Web Application Security Assessment Report

Name: Siyemukela Kheswa

Task 1: Web Application Security Testing

Program: Future Interns Cybersecurity Internship

Date: September 2025

Target Application: OWASP Juice Shop (Intentionally Vulnerable App)

Task Summary

This task is based on performing a vulnerability assessment on a deliberately vulnerable web application, to try and obtain vulnerabilities of the top 10 OWASP vulnerabilities. This task will be done on isolated environments (docker container). Each vulnerability is to be documented, tested and validated using ethical hacking tools.

Tools Used:

- Kali Linux
- OWASP juice shop
- Nikto
- OWAS ZAP

Procedure

- The OWASP Juice Shop was simulated on a docker container running locally on the kali virtual machine. This was also done to practise doing vulnerability testing locally.
- The application running locally was designated as the target system for both automated scanning and manual security testing using OWASP ZAP & Nikto.
- OWASP ZAP performed active scanning to identify input fields, user interactions, and potential vulnerabilities within the application.
- Nikto performed reconnaissance on the OWASP Juice shop, and it exposed leaked files and directories with sensitive information
- All identified vulnerabilities were analysed and mapped to the corresponding categories in the OWASP Top 10 framework, and mitigation measures were recommended to address the vulnerabilities.

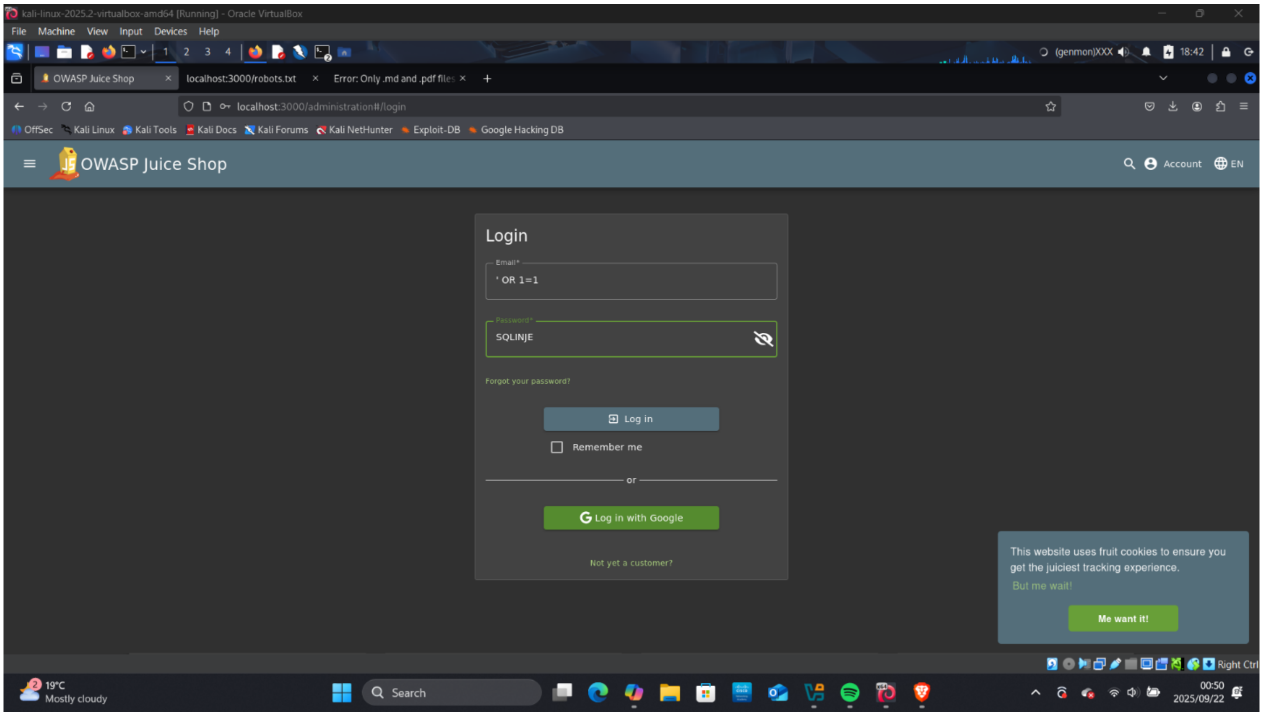
Identified Vulnerabilities

1. Broken Authentication – A01:2021 – Broken Access Control

After attempting to check the login field vulnerability for SQL Injection by injecting the code ' OR 1=1--, the system allowed us to gain access to the administrator profile. This is a big issue as the administrator account could have higher privileges and that would give a threat actor an upper hand.

- Impact: Full compromise of sensitive data and administrative functionality.

- ➢ Risk Rating: High
- ➢ Screenshot:



kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox

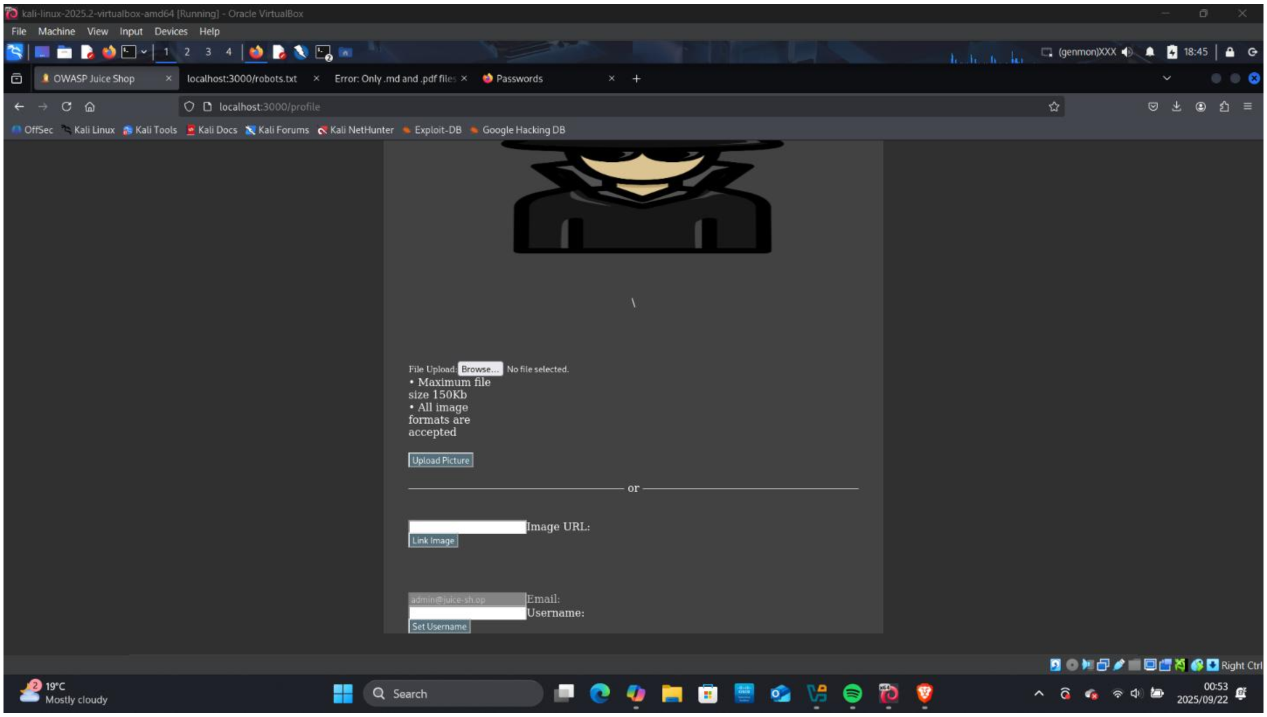
localhost:3000/administration#/login

Login

Email*: ' OR 1=1

Password*: SQLINJE

This website uses fruit cookies to ensure you get the juiciest tracking experience.



kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox

localhost:3000/profile

File Upload: Browse... No file selected.
- Maximum file size 150Kb
- All image formats are accepted

Image URL:

Email: admin@juice-sh.op

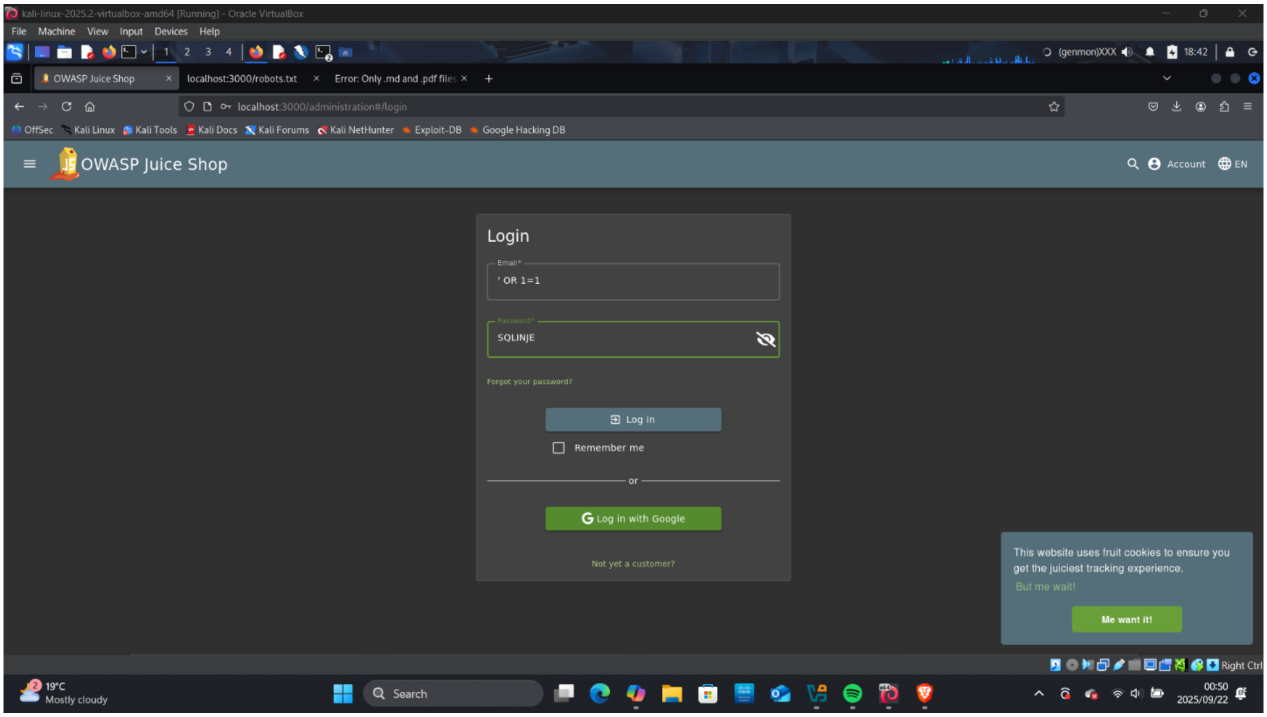
Username:

- Mitigation Strategies:
  - Implement Parameterized Queries
  - Enforce Input Validation
  - Apply Least Privilege to Database Accounts.

2. SQL Injection – A03:2021 - Injection

It has been determined in the above context that this application has a SQL injection vulnerability on the login form fields, which this can allow the threat actor to access admin account and possibly gain access to the database.

- Impact: Attacker can force the application to expose the database.
- Risk Rating: Medium
- Screenshot:



kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
localhost:3000/robots.txt
Error: Only .md and .pdf files
localhost:3000/administration#/login
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
OWASP Juice Shop
Account
EN
Login
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
Me want it!
19°C Mostly cloudy
Search
Right Ctrl
00:50 2025/09/22

Email*: ' OR 1=1

Password*: SQLINJE

□ Remember me

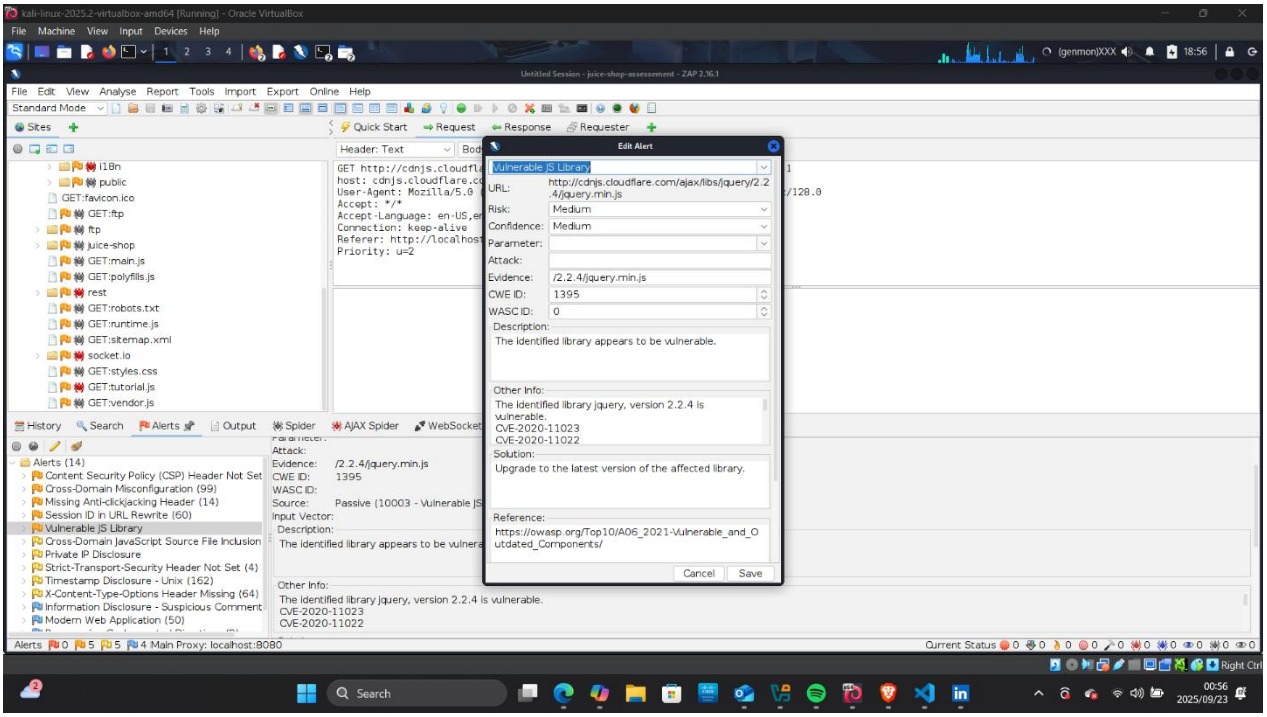
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

- Mitigation strategies:
  - Use parameterized queries
  - Validate and sanitize all user input
  - Deploy web application firewall

3. Outdated JavaScript Library – AO6:2021 – Vulnerable & Outdated Components

After the OWASP ZAP performed the reconnaissance on the web application, it reported that the OWASP Juice Shop has outdated JavaScript libraries, which can introduce vulnerabilities into the system. Allowing the threat actors to exploit them.

- Impact: Attackers can exploit the vulnerabilities introduced by the outdated component
- Risk rating: medium
- Screenshot



Edit Alert

Vulnerable JS Library

URL: http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js

Risk: Medium

Confidence: Medium

Parameter:

Attack:

Evidence: /2.2.4/jquery.min.js

CWE ID: 1395

WASC ID: 0

Description:
The identified library appears to be vulnerable.

Other Info:
The identified library jquery, version 2.2.4 is vulnerable.
CVE-2020-11023
CVE-2020-11022

Solution:
Upgrade to the latest version of the affected library.

Reference:
https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Alerts (14)
- Content Security Policy (CSP) Header Not Set
- Cross-Domain Misconfiguration (99)
- Missing Anti-clickjacking Header (14)
- Session ID in URL Rewrite (60)
- Vulnerable JS Library
- Cross-Domain JavaScript Source File Inclusion
- Private IP Disclosure
- Strict-Transport-Security Header Not Set (4)
- Timestamp Disclosure - Unix (162)
- X-Content-Type-Options Header Missing (64)
- Information Disclosure - Suspicious Comment
- Modern Web Application (50)

Alerts 0 5 5 4 Main Proxy: localhost:8080

- **Mitigation strategies:**
  - **Use dependency scanners**
  - **Keep libraries updated**
  - **Remove unused dependencies**

OWASP Top 10 Mapping

Vulnerability	OWASP Top 10(2021)	Risk Rating
Broken access control	**A01: Broken Access Control**	**High**
SQL injection	**A03: Injection**	**Medium**
Outdated JavaScript Library	**A06: Vulnerable & Outdated Components**	**Medium**

Conclusion

Performing the vulnerability assessment on this application has revealed great vulnerabilities which can lead to breach or a compromised system. It is better to implement security measures, fix patches and regular updates.