OWASP JUICE SHOP

Web Application Penetration Test Report

Date: July 20, 2025

Project: OWASP Juice Shop - Penetration Testing

Penetration Test Report

Target: OWASP Juice Shop (Local Lab)

Tester: Siti Aisyah Amat Jalani

Date: July 20, 2025

Tools Used: Burp Suite, Nmap, Firefox + FoxyProxy, Docker

Executive Summary

This penetration test focused on the OWASP Juice Shop web application to identify vulnerabilities aligned with the OWASP Top 10 and simulate a real-world black-box web application assessment. Key vulnerabilities such as Insecure Direct Object Reference (IDOR), Cross-Site Scripting (XSS), and SQL Injection were discovered and exploited in a controlled environment. The findings are intended for learning and portfolio purposes.

Methodology

Phase	Description
Reconnaissance	Identified application structure, input points, and backend logic.
Vulnerability Discovery	Manual and automated testing for OWASP Top 10 risks using Burp Suite and Nmap.
Exploitation	Exploited parameters using Burp Suite Repeater and manual payloads.
Documentation	Logged and scored findings using CVSS and proposed remediation steps.

Summary of Findings

Vulnerability	Risk Level	CVSS	Affected Endpoint	Status
IDOR	High	7.5	/rest/user/review/:id	Confirmed
Stored XSS	Medium	6.1	Search field	Confirmed
SQL Injection	High	8.1	/rest/user/login	Confirmed
Missing Security Headers	Low	3.7	All responses	Confirmed

Detailed Findings

1. Insecure Direct Object Reference (IDOR)

- **Endpoint:** /rest/products/:id/reviews/
- **Payload:** GET /rest/products/2/reviews/
- **Impact:** Allowed access to other users' feedback and edit user's existing reviews.
- **Recommendation:** Implement object-level access controls to validate user permissions.

2. Stored Cross-Site Scripting (XSS)

- **Field:** Product search input
- **Payload:** <script>alert('1')</script>
- **Impact:** JavaScript executes in user's browser
- **Recommendation:** Sanitize and encode user input before rendering on page.

3. SQL Injection

- **Endpoint:** /rest/user/login
- **Payload:** ' OR 1=1 --
- **Impact:** Bypasses login controls
- **Recommendation:** Use parameterized queries and ORM frameworks.

Vulnerability Summary

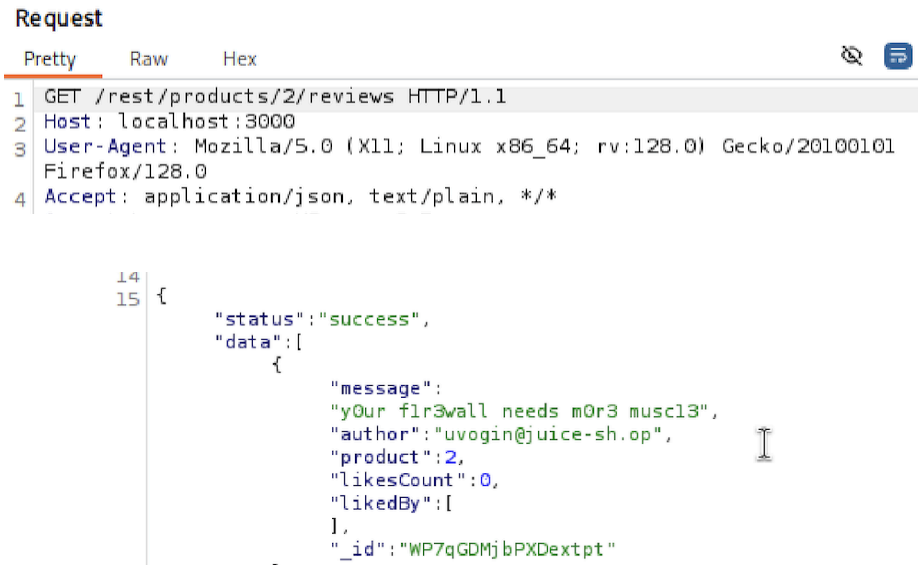
Technical Findings

Internal Penetration Test Findings

Vulnerability 1.1: IDOR (Insecure Direct Object Reference) (High)

Description:	Identified an IDOR vulnerability in the Review API by manipulating the review ID parameter. Gained unauthorized access to another user's feedback using `GET /rest/user/2/reviews`
Risk:	Impact: Very high - An authenticated user can access or enumerate feedback entries submitted by other users. This violates confidentiality and allows unauthorized access to internal data.
System:	All
Tools Used:	Burp Suite, Juice Shop (Docker), Firefox + FoxyProxy

Evidence



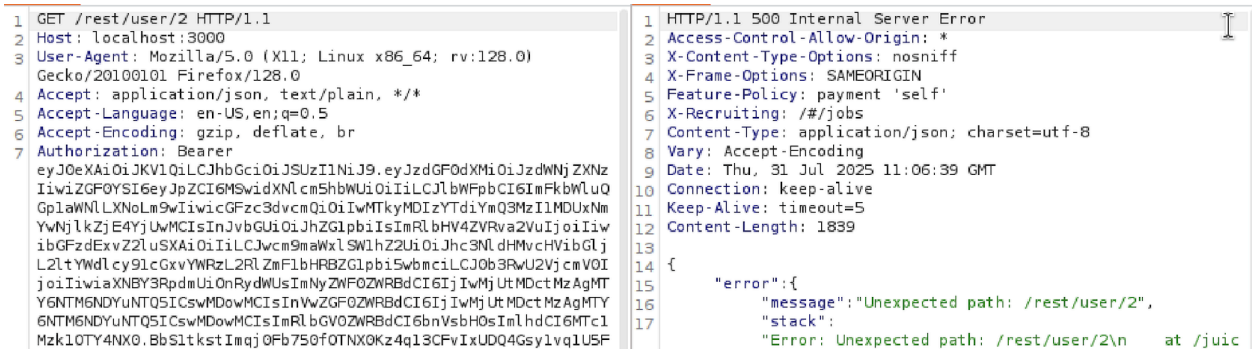
Remediation

Recommended implementing access control checks and **object-level access controls** for every user-specific resource.

Vulnerability 1.2: IDOR (Insecure Direct Object Reference) (High)

Description:	Identified an IDOR vulnerability in the User's info by changing the user ID parameter in the request. The response shows unauthorized or empty which means access control is working.
Risk:	Impact: Very high - Manipulation of the User ID gives access to attackers to access other user's data.
System:	All
Tools Used:	Burp Suite, Juice Shop (Docker), Firefox + FoxyProxy

Evidence



```
GET /rest/user/2 HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNz
IiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQ
GplaWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNm
YwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiw
ibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGlj
L2ltYWdlcy9lcGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0I
joiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMDctMzAgMT
Y6NTM6NDYuNTQ5ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMDctMzAgMTY
6NTM6NDYuNTQ5ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcl
MzklOTY4NX0.BbSltkstImqj0Fb750f0TNX0Kz4ql3CFvIxUDQ4Gsylvq1U5F
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Date: Thu, 31 Jul 2025 11:06:39 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 1839

{
    "error":{
        "message":"Unexpected path: /rest/user/2",
        "stack":
        "Error: Unexpected path: /rest/user/2\n    at /juic
```

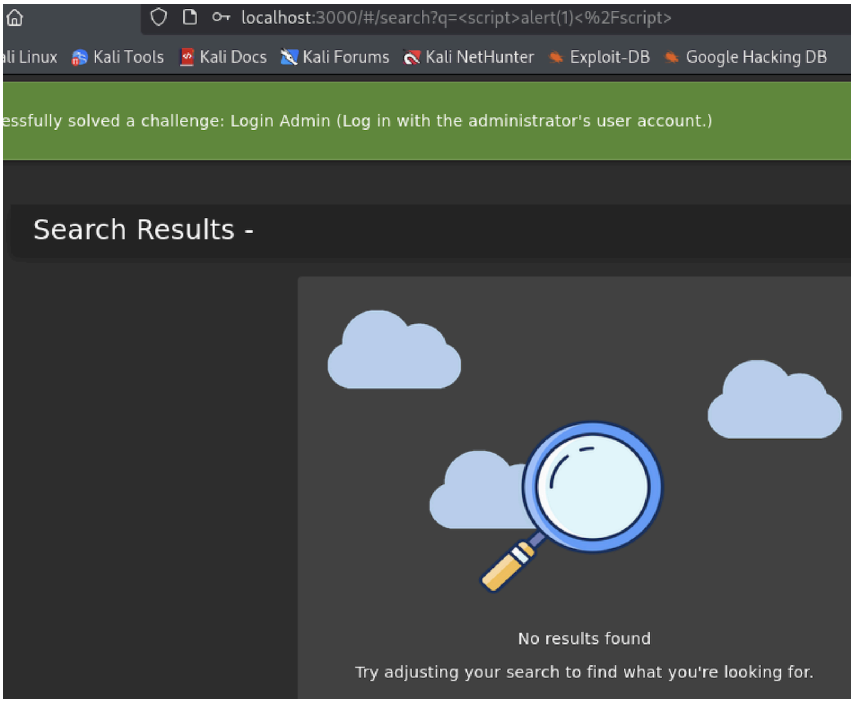
Remediation

Recommended implementing authorization checks for user-owned objects. Validate the logged-in user's permission server-side before returning data. Use secure frameworks or access control libraries.

Vulnerability 2: Stored XSS (Medium)

Description:	Investigation of search bar input by input payload `<script>alert("1")</script>` in the search bar.
Risk:	Impact: Medium - Executes script on all pages rendering search term
System:	All
Tools Used:	Burp Suite, Juice Shop (Docker), Firefox + FoxyProxy

Evidence



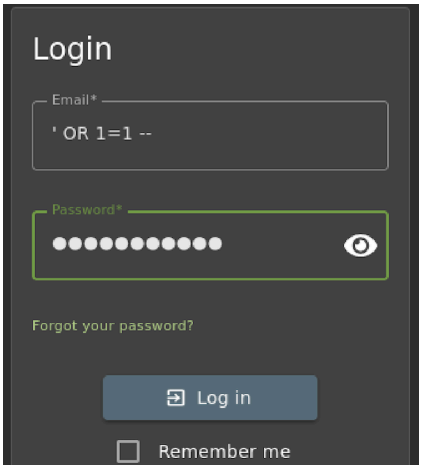
Remediation

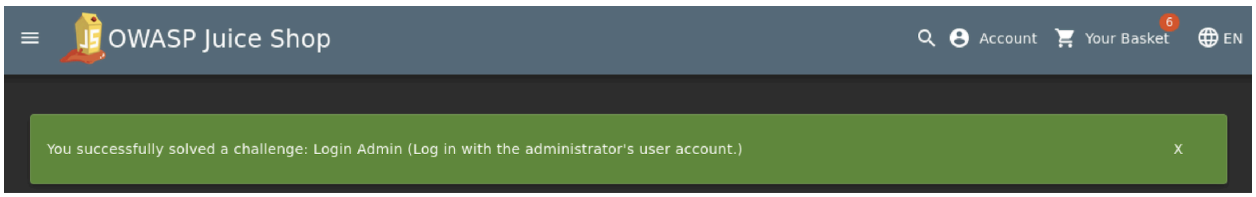
Recommended implementing input sanitization and encode user input before rendering on page.

Vulnerability 3: SQL Injection (High)

Description:	Identified an IDOR vulnerability in the User's info by changing the user ID parameter in the request. The response shows unauthorized or empty which means access control is working.
Risk:	Impact: Very high - Manipulation of the User ID gives access to attackers to bypass authentication.
System:	All
Tools Used:	Burp Suite, Juice Shop (Docker), Firefox + FoxyProxy

Evidence





Remediation

Recommended implementing using parameterized SQL queries and ORM frameworks.

Tools & Environment

- Docker container running Juice Shop (`localhost:3000`)
- Burp Suite Community Edition (interception and Repeater)
- Nmap (port/service discovery)
- Firefox + FoxyProxy for traffic interception
- Kali Linux terminal for command-line testing

Conclusion

The OWASP Juice Shop test demonstrated practical vulnerabilities aligned with real-world attack vectors. This lab provided a strong foundation for offensive security skills and highlights my readiness for professional penetration testing engagements.