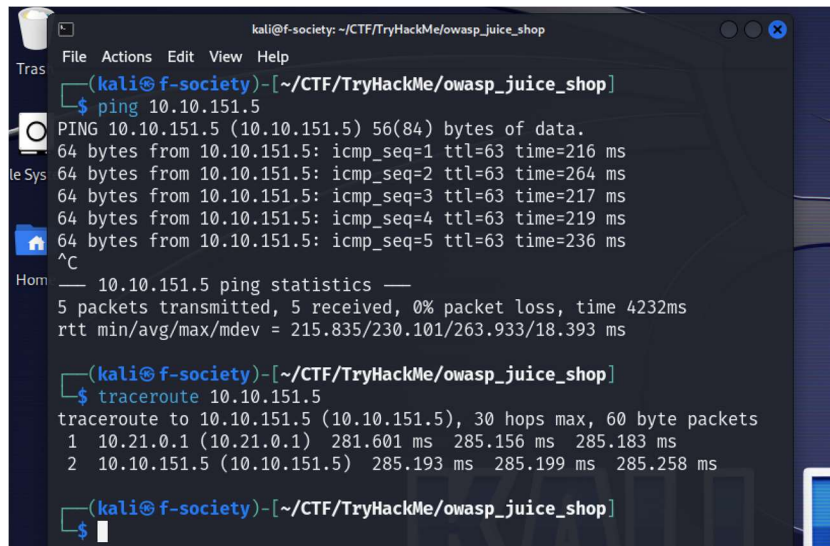


OWASP JUICE SHOP CTF from Tryhackme

This is a jeopardy type of CTF, so we will follow the hints.

1. As always connect your vpn:
 - `sudo openvpn {name_of_vpn}`
2. Then check if the machine is online
 - `ping {target_ip}`
 - `traceroute {target_ip}`

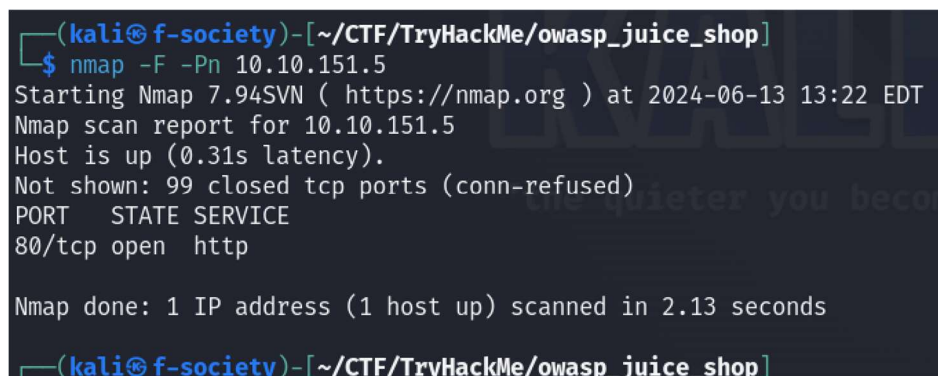
A terminal window from a Kali Linux machine. The prompt is `(kali@f-society)-[~/CTF/TryHackMe/owasp_juice_shop]`. The user enters `ping 10.10.151.5`. The output shows five successful ping requests with varying times (216ms to 236ms). After pressing `^C`, the terminal shows the ping statistics: 5 packets transmitted, 5 received, 0% packet loss, time 4232ms, and rtt statistics. Then the user enters `traceroute 10.10.151.5`. The output shows a two-hop traceroute from 10.21.0.1 to 10.10.151.5 with round-trip times around 285ms.

```
(kali@f-society)-[~/CTF/TryHackMe/owasp_juice_shop]
$ ping 10.10.151.5
PING 10.10.151.5 (10.10.151.5) 56(84) bytes of data.
64 bytes from 10.10.151.5: icmp_seq=1 ttl=63 time=216 ms
64 bytes from 10.10.151.5: icmp_seq=2 ttl=63 time=264 ms
64 bytes from 10.10.151.5: icmp_seq=3 ttl=63 time=217 ms
64 bytes from 10.10.151.5: icmp_seq=4 ttl=63 time=219 ms
64 bytes from 10.10.151.5: icmp_seq=5 ttl=63 time=236 ms
^C
--- 10.10.151.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4232ms
rtt min/avg/max/mdev = 215.835/230.101/263.933/18.393 ms

(kali@f-society)-[~/CTF/TryHackMe/owasp_juice_shop]
$ traceroute 10.10.151.5
traceroute to 10.10.151.5 (10.10.151.5), 30 hops max, 60 byte packets
 1  10.21.0.1 (10.21.0.1)  281.601 ms  285.156 ms  285.183 ms
 2  10.10.151.5 (10.10.151.5)  285.193 ms  285.199 ms  285.258 ms

(kali@f-society)-[~/CTF/TryHackMe/owasp_juice_shop]
$
```

3. Now let's scan our target using nmap
 - `nmap -F -Pn {target_ip}`
 - -F = fast mode
 - -Pn = no ping

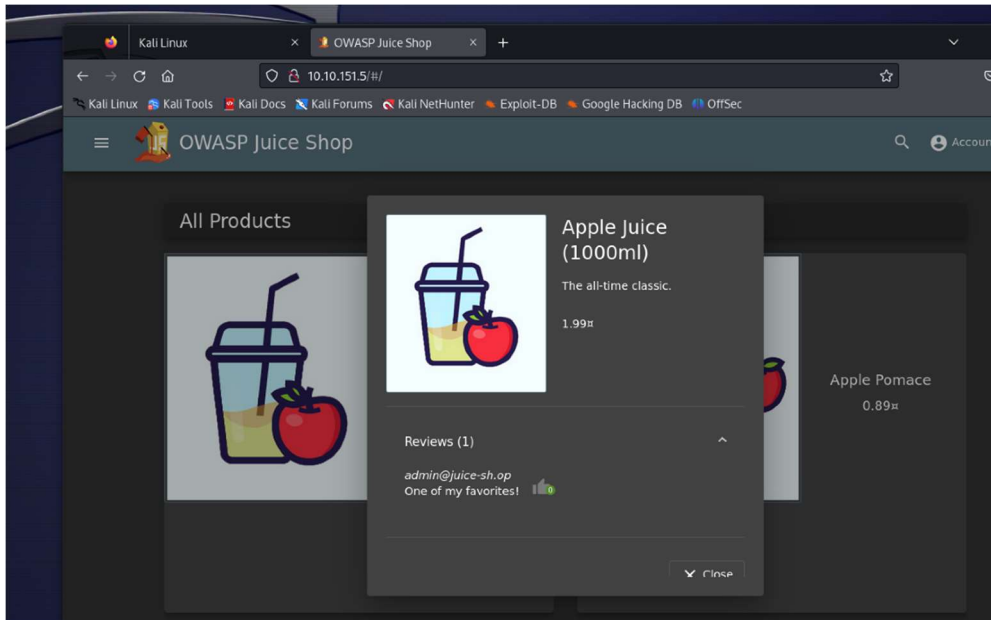
A terminal window showing the output of an nmap scan. The prompt is `(kali@f-society)-[~/CTF/TryHackMe/owasp_juice_shop]`. The user enters `nmap -F -Pn 10.10.151.5`. The output shows the nmap version (7.94SVN), the start time (2024-06-13 13:22 EDT), the scan report for 10.10.151.5, and the results: host is up, 99 closed tcp ports, and port 80/tcp is open and serving http.

```
(kali@f-society)-[~/CTF/TryHackMe/owasp_juice_shop]
$ nmap -F -Pn 10.10.151.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-13 13:22 EDT
Nmap scan report for 10.10.151.5
Host is up (0.31s latency).
Not shown: 99 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

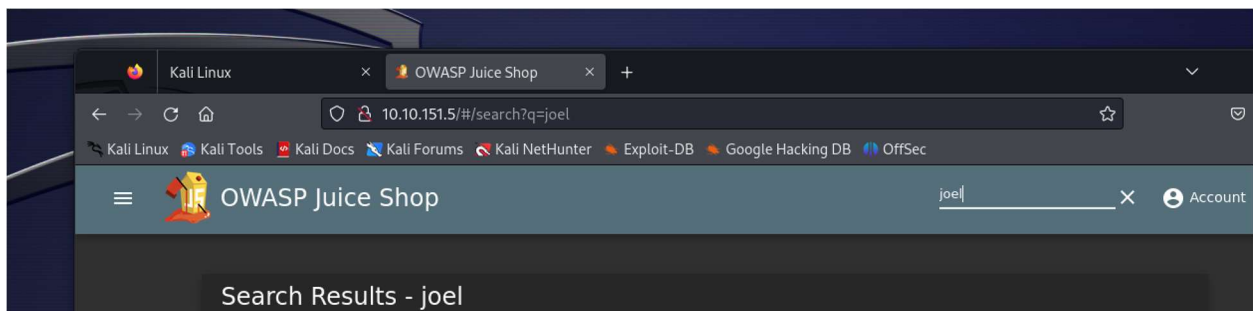
Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds

(kali@f-society)-[~/CTF/TryHackMe/owasp_juice_shop]
$
```

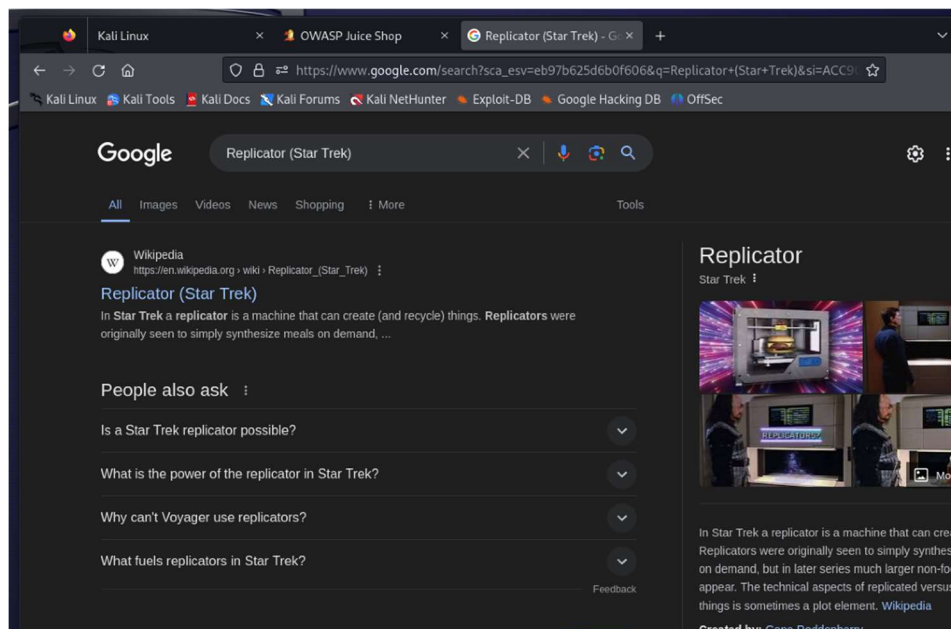
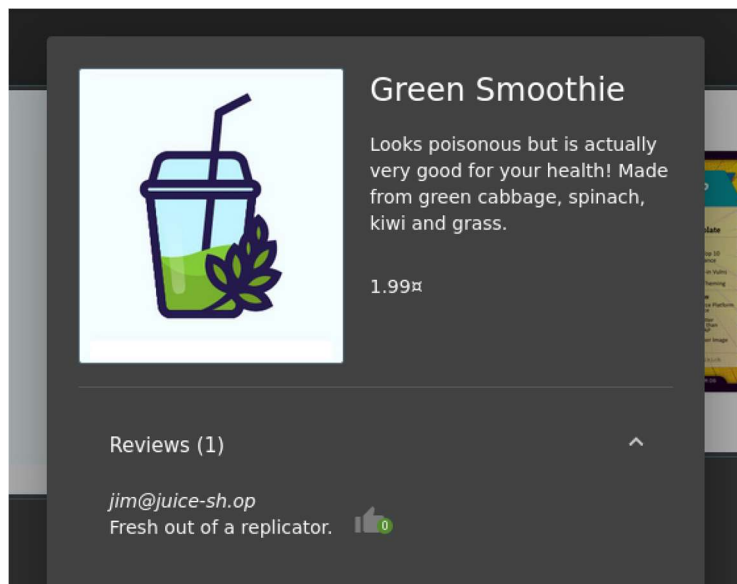
4. Since we see that port 80 which is http is open, we navigate to the website.
5. After opening the website, we investigate it.
6. On clicking the links, we find a review and on clicking the review we find there are emails of employees.



7. We take note of the usernames and move on to the next task.
8. When we search for staff using the search bar and notice the url we see what the search parameter is.

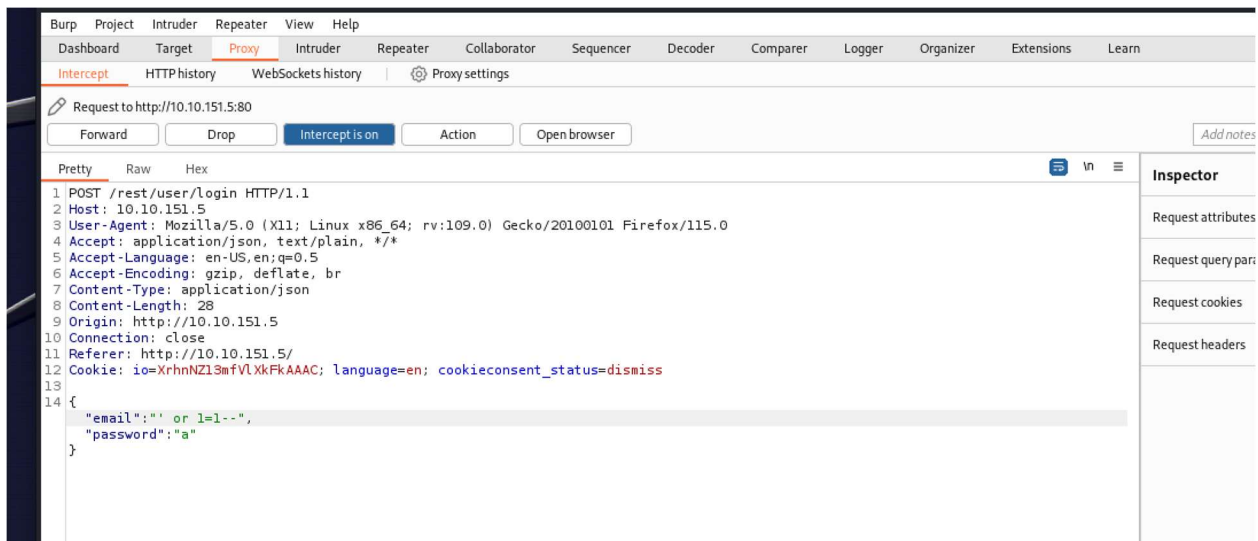
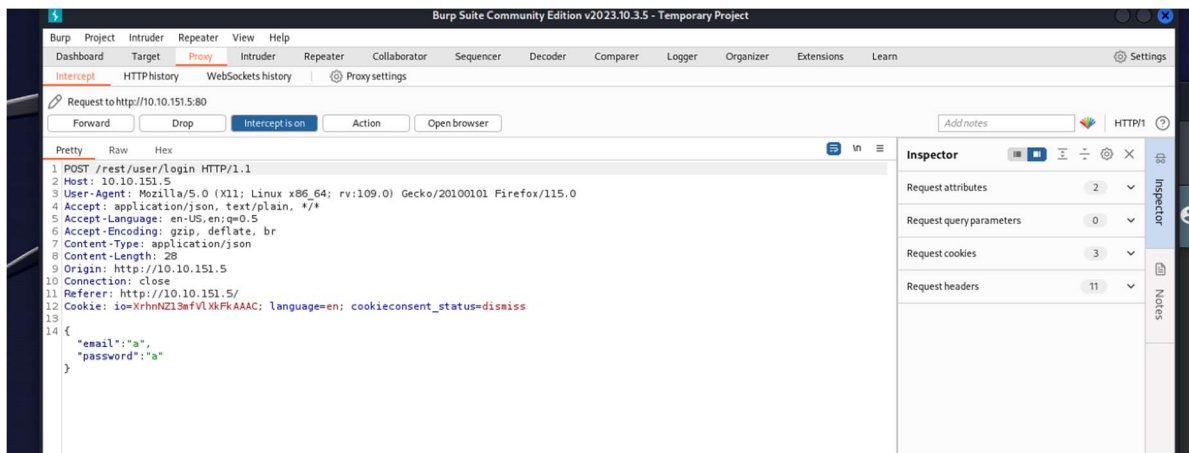


9. On reviewing the green smoothie, we find the username of jim and clue which is word (replicator).
 - Searching for the word replicator we find another clue (star trek), which is a movie name.

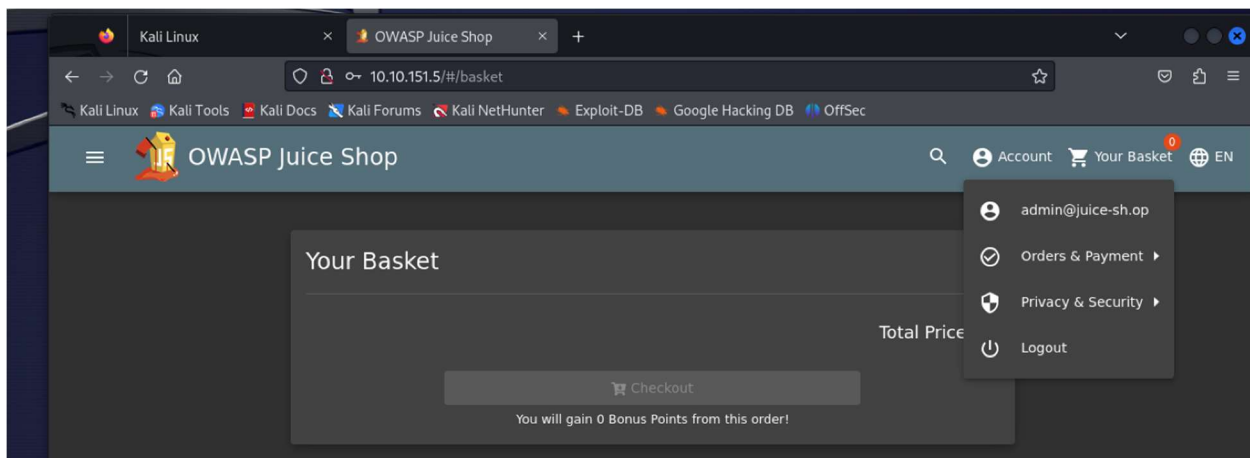


10. Now we open our burpsuite and turn the intercept on and turn our foxy proxy to burp. Then we will capture the login and use **sql injection** to login to the admin page.

- On the capture we will change the email with “ ‘ or 1=1- -”
 - ‘ = will close the brackets on sql query
 - Or = return true if either is true and 1=1 is always true.
 - - - = used in sql to comment data.



- When forwarding the request, we will login to the admin page.

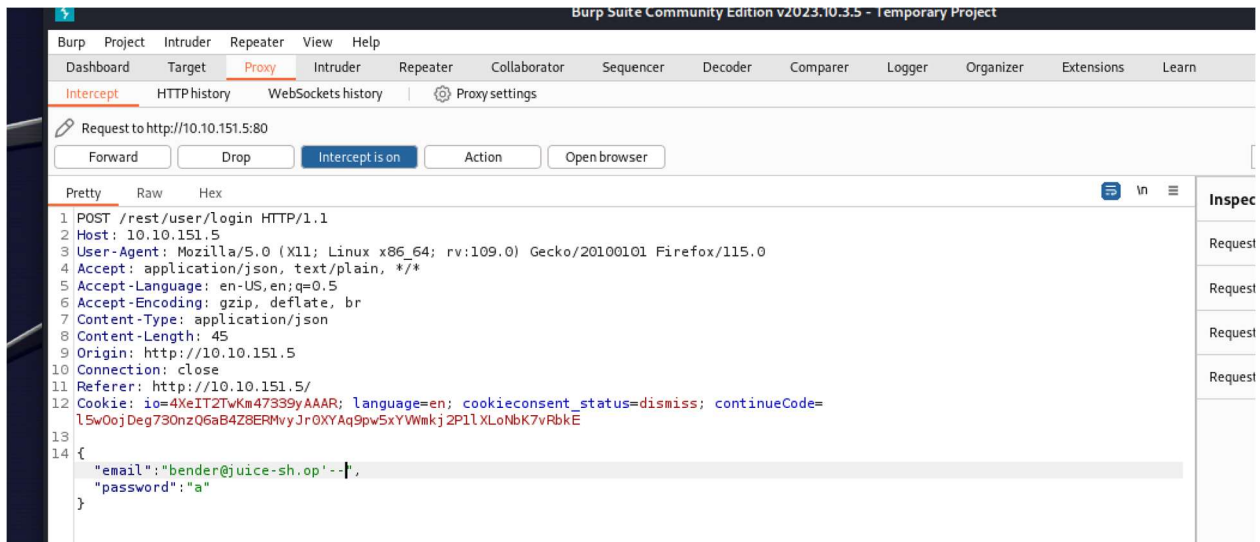


11. Now let's try to bypass another login page with a known email, for instance for Bender.

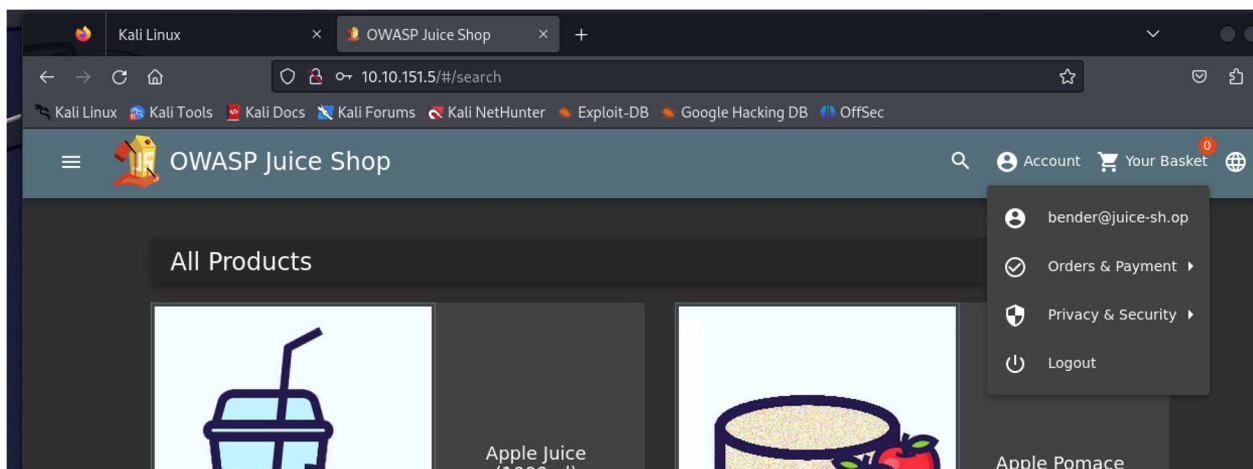
- When we capture the login for Bender, we will alter the email with bender@juice-sh.op
 - Here 1=1 is not needed because we know the email, or the email is valid so we only use '-' - bypass the login.

NOTE

- ❖ 1=1 is used when email or username is not known or not valid.

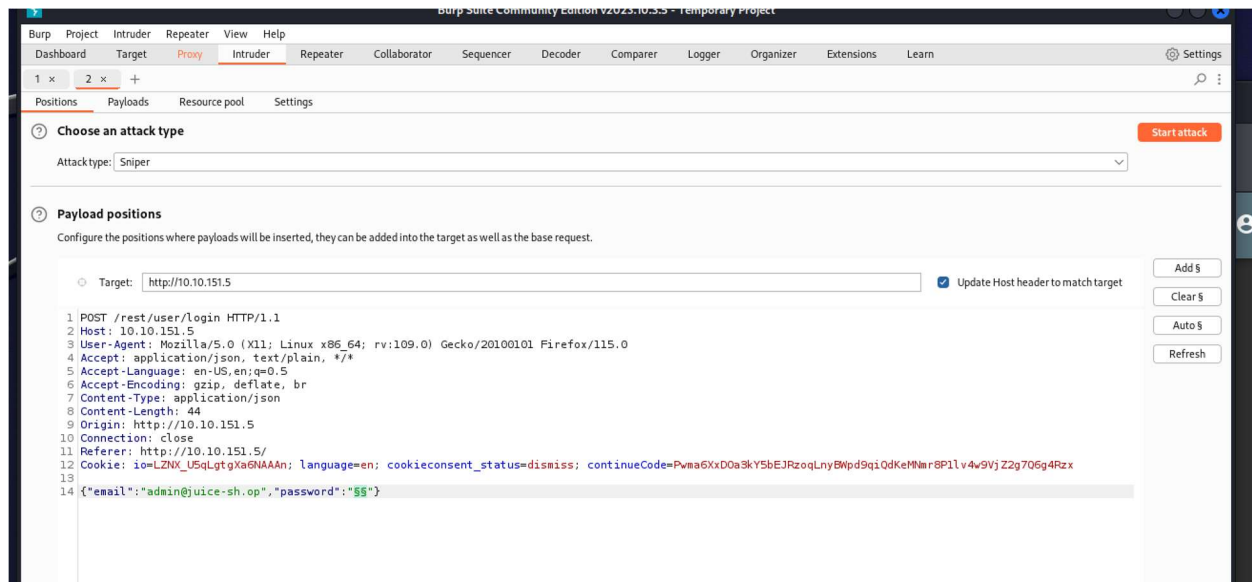


- We logged into bender account bypassing the login.



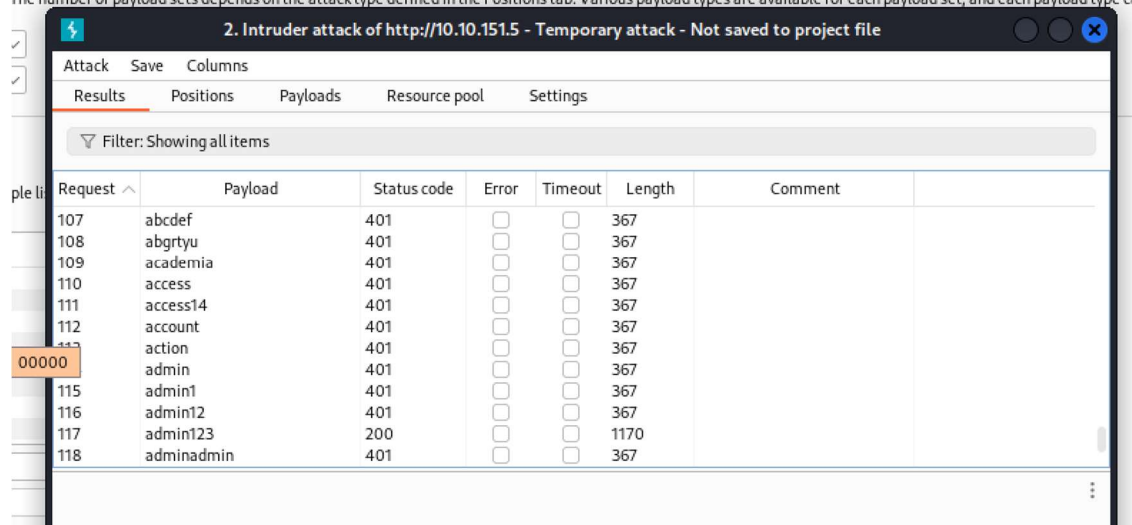
12. On the above method we tried to alter the database to login now we will try to brute force to know the password of the admin.

- We will once again capture a login request, but instead of sending it through the proxy, we will send it to Intruder and change the password using the “add\$” option on right corner.



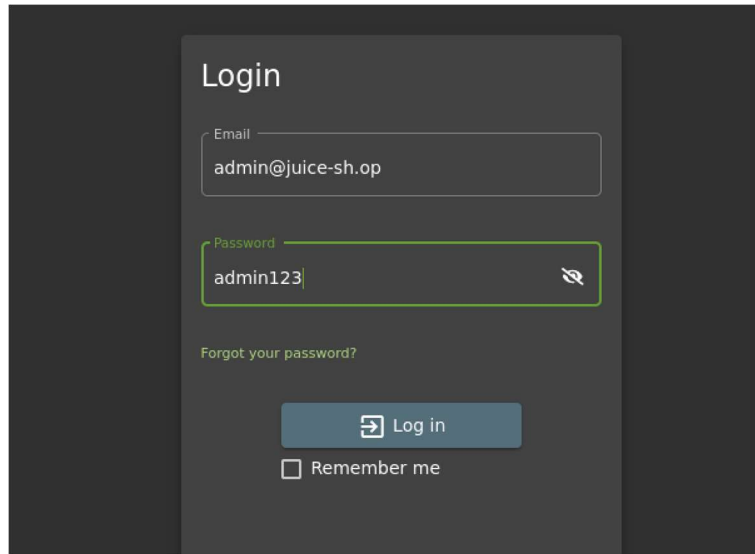
- Then go to the payload option and we will choose the **best1050.txt** from **SecLists** from the following path:
 - /usr/share/wordlists/SecLists/Passwords/Common-Credentials/best1050.txt
 - And then we start the attack and look for status code of 200.

The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can



❖ As you can see there is a status code of 200 on **admin123** (so this is the password).

- Now we can login into the admin page using the password and username.



The screenshot shows a dark-themed login interface. At the top, the word 'Login' is displayed. Below it, there are two input fields: 'Email' containing 'admin@juice-sh.op' and 'Password' containing 'admin123'. A green border highlights the password field. To the right of the password field is an eye icon for toggling visibility. Below the password field is a link that says 'Forgot your password?'. At the bottom, there is a blue 'Log in' button with a right-pointing arrow icon, and a checkbox labeled 'Remember me'.

13. Now we will try to reset Jim's password using the forgot password option on the login page.

- Jim's security question is set to "Your eldest siblings middle name?".
- And since we have gathered information on jim we search for "**Jim star trek**" and we find the following data.

Family	George Kirk (father) Winona Kirk (mother) George Samuel Kirk (brother) Tiberius Kirk (grandfather) James (maternal grandfather) Aurelan Kirk (sister-in-law) Peter Kirk (nephew) 2 other nephews
---------------	---

❖ As you can see, he has only one brother with the name **George Samuel** and when we try, we find out that the answer for the security question is **Samuel**.

- Now let's change the password to whatever we want to be.

Forgot Password

Email

Security Question

New Password

Password must be 5-20 characters long. 8/20

Repeat New Password

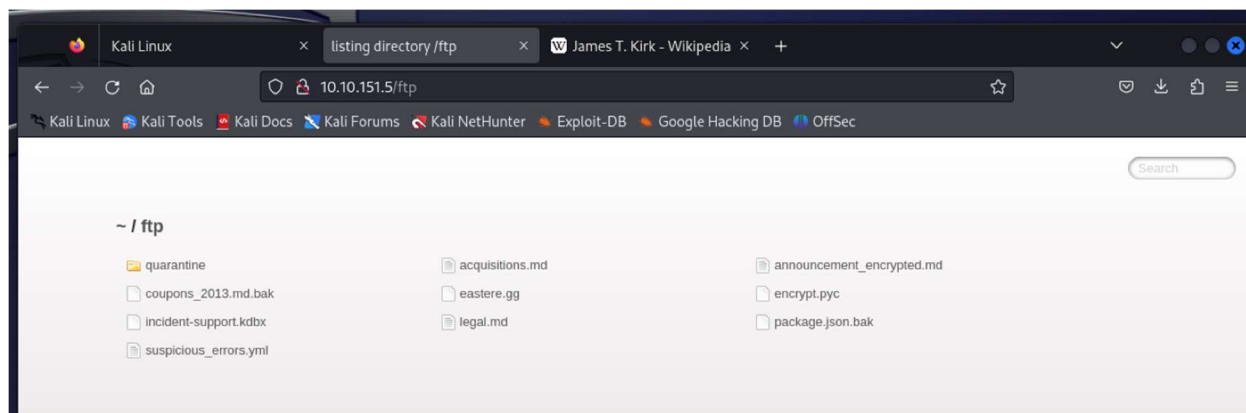
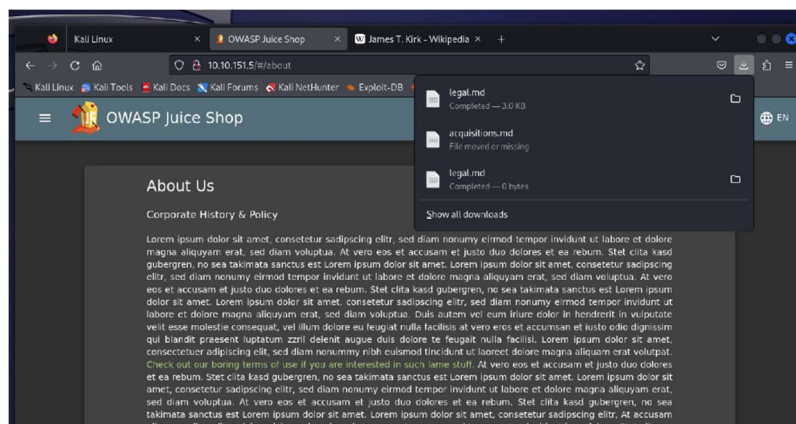
8/20

☐ Show password advice

[Change](#)

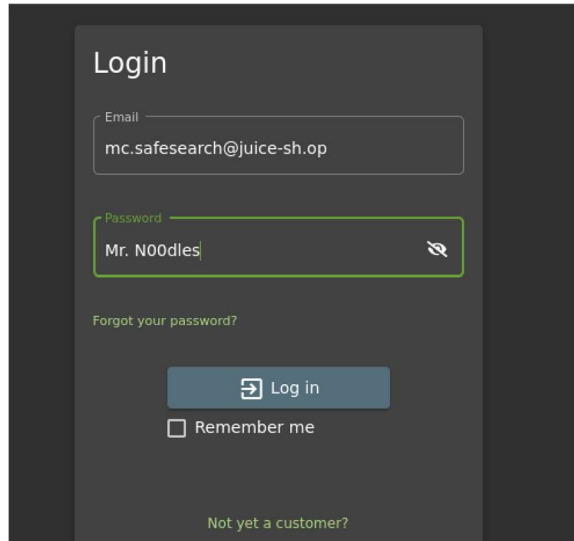
14. Now we will try to access sensitive information, in our case lets go to the about us page and click the link and we will download a file.

- Now on the url let's navigate to the subdirectory of ftp and we will find a page with juicy files and let's download **acquisition.md** file.

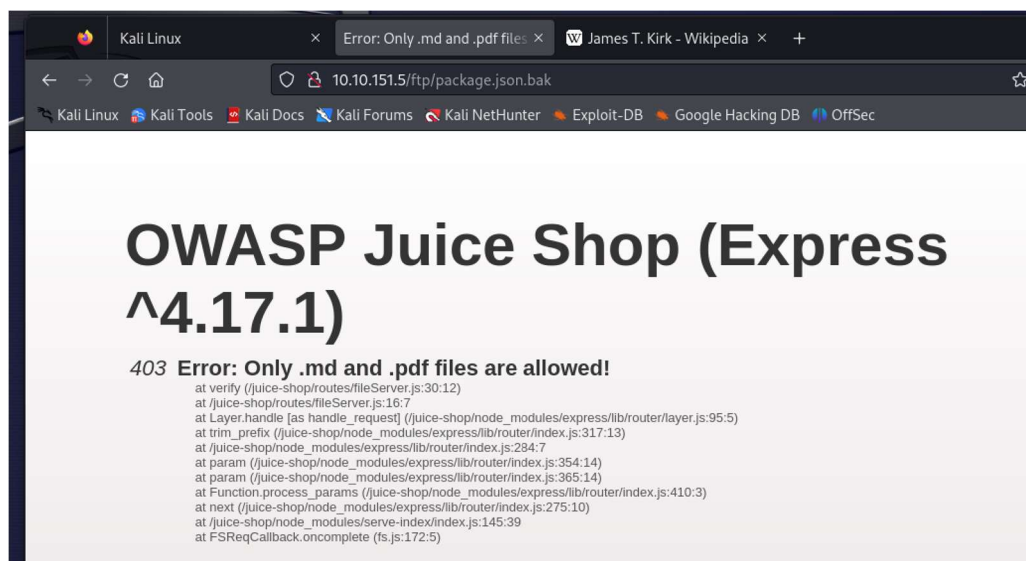


15. Next, we will listen to music and try to get the username and password by listening to the music.

- From the music we find that the singer is disclosing information which might be helpful to us.



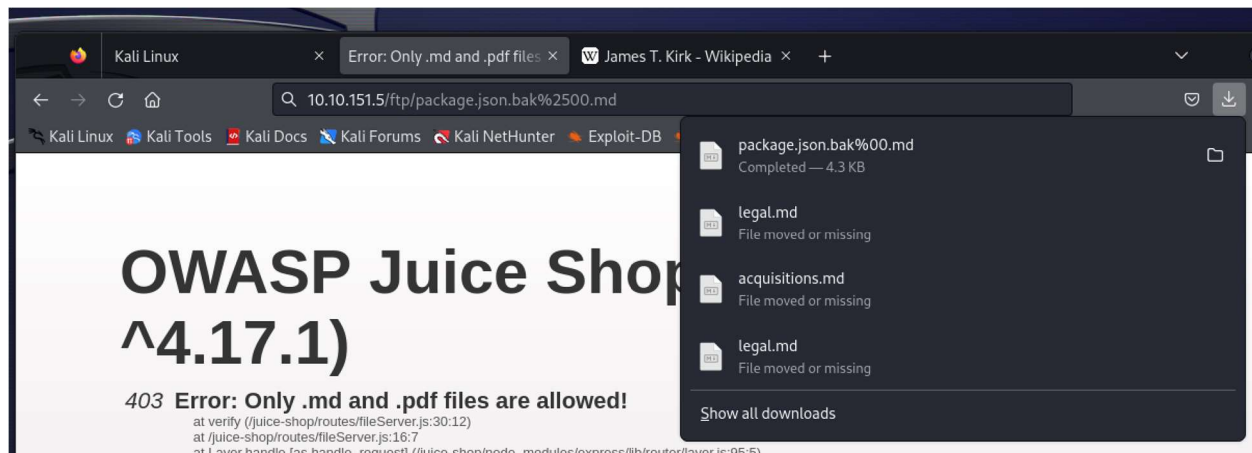
16. Now we will try to download a file called **package.json.bak** from the ftp page but we encounter a **403 error** which means access is forbidden.



- To bypass this error, we will use **Poison Null Byte** attack by adding **%2500** and then a **.md** to the end will bypass the 403 error.

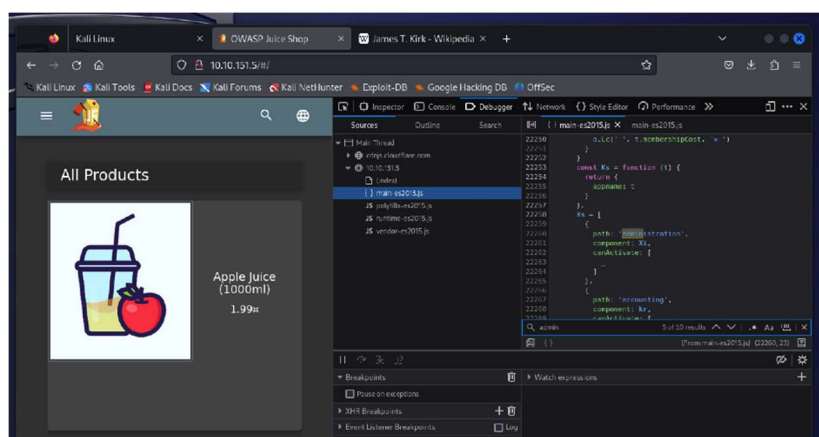
NOTE

- ❖ Poison Null Byte attack places a NULL character in the string at a certain byte, the string will tell the server to terminate at that point, nulling the rest of the string.

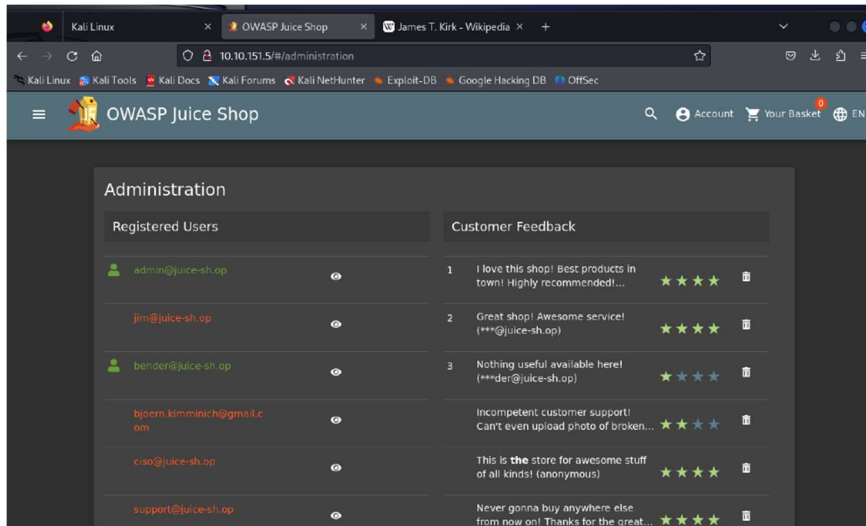


17. Here we will see privilege escalation but first let's see two types of privilege escalation:

- **Horizontal Privilege Escalation:** Occurs when a user can perform an action or access data of another user with the same level of permissions.
 - **Vertical Privilege Escalation:** Occurs when a user can perform an action or access data of another user with a higher level of permissions.
- ❖ Now to access the administration page we right click on the page and click inspect and go to the **debugger** and there open the javascript file **main-es2015.js**.
 - Then searching for administration, we see there is a path and when we try to navigate to it we see 403 error (Forbidden).

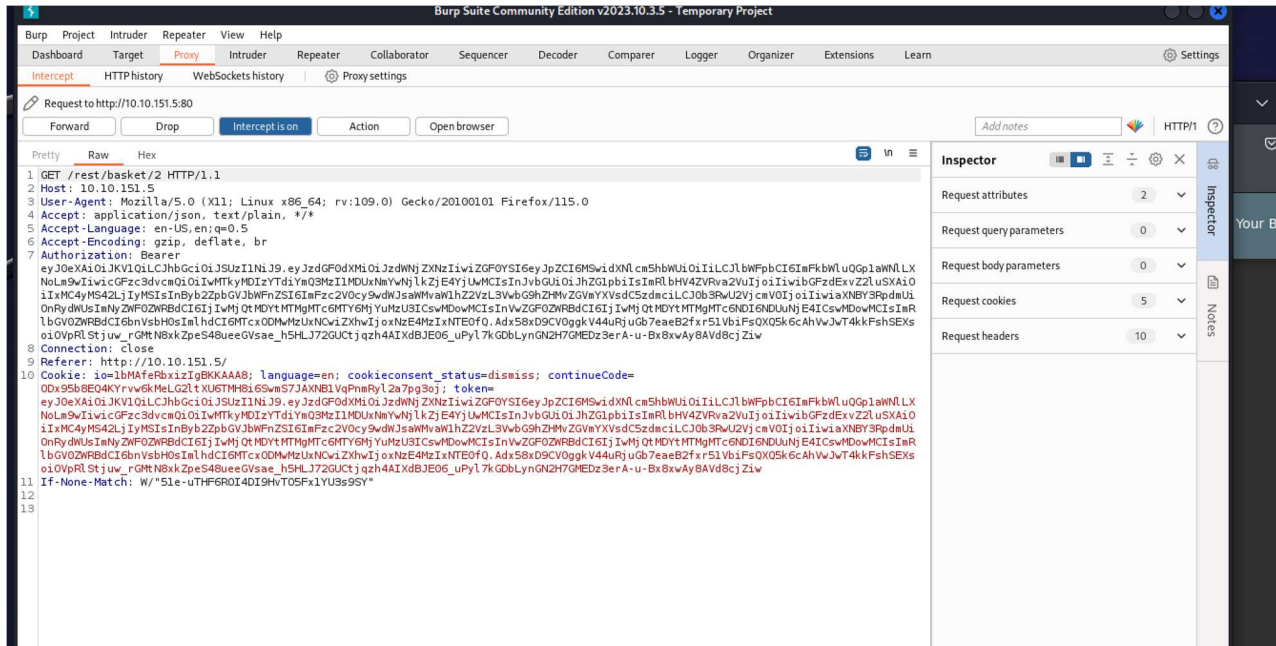


- When we login using the admin username and password and navigate to the administration page, this is what it looks like.

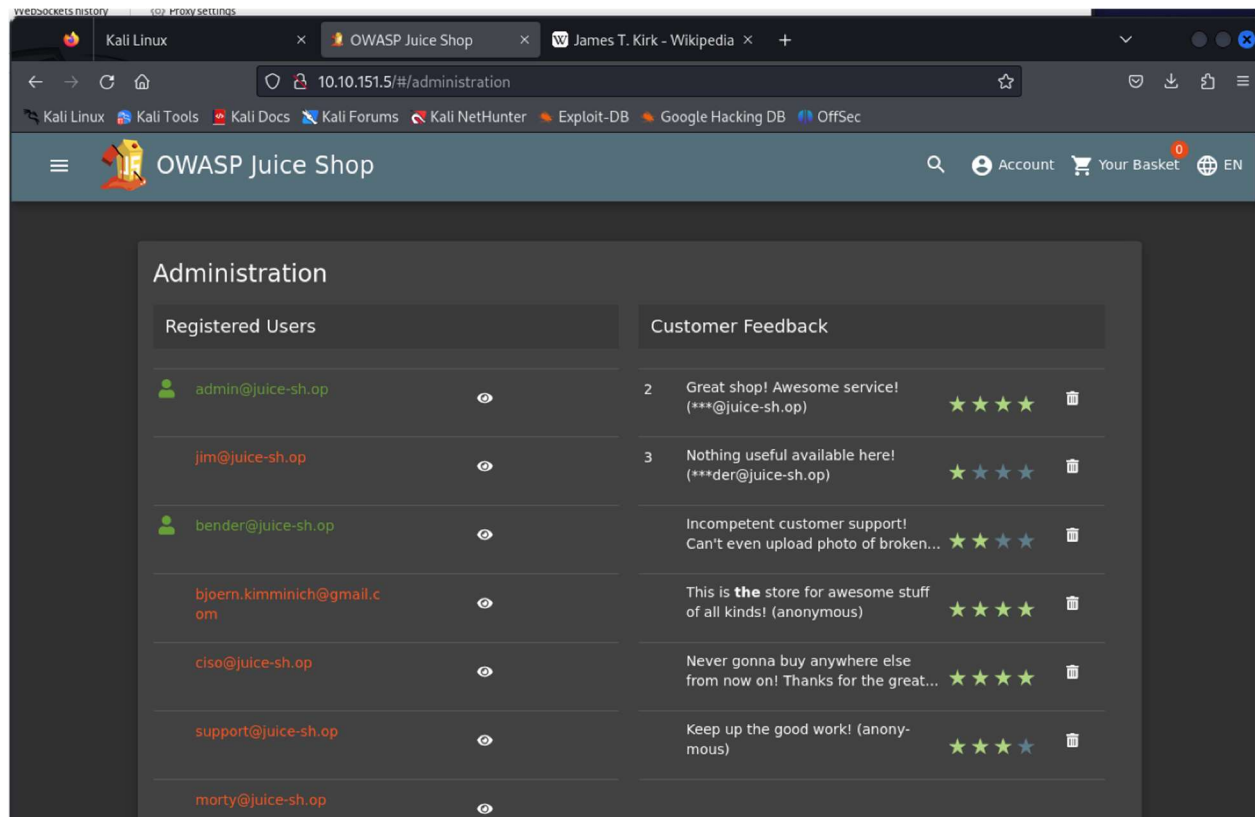


18. Login to the Admin account and clicking on 'Your Basket' and capturing the request using burp suite and altering the request.

- we are going to change the number 1 after /basket/ to 2 on GET



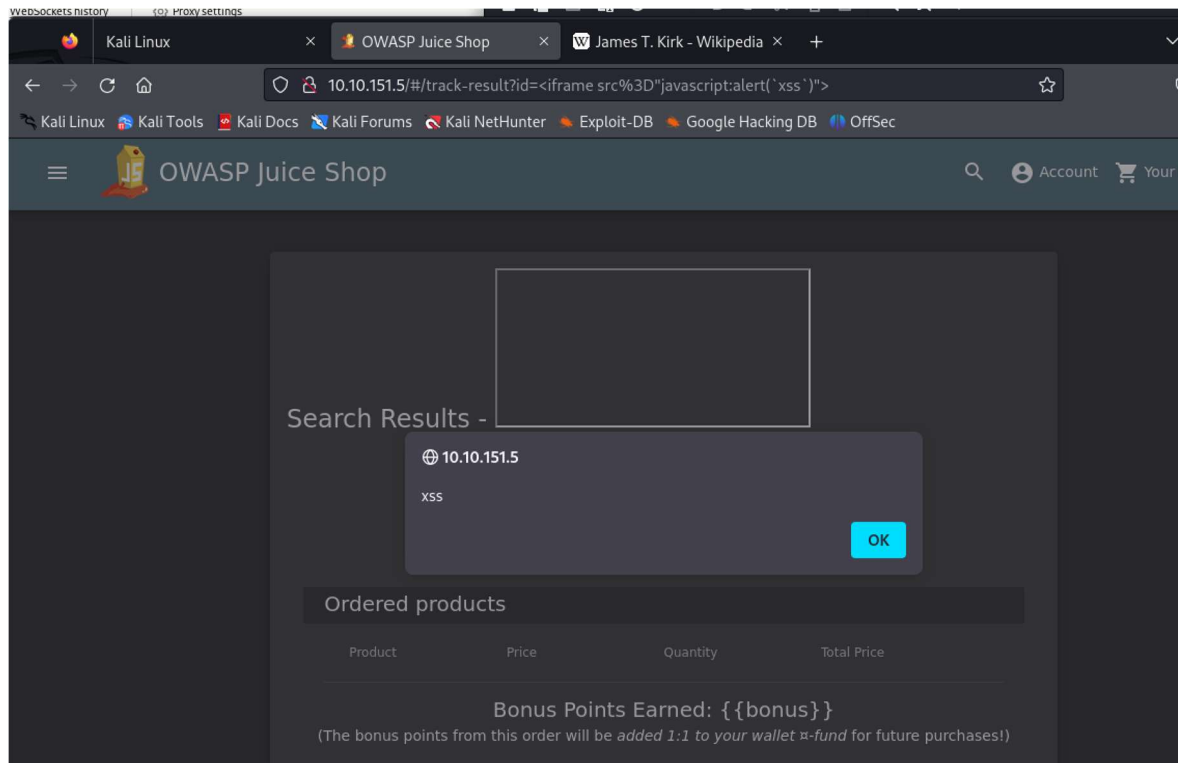
19. We can also delete staff after privilege escalation, for instance we will delete the review with 5 stars on the administration page we saw above.



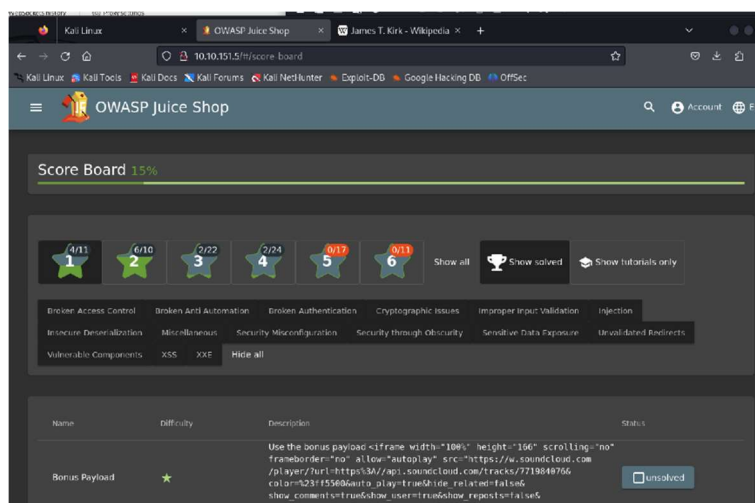
20. Here we will see XSS (Cross site scripting), so let's define it and its types.

- ❖ **XSS**: is a vulnerability that allows attackers to run javascript in web applications.
 - **DOM XSS**: uses the HTML environment to execute malicious javascript.
 - **Persistent XSS**: is javascript that runs when the server loads the page containing it.
 - **Reflected XSS**: is javascript that is run on the client-side end of the web application.
- ❖ Now to perform DOM XSS attack we are going to use a HTML tag called **iframe** with javascript alert tag.
 - `<iframe src="javascript:alert(`xss`)">` we will type this on our search bar and attack the server cause it doesn't have correct input sanitation.
 - This type of XSS is called Cross-Frame Scripting.

- ❖ To perform a reflected XSS, we will be doing the following:
 - Login to the admin page and navigate to the order history
 - Then click the truck icon and you will see the truck result on the url with id=
 - Now replace what is after the id= with `<iframe src="javascript:alert(`xss`)">` on the url and run the script



21. Finally, we will explore the `/#/score-board` and see what tasks we have done



22. Last but not least the accomplishments page

