PSP0201

Week 2

Writeup

Group Name: urkomputerhaspirus

Members

ID	Name	Role
1211102272	Tee Cheng Jun	Leader
1211101114	Chong Yi Jing	Member
1211101591	Ian Leong Tsung Jii	Member
1211101734	Ernest Leong Zheng Yang	Member

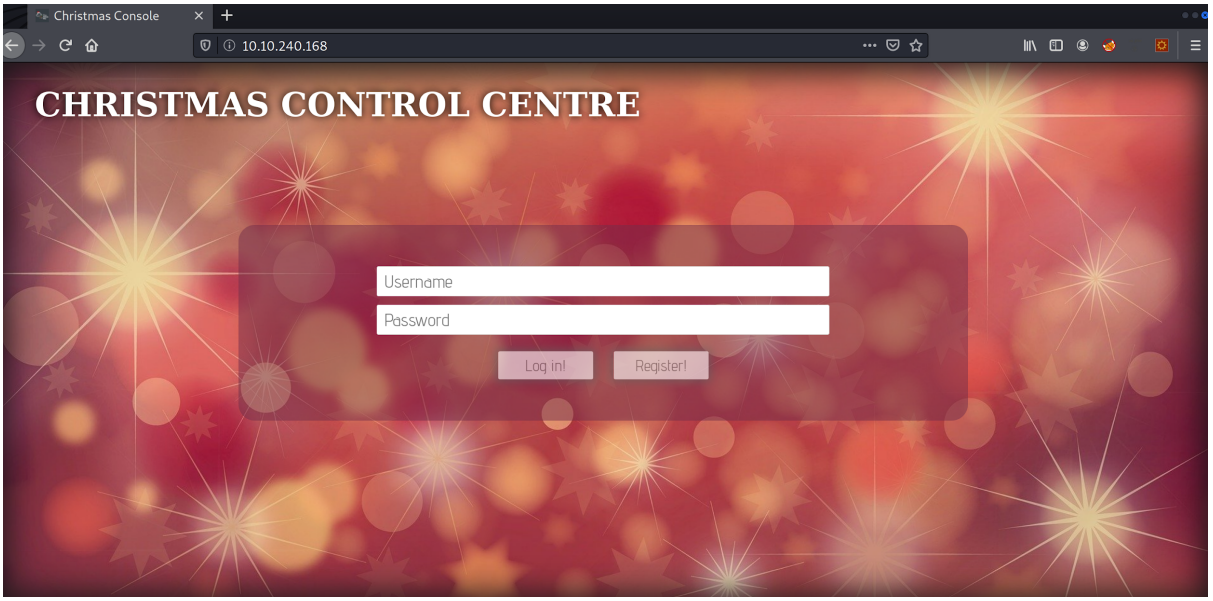
Day 1: Web Exploitation – A Christmas Crisis

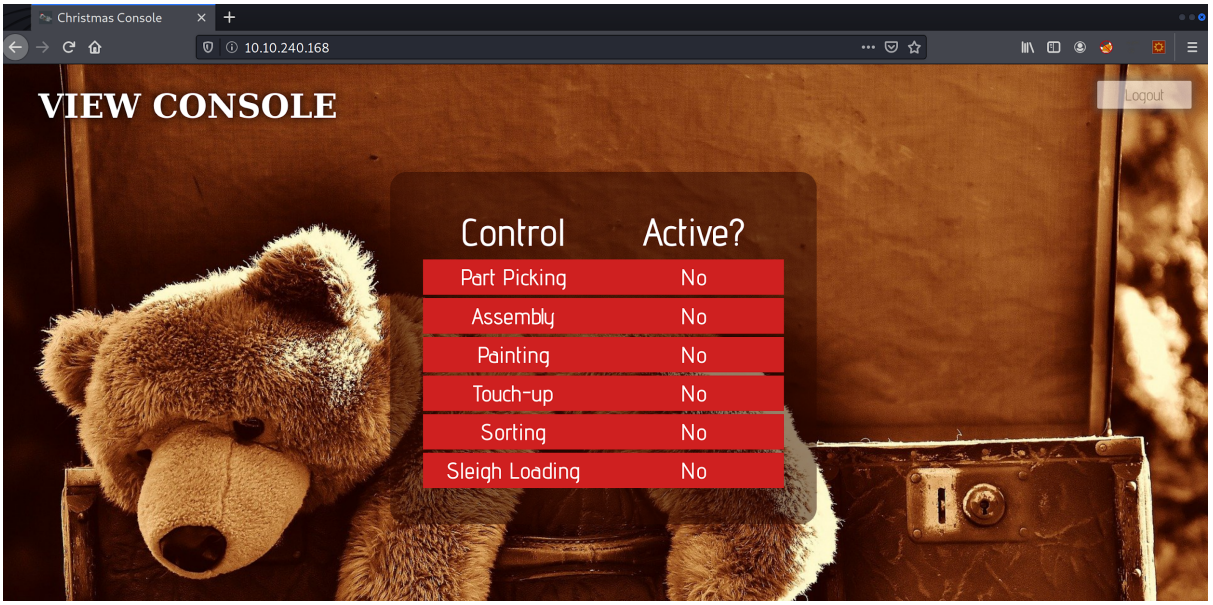
Tools used: Kali Linux, Firefox

Solution/walkthrough:

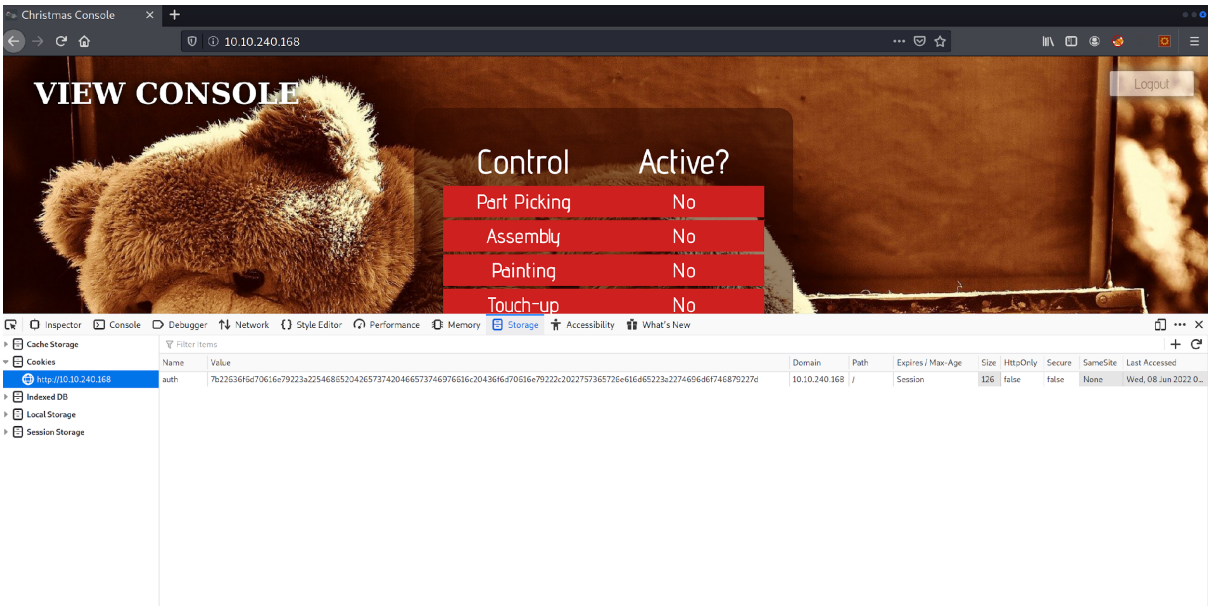
Question 1

Open the page by putting the I.P given in the search bar.





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



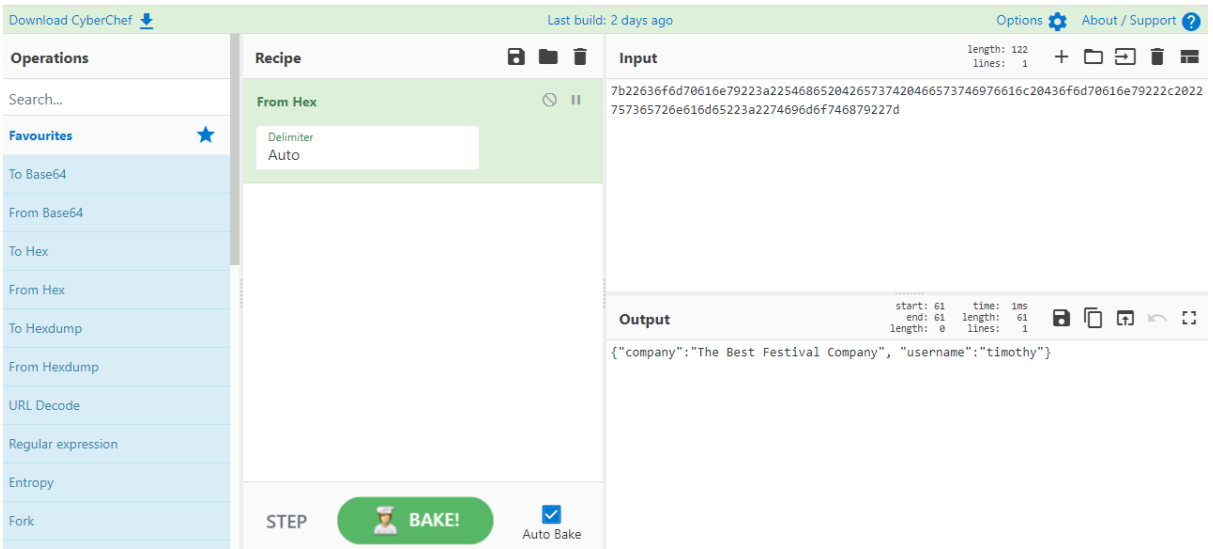
Question 2

Obtain the value of the cookie.

Value
7b22636f6d70616e79223a2254686520426573742046657374976616c20436f6d70616e79222c2022757365726e616d65223a2274696d6f746879227d

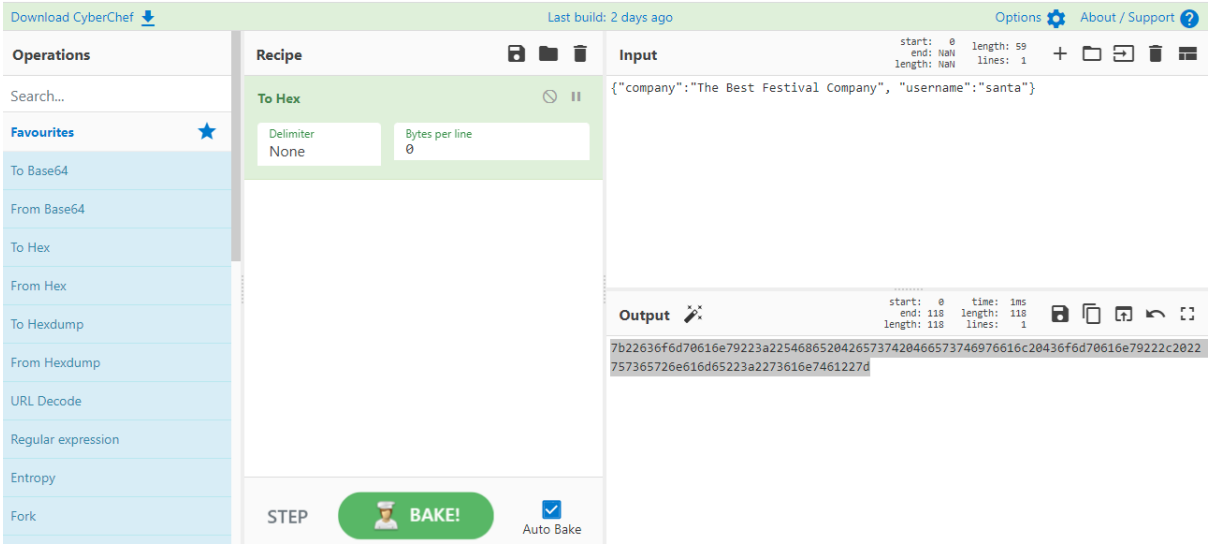
Question 3

Using Cyberchef, convert the cookie value from hexadecimal to string.



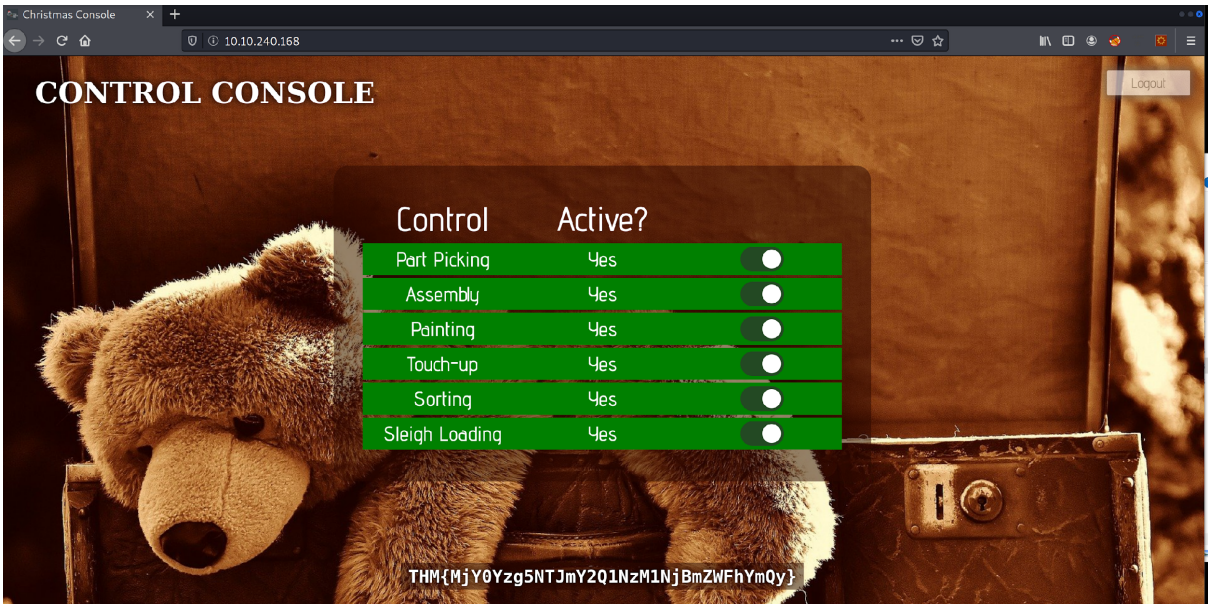
Question 4

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



Question 5

After copy pasting Santa’s cookie into the website and hitting refresh, we now have access to the controls. We can then switch on every control and the the flag will be presented to us.



Thought Process/Methodology:

Having accessed the target machine, we were shown a login/registration page. We proceeded to register an account and login. After logging in, we open the browser's developer tool and viewed the site cookie from the Storage tab. Looking at the cookie value, we deduced it to be a hexadecimal value and proceeded to convert it to text using Cyberchef. We found a JSON statement with the username element. Using Cyberchef, we altered the username to 'santa', the administrator account, and converted it back to hexadecimal using Cyberchef. We replaced the cookie value with converted one and refreshed the page. We are now show an administrator page (Santa's) and proceeded to enable every control, which in turn showed the flag.

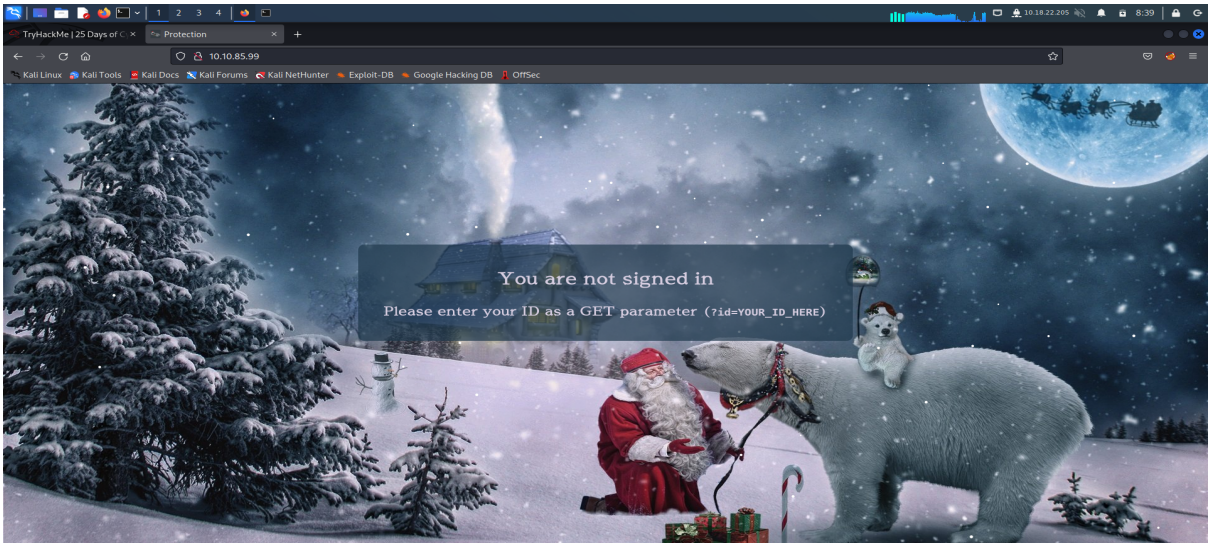
Day 2: Web Exploitation - The Elf Strikes Back!

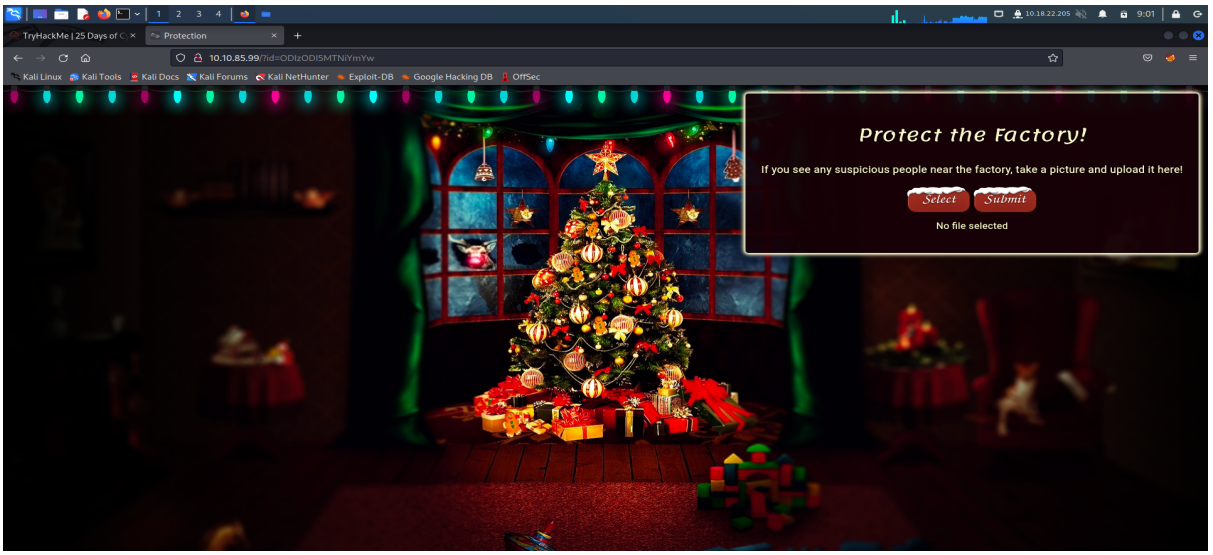
Tools used: Kali Linux, Firefox, Netcat, Nano(text editor)

Solution/walkthrough:

Question 1

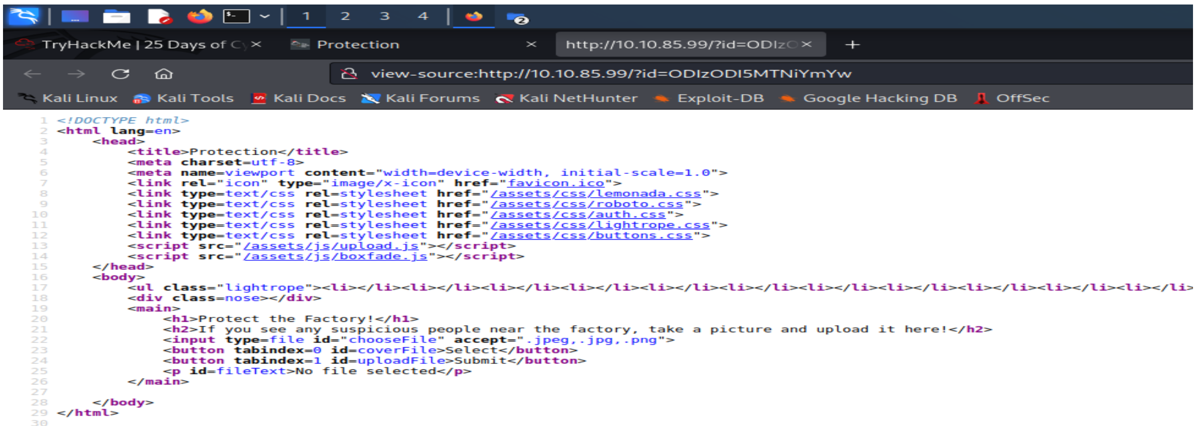
Discovered the page for uploading files by adding “?id=ODIzODI5MTNiYmYw” at the end of the ip address.





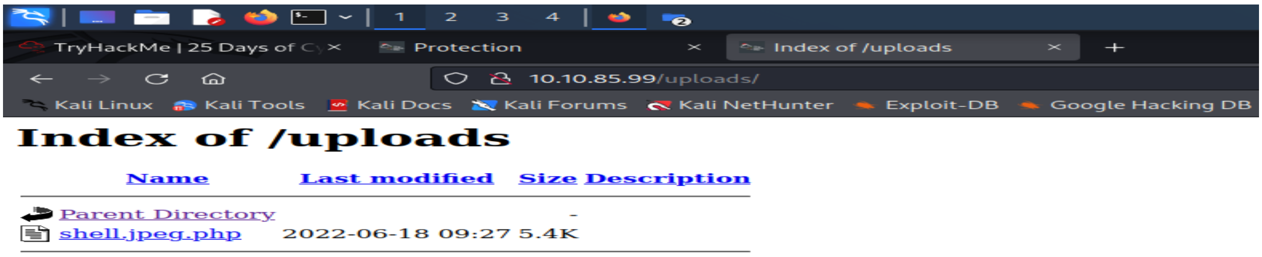
Question 2

By viewing the source for the file upload page, we can find out what type of files are allowed to be submitted. In this case, it accepts .jpeg,.jpg, and .png.



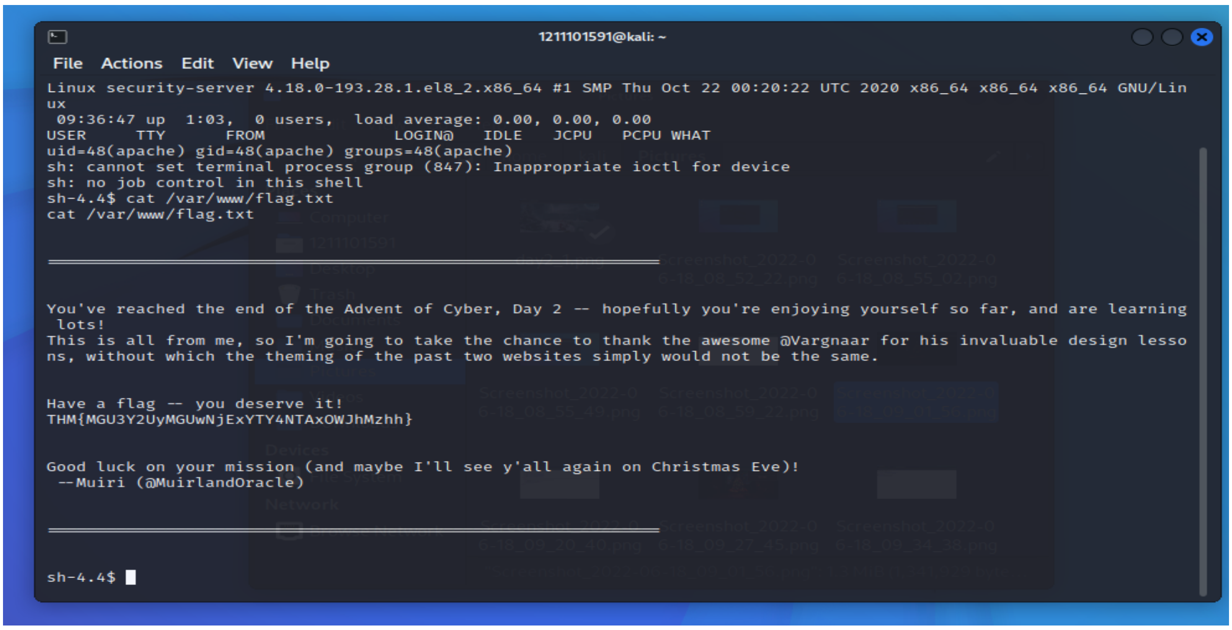
<u>Question 3</u>

Uploaded files are stored in the /uploads/ directory. I have uploaded shell.jpeg.php.



<u>Question 4</u>

After our reverse-shell is connected, typing out the directory /var/www/flag.txt gives us the flag.



Thought Process/Methodology:

Having accessed the page for uploading files, we inspected the page source to find out what types of files that it accepts. As it accepts only image files, our PHP reverse shell script needs to have either .jpeg,.jpg, or .png. Therefore we have renamed the reverse shell script given in /usr/share/webshells/php/php-reverse-shell.php to shell.jpeg.php. After submitting the file on the website, we started up netcat listener to listen on port 1234. After clicking the uploaded file on the /uploads/ directory, we now have a connection. Upon typing /var/www/flag.txt into the terminal, the flag is revealed.

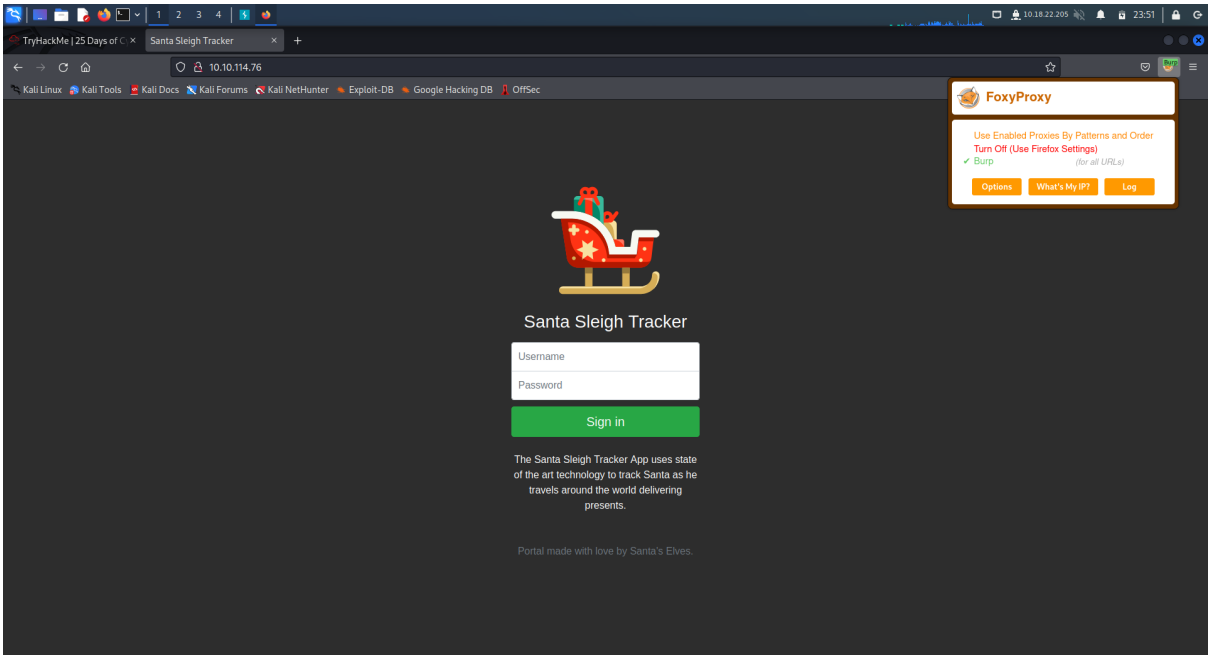
Day 3: Web Exploitation - Christmas Chaos

Tools used: Kali Linux, Firefox, Burpsuite, FoxyProxy

Solution/walkthrough:

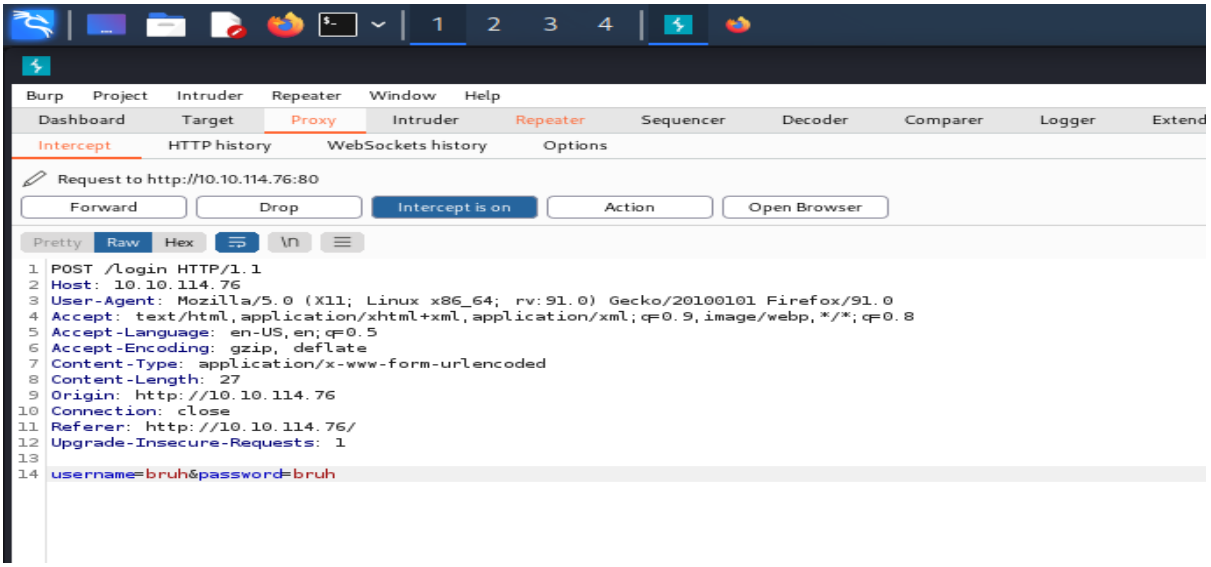
Question 1

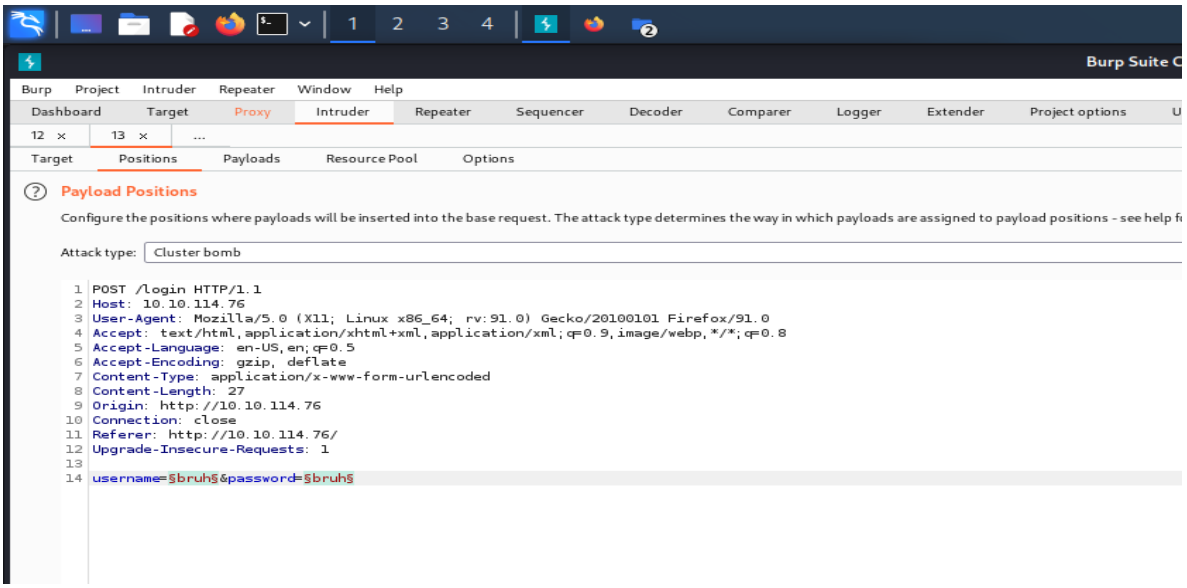
After accessing the website, we turn on burp via FoxyProxy. After that, we turn on intercept in the proxy menu in burpsuite. We then enter values into the field and click sign in. Burpsuite will now hold our request and not forward it until we tell it to.



Question 2

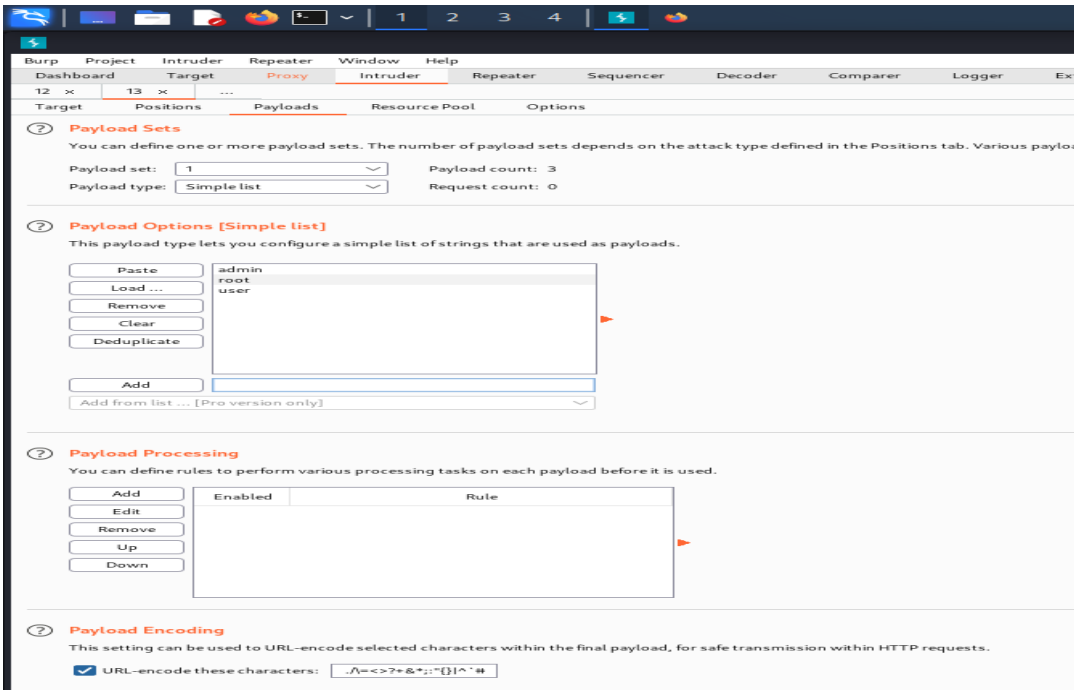
We then forward the request to intruder. From the positions tab we configure our attack type as cluster bomb and select the fields where the payloads will be inserted.

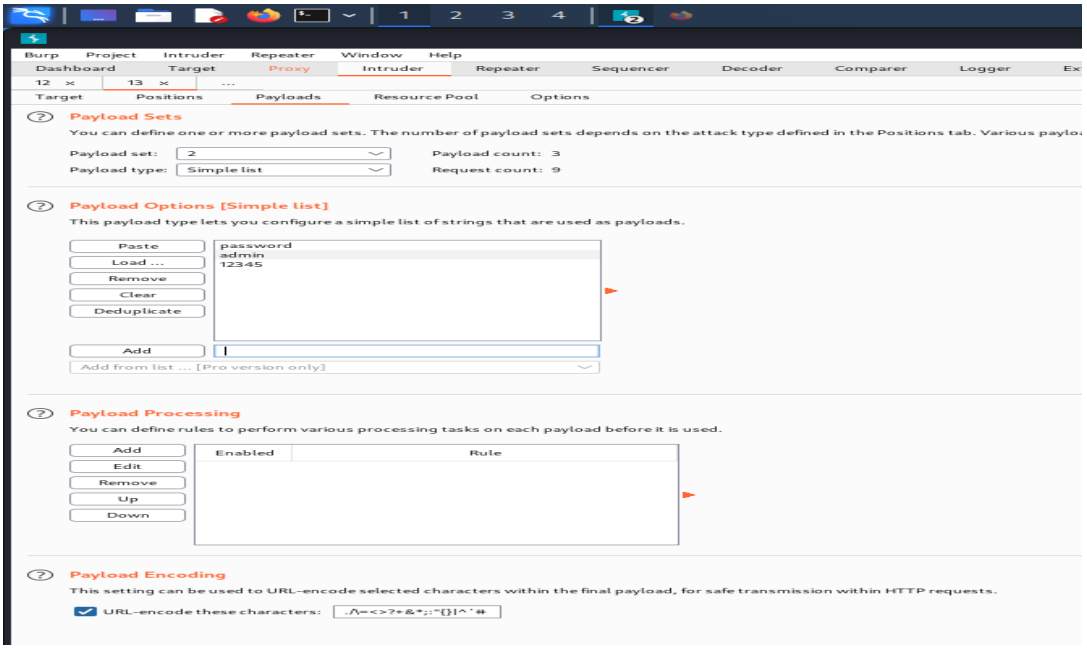


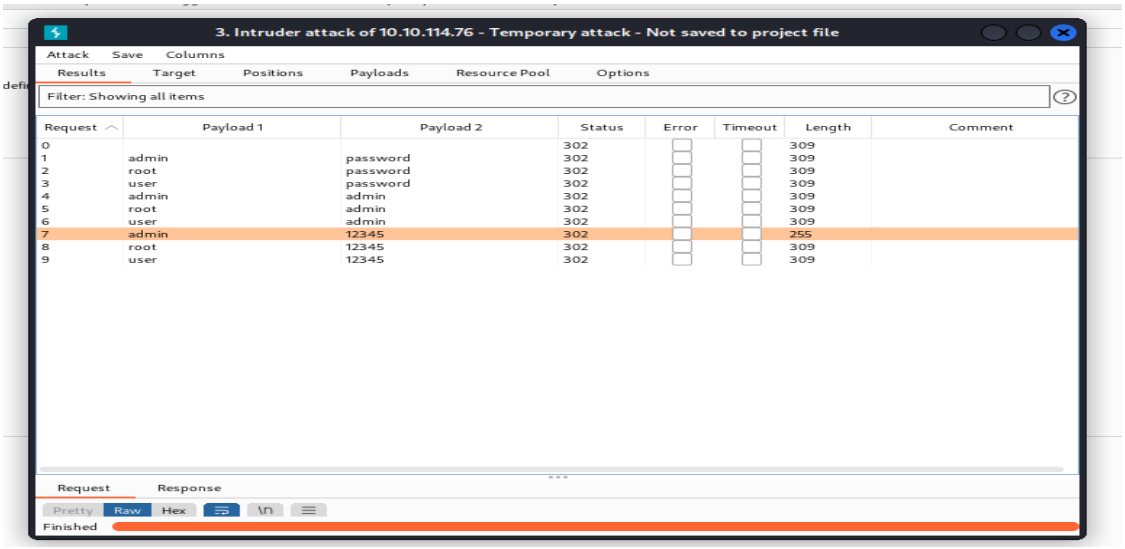


Question 3

We then click the payloads tab and enter the values that we will be trying in set 1(username) and set 2(password). Then we click the attack button. When the attack is complete we can see that one combination of username and password shows a different status code.

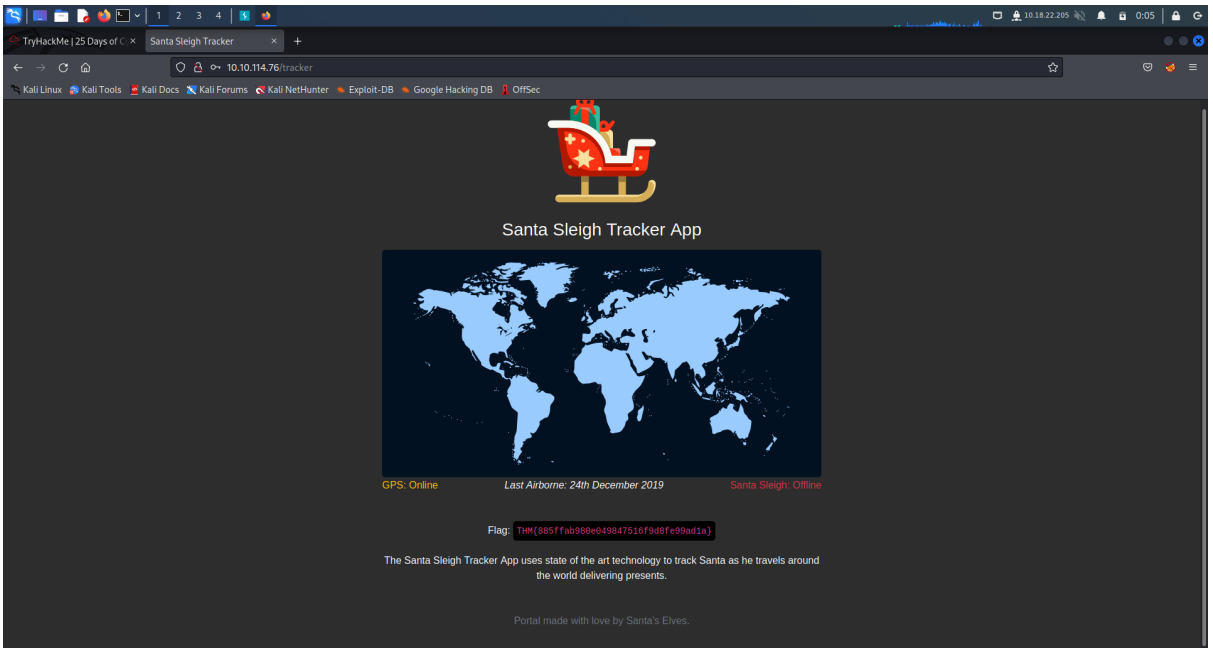






Question 4

We try the username and password from the previous question and it brings us to the Santa Sleigh Tracker App. From this page we obtained the flag THM{885ffab980e049847516f9d8fe99ad1a}.



Thought Process/Methodology:

Having accessed the target machine, we were shown a sign-in page. As there was no registration option, we had to use burpsuite in order to brute force the username and password in order to sign-in. We started by turning on burp using Foxy Proxy and also making sure that intercept was on in Burpsuite. After that we typed in some random details in the page and clicked sign-in. Burpsuite will now capture our request and we can send it to the intruder tab in Burpsuite. After selecting the attack type and entering in our username and password list we press attack and wait for it to finish. From the results, we can see that there is one combination that returned a different status code which is ‘admin’ and ’12345’. We then entered the details into the website and was granted access to the Santa Sleigh Tracker APP.

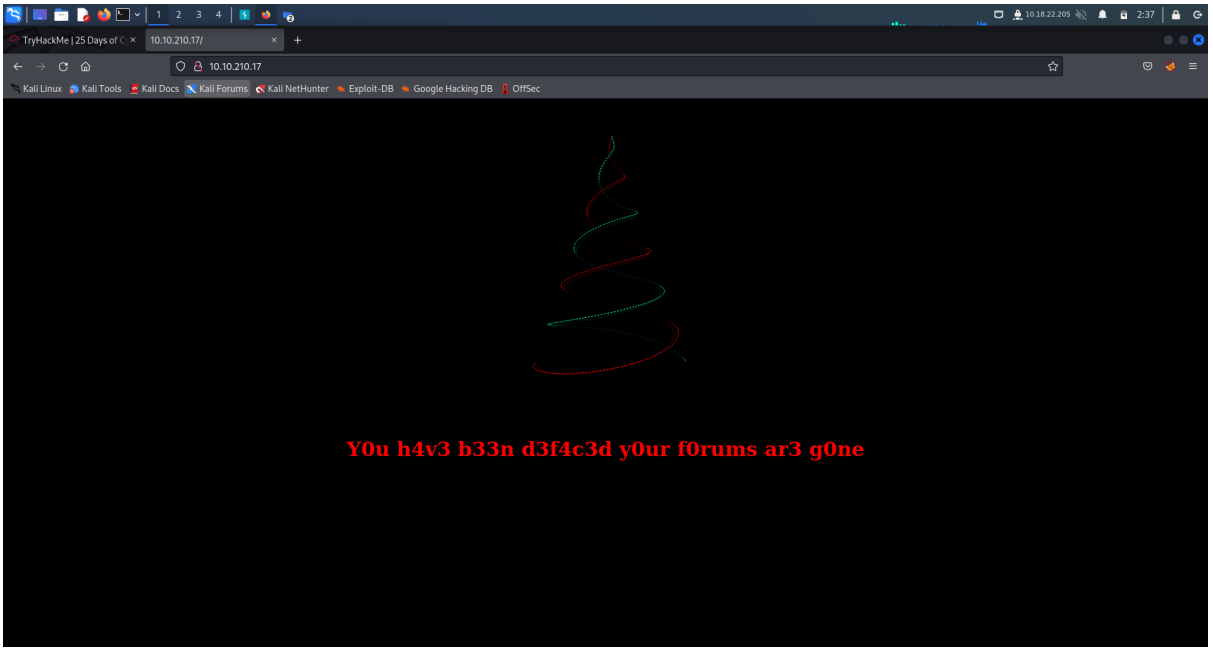
Day 4: Web Exploitation - Santa's Watching

Tools used: Kali Linux, Firefox, Gobuster, Wfuzz

Solution/walkthrough:

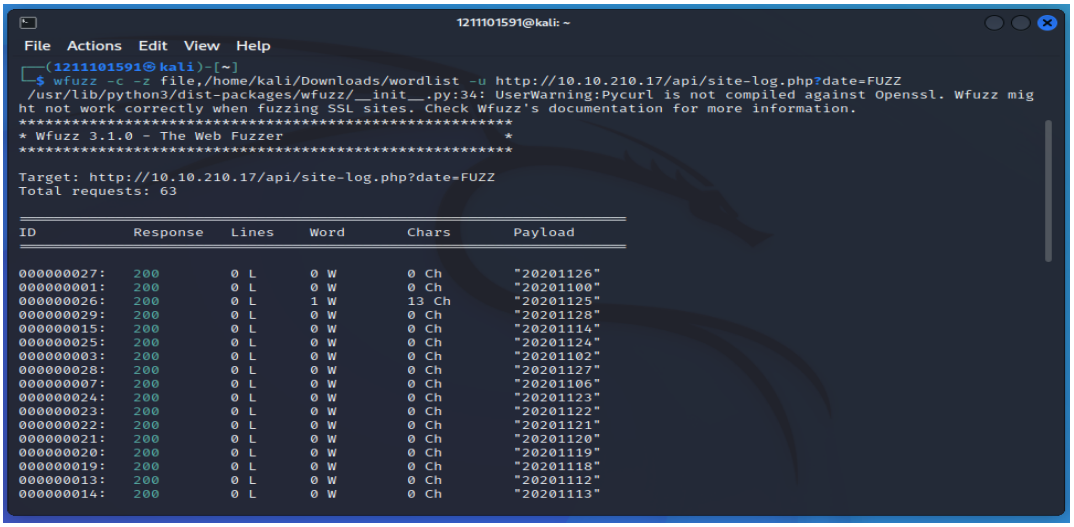
Question 1

Only a christmas and a line of text remains on the website. To find out the api we used gobuster using the list given which is big.txt. We found out that the api is located at /api. In the /api page we find a file called site-log.php



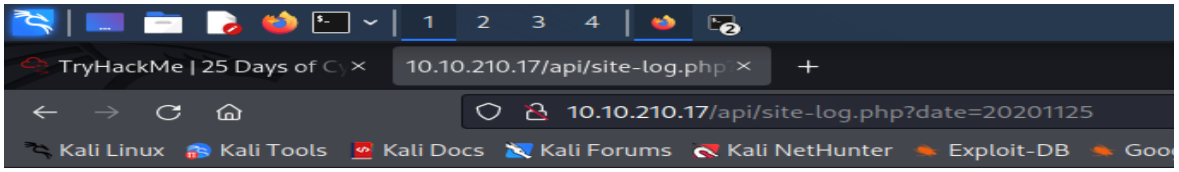
Question 2

Next we know that the api takes a date in the form of YYYYMMDD so we used wfuzz to numerate through a list of dates called wordlist. We found out that the date “20201125” has a different amount of characters than the others.



Question 3

We typed in the date found previously by adding “?date=20201125” and discovered the flag.



THM{D4t3_AP1}

Thought Process/Methodology:

By using gobuster, we found the api directory of our target domain. After we found the directory, we fuzzed the api/site-log.php directory and managed to find the payload to get the flag.

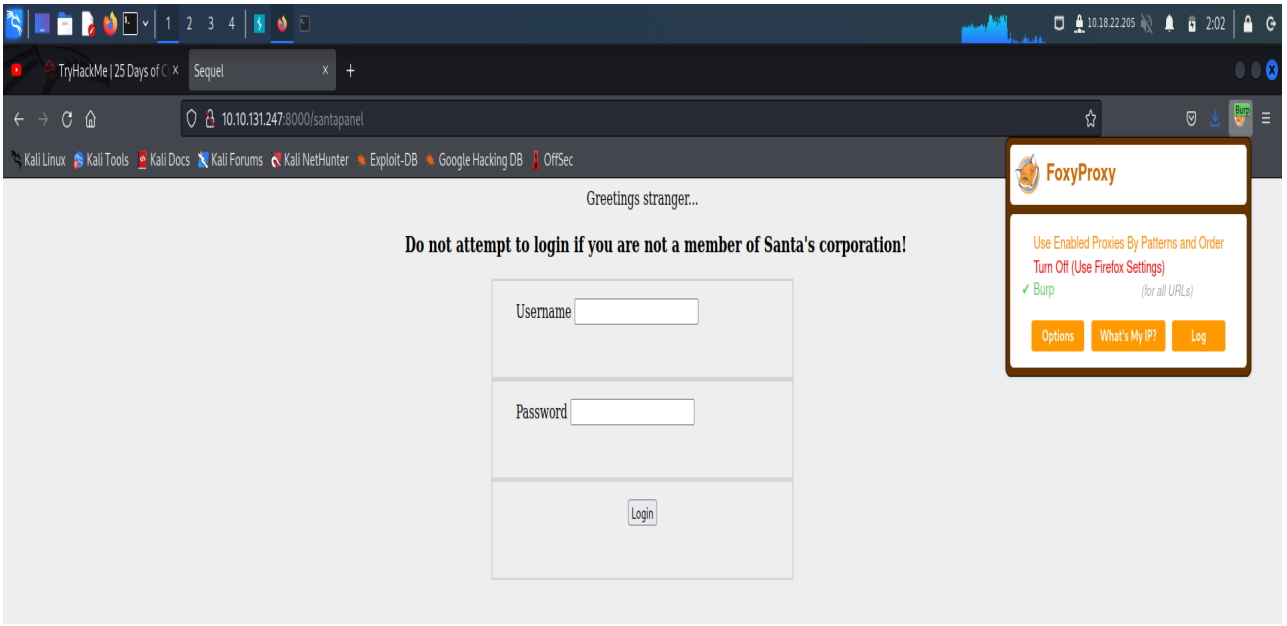
Day 5: Web Exploitation - Someone stole Santa's gift list!

Tools used: Kali Linux, Firefox, Burpsuite, SQLmap, FoxyProxy

Solution/walkthrough:

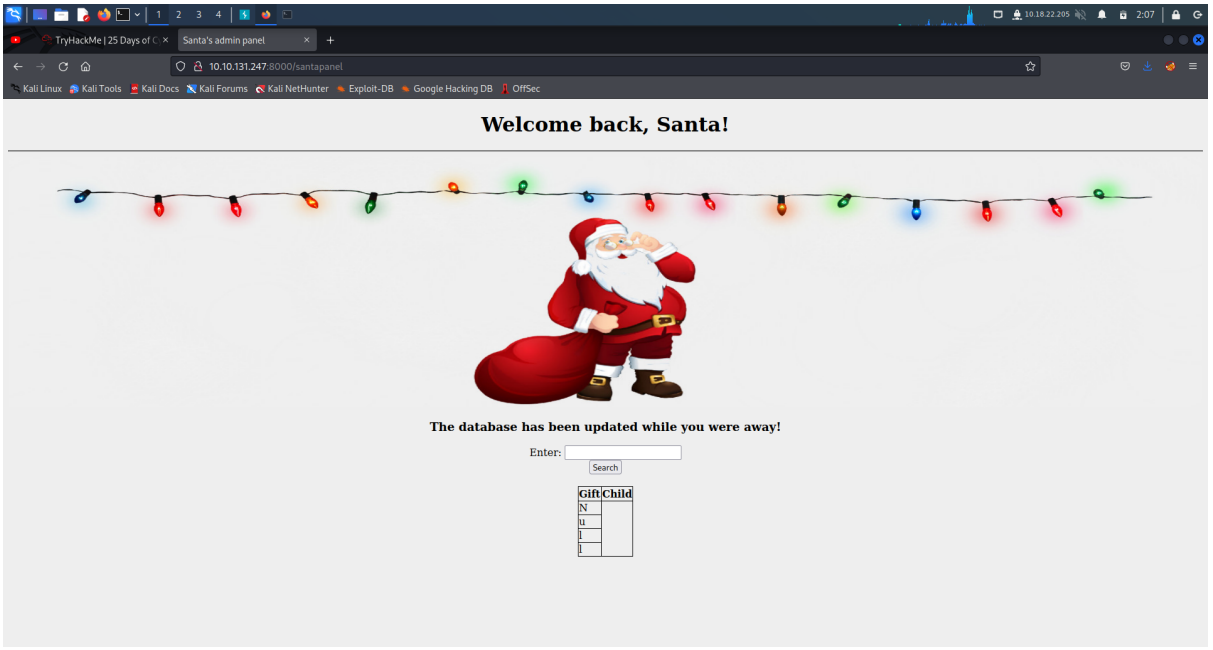
Question 1

By guessing, we figured out Santa's secret login panel.



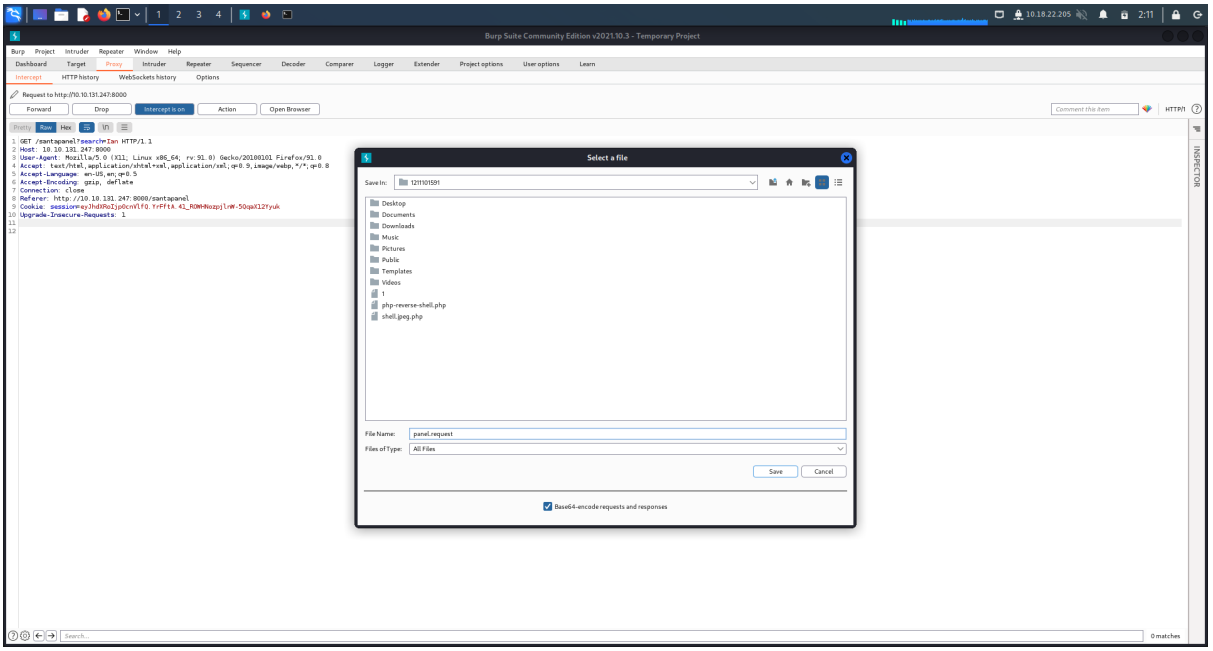
Question 2

By using a simple SQL statement such as ' or true; - - in the username field will bypass the login

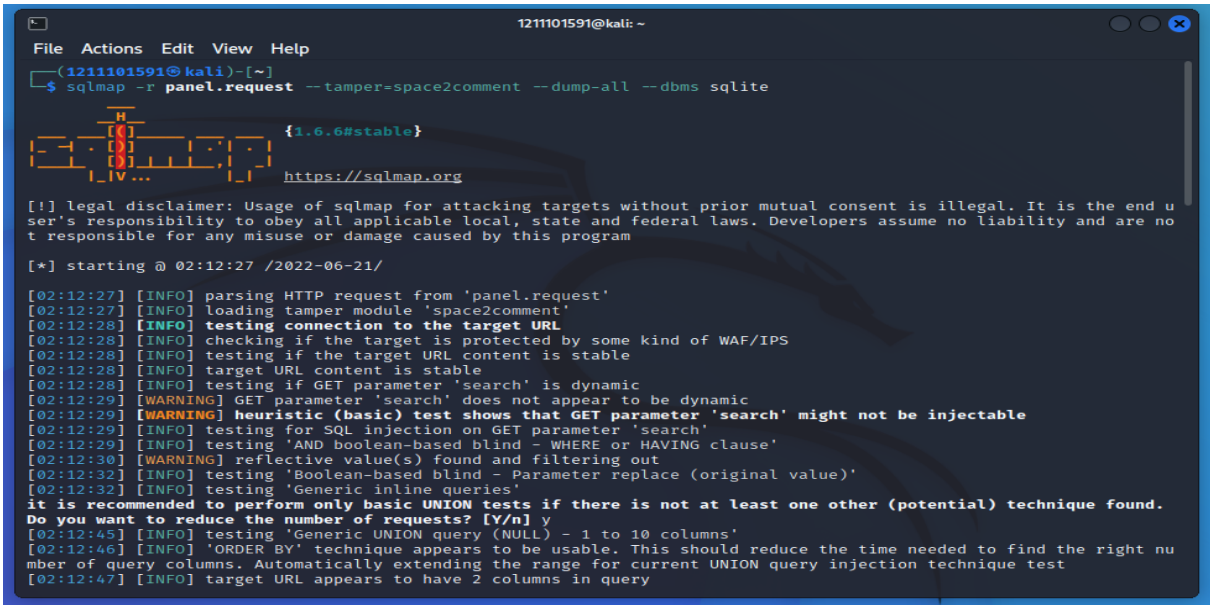


Question 3

We then make a query to the database and intercept it using burpsuite. After that we save the request as a file.

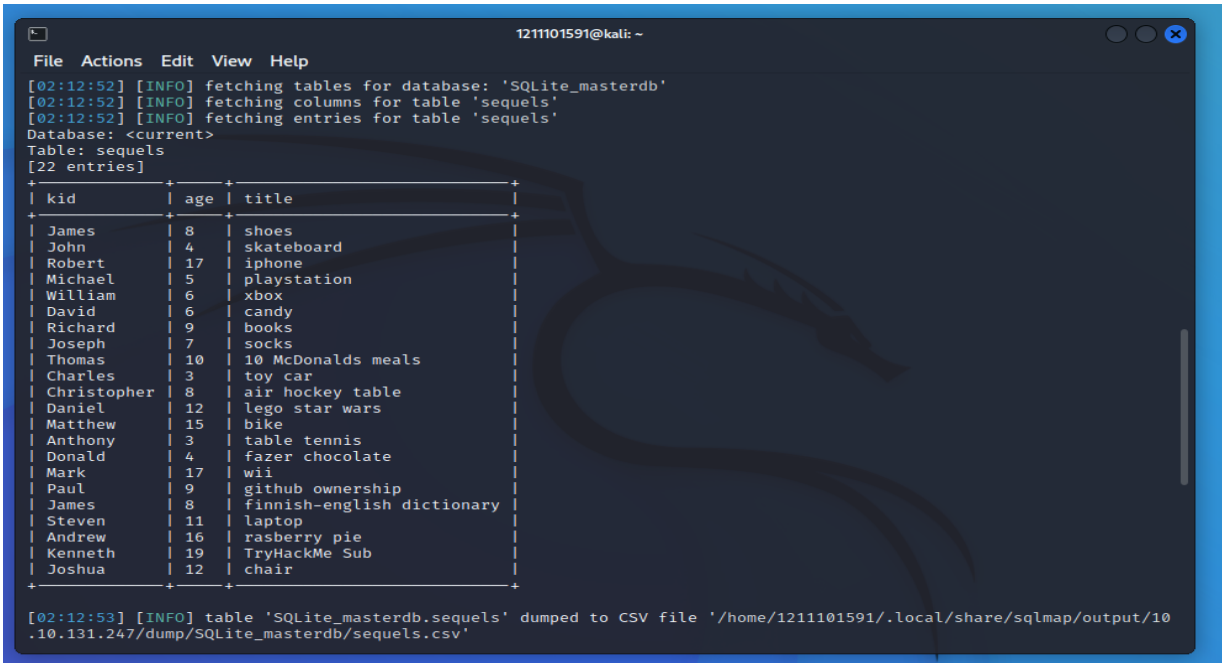


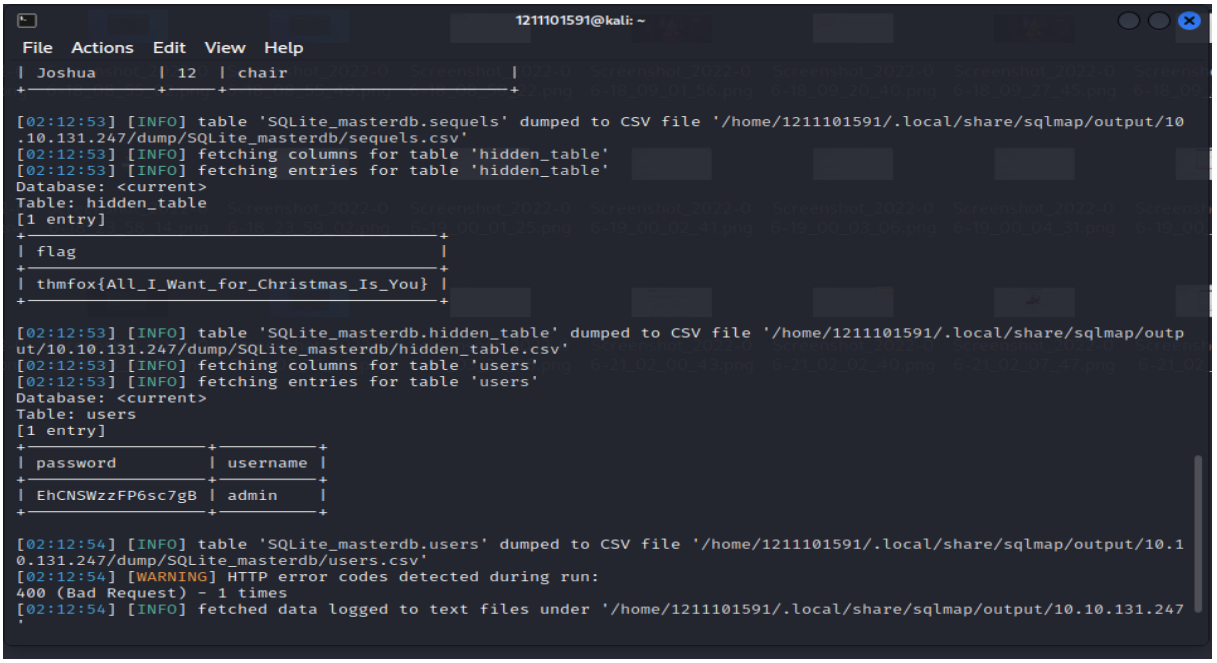
We then run SQLmap using the request file to file dump the database. We specified DBMS as SQLite as it was mentioned in santa's notes.



Question 4

There are a total of 22 entries in the gift database and paul asked for a github ownership. The flag and admin's password can also be seen below.





Thought Process/Methodology:

After accessing a page with nothing to interact with, we found out a hidden directory by using guessing/ trial and error which is /santapanel. Using SQLi we were able to bypass the login page and we were redirected to a database query page. We made a query and intercepted it using BurpSuite and saved it as a request file. After that, we used the request file to dump the whole database using SQLMap. We found the flag inside the “hidden_table” table.