PSP0201 Week 2 Writeup

Group Name: Siuuu

Members

ID	Name	Role
1211103423	Rino Frawidiya bin Suheri	Leader
1211104232	Muhammad Amirul Haiqal Bin Zameri	Member
1211101924	Nur Ayu Farisha Binti Hamdan @ Hood	Member

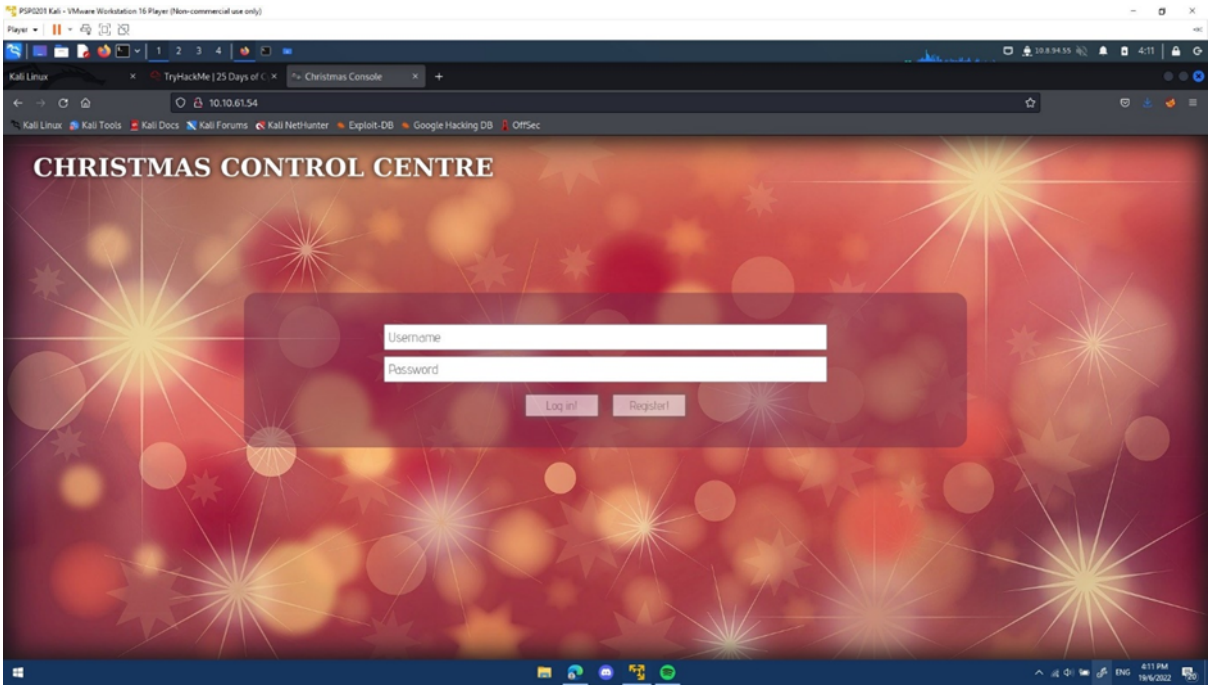
Day1: Web Exploitation – A Christmas Crisis

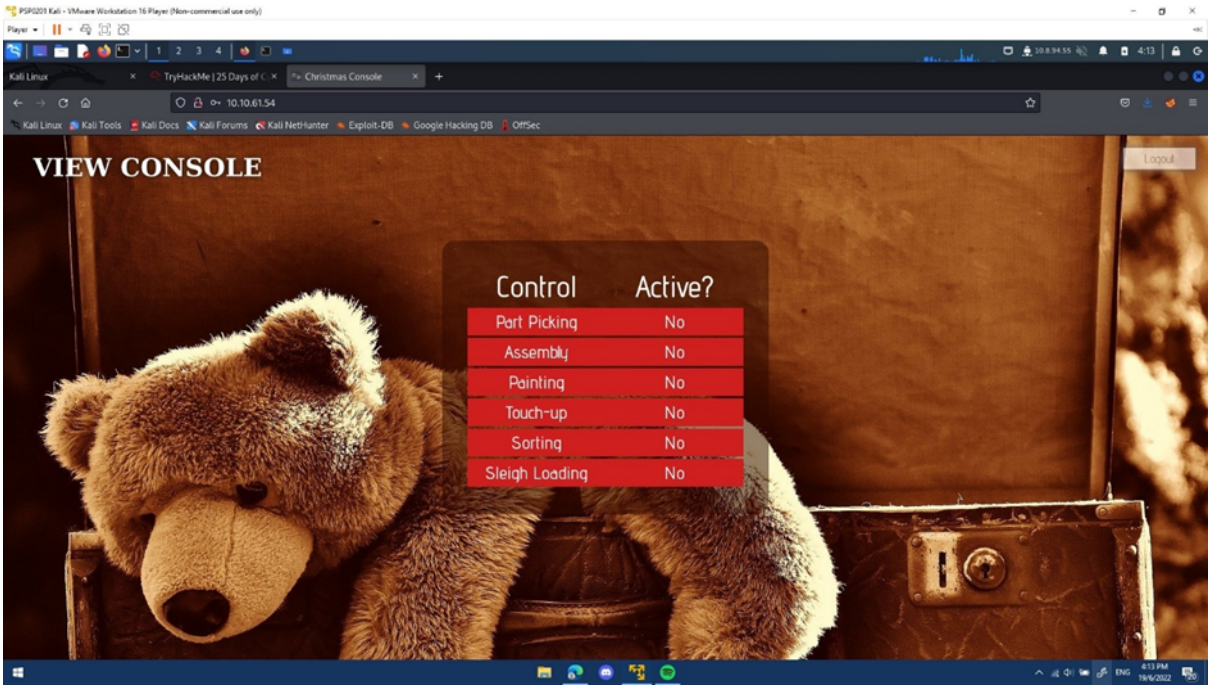
Tools used: Kali Linux, Firefox

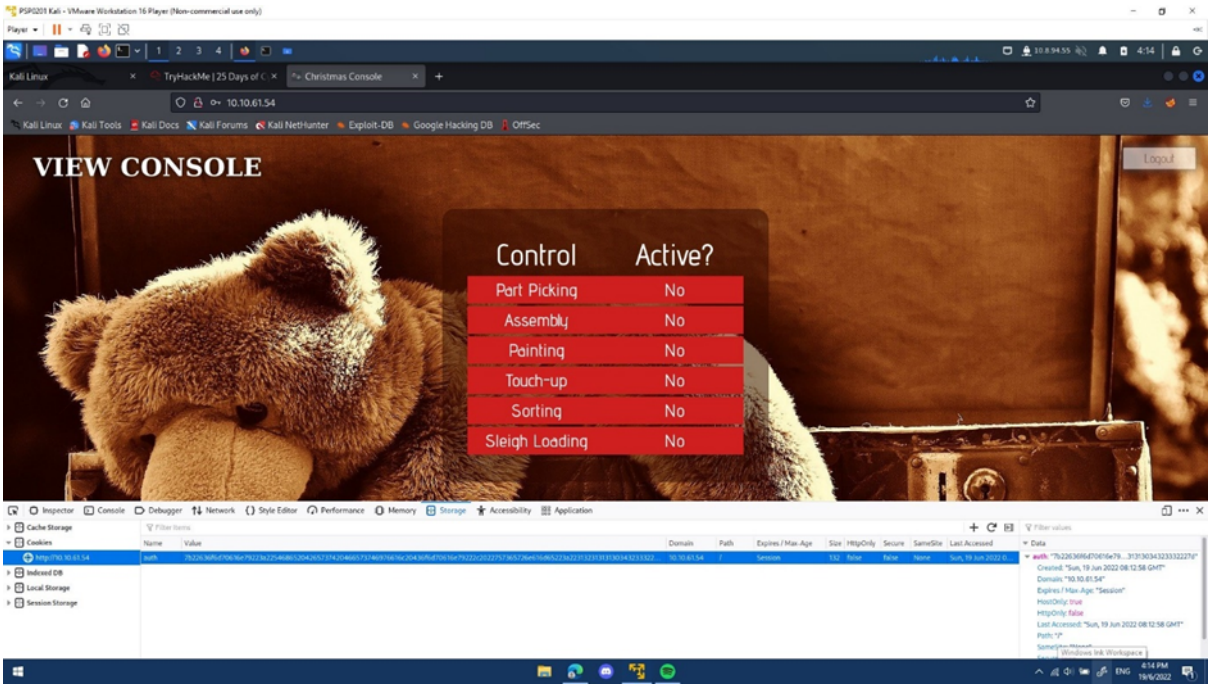
Solution/Walkthrough:

Question 1

Opening up the browser developer tools to check on the cookie.

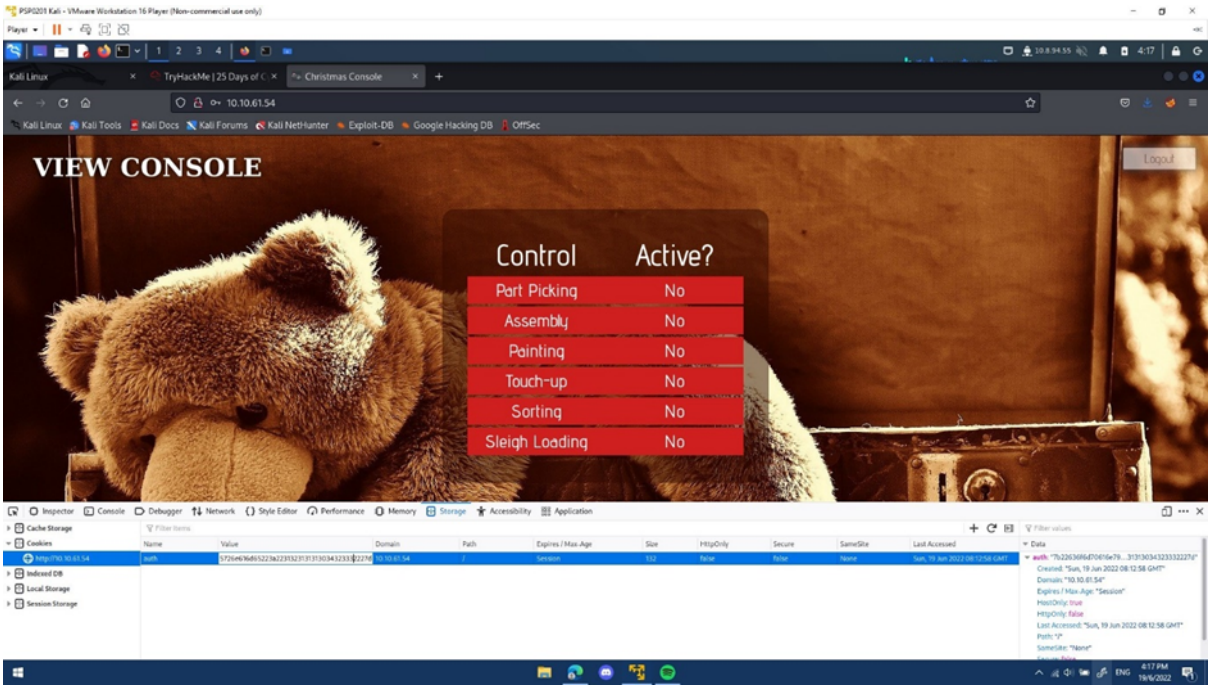






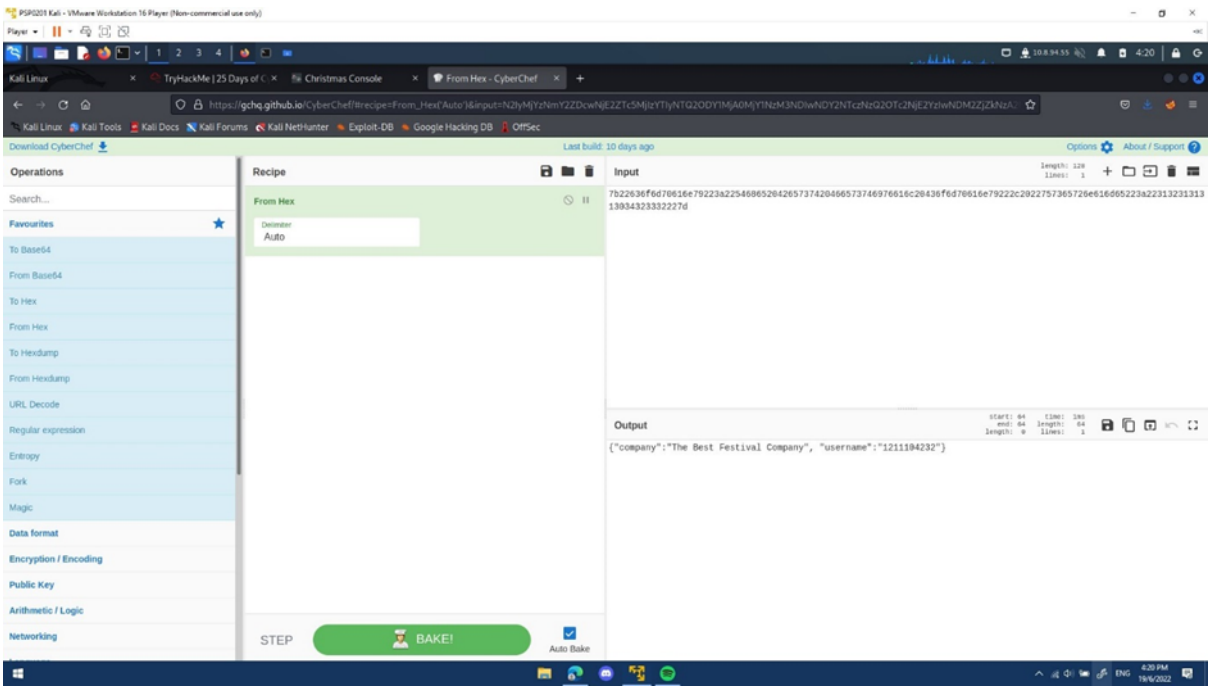
Question 2

Obtain the value of the cookie.



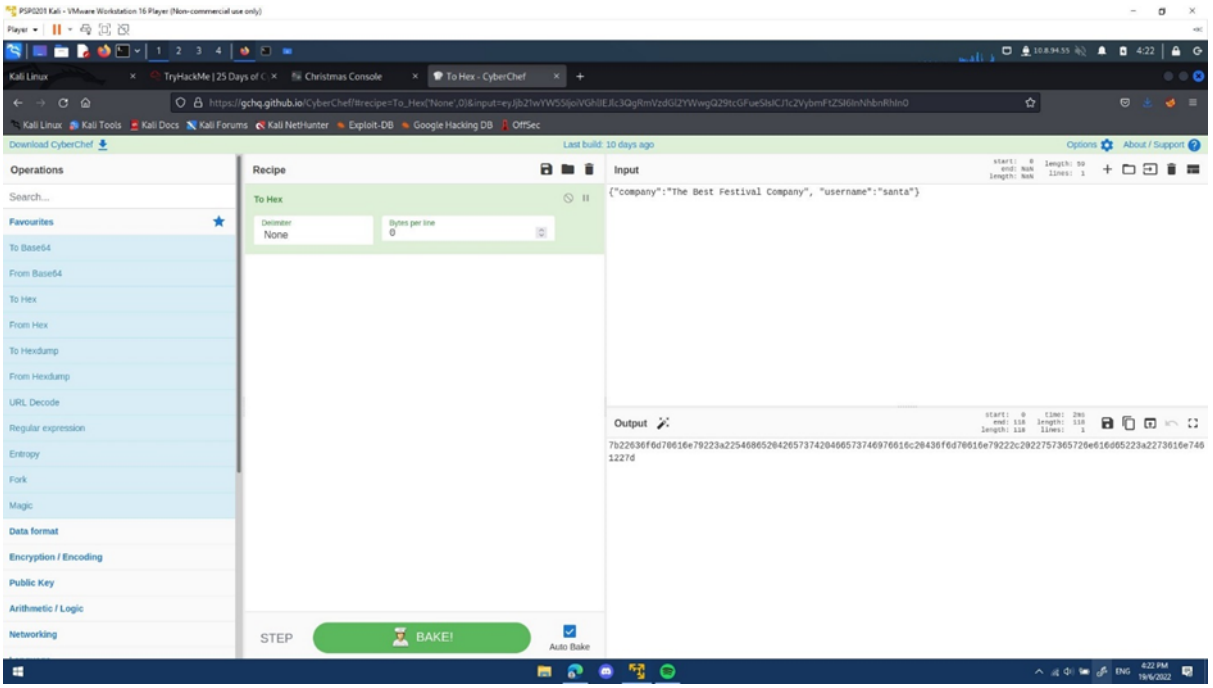
Question 3

Using Cyberchef, convert the cookie value to string.



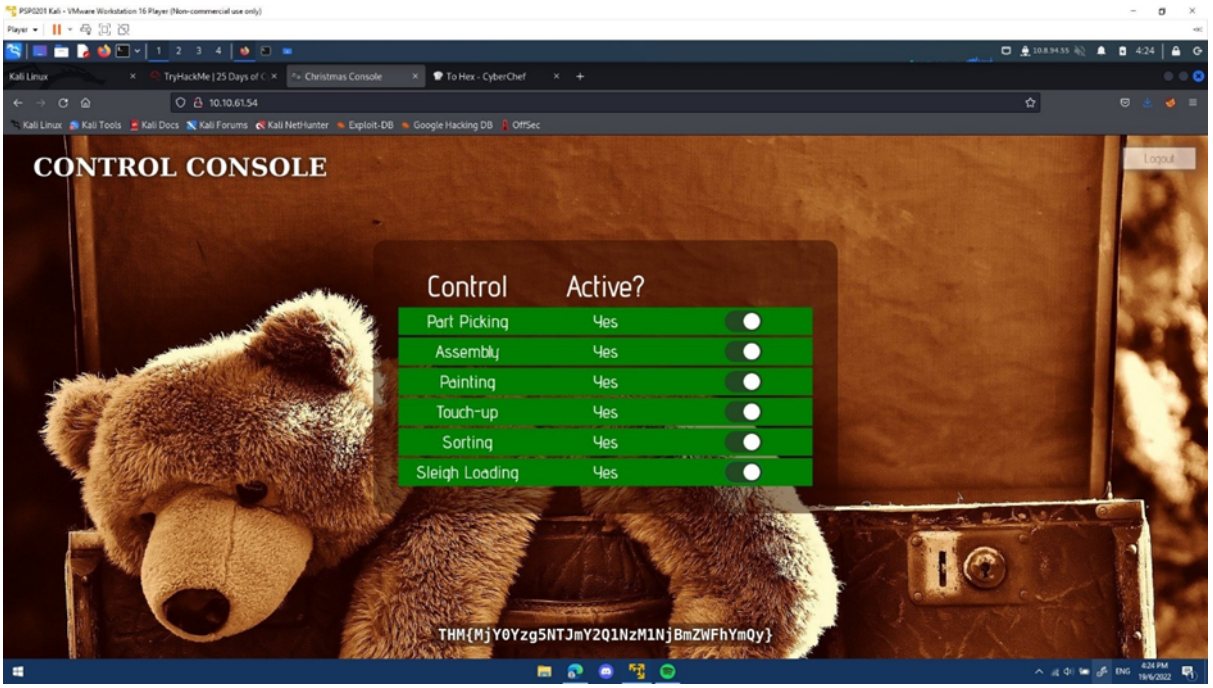
Question 4

Changing the username to ‘santa’, convert the JSON statement to hex.



Question 5

Having access to the controls, switching on every control shows the flag.



Thought Process/Methodology:

Pasted the IP address to access the page. We registered for an account and logged in. After that, we opened the Browser Developer Tools by pressing F12 key and proceeded to view the site cookie from the Storage. We searched for the format of the value of this cookie by deducing it to be a hexadecimal value and turned it into text by using Cyberchef. The JSON statement was founded with a username element. We changed the value of the username to 'santa' to access the administrator account and converted it back to hexadecimal by using Cyberchef. Replacing the cookie value with the one we had converted to access the administrator page. After refreshing the page, we turned on every control which led us to see the flag.

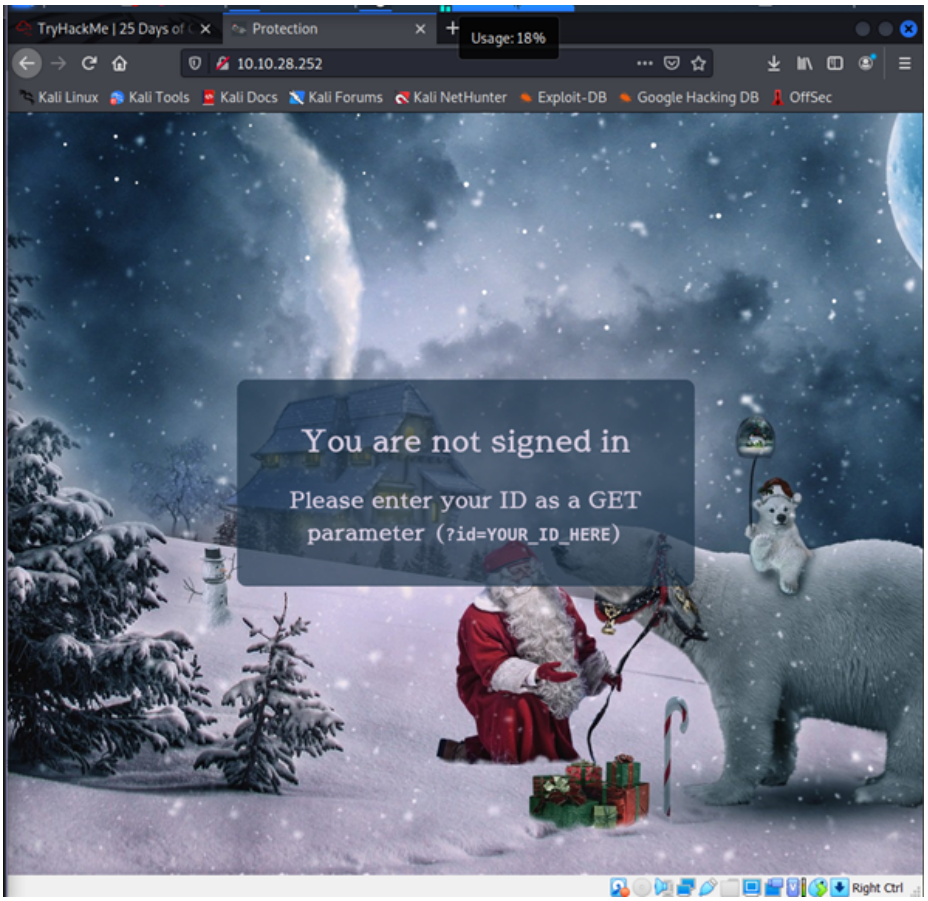
Day 2: Web Exploitation – The Elf Strikes Back!

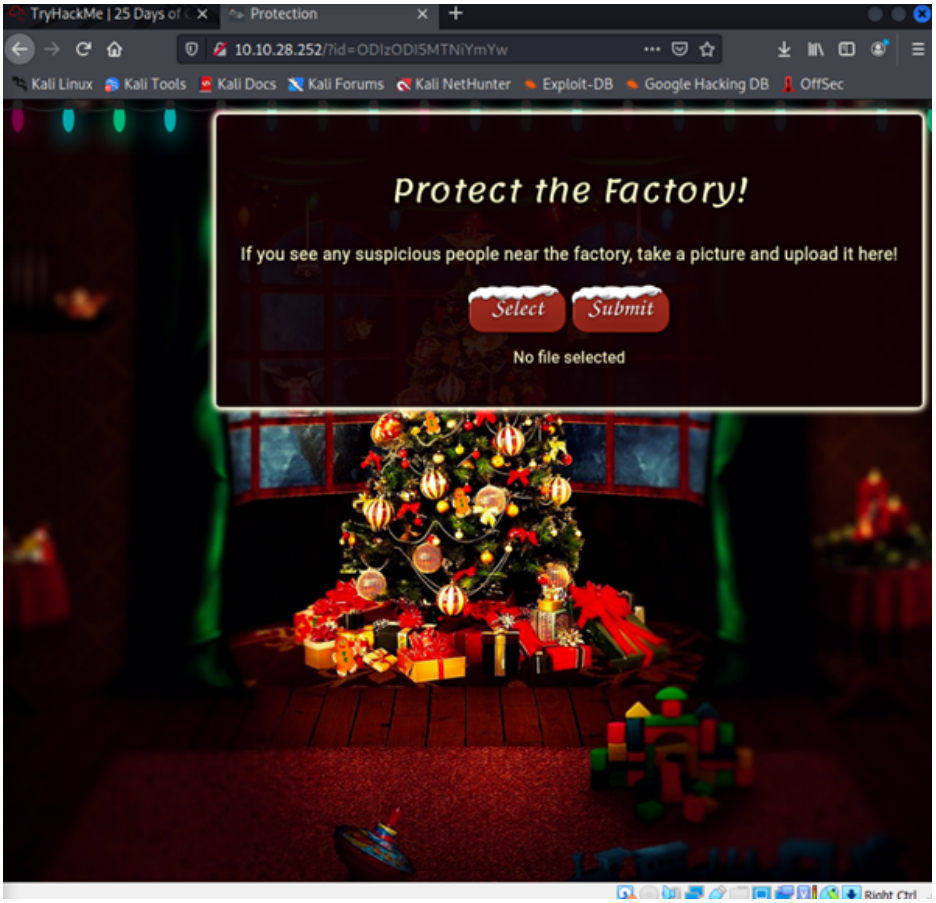
Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1

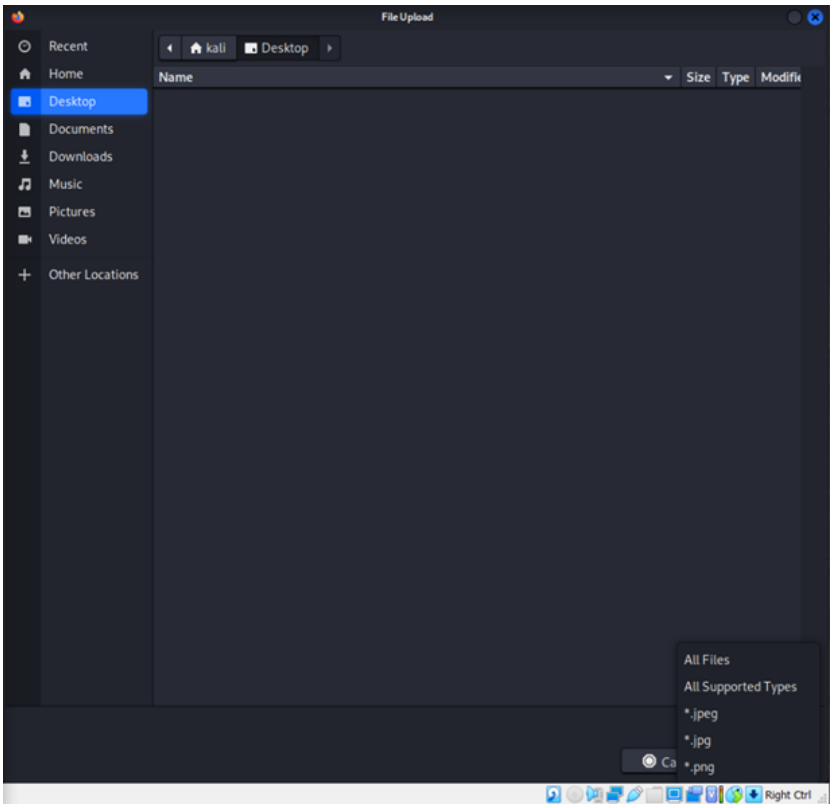
Signed in using the ID given.



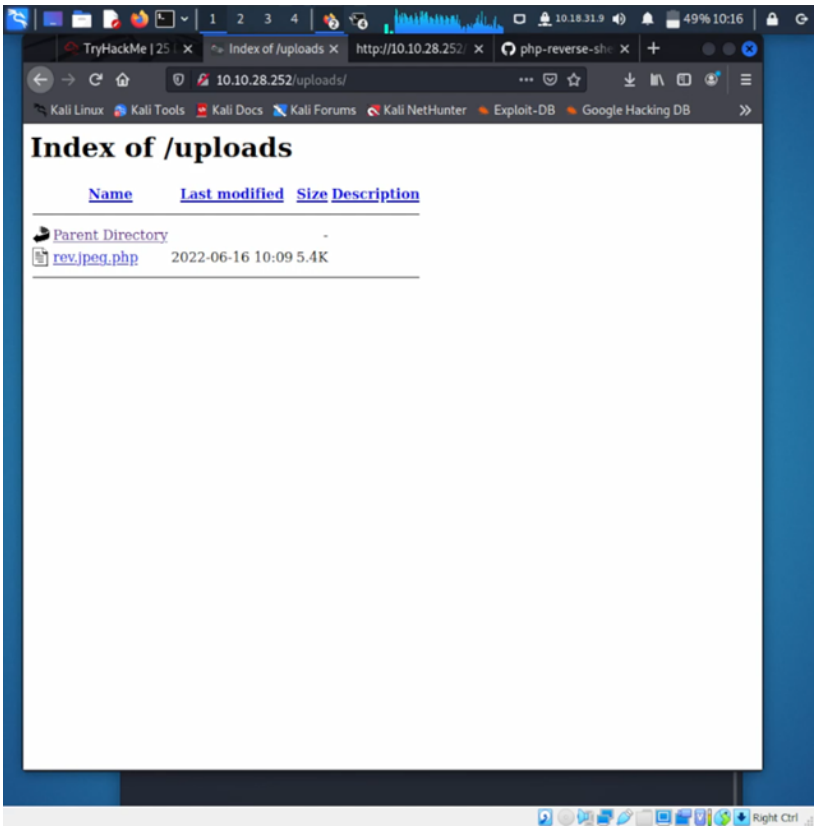


Question 2

Checking the supported types.

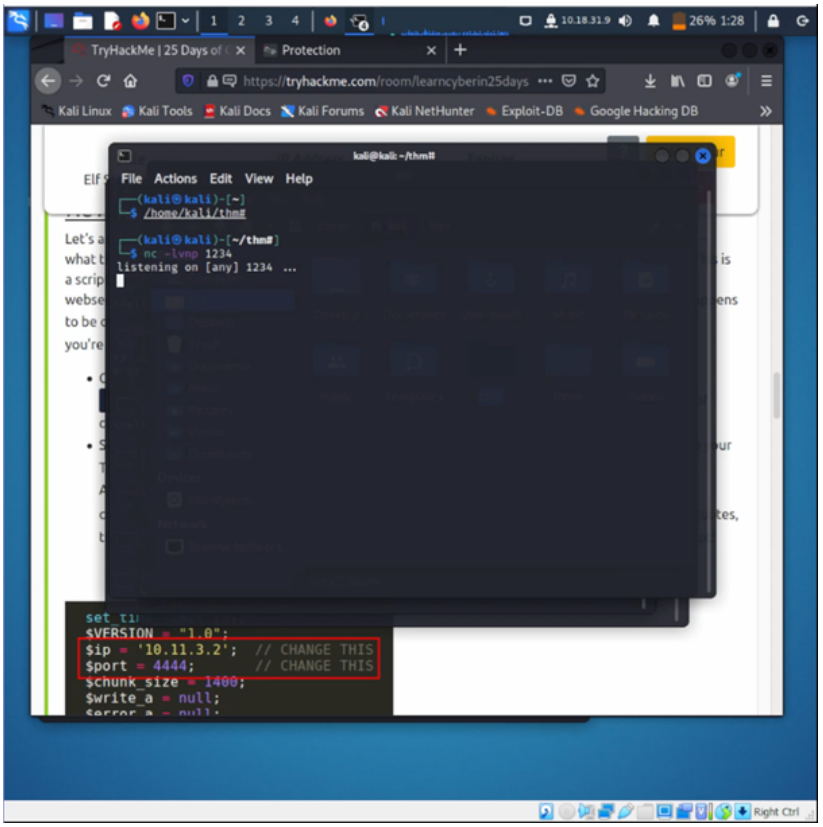


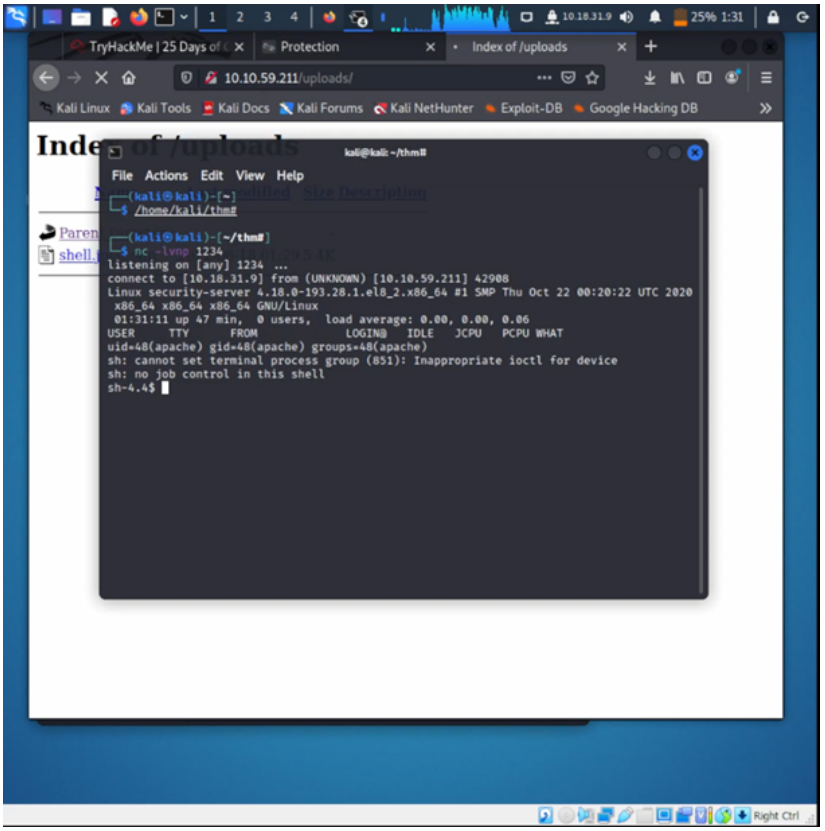
Question 3



Question 4

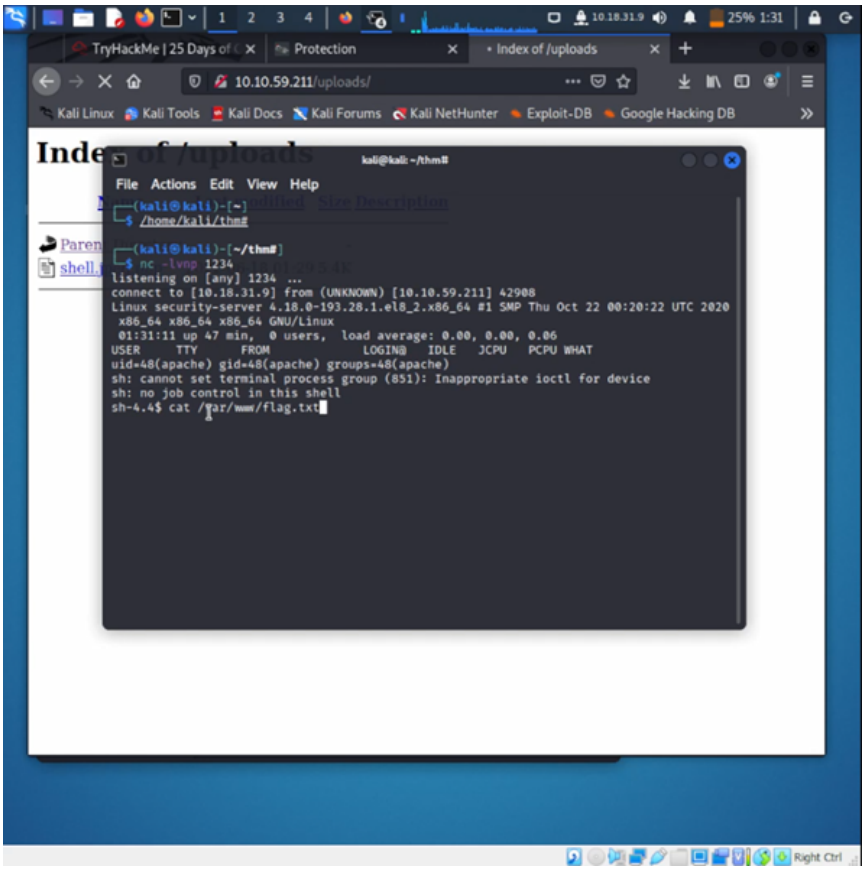
Using the command active the reverse shell.

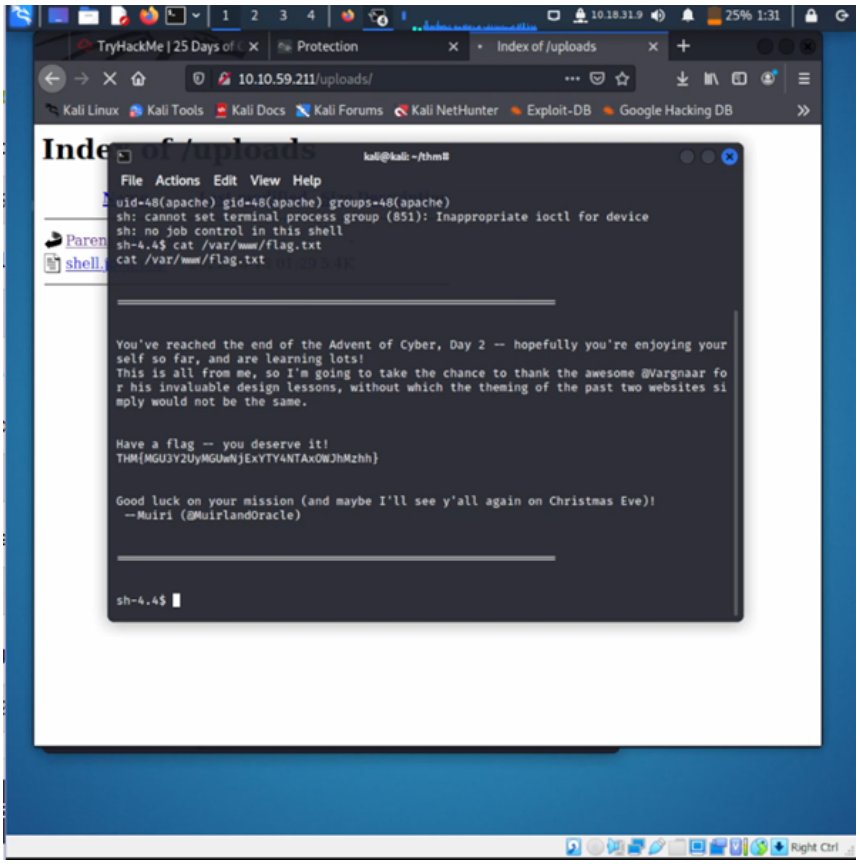




Question 5

Search the flag in `/var/www/flag.txt ‘.





Thought Process/Methodology:

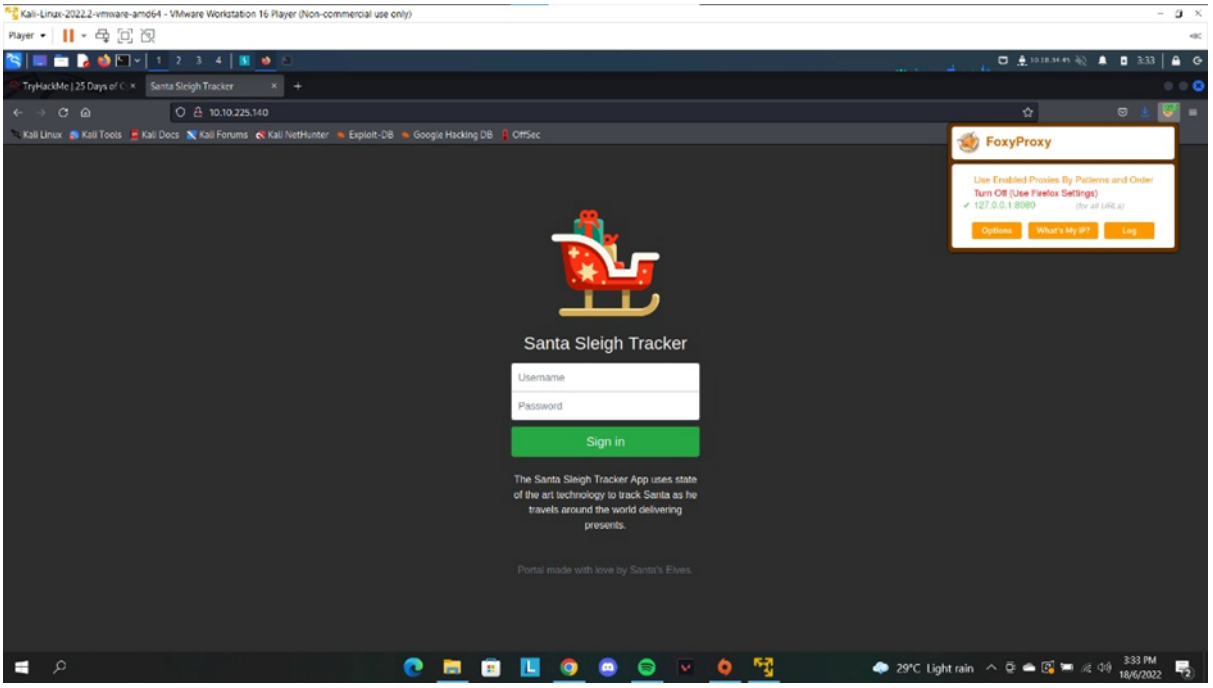
Having accessed the target machine, we were shown a sign in page. We are using the ID that already assigned for the system. After signing in, we open the select button to checking the supported files to submit. We found that the supported files is image types. After that, we create a file for reverse shell. We found that the ip need to change, so we change the ip in the reverse shell to our own ip. After that, we save that file. Later, we rename the file to `shell.jpeg.php' and we submit the file. We try one by one the subdirectory and we find that in /uploads directory are the uploaded files stored. Later, we are listening and active the reverse shell. From the netcat we find the flag from `/var/www/flag.txt'.

Day 3: Web Exploitation-Christmas Chaos

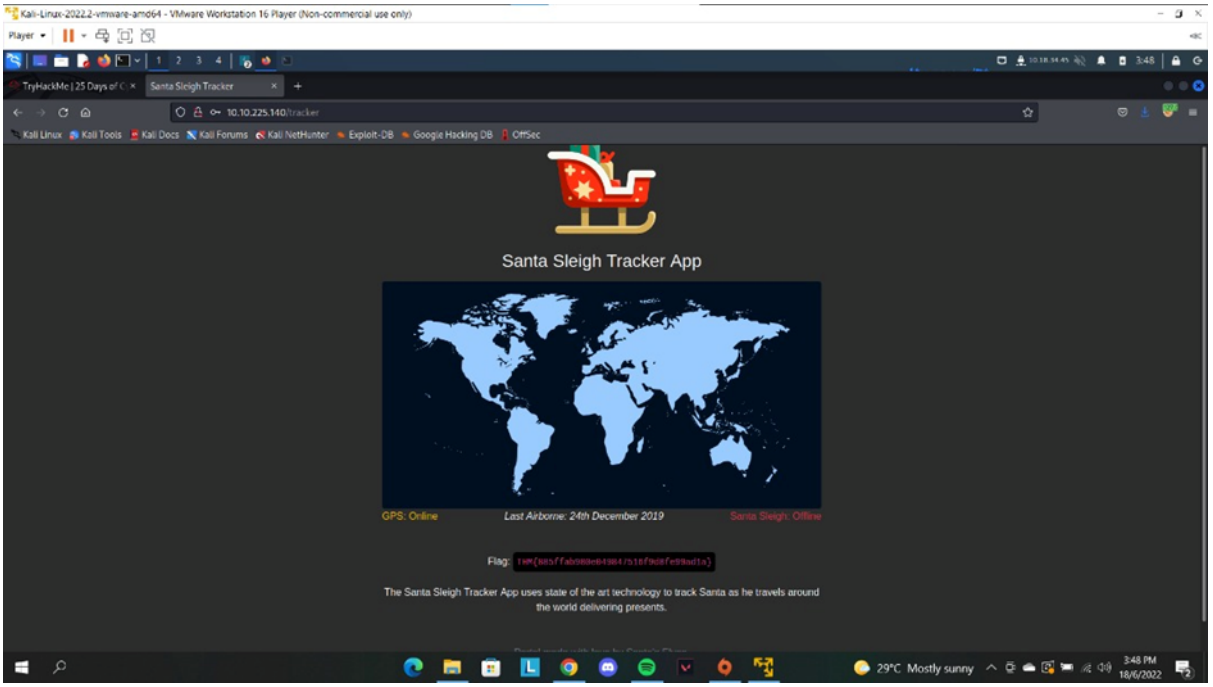
Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1



Question 2



Thought Process/Methodology:

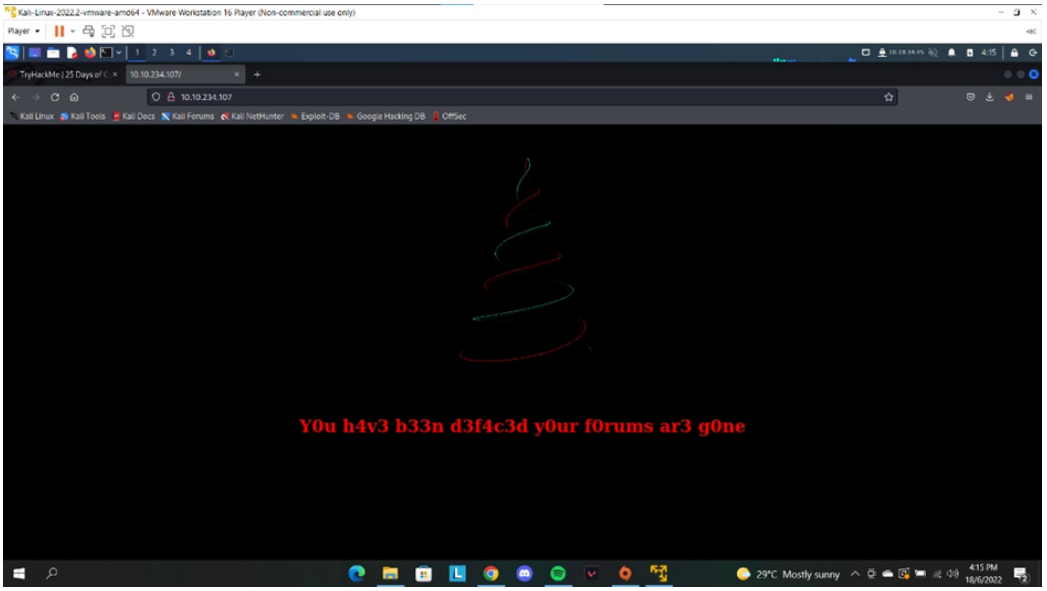
We launched BurpSuite first, followed by Firefox. After that, when we visit the website, a sign-in page appears. We enter a username and password and send it through BurpSuite. Later, we received a request, which we sent to the intruder. After that, we add the credential to payloads by using payloads set 1 for the username and payloads set 2 for the passwords, and then we start to attack. Then all of the requests are redirected, and we check the length to determine which one has 255 and use it to sign in. We were able to get in and obtain the flag.

Day 4: Web Exploitation- Santa' Watching

Tools used: Kali Linux, Firefox

Solution/walkthrough:

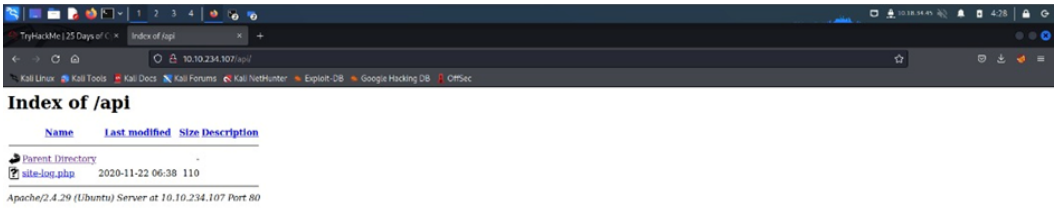
Question 1



Question 2

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

Question 3



Question 4

Thought Process/Methodology:

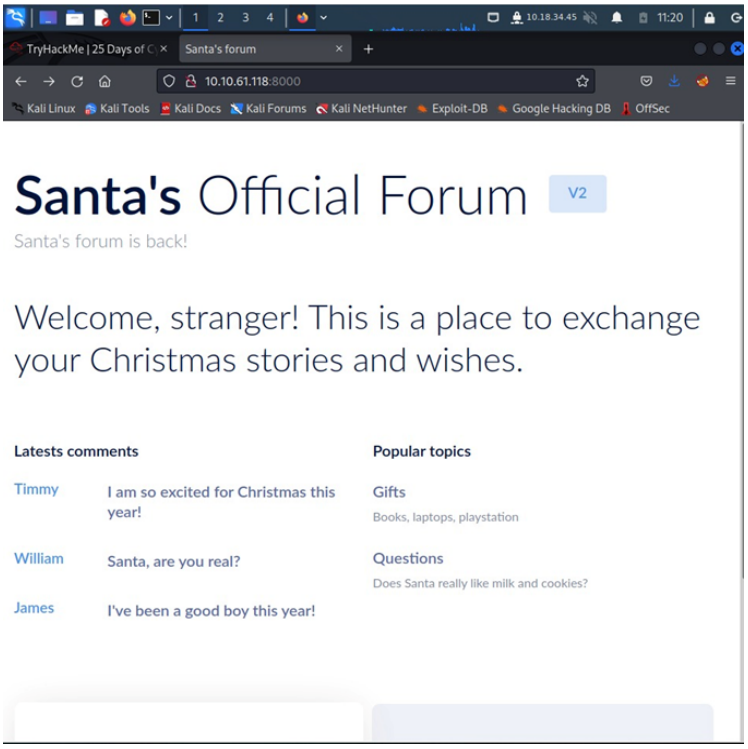
We enter our IP address, and it displays "Y0u h4v3 b33n d3f4c3d y0ur f0rums ar3 g0ne." After that, we went to cmd, installed gobuster, and then ran the gobuster command. Later, we see that the API directory and we go back to our website and type "/api". Following that, we downloaded the file "wordlist" and wfuzzed the parameter in the API directory. After that, we run the wordlist file using the wfuzz command. We found one with a difference in characters and used it for our link, and we received the flag.

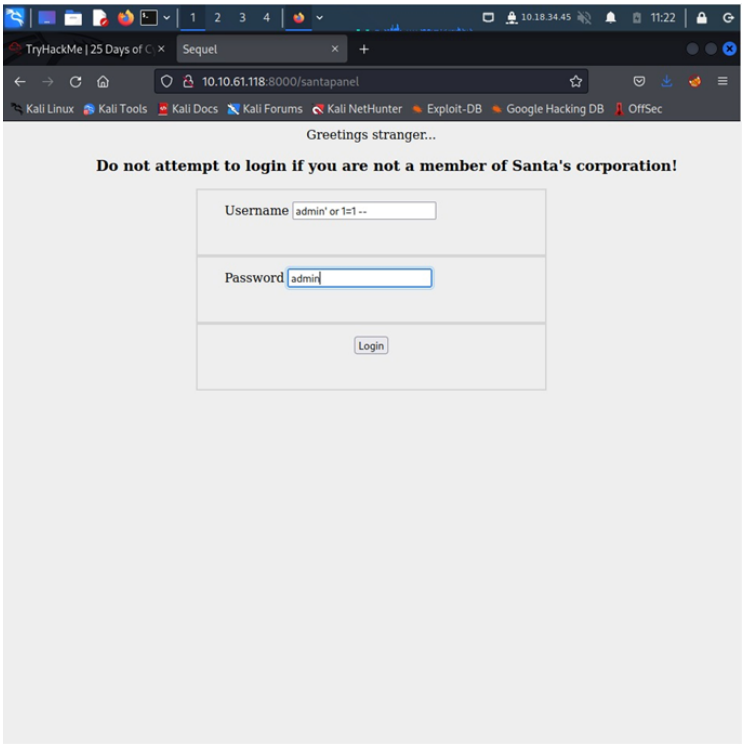
Day 5 : Web Exploitation-Someone stole Santa's gift list!

Tools used: Kali Linux, Firefox

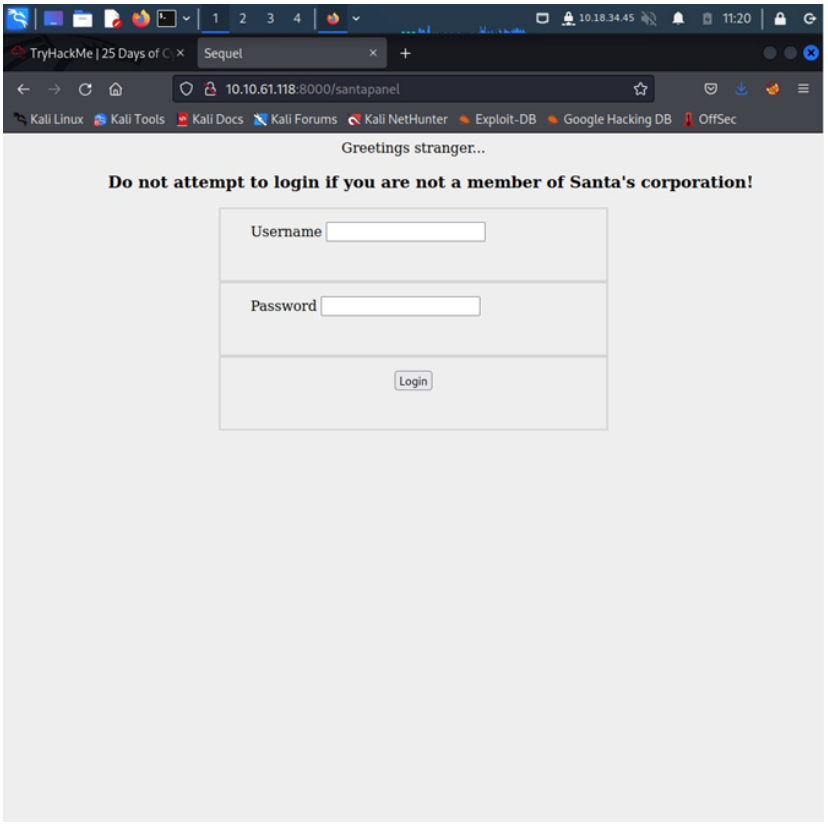
Solution/walkthrough:

Question 1

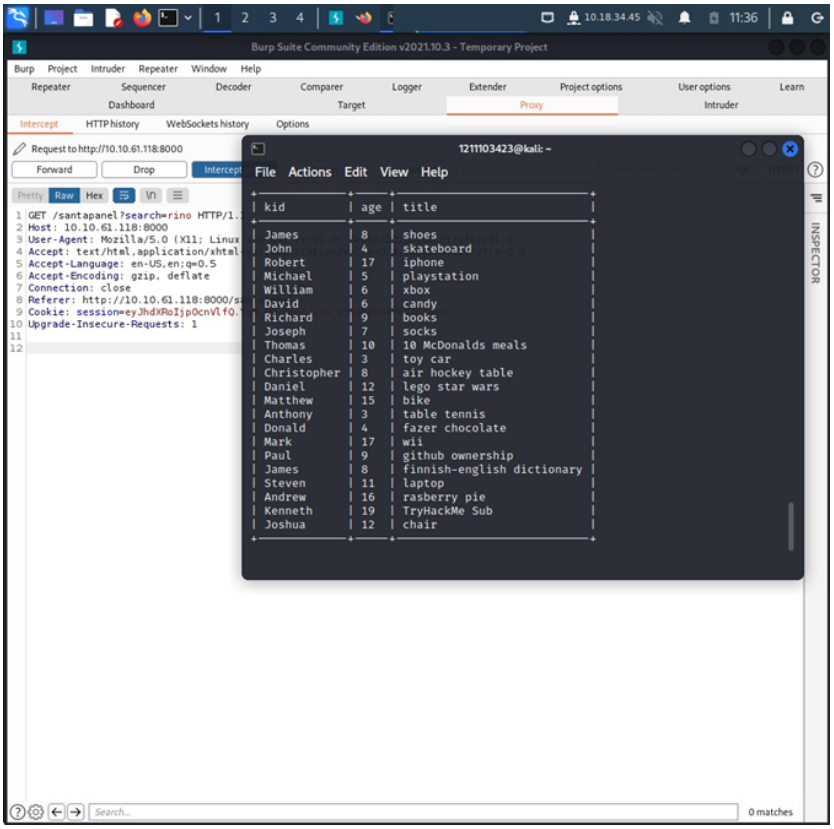




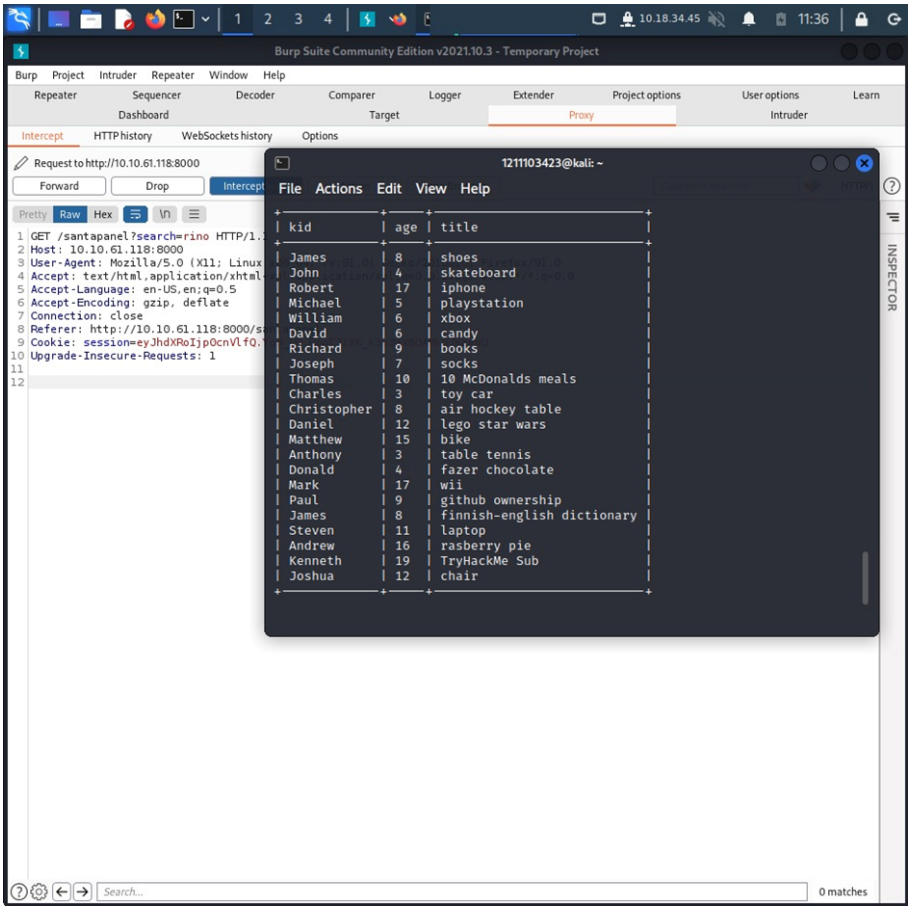
Question 2



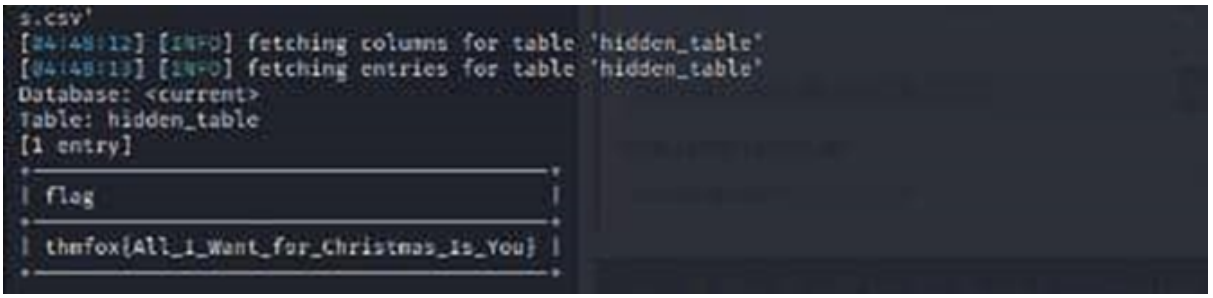
Question 3



Question 4



Question 5



Question 6

Thought Process/Methodology:

We opened the website using our ip and it showed Santa's official forum. After that, we guessed from the hint and tried "/santapanel" and it directed us to the santa login panel. We logged in using "admin or 1=1" as username and "admin" as password and then we were directed to a page that showed Santa's database. After that, we open BurpSuite and run it to our firefox. We entered "darkstar" and it sent the request. After that, we save the item and run the sqlmap using the dump command. Later, we scrolled down and got the flag and the admin password.