PSP0201
Week 2
Write-Up

Group Name : Fsociety

Members :

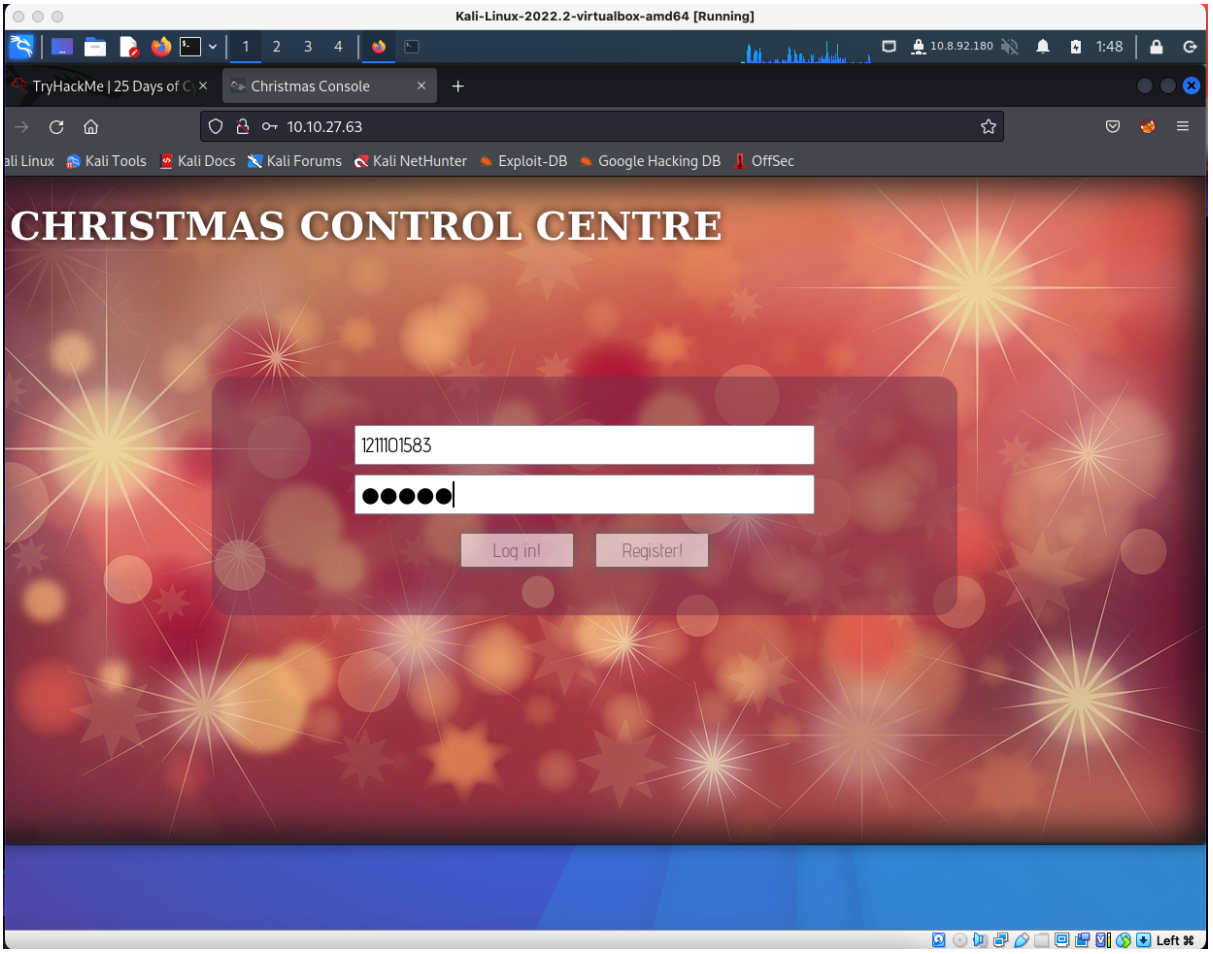
ID	Name	Role
1211102908	Wan Muhammad Ilhan Bin Wan Zil Azhar	Leader
1211101583	Luqman Hakim Bin Noorazmi	Member
1211203101	Jazlan Zuhair Bin Mohamed Zafrualam	Member
1211102054	Mithesh Kumar	Member

Day 1
(A Christmas Crisis)

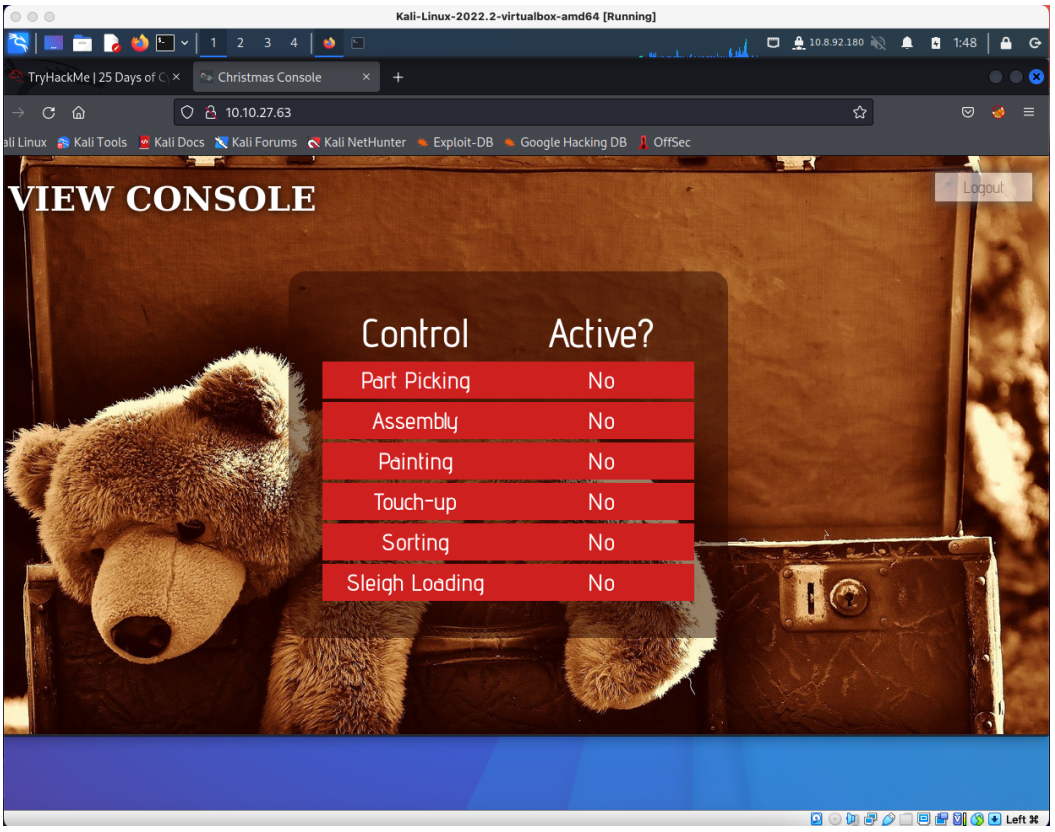
Tools: Kali Linux, Firefox

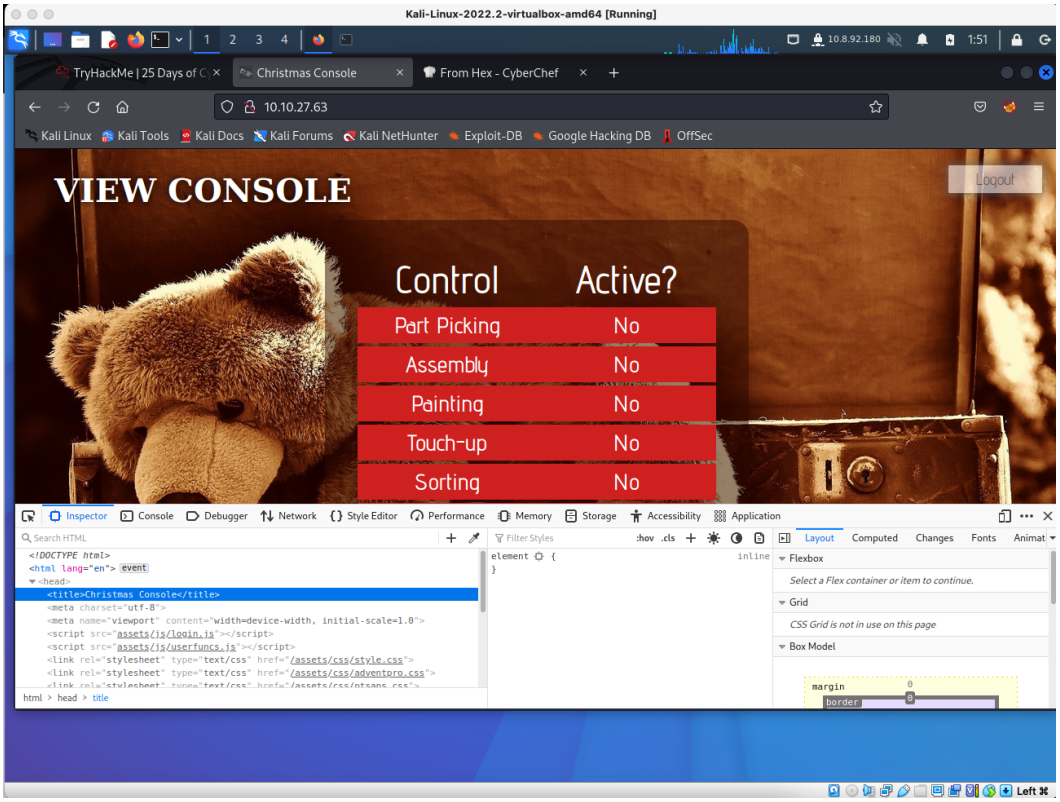
Question 1:

The URL of the website can be obtained from the machine (IP address). Copy and paste the URL and complete the registration and login into the website.



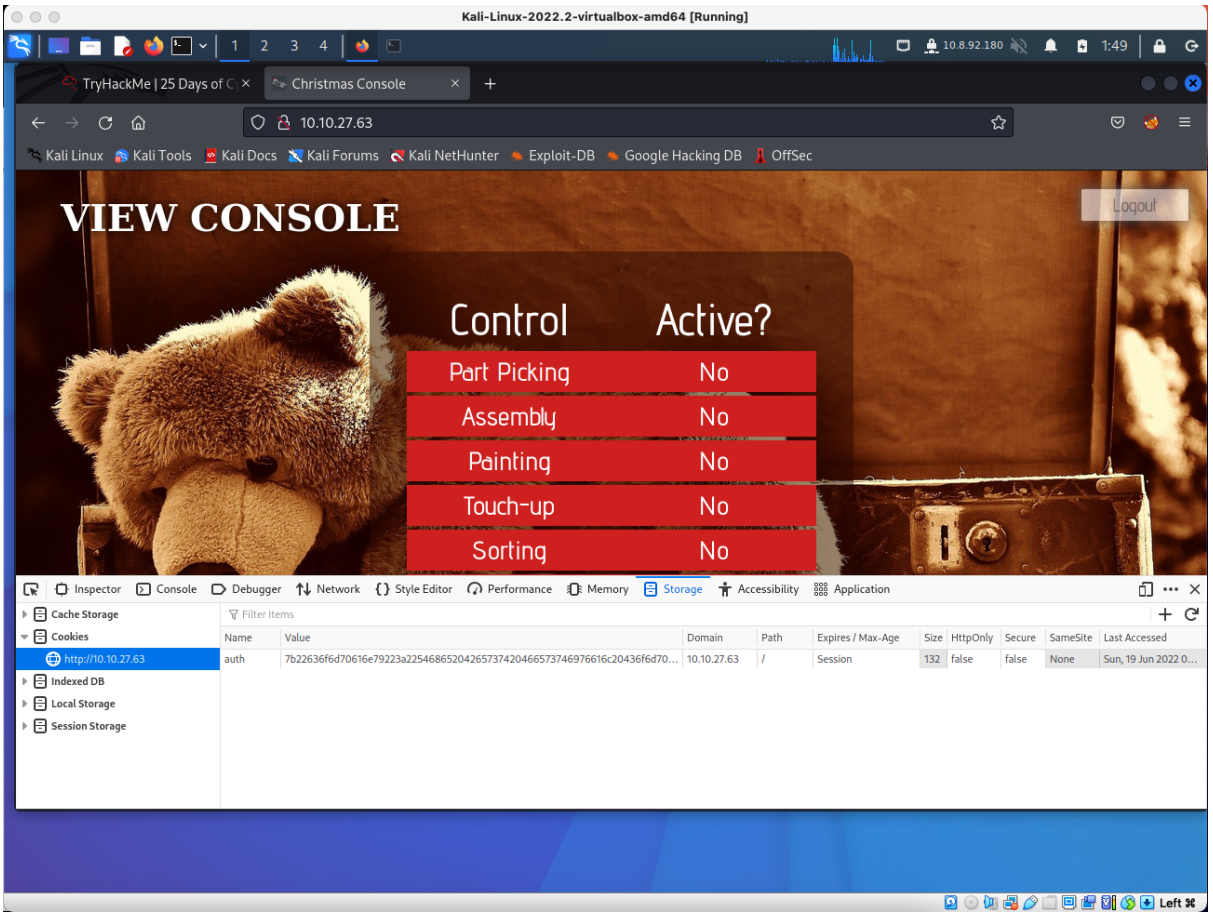
After pressing F12, the website title can be obtained by looking at the HTML title tag





Question 2:

The name of the cookie can be obtained from Storage > Cookies > http://10.10.27.63. It's the value under "Name".



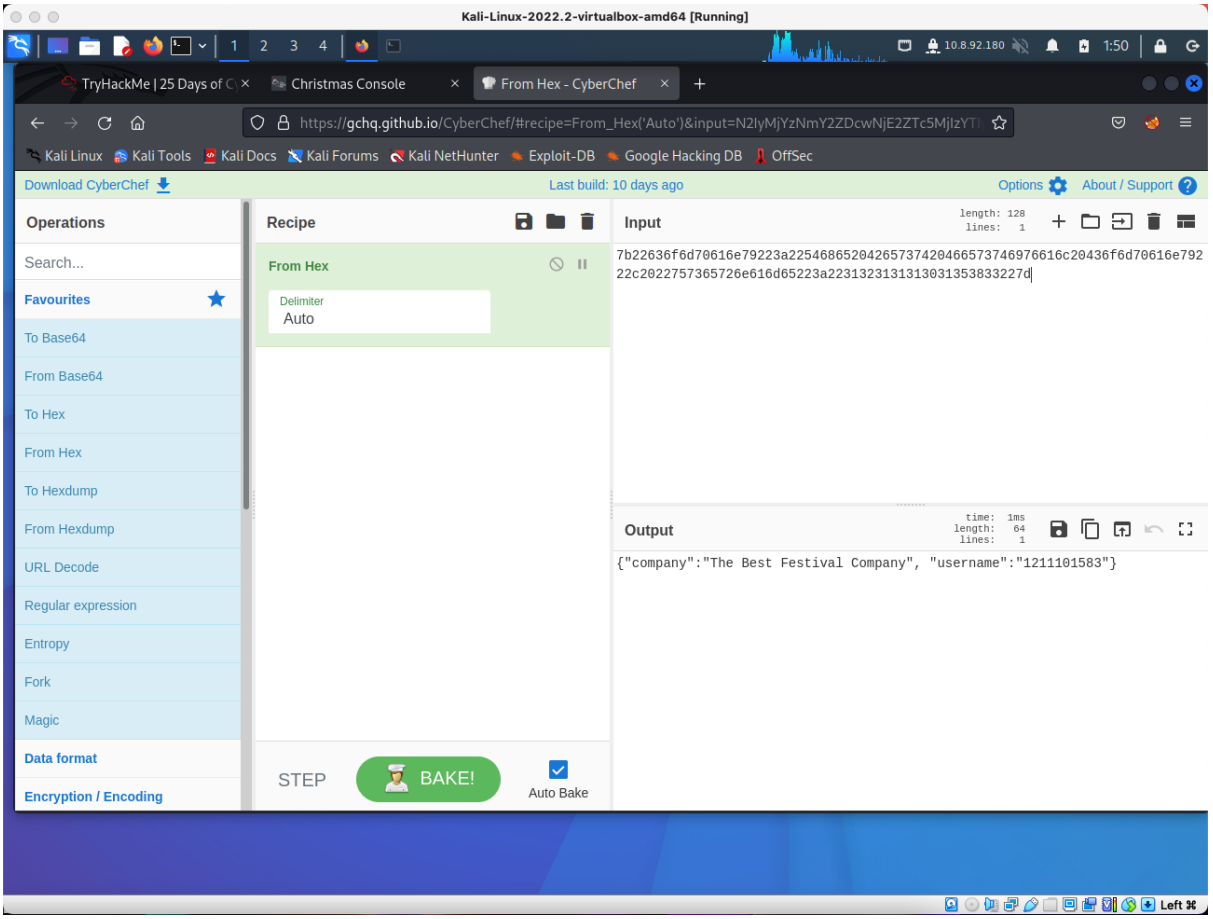
Question 3:

The value of the cookie is in Hexadecimal format.

```
7b22636f6d70616e79223a225468652042657374204657374976616c20436f6d70616e792
22c2022757365726e616d65223a223132313131303135383322 7d
```

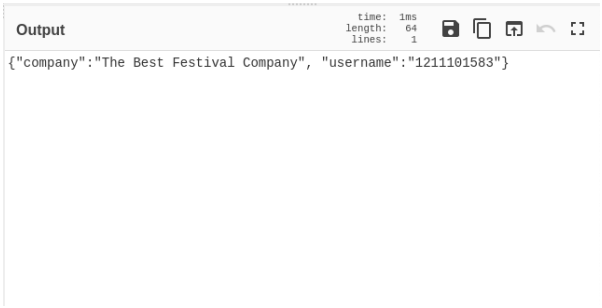
Question 4:

After decoding the cookie value in cyberchef.com, it was later discovered that the data was stored in JSON format.



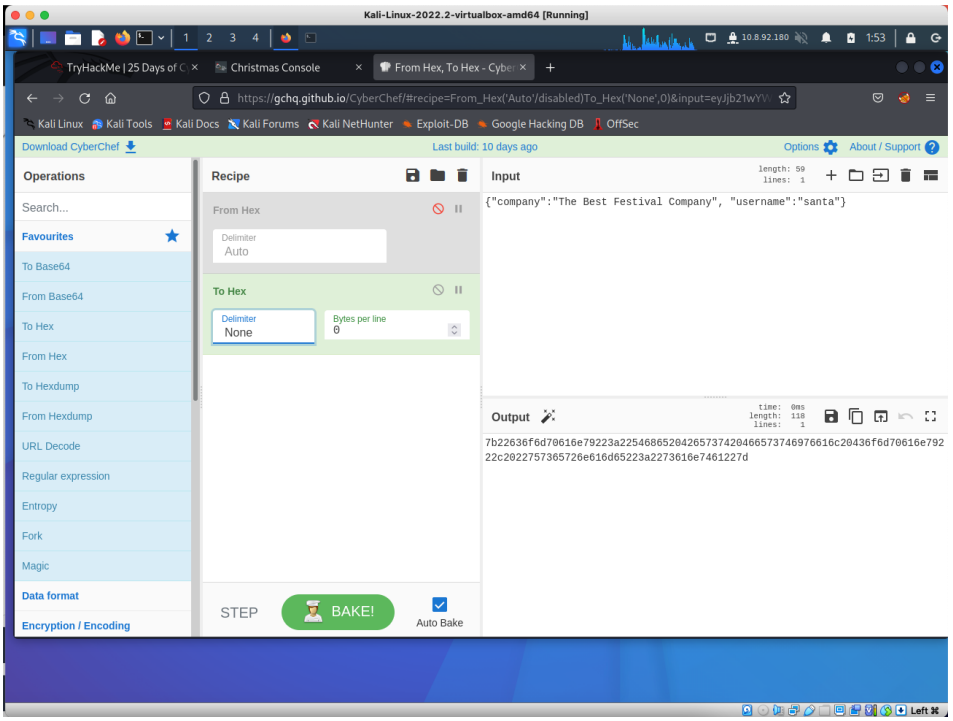
Question 5 and Question 6:

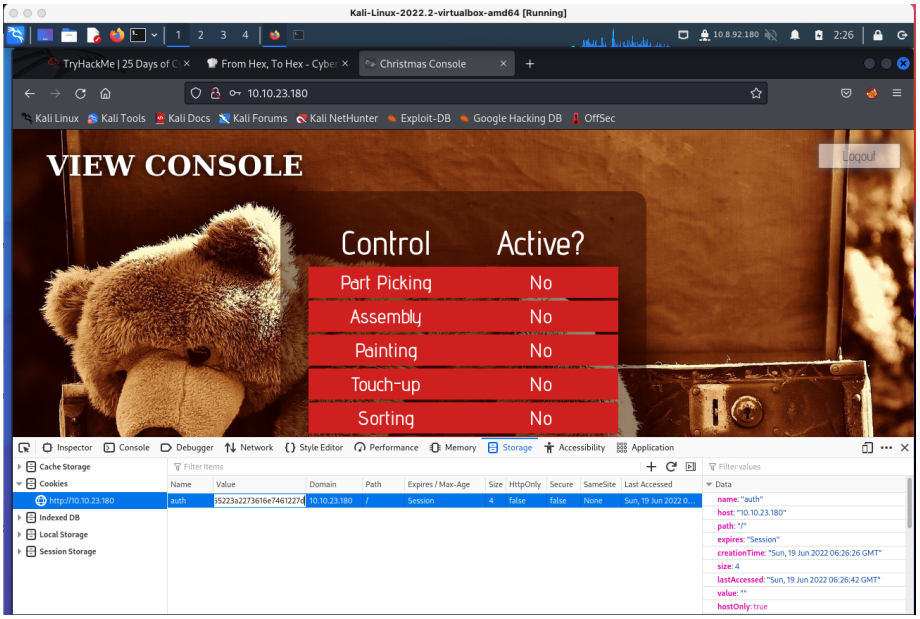
Q5: The value for the company field is *The Best Festival Company*
Q6: The other field in the cookie is username with the current user's username as value



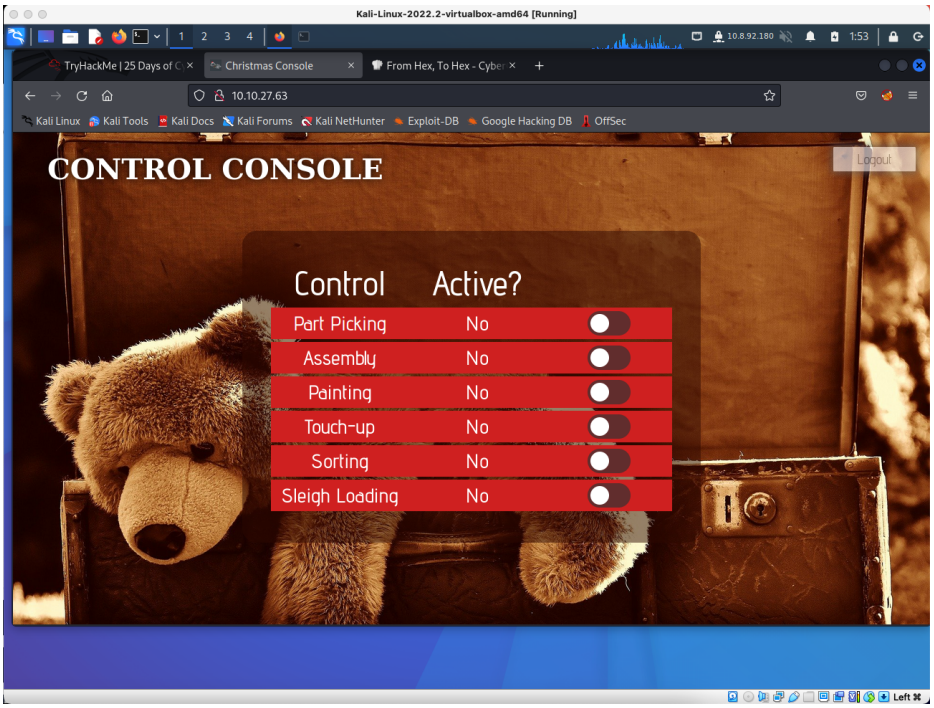
Question 7:

By copying the data obtained from the cookie, we can change the current value on the website with the one that's the username has been changed to santa's.



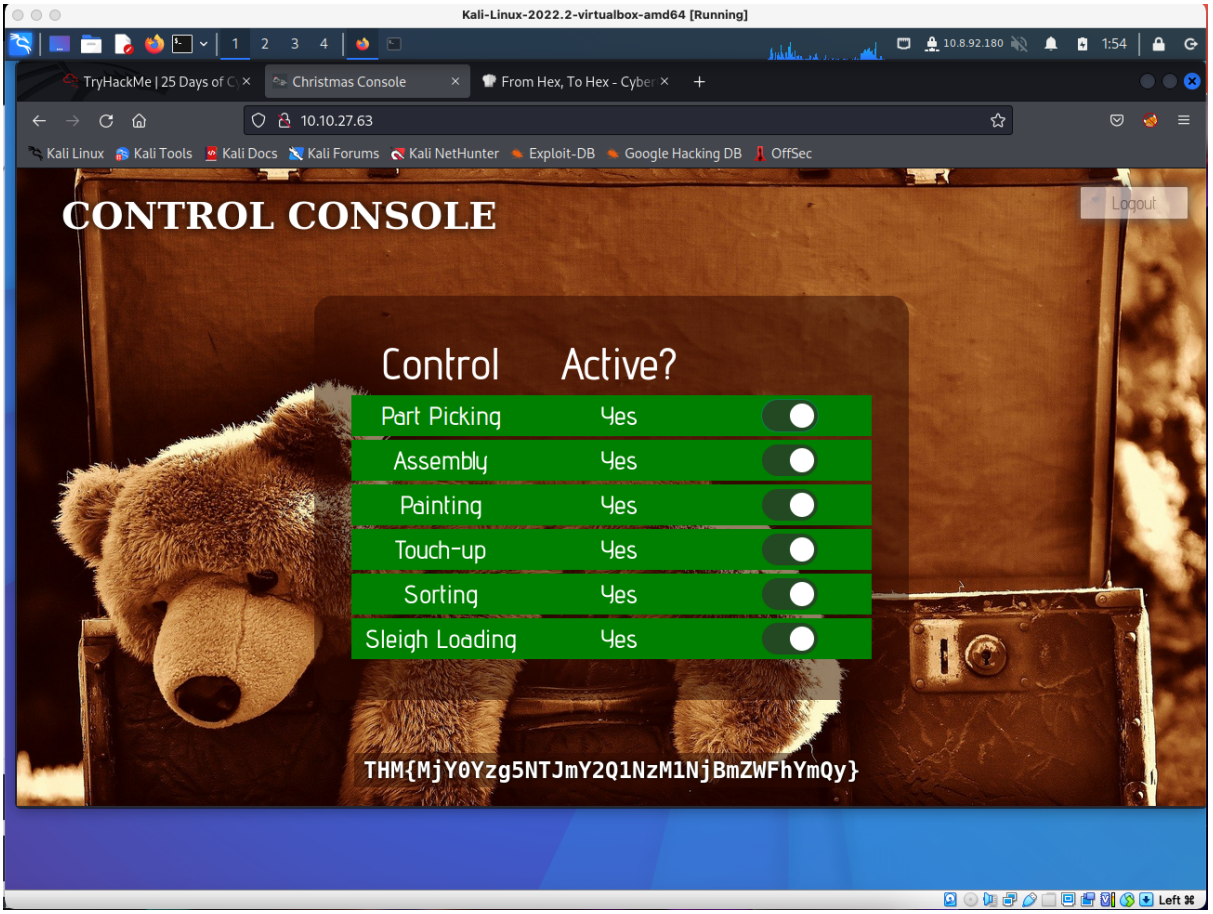


After refreshing the page, we are now logged in to the website as santa.



Question 8:

After activating all of them, the flag is displayed.

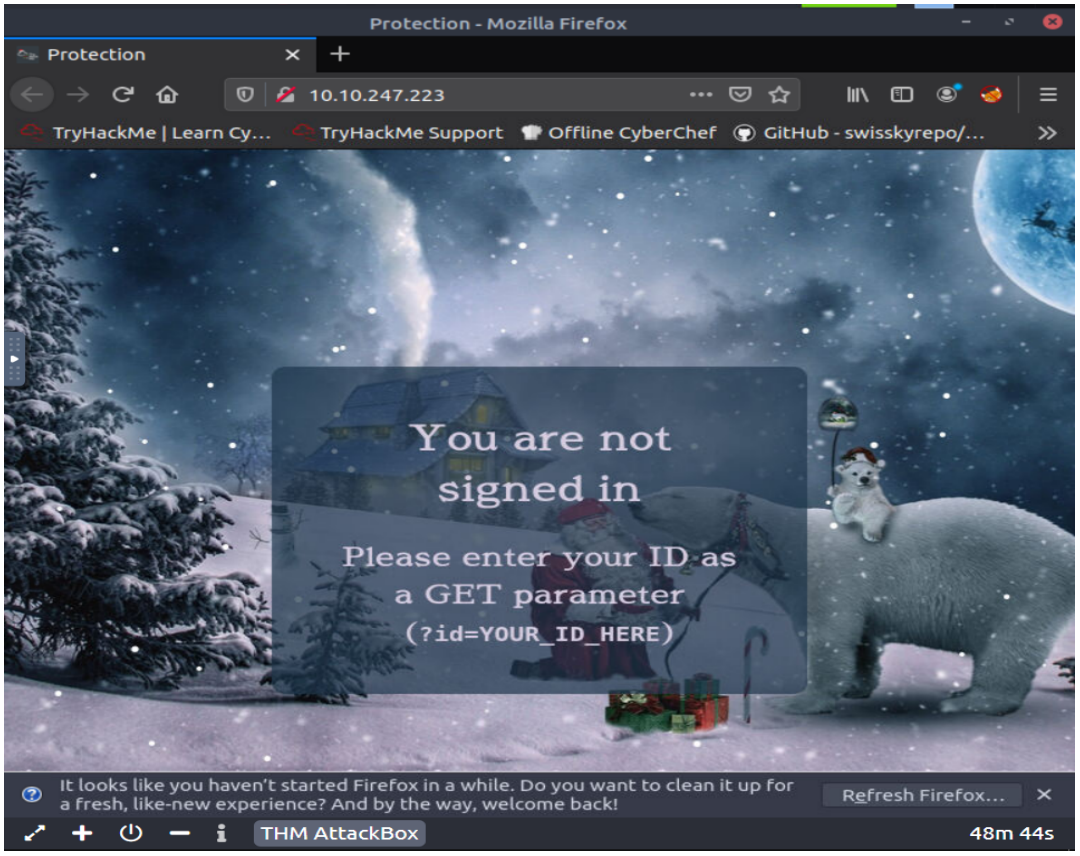


Day 2
(The Elf Strikes Back!)

Tools : Kali Linux, Terminal, Firefox, Text Editor

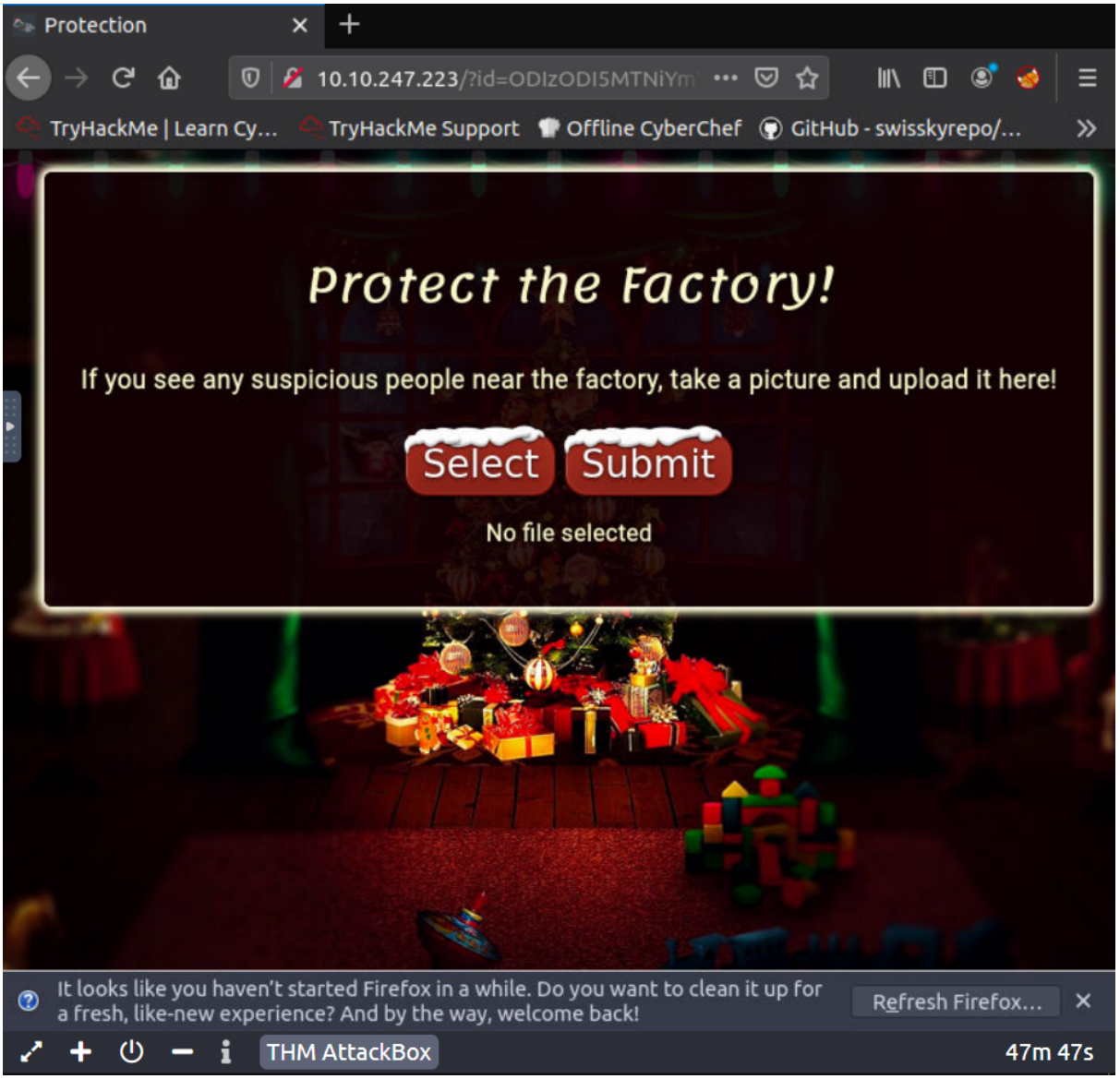
Question 1:

Start by navigating to the displayed IP Address in your browser.



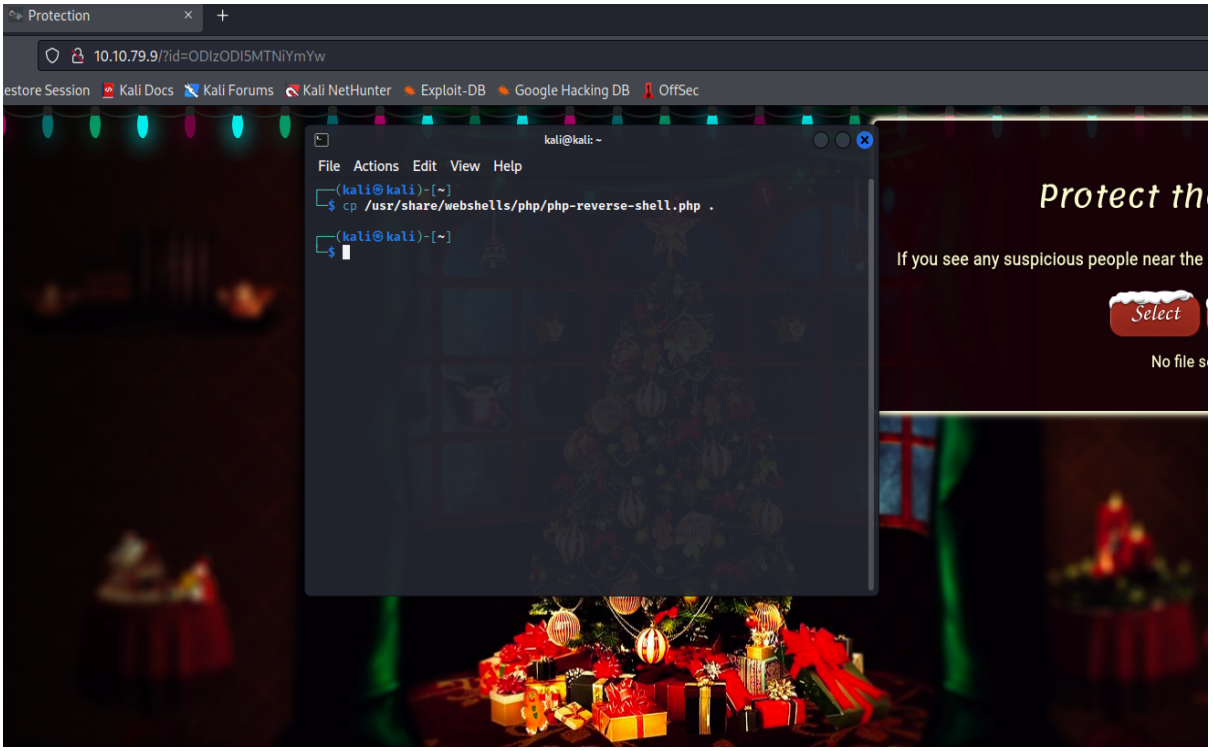
Question 2:

Navigate to the upload section by adding the string of ID to the URL of the page :



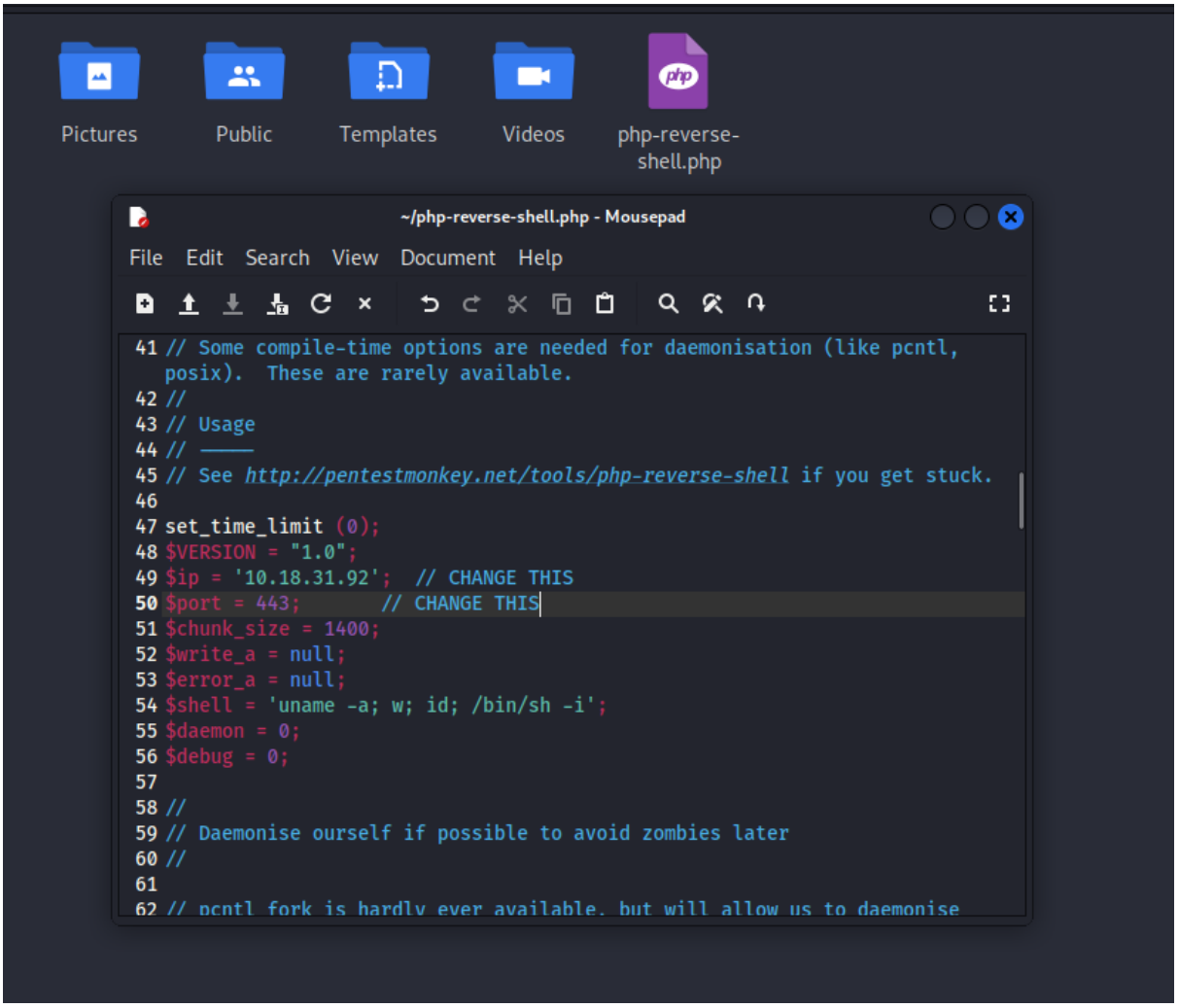
Question 3:

Open terminal and copy the reverse shell directory :



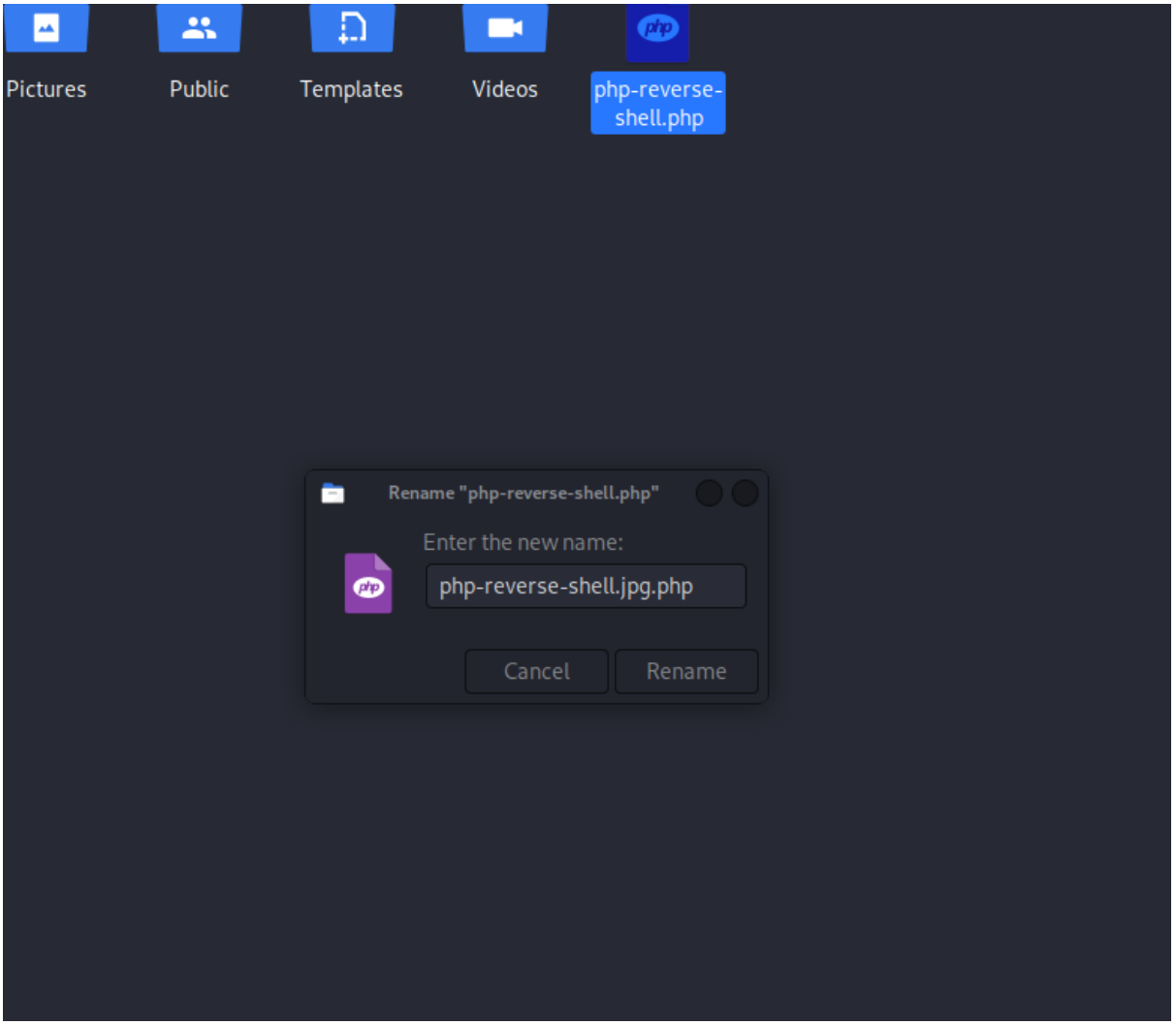
Question 4:

Open the reverse shell and change the $ip to the connected OVPN address and port to 443 :



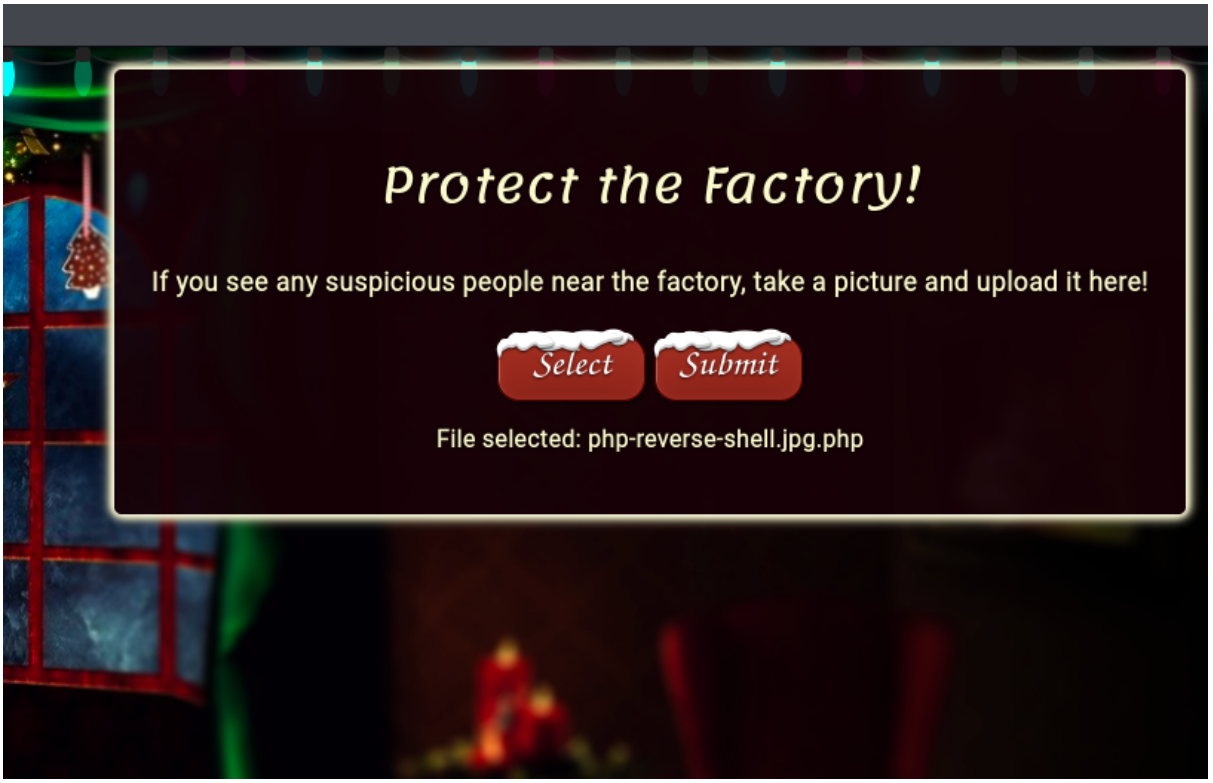
Question 5:

Rename the edited reverse shell as an innocent file format such as jpg, png, etc. :



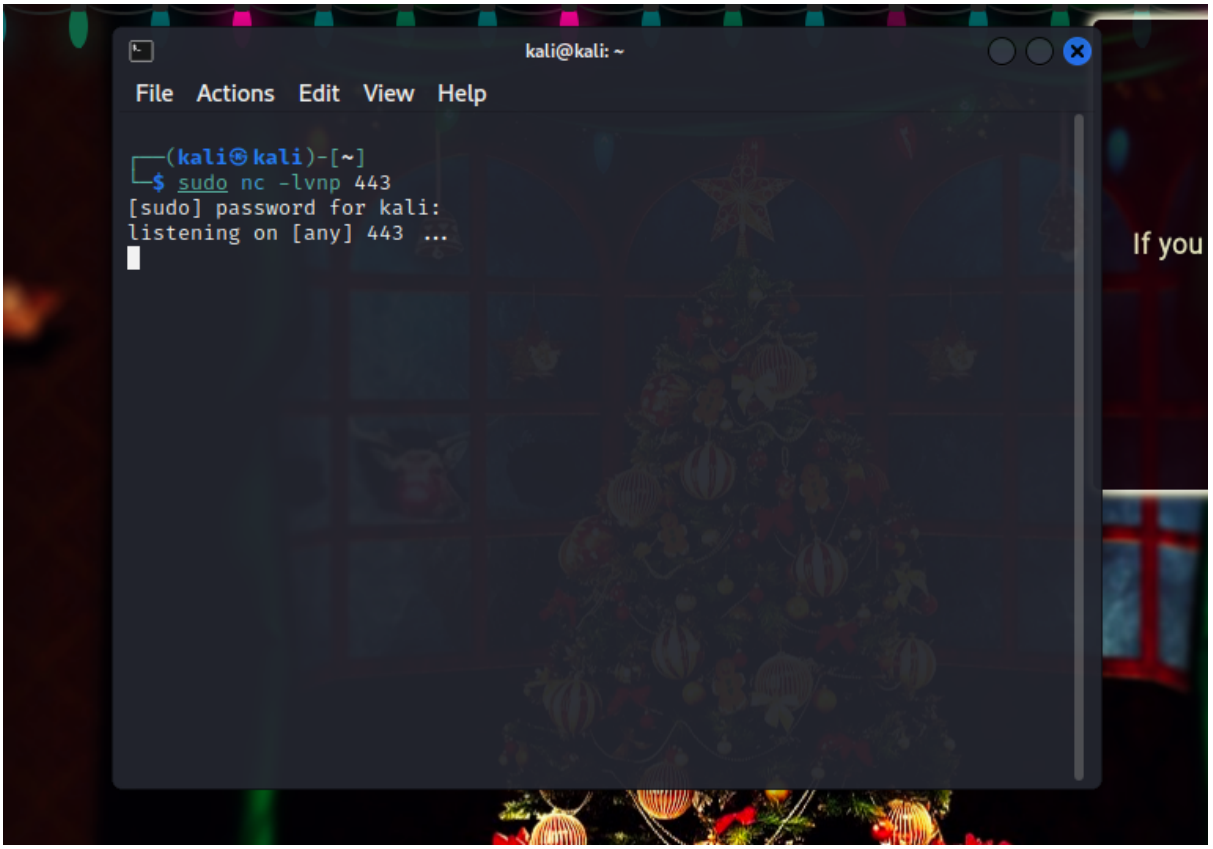
Question 6:

Upload the reverse shell file to the website :



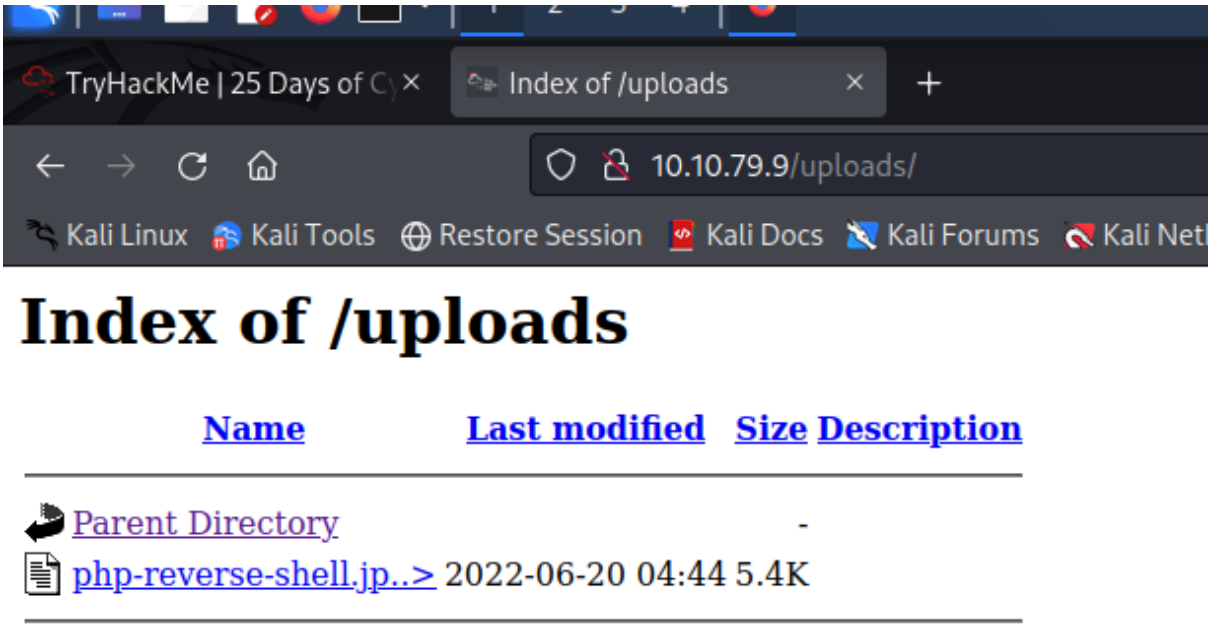
Question 7:

Open terminal and run the command sudo nc -lvpn 443 to start a netcat listener (to receive and read the reverse shell) :



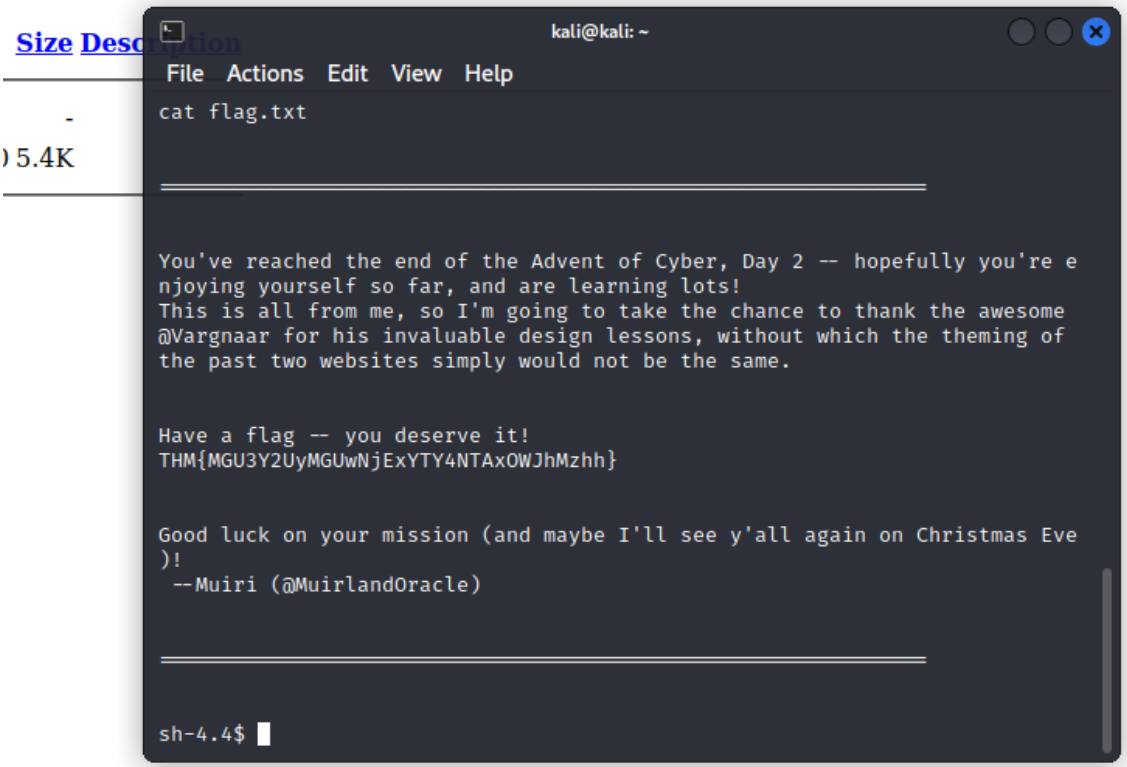
Question 8:

Navigate to the /uploads/ section of the website and find the reverse shell, execute the shell as the listener is running :



Question 9:

Finally, once the listener received the reverse shell. Enter command cat /var/www/flag.txt to get the THM flag :



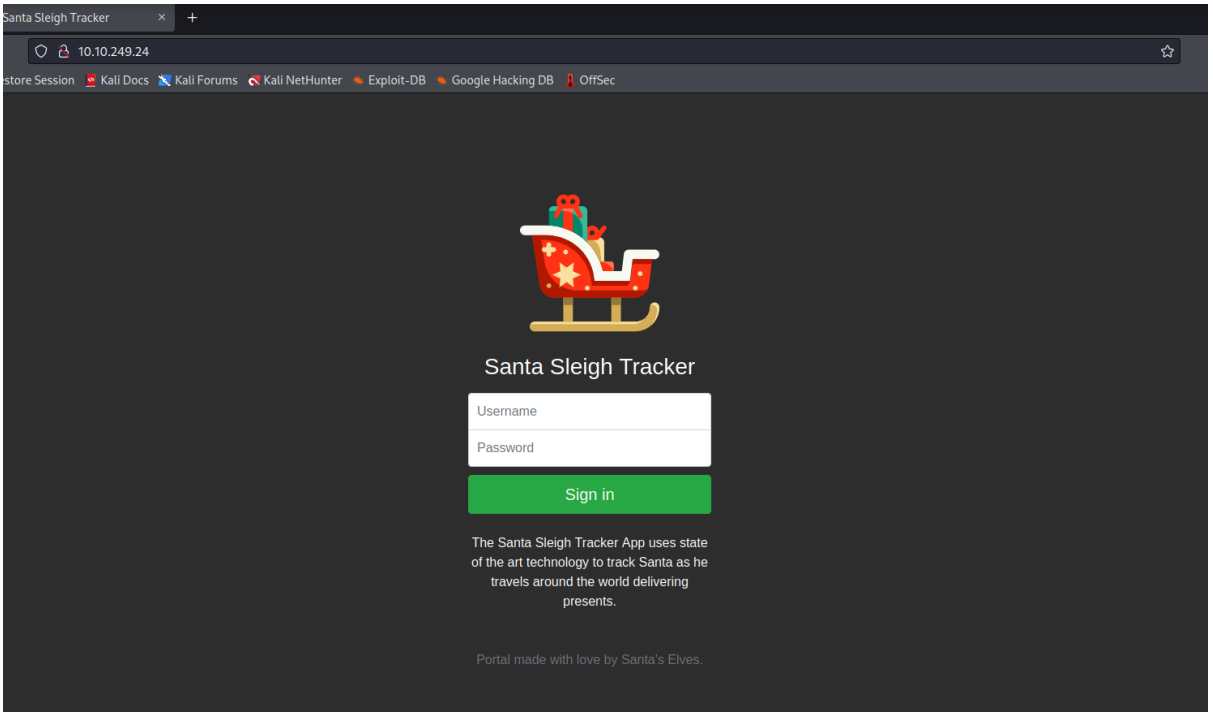
Thought Process/Methodology :

Day 3
(Christmas Chaos)

Tools: Kali Linux, Terminal, Firefox, Burpsuite, FoxyProxy

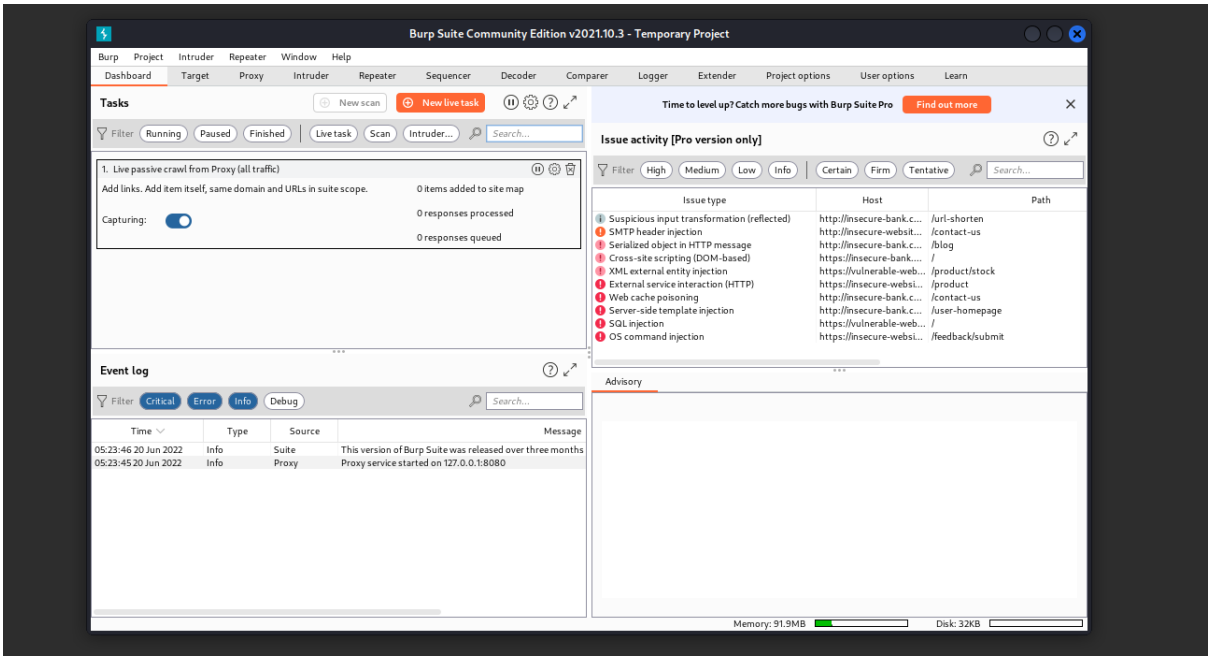
Question 1:

Start by navigating to the displayed IP Address in your browser.



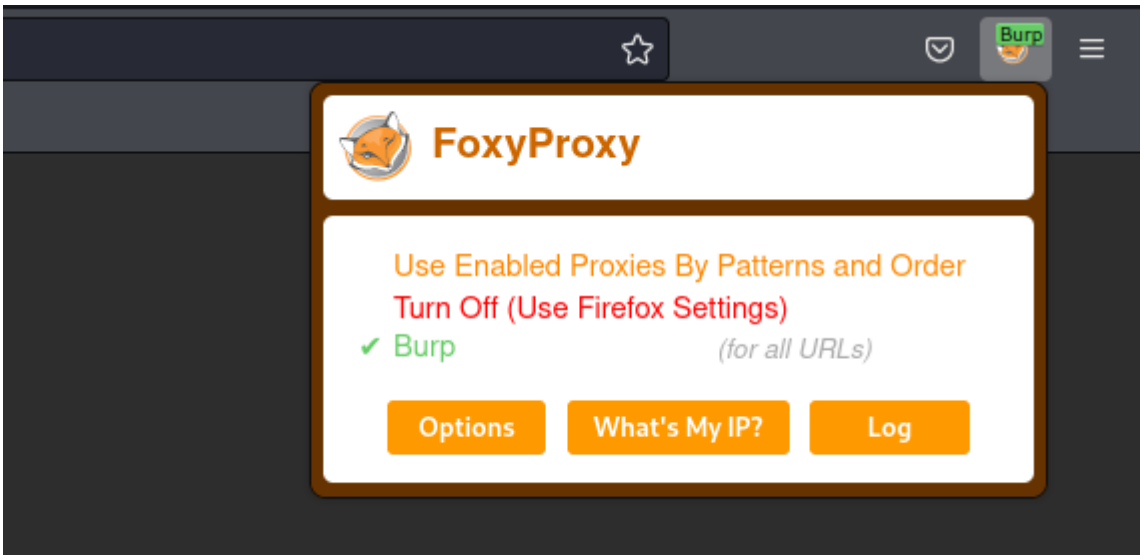
Question 2:

Download Burpsuite and start a new burp :



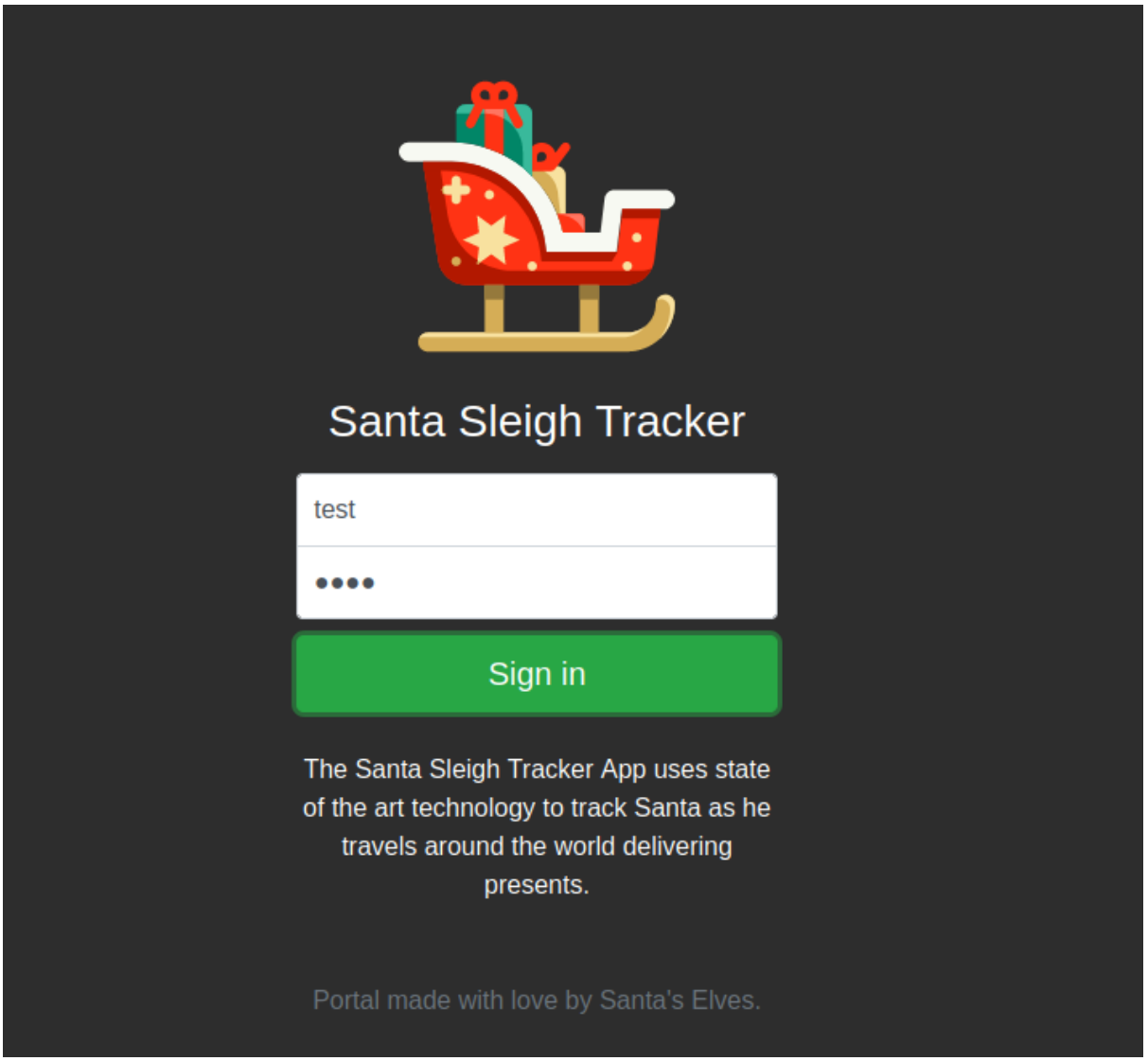
Question 3:

Download FoxyProxy and change to burp mode :



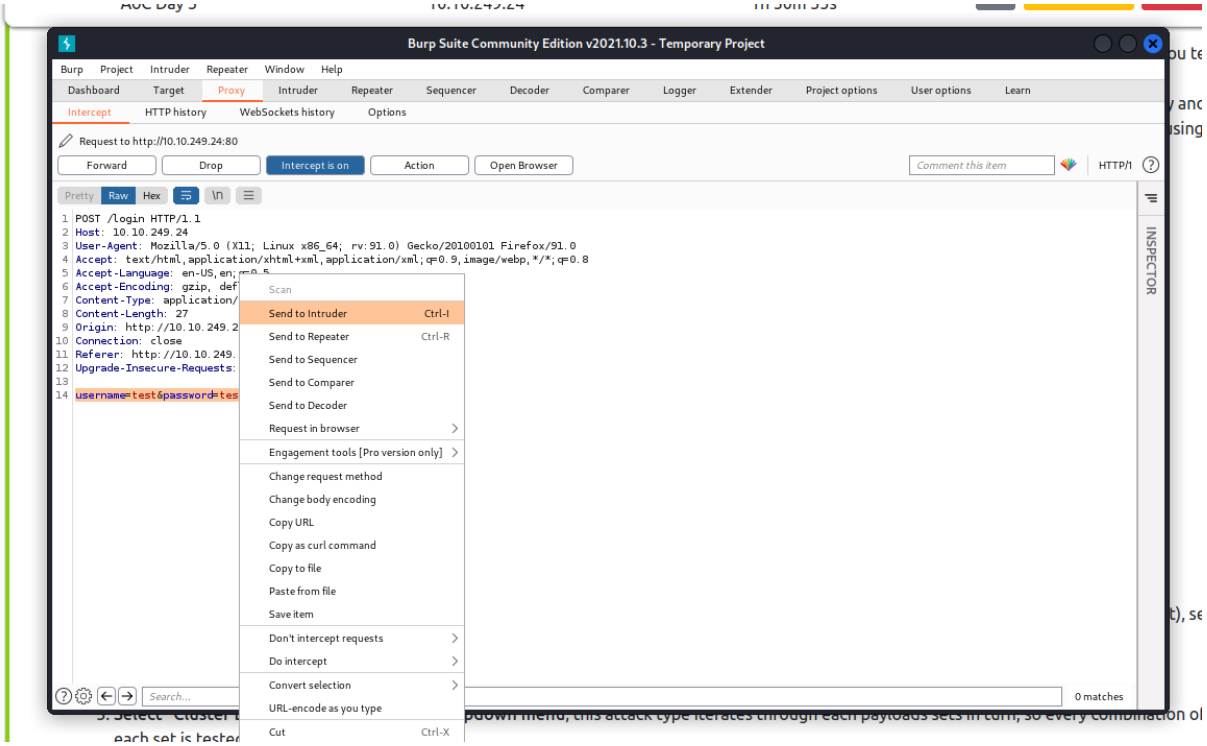
Question 4:

Enter any id and password into the login form and check BurpSuite :



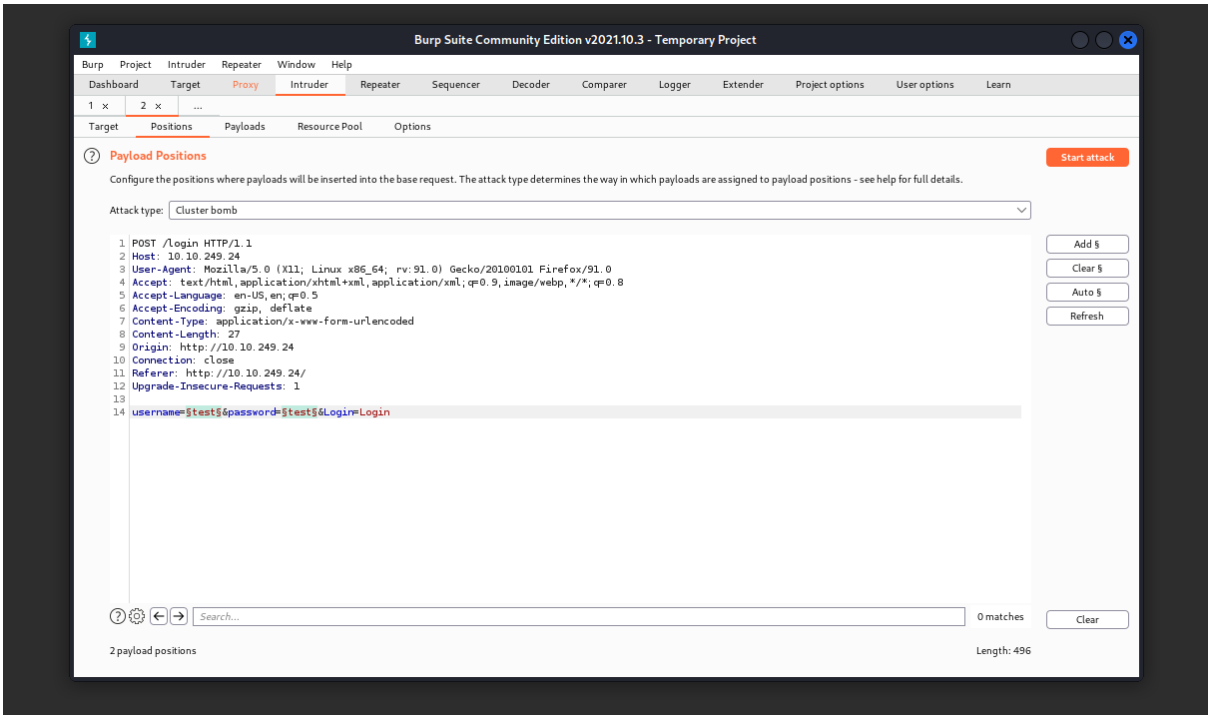
Question 5:

Navigate to ‘Intercept’ in BurpSuite and send the received login info to Intruder :



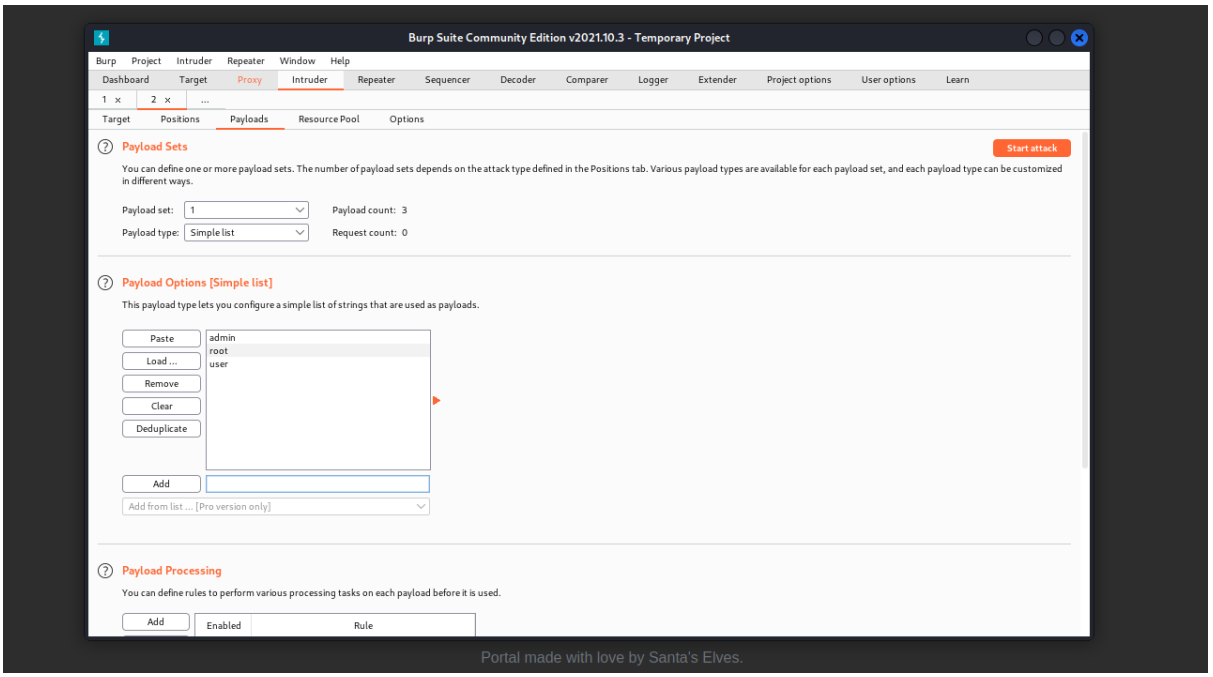
Question 6:

Navigate to ‘Intruder’ and click Add initials to username and password, change the attack type to Cluster bomb :



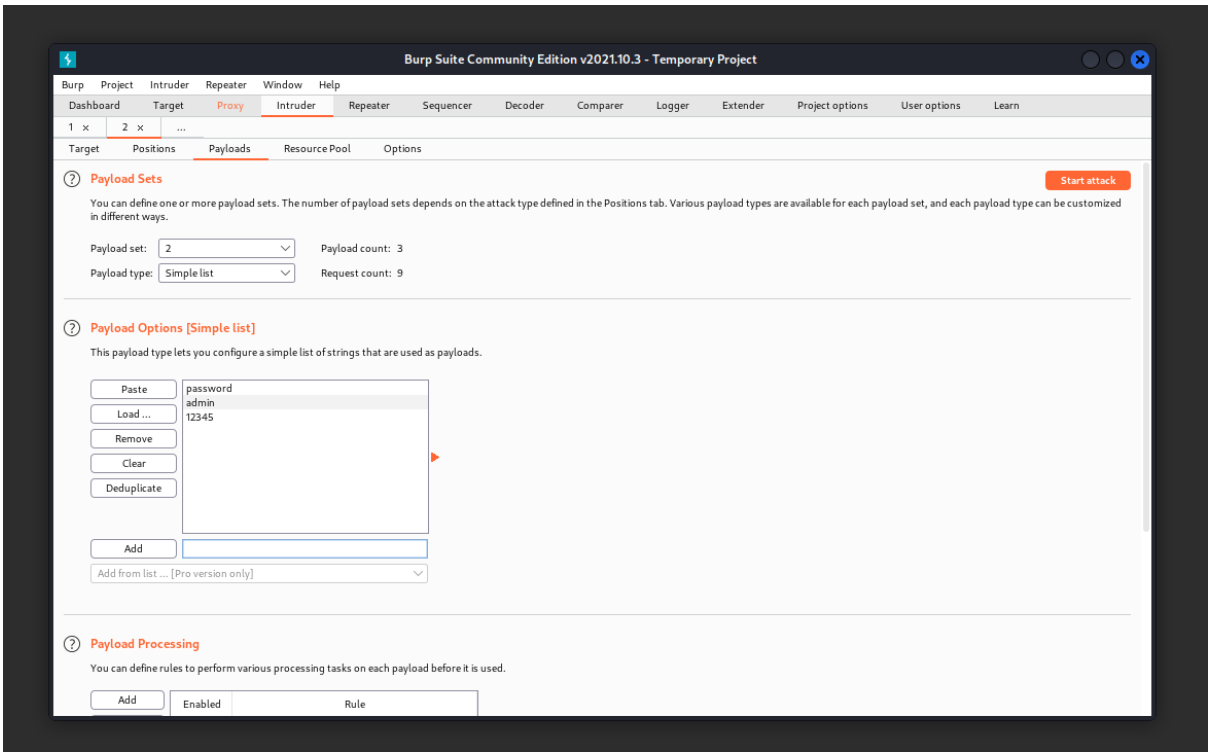
Question 7:

Go to Payload and insert ‘admin, root, user’ as new payload options :



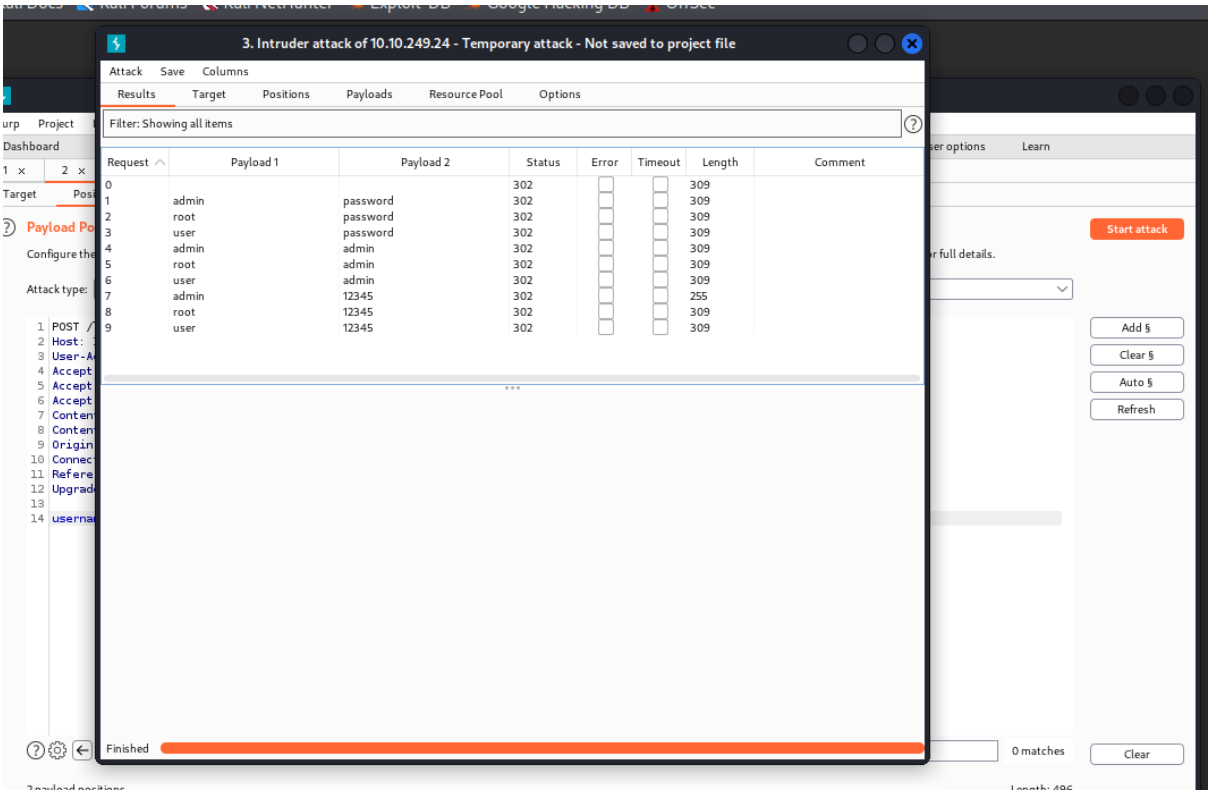
Question 8:

Go to payload set 2 and do the same thing for passwords with ‘password, admin, 12345’ :



Question 9:

Start attack, then filter the results by length. The shortest length should be the correct combination. :



Question 10:

Insert the combination and login to the admin tracker! :

Though Process/Methodology :

Day 4
(Santa's Watching)

Tools: Kali Linux, Terminal, Firefox

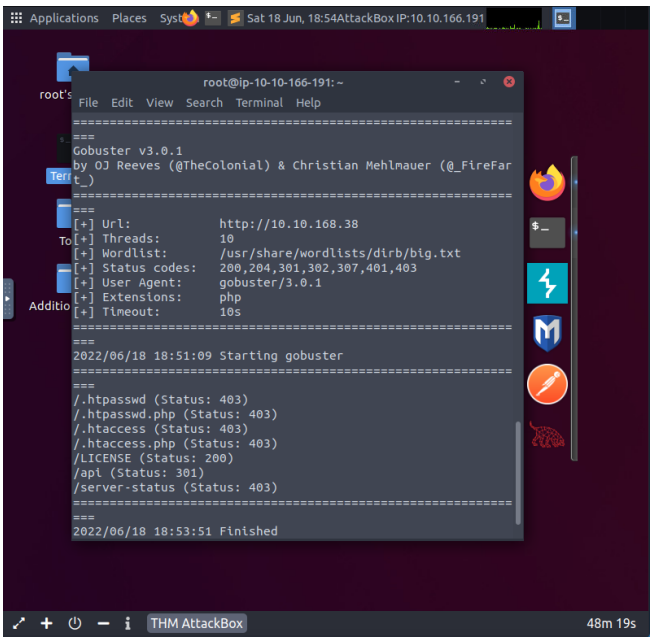
Question 1:

The full command: wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ

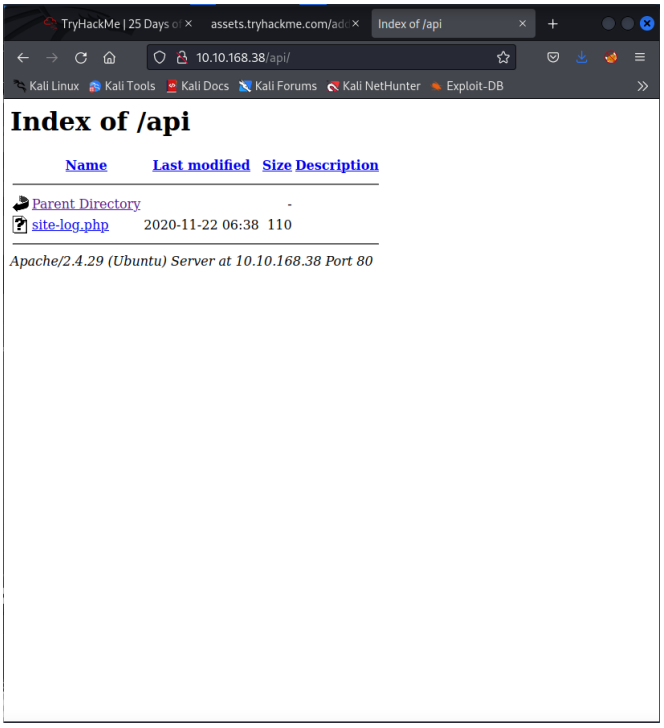
- For wfuzz command
- Wordlist
- URL
- File Extension
- GET Parameter

Question 2:

By using the GoBuster command in the terminal, it was revealed that the file located in the *http://10.10.168.38*'s API directory is *site-log.php*.

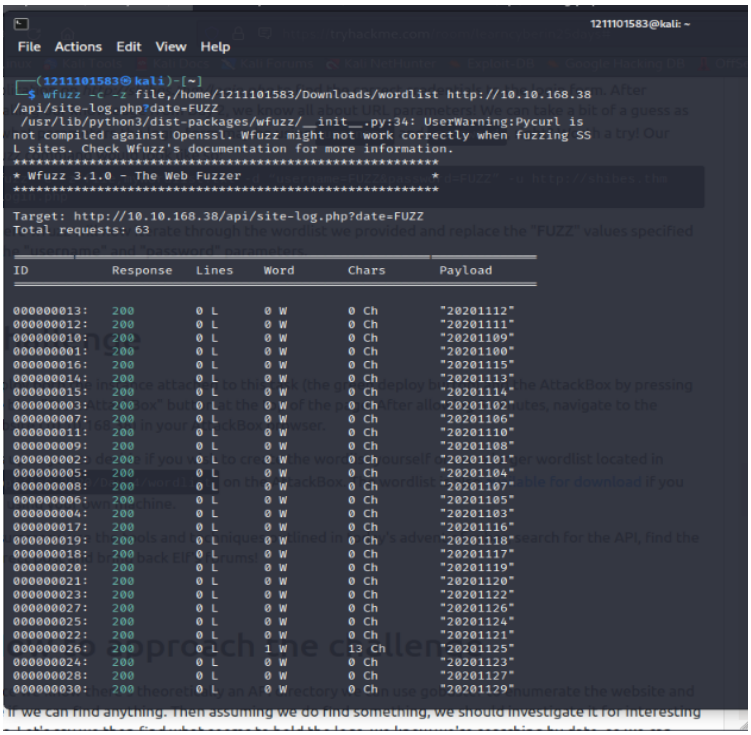


The link for the API directory: *http://10.10.168.38/api*



Question 3:

After Fuzzing the file found on the API directory, the date *20201125* turned out to be the correct date for it to be put in the URL as the GET parameter to reveal the flag.



The URL containing the flag: http://10.10.168.38/api/site-log.php?date=20201125

THM{D4t3_AP1}

Question 4:

Copied from https://www.kali.org/tools/wfuzz/:

```
-f filename,printer        : Store results in the output file
using the specified printer (raw printer if omitted).
```

Day 5
(Someone stole Santa's gift list)

Tools: Kali Linux, Terminal, Firefox, Burpsuite, FoxyProxy

Question1:

Based on the Microsoft Documentation, the default port number for SQL Server running on TCP is port 1433.

Question 2:

Santa's secret login panel is */santapanel*. This was achieved through a certain amount of time of trial and error.

Question 3:

After navigating to the URL (IP:8000/santapanel), we were able to bypass the login using SQL injection.

By adding " *' or true –*" to the username, we were able to log in to the website.

Question 4:

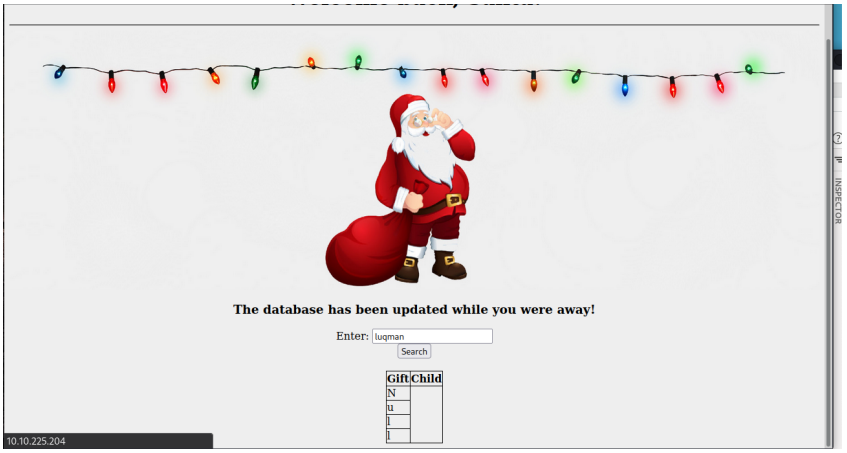
Based on the santa TODO's list, the database used is sqlite.

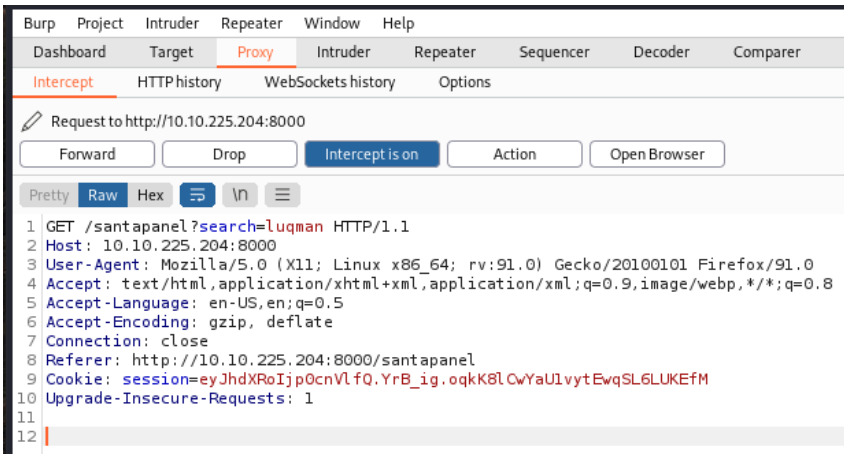
Santa's TODO: Look at alternative database systems that are better than sqlite. Also, don't forget that you installed a Web Application Firewall (WAF) after last year's attack. In case you've forgotten the command, you can tell SQLMap to try and bypass the WAF by using `--tamper=space2comment`

Pre-Question 4:

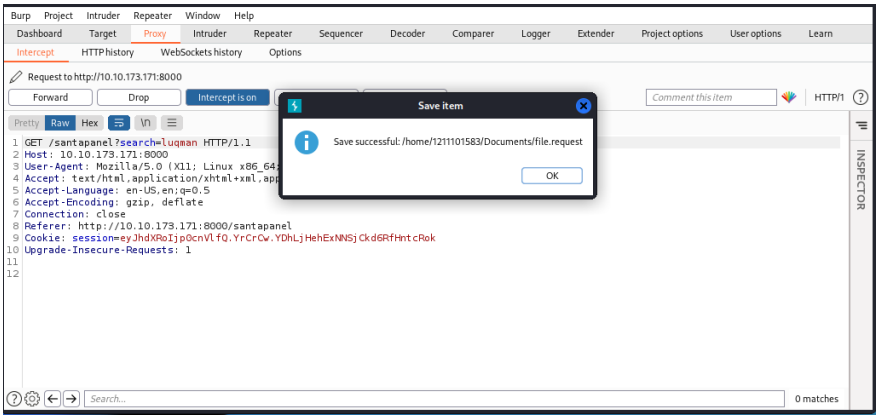
To get the answer for question 3 until question 6, we first have to use sqlmap and BurpSuite.

After turning on burp with FoxyProxy and filling in the search bar then pressing enter, we were able to see the request in BurpSuite on the proxy tab.





After sending the request to the repeater, save the file into the machine.



Now, using sqlmap's command on the terminal, we were able to translate the request and the database is now exploited.

All the answers for question 4 until 8 can be seen from the terminal.

The sqlmap command: *sqlmap -r ~/Documents/file.request –tamper=space2comment –dbms sqlite –dump-all*

–tamper=space2comment is used to bypass the WAF
–dbms sqlite is used to tell sqlmap what database is being used
–dump-all is used to dump the entire database

Question 4:

There are a total of 22 entries in the gist database

kid	age	title
James	8	shoes
John	4	skateboard
Robert	17	iphone
Michael	5	playstation
William	6	xbox
David	6	candy
Richard	9	books
Joseph	7	socks
Thomas	10	10 McDonalds meals
Charles	3	toy car
Christopher	8	air hockey table
Daniel	12	lego star wars
Matthew	15	bike
Anthony	3	table tennis
Donald	4	fazer chocolate
Mark	17	wii
Paul	9	github ownership
James	8	finnish-english dictionary
Steven	11	laptop
Andrew	16	rasberry pie
Kenneth	19	TryHackMe Sub
Joshua	12	chair

Question 5:

Jame's age is 8 years old.

kid	age	title
James	8	shoes

Question 6:

Paul asked for a *github ownership*.

kid	age	title
James	8	shoes
John	4	skateboard
Robert	17	iphone
Michael	5	playstation
William	6	xbox
David	6	candy
Richard	9	books
Joseph	7	socks
Thomas	10	10 McDonalds meals
Charles	3	toy car
Christopher	8	air hockey table
Daniel	12	lego star wars
Matthew	15	bike
Anthony	3	table tennis
Donald	4	fazer chocolate
Mark	17	wii
Paul	9	github ownership
James	8	finnish-english dictionary
Steven	11	laptop
Andrew	16	rasberry pie
Kenneth	19	TryHackMe Sub
Joshua	12	chair

Question 7:

The flag is *thmfox{All_I_Want_for_Christmas_Is_You}*

flag
thmfox{All_I_Want_for_Christmas_Is_You}

Question 8:

The password for admin is *EhCNSWzzFP6sc7gB*

password	username
EhCNSWzzFP6sc7gB	admin