Final Project Intro Cyber Report

Name of members:

Mohamed Ayman Yakout. G2 2305104

Ahmed Sameh Ragab. G2 2305122

Tarek Mohamed Saeed. G2 2305111

Executive Summary:

We have worked on the enumeration to find admin path, brute force on admin credintals and xss in product search.

Scope and Methodology:

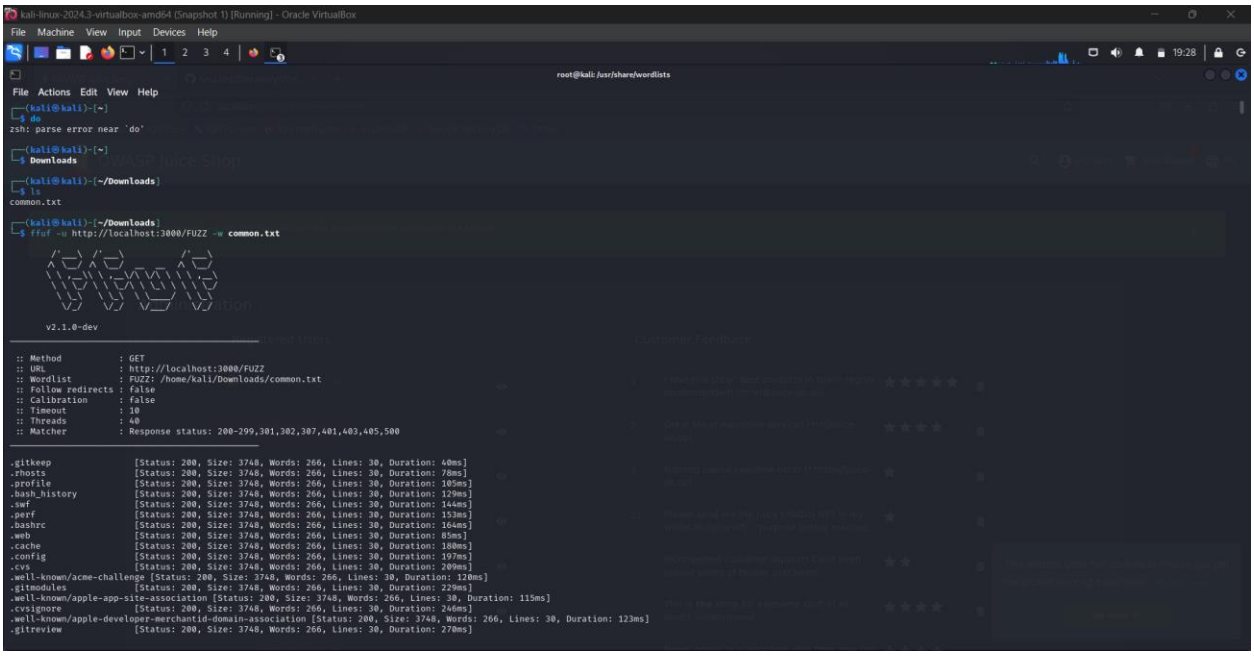
Scope: owasp juice shop,

Approach: Black-box where penetration tester has no access to the IT environment.

Tools used: hydra - docker.io - ffuf.

Vulnerability Findings:

1- First we use this command ‘’sudo apt update && sudo apt install docker.io’’ to set up docker on our machine, then we use this command ‘’ sudo docker run -d -p 3000:3000 bkimminich/juice-shop’’ to runs the juice shop application using docker, making it available for security testing.



Here we download this txt file that named by (common.txt) from github in fire fox browser in kali linux then we use this command ’’ ffuf -u http://localhost:3000/FUZZ -w common.txt ’’ that a web fuzzer tool to perform directory or endpoint fuzzing on the URL http://localhost : 3000.

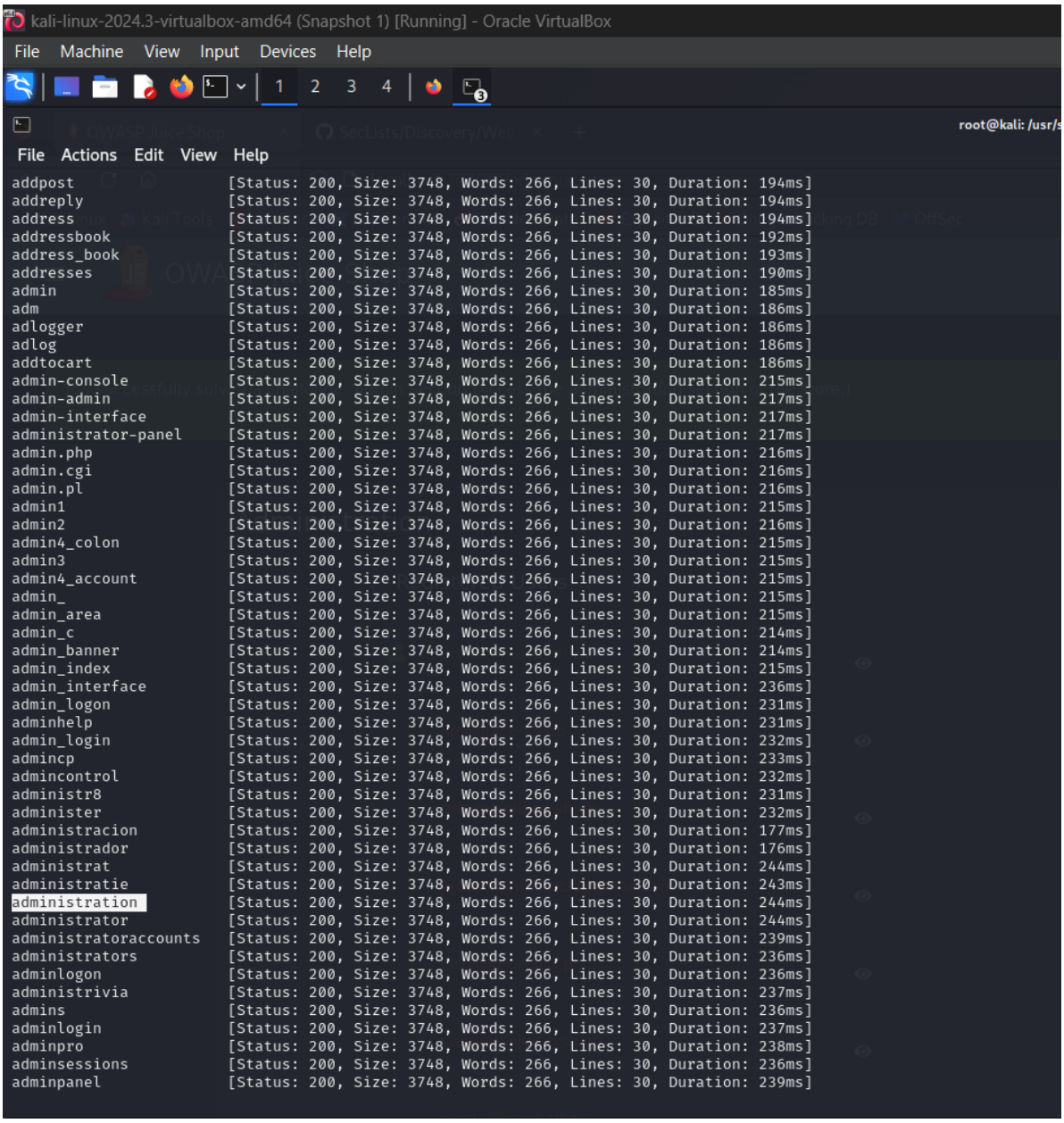
The ffuf tool is being used for fuzzing and automates the process of finding hidden directories, files.

-u http: //localhost : 3000/FUZZ:

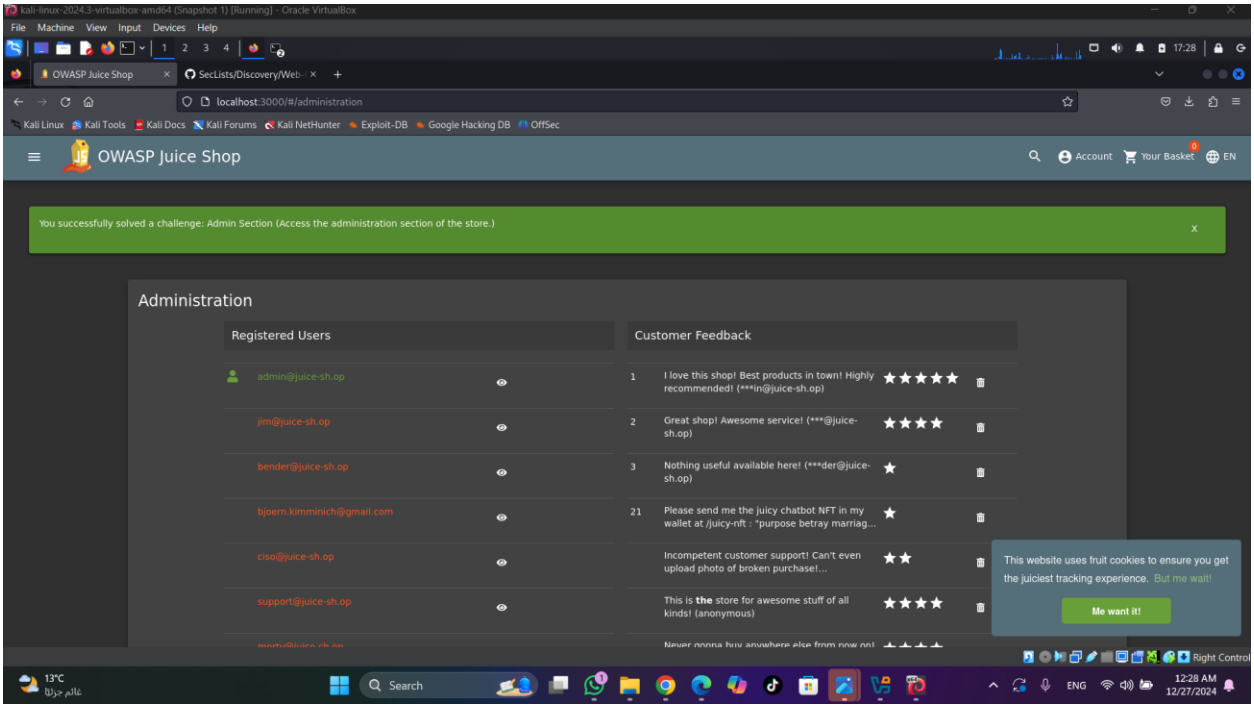
Specifies the URL to test and fuff will inject payloads to attempt different requests.

-w common.txt:

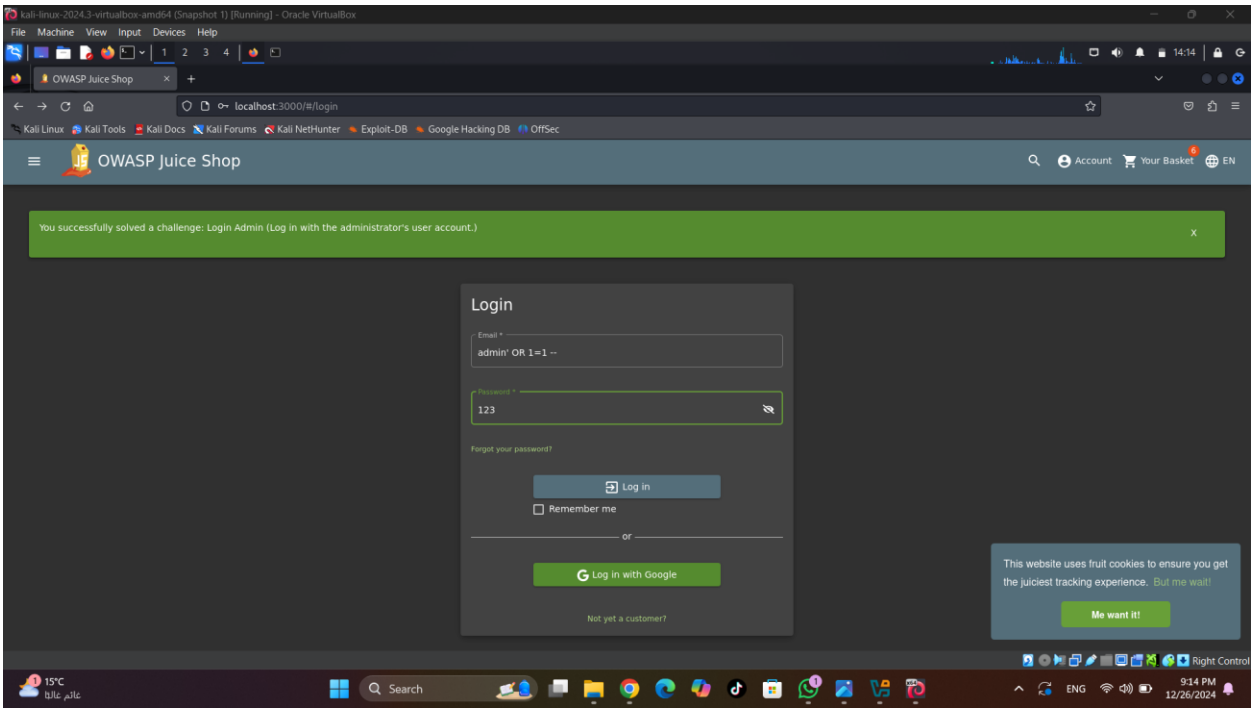
Specifies the wordlist to use.



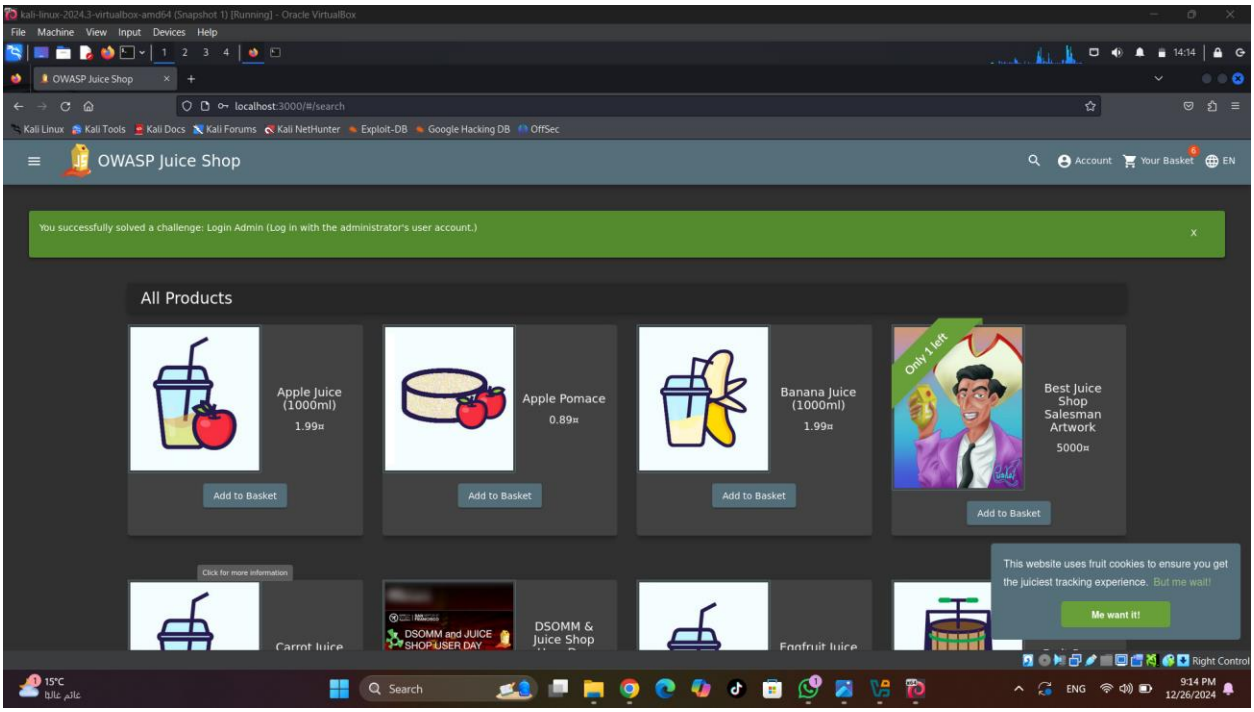
We copy the administration then we paste it in the URL of the Owasp juice shop.



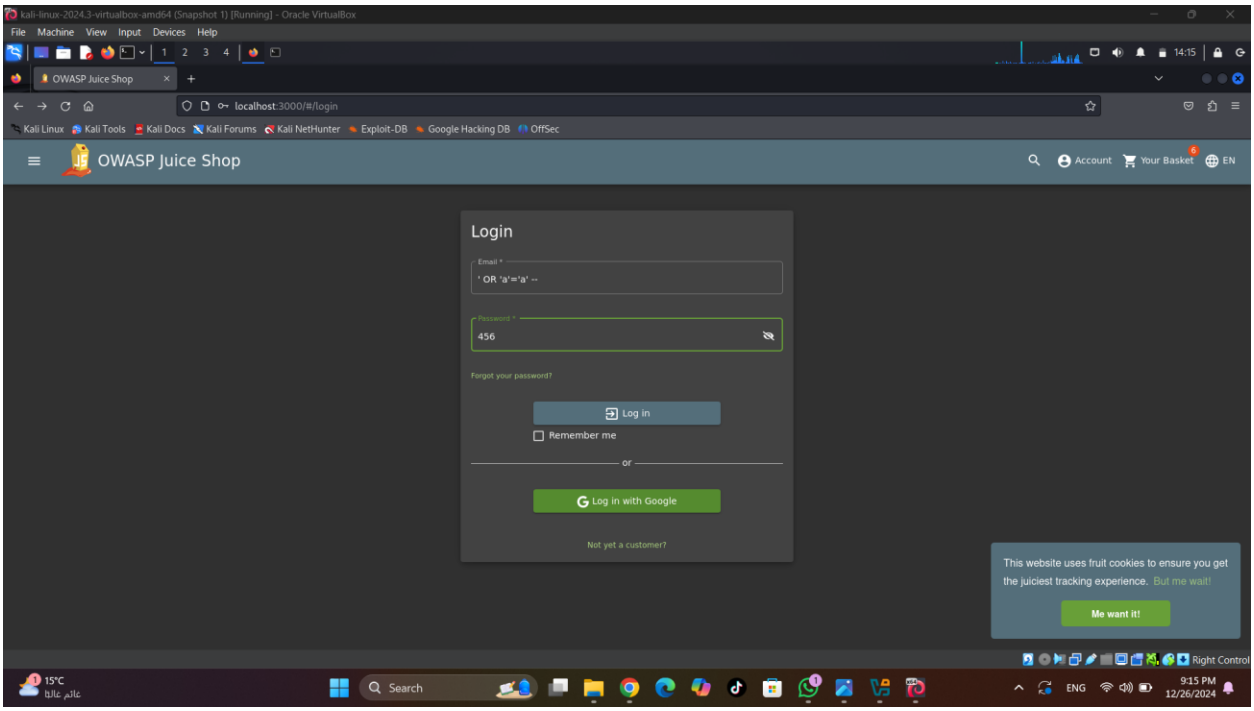
Then the step of enumeration to find admin path is done successfully.



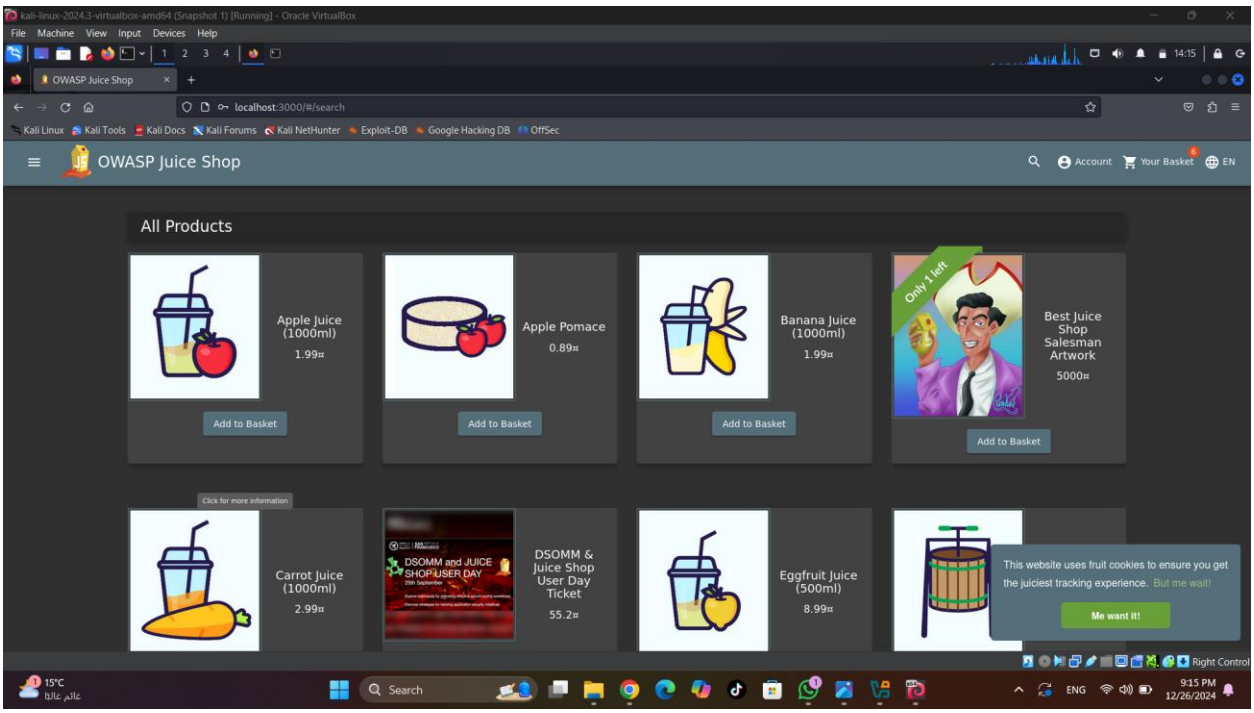
Here we used this payload (admin' OR 1=1 --) to make sql injection and we type any password.



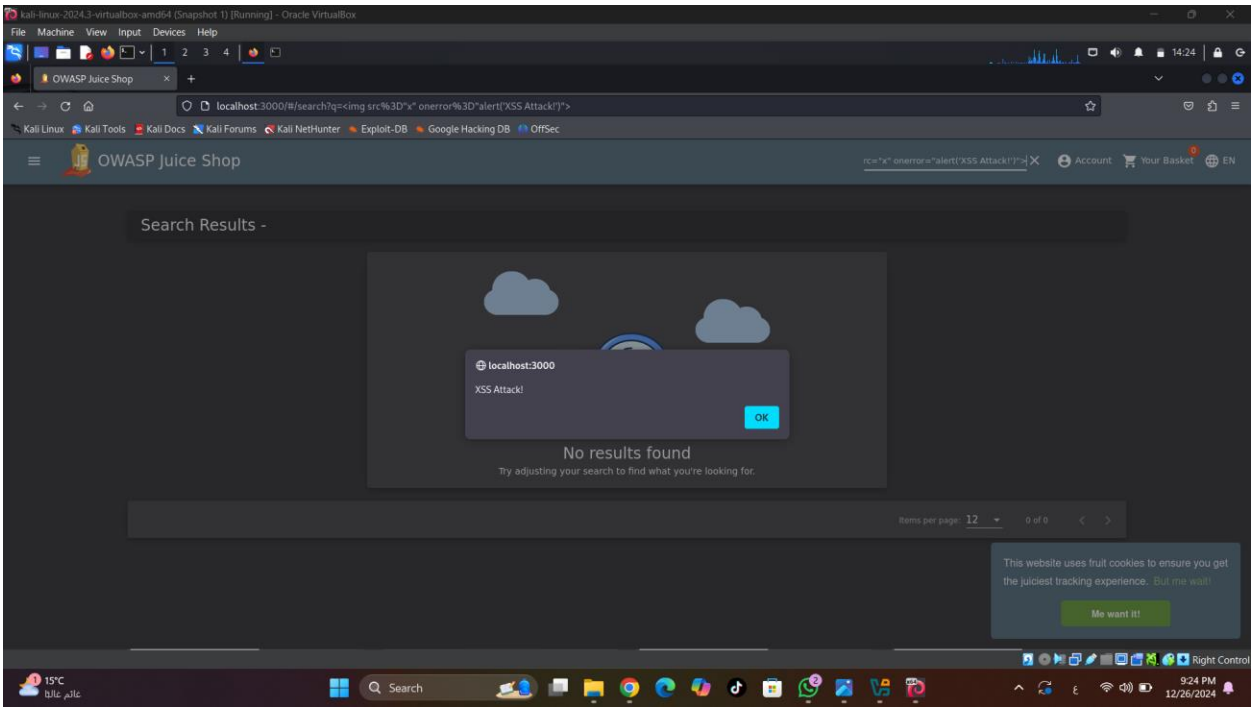
Here we login successfully.



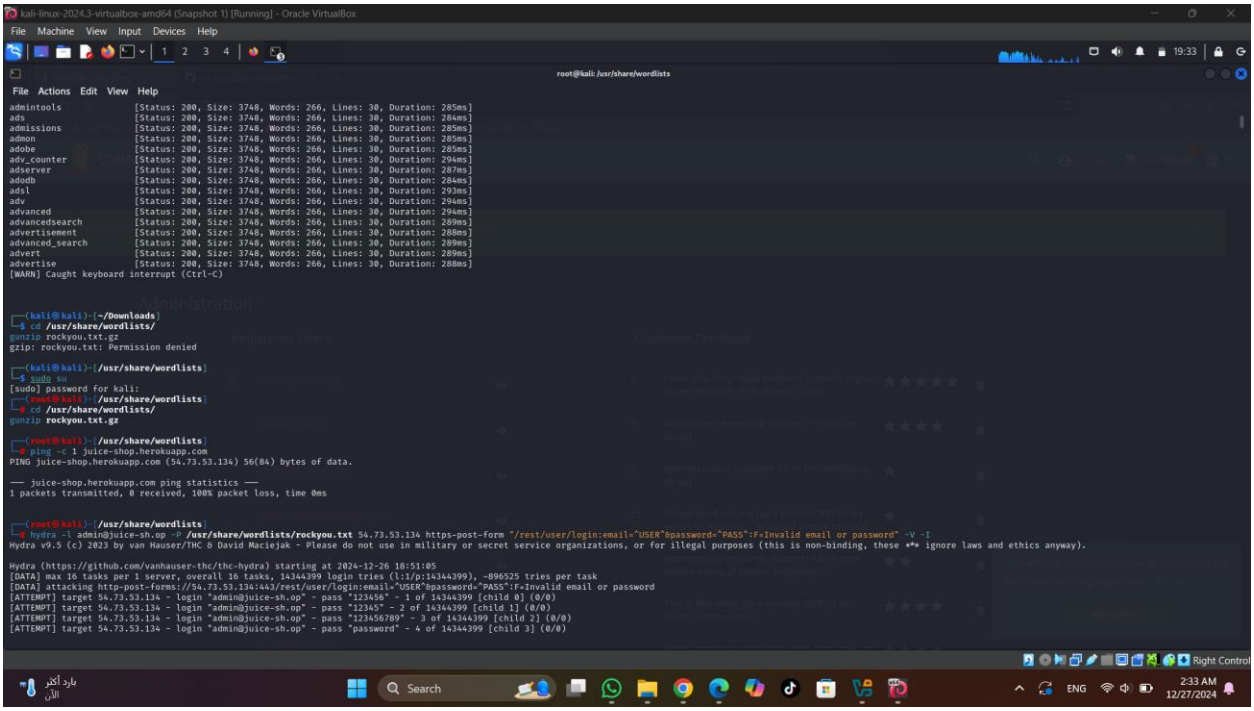
Here we used another payload (' OR 'a'='a' --) and type any password.



The we login successfully.



Here the XSS in the product search is done by using this payload (<img src="x" onerror="alert('XSS Attack!')">)



Here we used (cd /usr/share/wordlists/gunzip rockyou.txt.gz)

This command used in the context of penetration testing, the first part of this command to change the working directory to /usr/share/wordlists this directory typically contains wordlists used for brute-forcing or password cracking as rockyou.txt.gz.

The second part of this command to decompresses the rockyou.txt.gz file to extract the plaintext wordlists file rockyou.txt.

Then we use this command (ping -c 1 juice-shop.herokuapp.com) to ping the link of website to get the ip address of this website then, we get the ip (54.73.53.134) to put in this command (hydra -l admin@juice-sh.op -P /usr/share/wordlists/rockyou.txt 54.73.53.134 https-post-form "/rest/user/login:email=^USER^&password=^PASS^:F=Invalid email or password" -V –I) this command uses hydra, a popular brute-forcing tool, to attempt to crack the login credentials and to brute-force the password for the admin@juice-sh.op .

-l admin@juice-sh.op:

Specifies the username to test.

-p /usr/share/wordlists/rockyou.txt:

Specifies the password list (wordlist) to use. This points to the rockyou.txt wordlist, which contains millions of potential passwords.

54.73.53.134:

The target IP address where the web application is hosted.

https-post-form "/rest/user/login:email=^USER^&password=^PASS^:F=Invalid email or password":

Tells Hydra to brute-force an HTTPS POST form. Here's how it works:

/rest/user/login: The endpoint for the login request.

email=^USER^&password=^PASS^: This is the POST data where Hydra substitutes ^USER^ with the username (admin@juice-sh.op) and ^PASS^ with passwords from the wordlist.

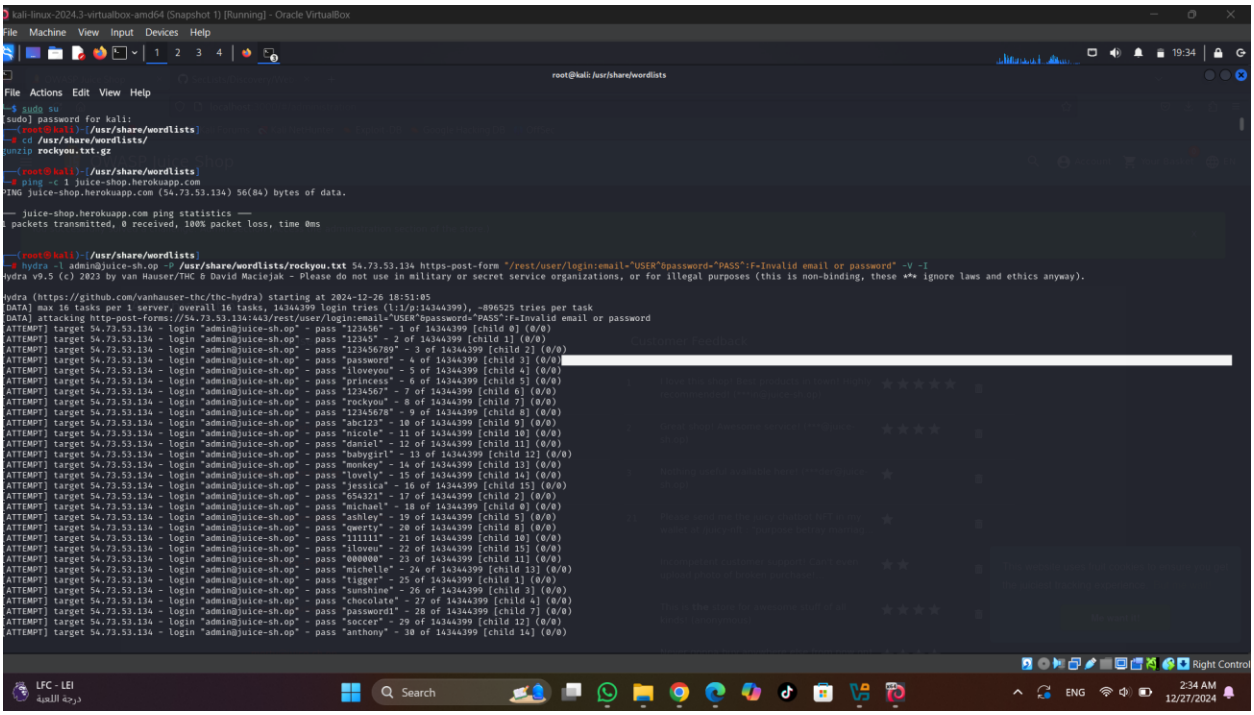
:F=Invalid email or password: Specifies the failure condition. If the response contains "Invalid email or password," Hydra will know the attempt failed and will try the next password.

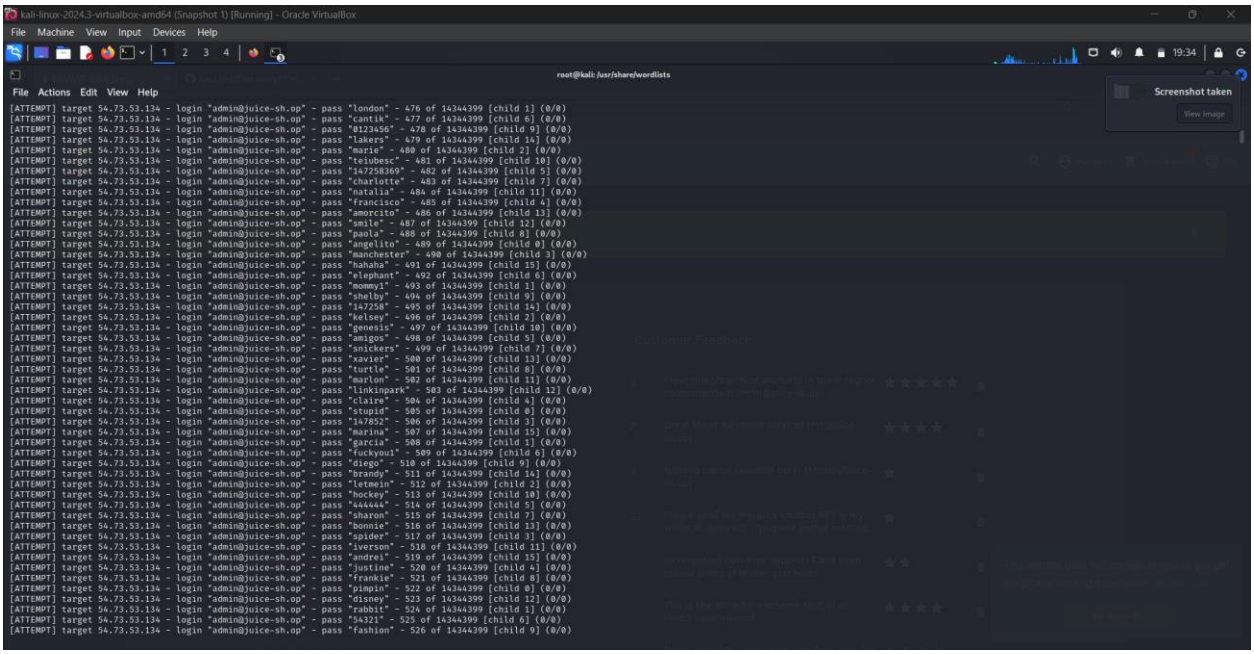
-V:

Enables verbose mode. Hydra will show each login attempt, including the username and password being tested.

-I:

Forces immediate execution. Hydra will not wait for previous tasks to complete before moving to the next attempt.





Then the brute force is done successfully and the password is admin123.

The End.