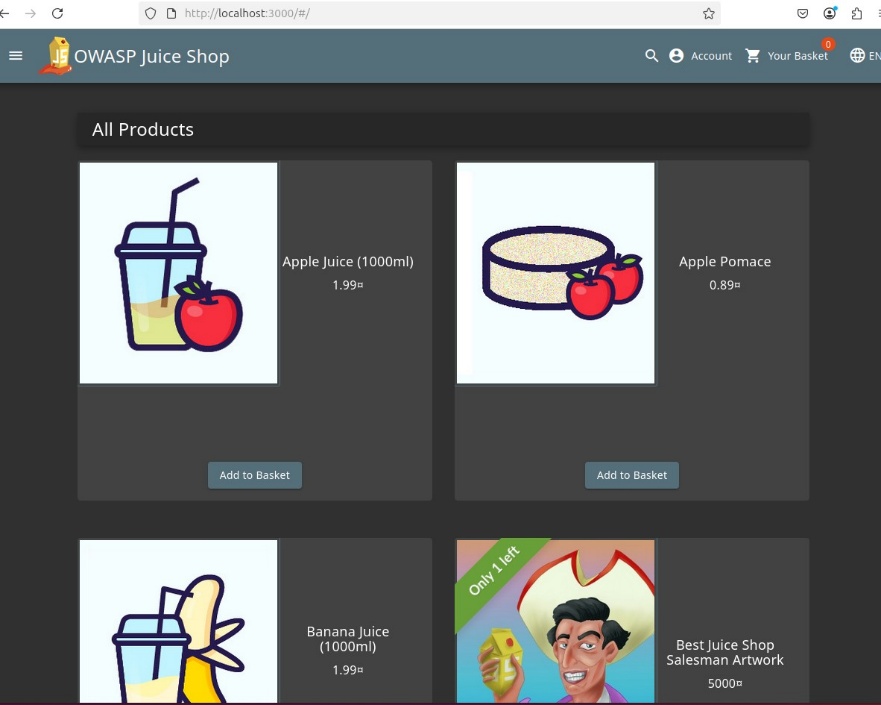
Screenshots and logs saved

Code updated and committed

Lessons documented







**Stakeholder Communication**

Post summary in Teams Crisis-Updates

Escalate to CISO via direct call

**Completion Criteria**

No longer reproducible XSS

Team debrief completed

Playbook updated if needed