VULNERABILITY ASSESSMENT & PENETRATION TESTING (VAPT)

Target Application: OWASP Juice Shop (v19.1.1)

Date: 11 December 2025

Tester: MILIND M PATIL

Tools Used: Kali Linux, Burp Suite, OWASP ZAP

1. EXECUTIVE SUMMARY

A security assessment was performed on the OWASP Juice Shop web application to identify security flaws. The assessment followed standard ethical hacking procedures. During the test, three (3) critical vulnerabilities were identified:

- SQL Injection: Allowing unauthorized administrative access.
- Cross-Site Scripting (XSS): Allowing execution of malicious scripts.
- Broken Access Control: Exposing sensitive internal pages.

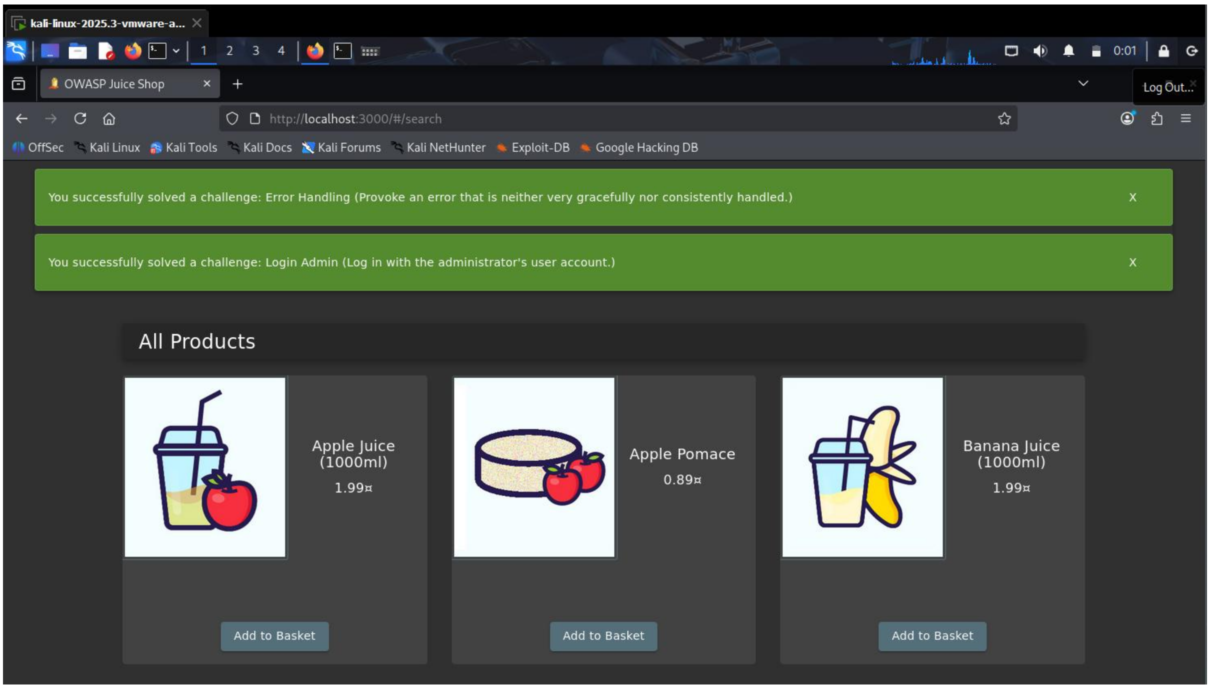
These vulnerabilities pose a high risk to the application and require immediate remediation.

2. VULNERABILITY FINDINGS

Finding 1: SQL Injection (Authentication Bypass)

- Severity: Critical
- OWASP Category: A03:2021 – Injection
- Description: The login form is vulnerable to SQL Injection. By injecting a standard payload, an attacker can manipulate the database query to log in as the Administrator without a valid password.
- Proof of Concept:
  - **Payload:** ' OR 1=1 –
  - **Result**: The application accepted the payload and granted administrative access.

- **Evidence:**



You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)

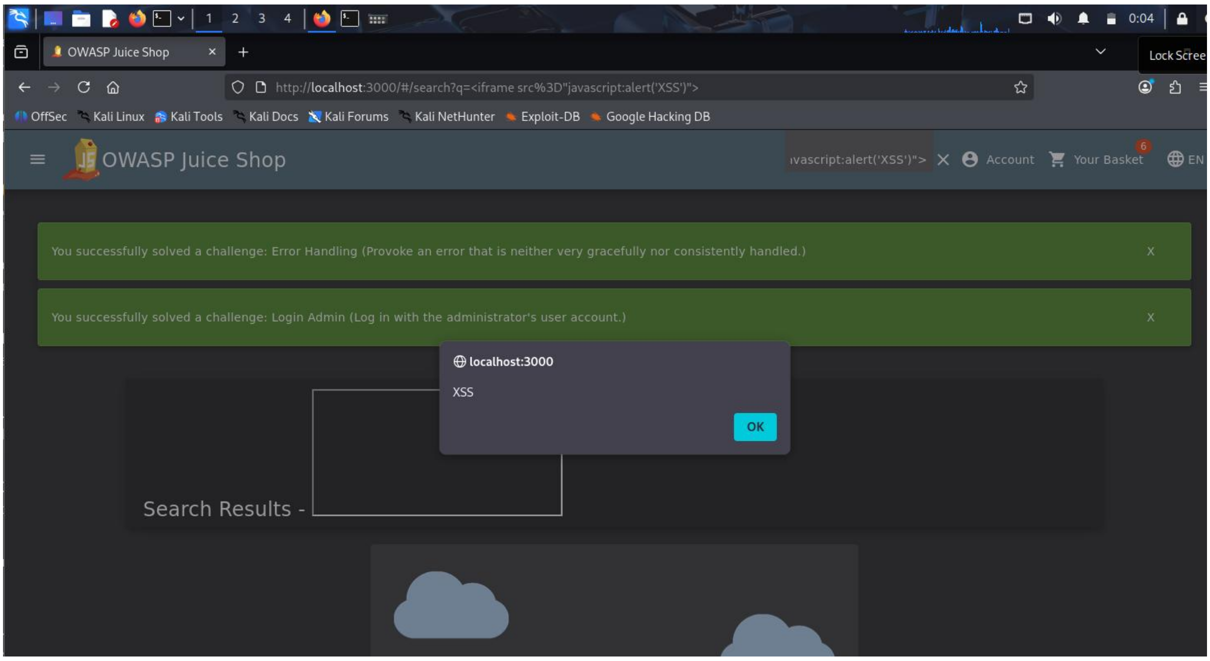
You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

- **Remediation:** Implement parameterized queries (Prepared Statements) for all database inputs to prevent code injection.

Finding 2: Reflected Cross-Site Scripting (XSS)

- Severity: High
- OWASP Category: A03:2021 – Injection
- Description: The application's search function fails to sanitize user input. This allows an attacker to inject JavaScript code that executes in the victim's browser.
- Proof of Concept:
    - **Payload:** <iframe src=” javascript:alert(‘XSS’)”>
    - **Result:** The application executed the script, displaying an alert popup.

- **Evidence:**



http://localhost:3000/#/search?q=<iframe src%3D"javascript:alert('XSS')">

You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)

You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

localhost:3000

XSS

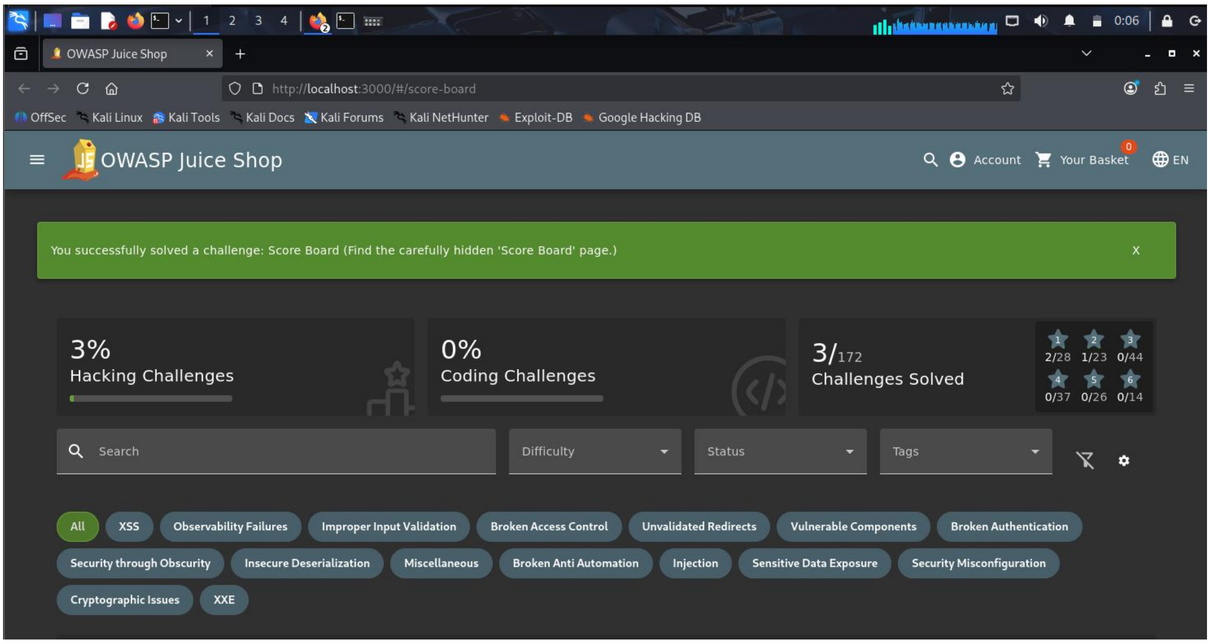
Search Results -

- **Remediation:** Implement strict input validation and output encoding (sanitization) for all user-supplied data.

Finding 3: Broken Access Control (Sensitive Page Exposure)

- Severity: Medium
- OWASP Category: A01:2021 – Broken Access Control
- Description: The application relies on "security by obscurity" to hide sensitive pages. The "Score Board" page is accessible to any unauthenticated user who guesses the correct URL, bypassing access controls.
- Proof of Concept:
    - **URL:** http://localhost:3000/#/score-board
    - **Result:** The user successfully accessed the restricted internal scoreboard.

- **Evidence:**



http://localhost:3000/#/score-board

You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)

3% Hacking Challenges

0% Coding Challenges

3/172 Challenges Solved

- **Remediation:** Implement proper role-based access control (RBAC) checks on the server side to ensure only authorized users can load restricted pages.