PSP0201

Week 2 Writeup

Group Name : Ilomilo

Members:

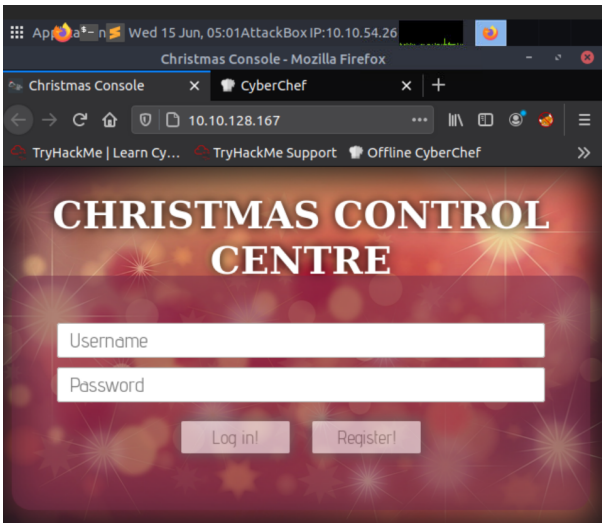
ID NUMBER	STUDENT NAME	Role
1211103196	Adriana Iman binti Noor Azrai	Leader
1211103282	Aida Maisarah binti Hisam	Member
1211103216	Sofea Hazreena binti Hasdi	Member
1211103227	Wan Alia Adlina binti Wan Azman	Member

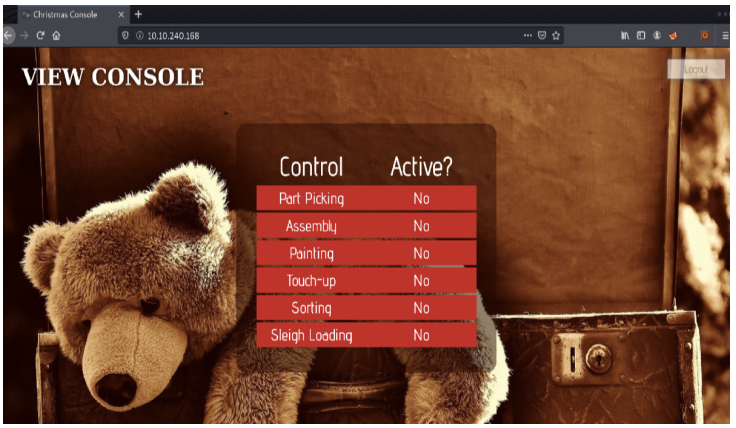
Day 1 - Web Exploitation A Christmas Crisis

Tools Used : Firefox

Solution/Walkthrough:

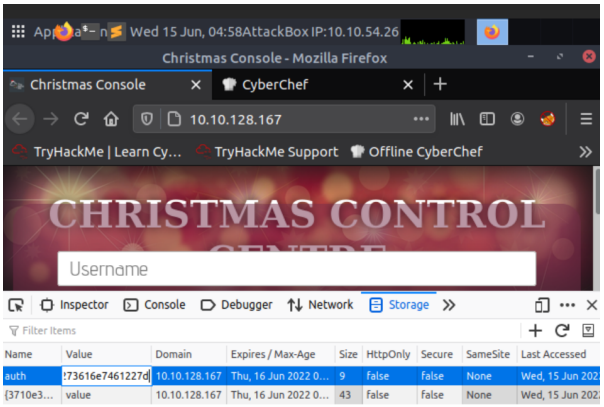
Question 1 : Inspect the website. What is the title of the website?
Register and log in to the Christmas Control Centre. No access to the control console and all were not active.
Username: adrnaimn
Password: **********





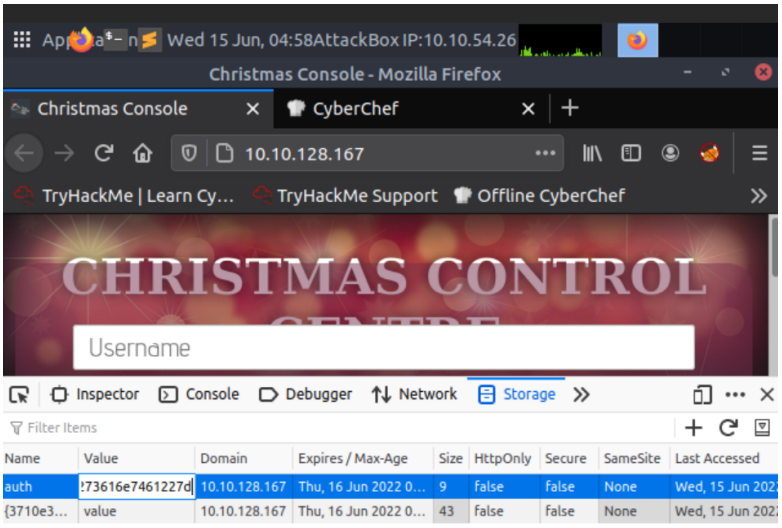
Question 2: What is the name of the cookie used for authentication?
Open up the browser development to see the cookies

\

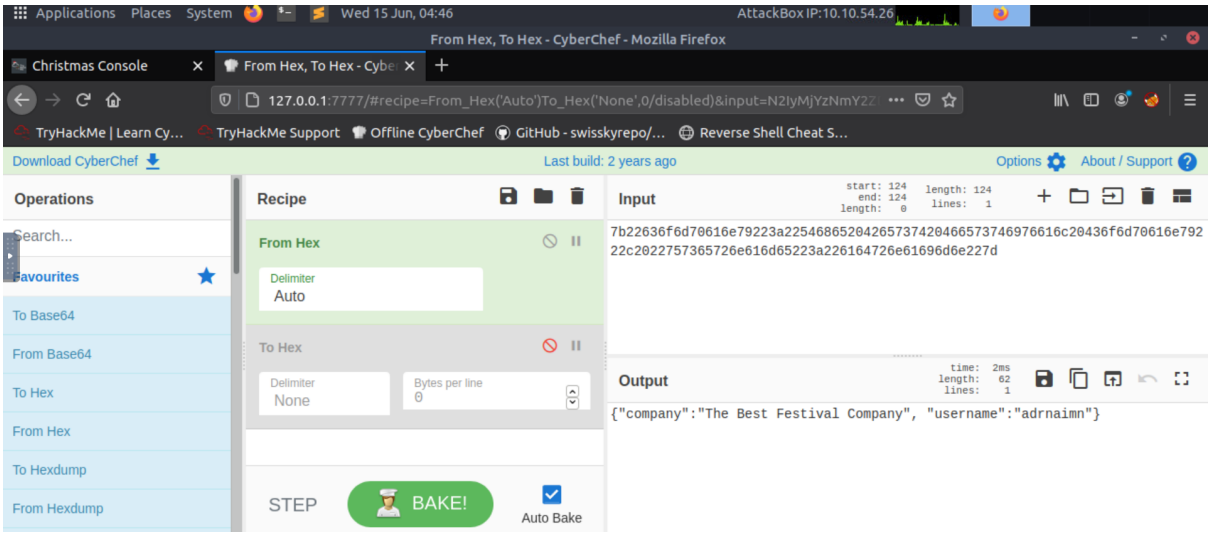


* Got the name of the cookie used : auth

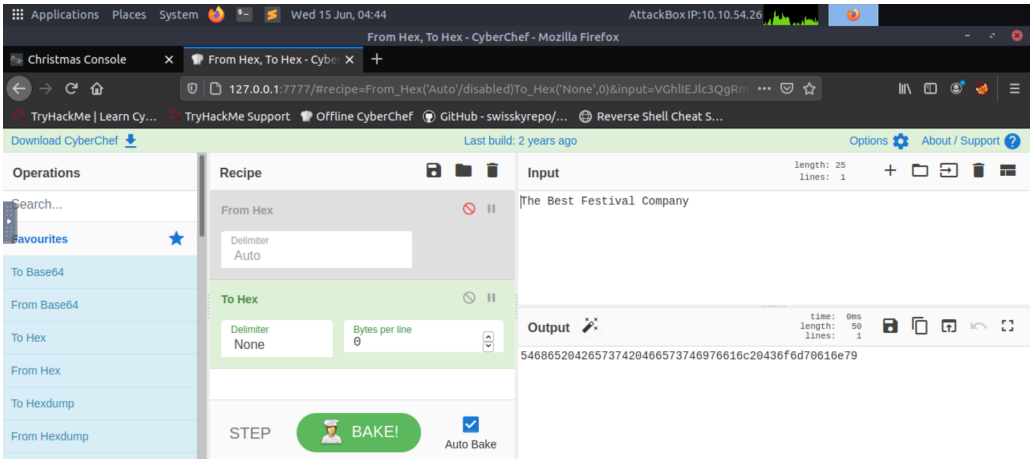
Question 3: In what format is the value of this cookie encoded?
Along with the cookie used, we also obtain the value of the cookie in a hexadecimal form.



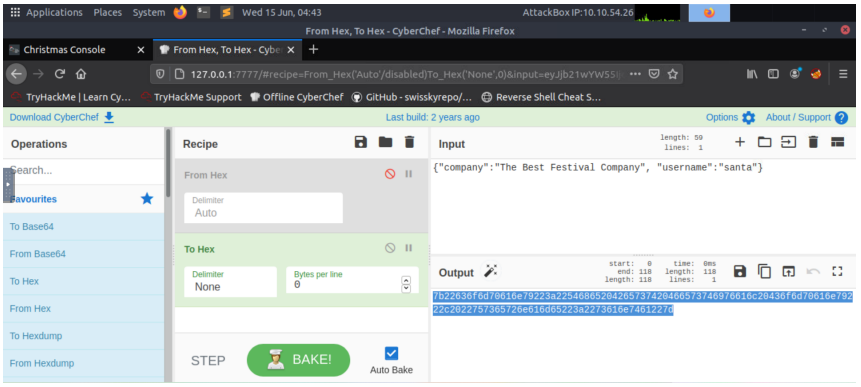
Question 4: Having decoded the cookie, what format is the data stored in?
Using Cyberchef, we convert the cookie value to string.



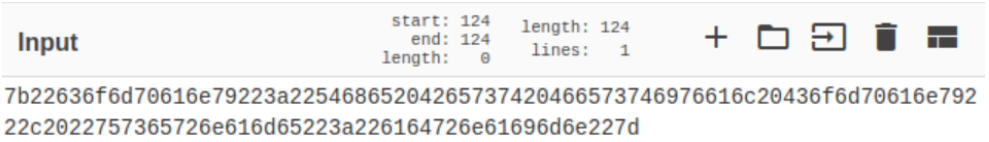
Question 5: What is the value for the company field in the cookie?
We copy pasted the company field in the cookie to obtain the value.

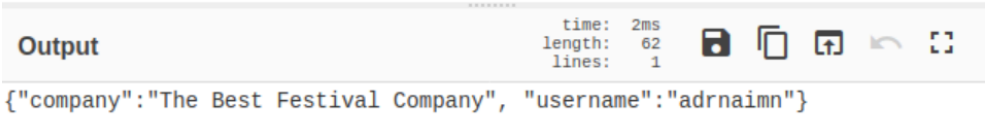


Question 6: What is the value of Santa's cookie?
We change the username from “adrnaimn” to “santa” and convert the JSON statement to hex

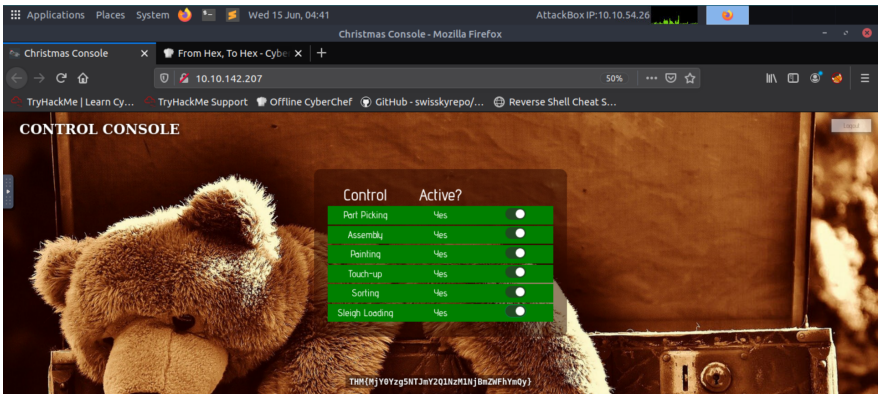


Question 7: What is the other field found in the cookie?
After we enter the cookie in the input, we find out that other than company, we also found there is a username, which is the username we insert during the sign up at the first step.





Question 8: What is the flag you're given when the line is fully active?
Now, we have access to the website and activate the control console and receive the flag.



Throughout process:
Having accessed the target machine, we were shown a login page. However, we needed to register with our own username and password and we were accessed to the control console and each of the controls was inactive. Thus, we chose to view the site cookie from the Storage Tab. Looking at the cookie value, we examined it to be a hexadecimal value and proceeded to convert it to text using Cyberchef. Using the platform, we altered the ‘adrnaimn’ username to ‘santa’ and converted it to hexadecimal again. We changed the cookie value and we refreshed the website. We are now shown the ‘Santa’s’ administrator page and managed to enable every control, which proceeds to be revealed with a flag code.

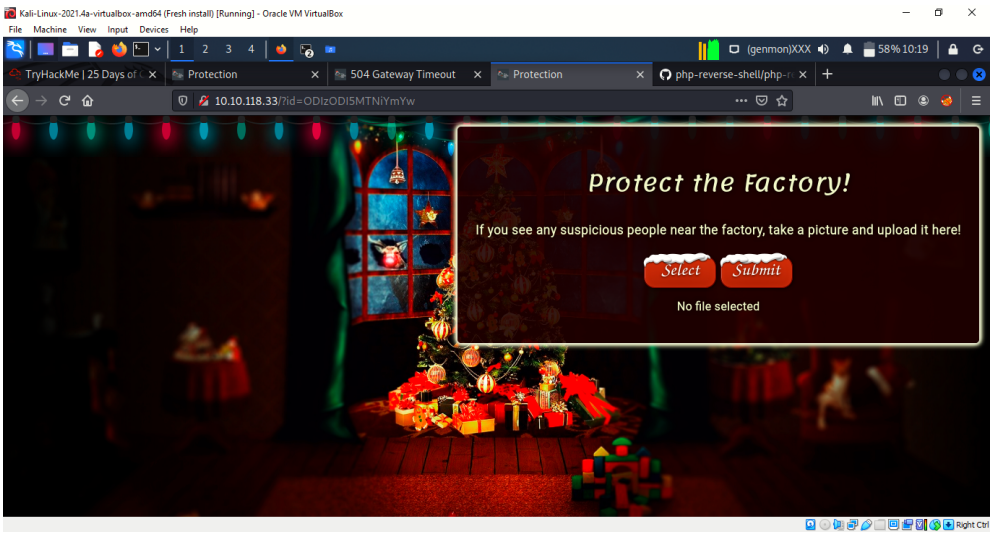
Day 2 - Web Exploitation The Elf Strikes Back!

Tools used: Kali linux, Firefox, Terminal

Solution/Walkthrough:

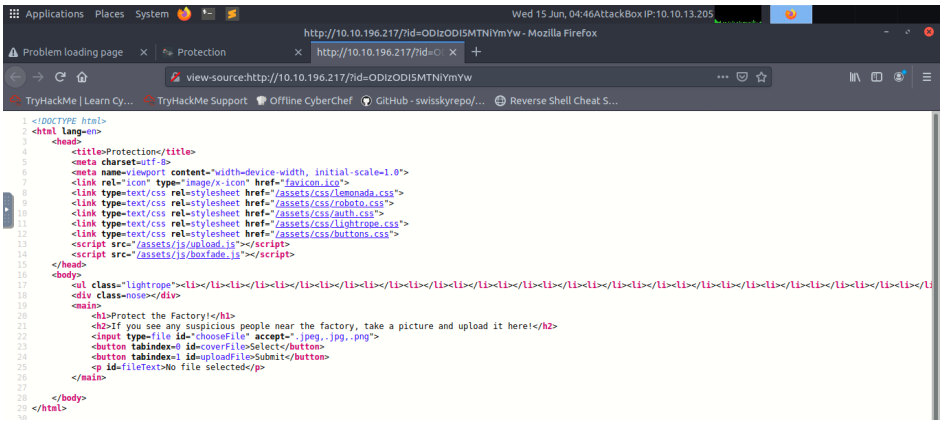
Question 1: What string of text needs adding to the URL to get access to the upload page?

Add the GET parameter to the Ip Address and paste the id number.



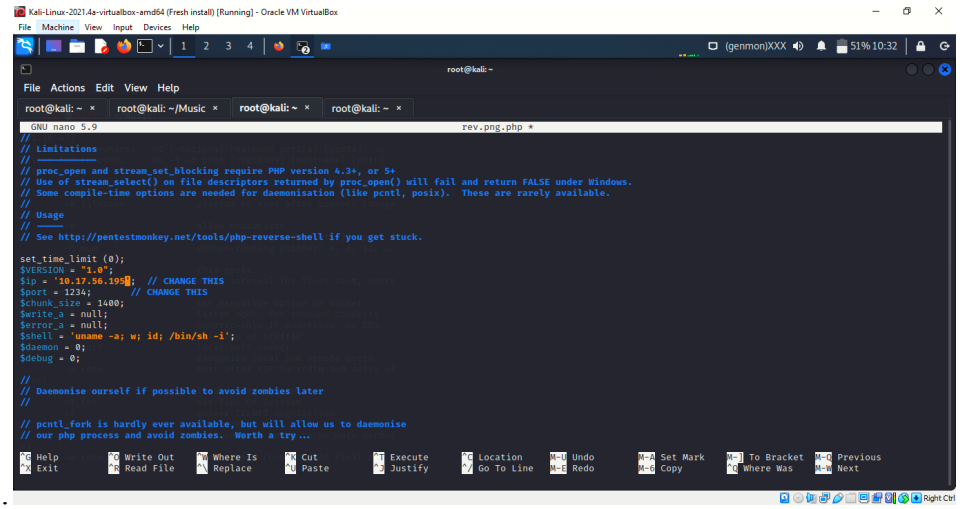
Question 2: What type of file is accepted by the site?

View the page source and the file accepted by the site is in .png, .jpg and .jpeg.



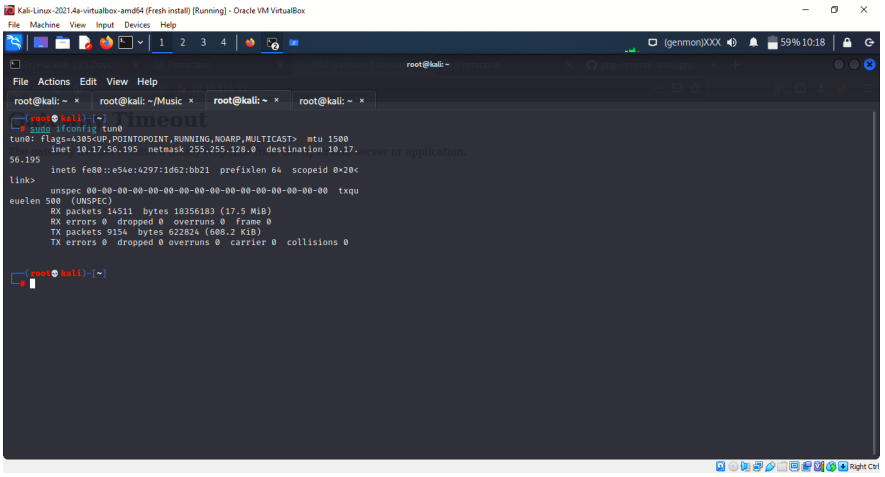
Question 3: In which directory are the uploaded files stored?

Copy the webshell out to the directory and rename the title and extension. Open it with nano. Change the ip and port number remains the same .

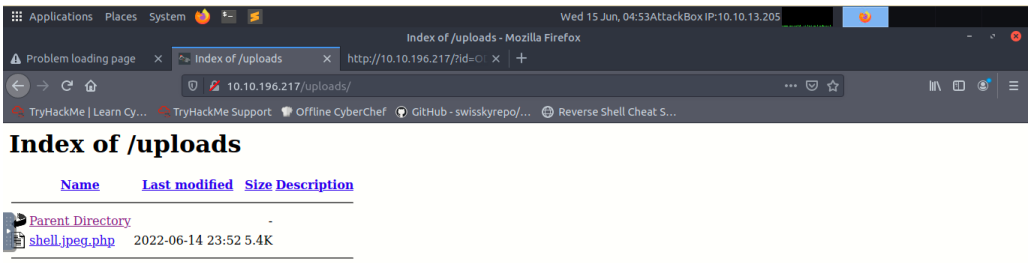


.

Ip can be found by running ‘sudo ifconfig tun0’ .



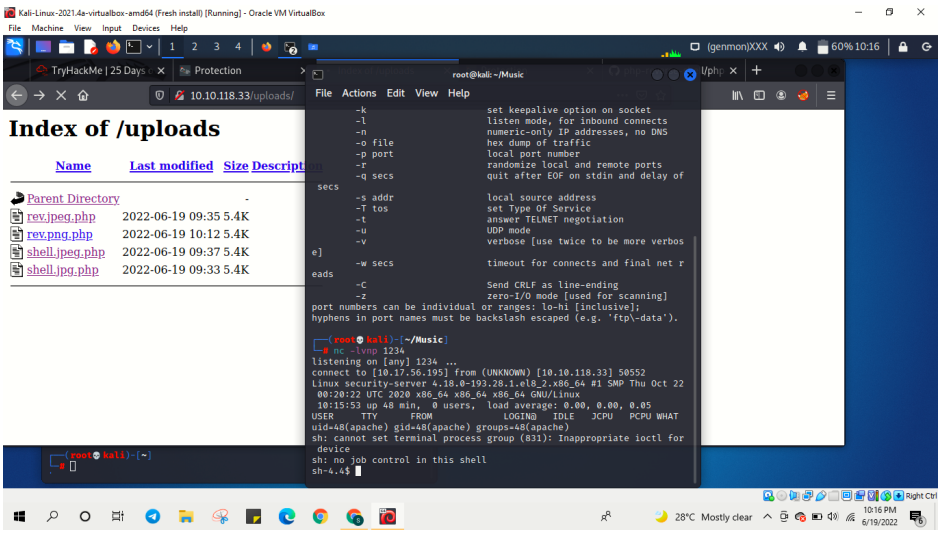
Remove the parameter and change it to /uploads/. The uploaded file has shown.



Addition: Activate your reverse shell and catch it in a netcat listener!

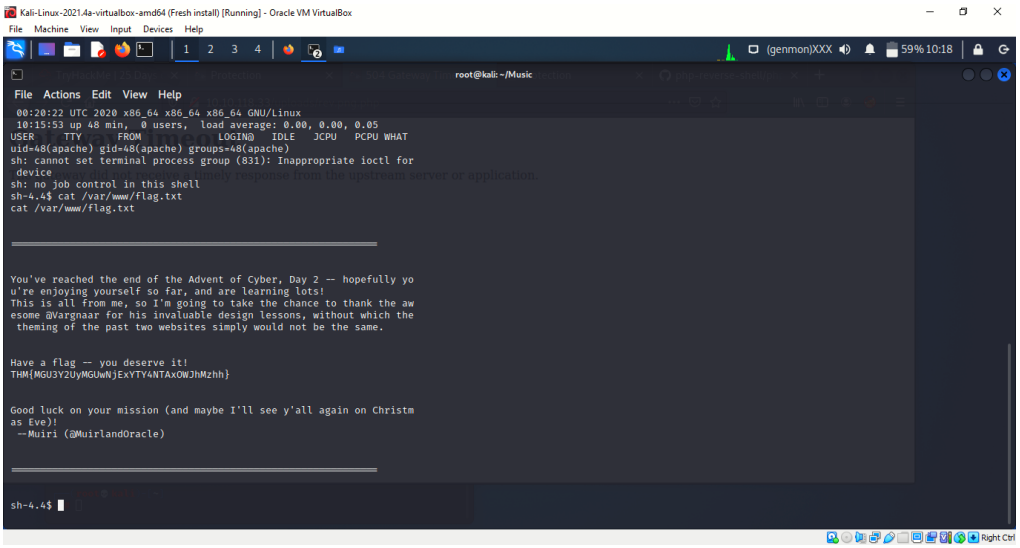
Question 4: Read up on netcat's parameter explanations. Match the parameter with the explanation below.

In the next tab, create the listener for the uploaded reverse shell by using ‘nc lvnp 1234’ command. Upload a reverse shell and then start the cat listener to receive their shell navigate and receive the connection.



Question 5: What is the flag in /var/www/flag.txt?

Run the command cat /var/www/flag.txt and the content of the flag is displayed.



Throughout Process:

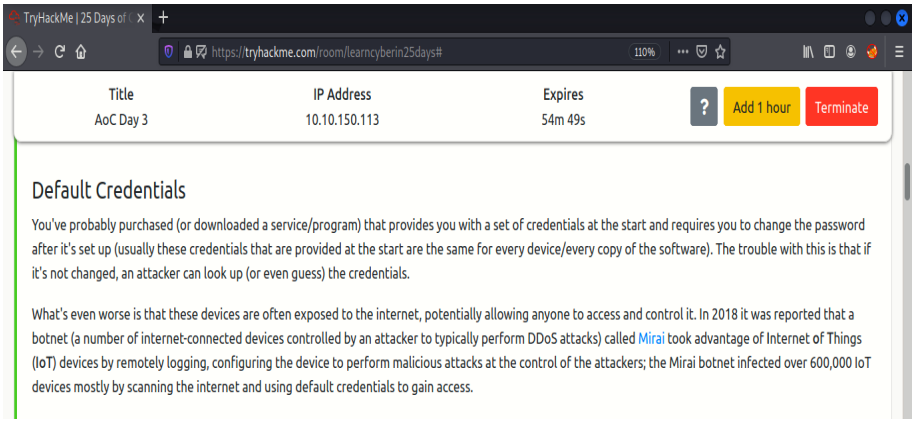
Copy the Ip Address then add the GET parameter and the id number to gain access to the upload section. Right click on the page to view the page source and it shows that the file accepted by the site is in .png, .jpg and jpeg. After that, copy the webshell to the directory and rename the title and extension according to the file name. Open it with nano and scroll down to set the ip. Change the ip which can be found by running ‘sudo ifconfig tun0’ and the port remains the same. To see the uploaded file, change the parameter and id number to /uploads/. Next, in the next tab, use the 'nc lvnp 1234' command to create a listener for the uploaded reverse shell. Upload a reverse shell, then start the cat listener to get their shell navigation and connection. Lastly, the content of the flag is revealed when we run the command cat /var/www/flag.txt.

Day 3 - Web Exploitation Christmas Chaos

Tools used: Firefox, Kali linux, Burp Suite

Solution/Walkthrough:

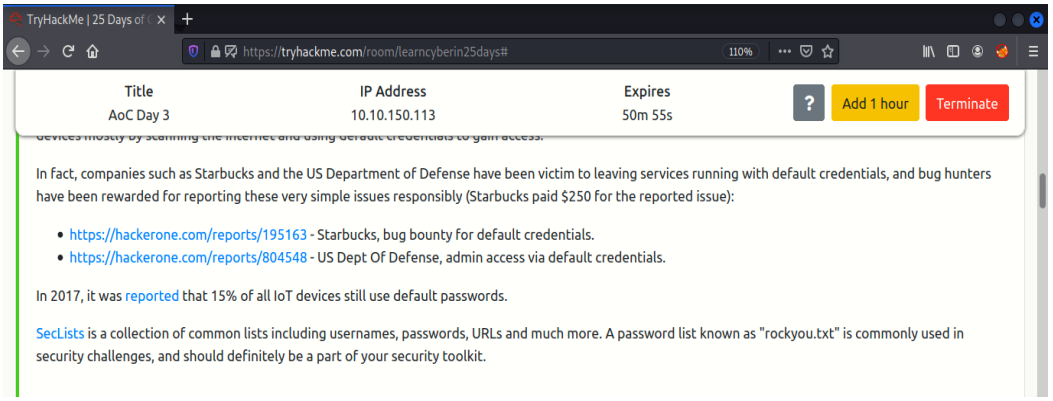
Question 1: What is the name of the botnet mentioned in the text that was reported in 2018?



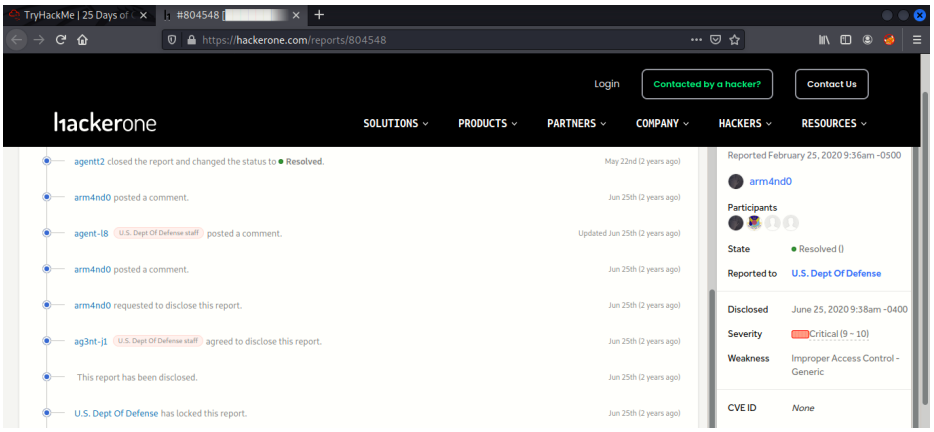
*In the second paragraph, the second line tells us that the name of the botnet that was reported in 2018 is Mirai.

Question 2: How much did Starbucks pay in USD for reporting default credentials according to the text?

*in the bracket, it tells us that Starbucks paid 250 USD for the reported issue.



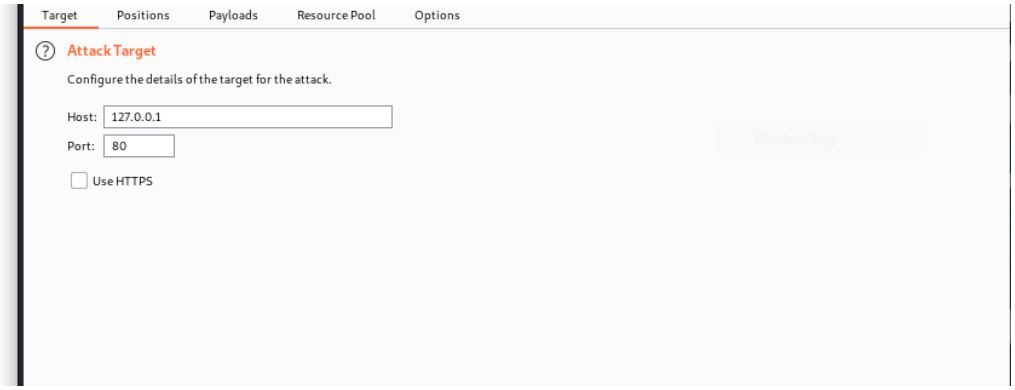
Question 3: Read the report from Hackerone ID:804548 - who was the agent assigned from the Dept of Defense that disclosed the report on June 25th?



*Based on the report from Hackerone ID:804548, it was reported that ag3nt-j1 was the agent who agreed to disclose the report.

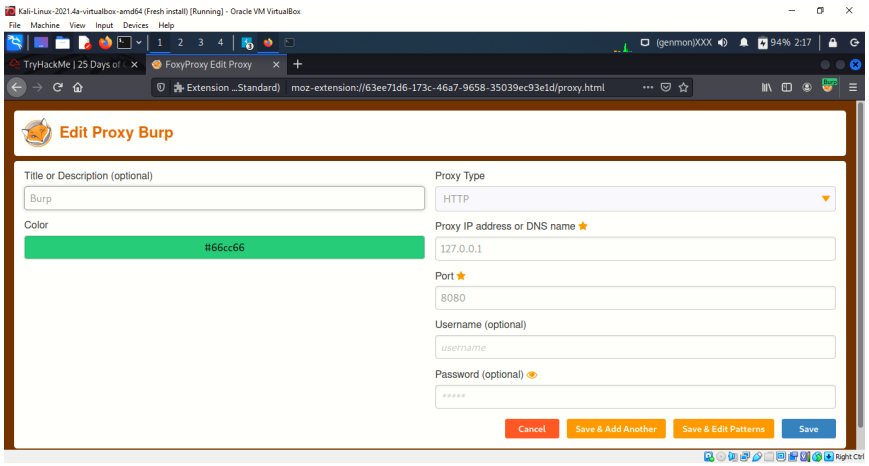
Question 4: Examine the options on FoxyProxy on Burp. What is the port number for Burp?

At the burpsuite, we select the intruder button and then we will see the host and port number for burp.



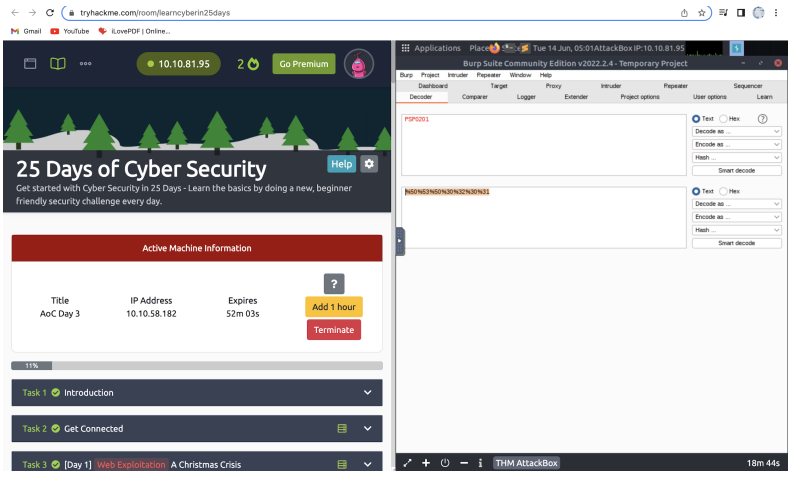
Question 5: Examine the options on FoxyProxy on Burp. What is the proxy type?

Back to firefox, on the sidebar there is the FoxyProxy button, we then click on the “options” button and we are directed to a new webpage. On the left side of the webpage there’s a button called “add”, we click it and then we can see the proxy type.



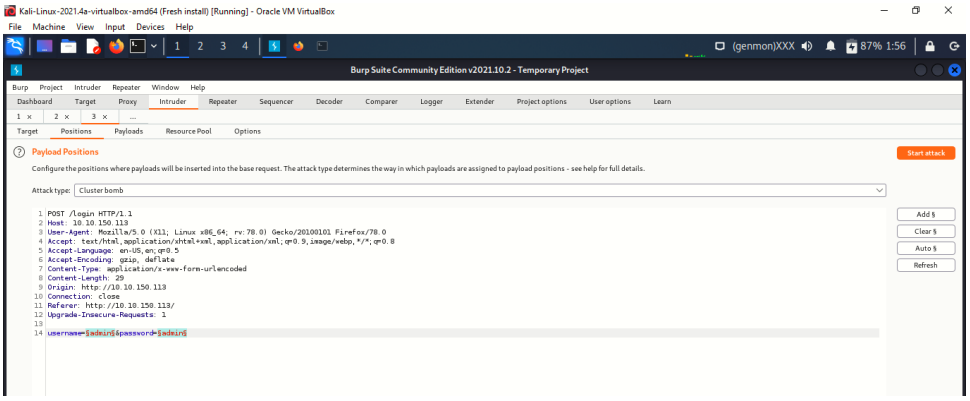
Question 6: Experiment with decoder on Burp. What is the URL encoding for "PSP0201"?

Using the decoder on Burp, we typed in PSP0201 and got the URL encoding in the Burp.

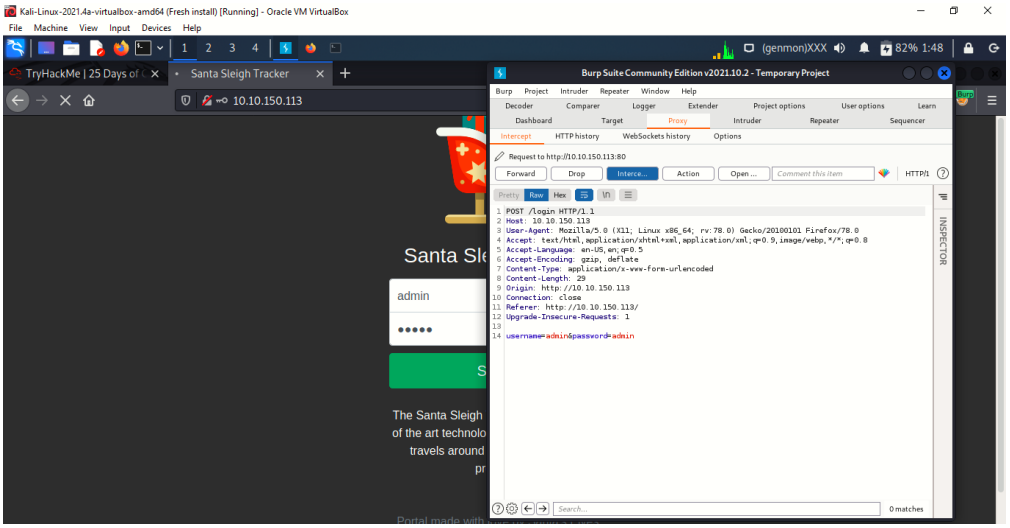


Question 7: Look at the list of attack type options on intruders. Which of the following options matches the one in the description?

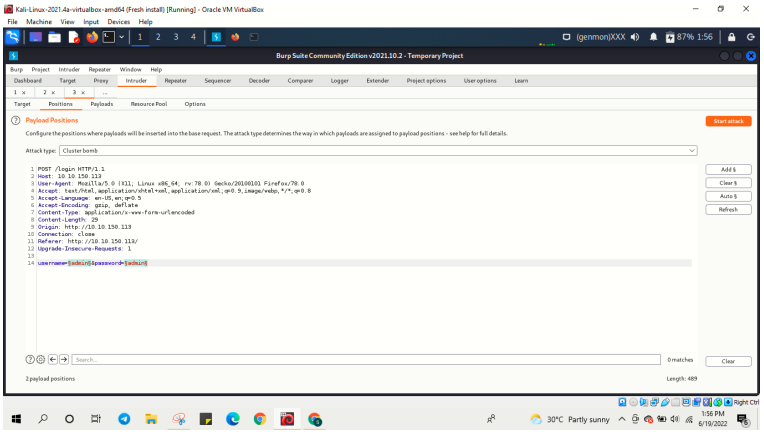
On the burpsuite, we then select the intruder and position button. We then add the username and password values positions. We highlighted the username and password and then clicked the "add $" button. After that, at the attack type dropdown, we then select cluster bomb as the attack type. In the payloads tab, we select our payload set and add select the list in the 'Payload Options'. Then, we add a few common default username entries such as "admin", "root" and "user". We also add a few common default passwords such as "password", "root", "12345". When we click the "Start Attack" button, it will loop through each position list in every combination.



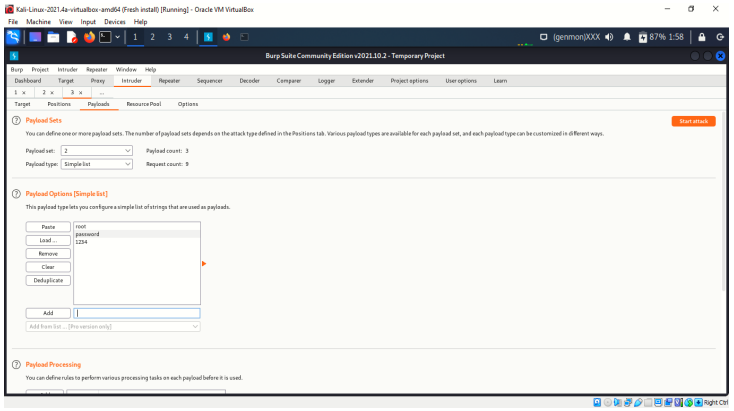
Question 8: What is the flag?

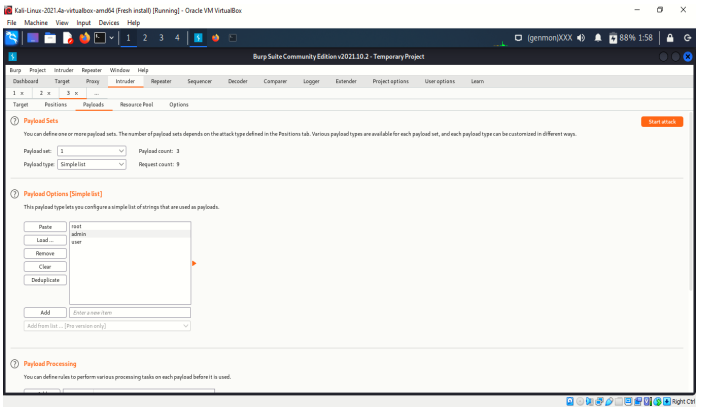


All the data that we received we send it to the intruder for the intruder to automate customised web attacks. We click the ‘Add $’ to highlight the username and password.

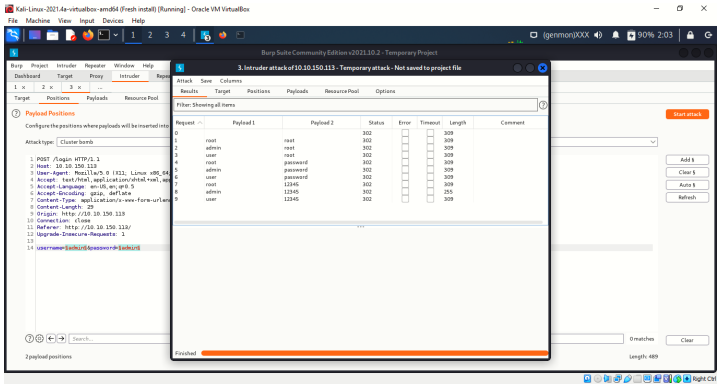


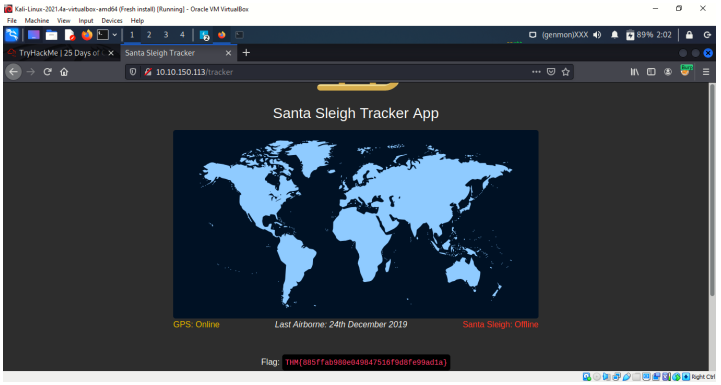
Then, we add a few common default username entries such as “admin”, “root” and “user”. We also add a few common default passwords such as “password”, “root”, “12345”.





When we click the “Start Attack” button, it will loop through each position list in every combination. Using the following lists of the username and password, we logged in the website, and we will receive the flag for day 3.





Throughout process:

Before we went through our Kali, we went through the description and instruction given in the task. There, we find out the name of the botnet mentioned that was reported in 2018. We also found out the answer for how much Starbucks pays in USD. Reading the report from Hackerone ID:804548, we find out the agent assigned from the Dept of Defense was ag3nt-j1. Next, having accessed the target machine, Santa Sleigh Tracker, we were shown a sign in page. However, we were required to visit the burp suite to examine the options on FoxyProxy. There we can find the port number of Burp and also the proxy type of it. In Burp, we were able to find the URL encoding for PSP0201 using the decoder on Burp. After that, we reload the Santa Sleigh tracker. We forward the intercept in the Burp to make sure the website is actually loaded. Then, we sign in the website with username: admin and password: ****. Then, under proxy, we managed to get the data along with the username and password that we created on the website. All the data that we received we send it to the intruder for the intruder to automate customised web attacks. Then, we go to the intruder tab and under the position tab, we clear the pre-selected position and add the username and password values as position. We highlight the text using 'add $' box and select cluster bomb as the attack type. In the payloads tab, we select our payload set and add select the list in the 'Payload Options'. Then, we add a few common default username entries such as "admin", "root" and "user". We also add a few common default passwords such as "password", "root", "12345". When we click the "Start Attack" button, it will loop through each position list in every combination. Using the following lists of the username and password, we logged in the website, and we will receive the flag for day 3.

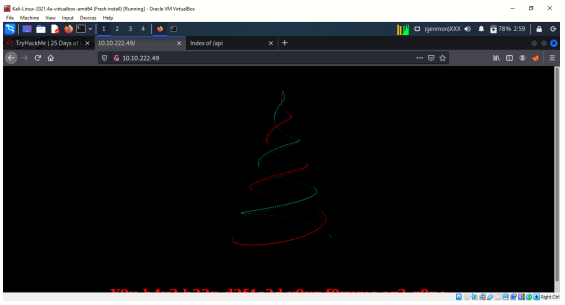
Day 4 - Web Exploitation Santa's watching

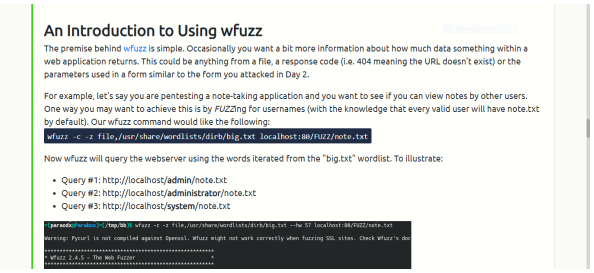
Tools used: Kali linux, Terminal, Firefox

Solution/Walkthrough:

Question 1: Given the URL "http://shibes.xyz/api.php", what would the entire wfuzz command look like to query the "breed" parameter using the wordlist "big.txt" (assume that "big.txt" is in your current directory

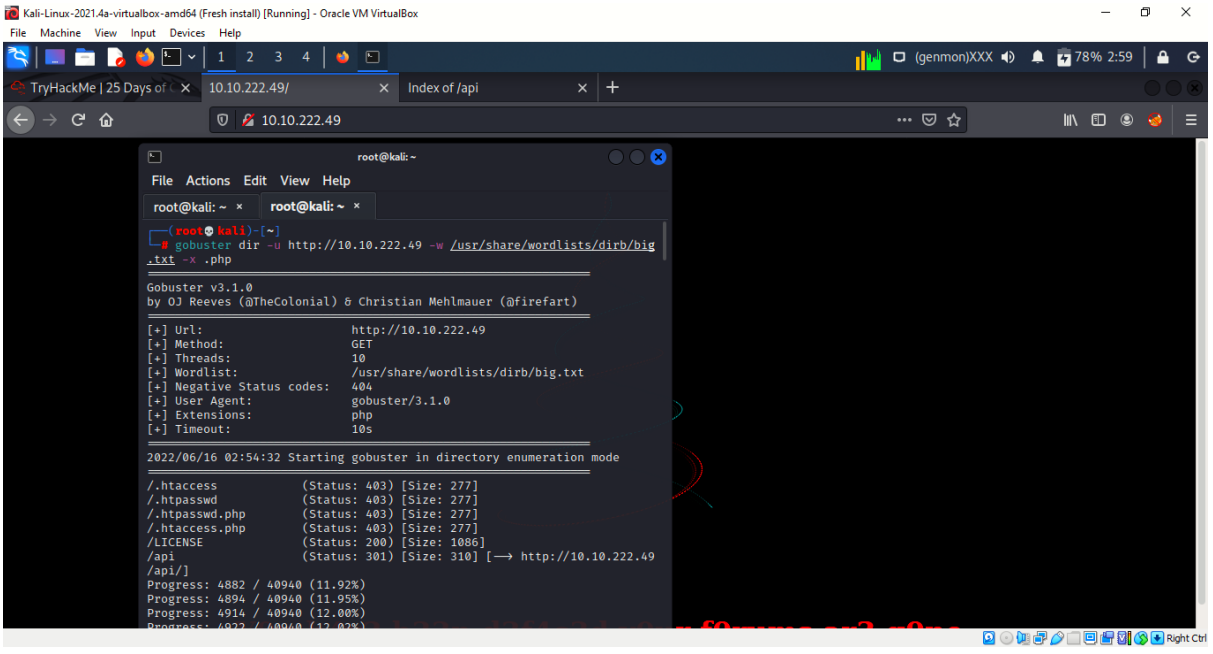
Paste the wfuzz command into the directory. Change the local host part with the URL given and add 'breed' parameter.



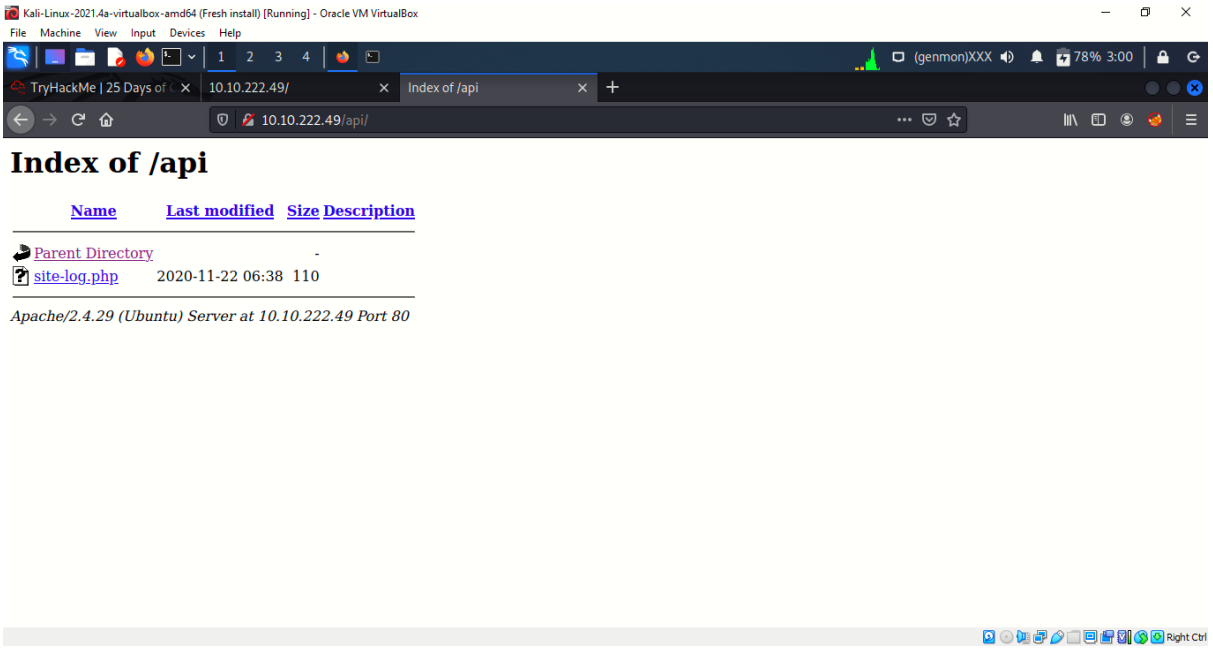


Question 2 : Use GoBuster (against the target you deployed -- not the shibes.xyz domain) to find the API directory. What file is there?

In the terminal, use GoBuster to find the possible directory. Insert Ip address in the command and it starts working.

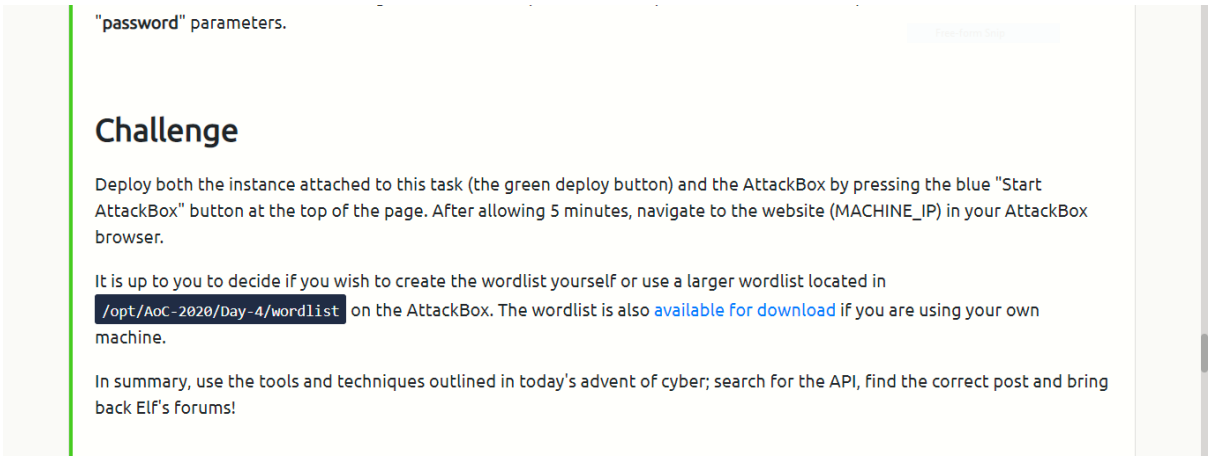


Open Firefox and search Ip Address/api/

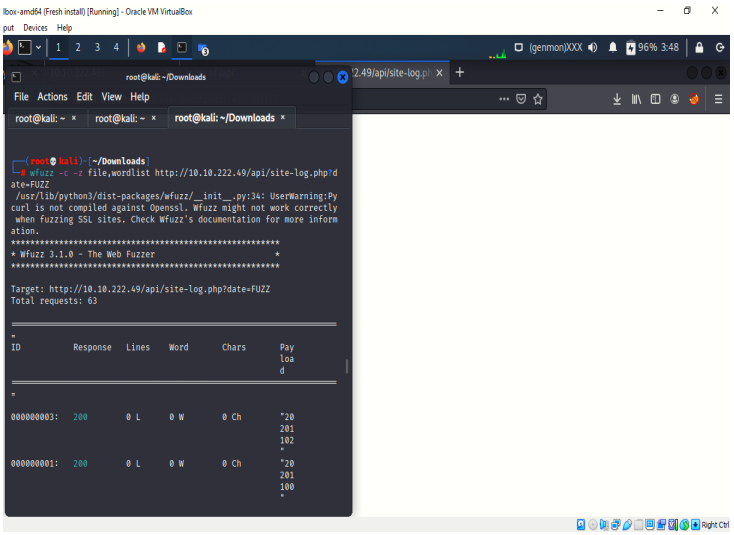


Question 3: Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?

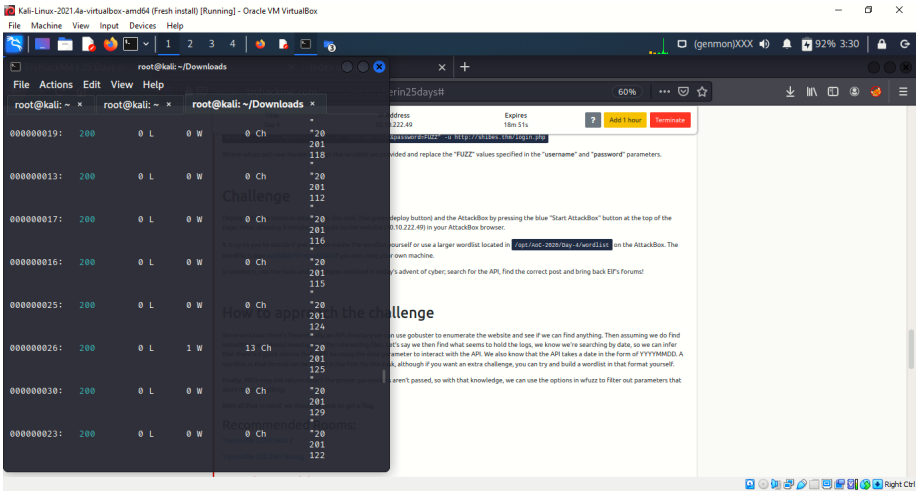
Download the wordlist and save in the download file.



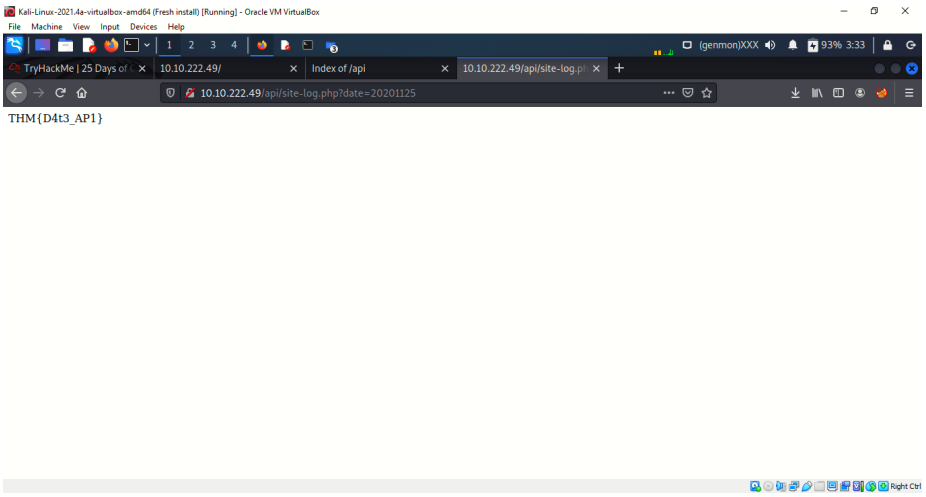
Insert wfuzz command in the terminal and paste the name of the wordlist file.



Scroll down and find the specific id (1 word and 13 characters)



Go to Firefox, insert the date(20201125) and enter, the flag is displayed.



Throughout process:

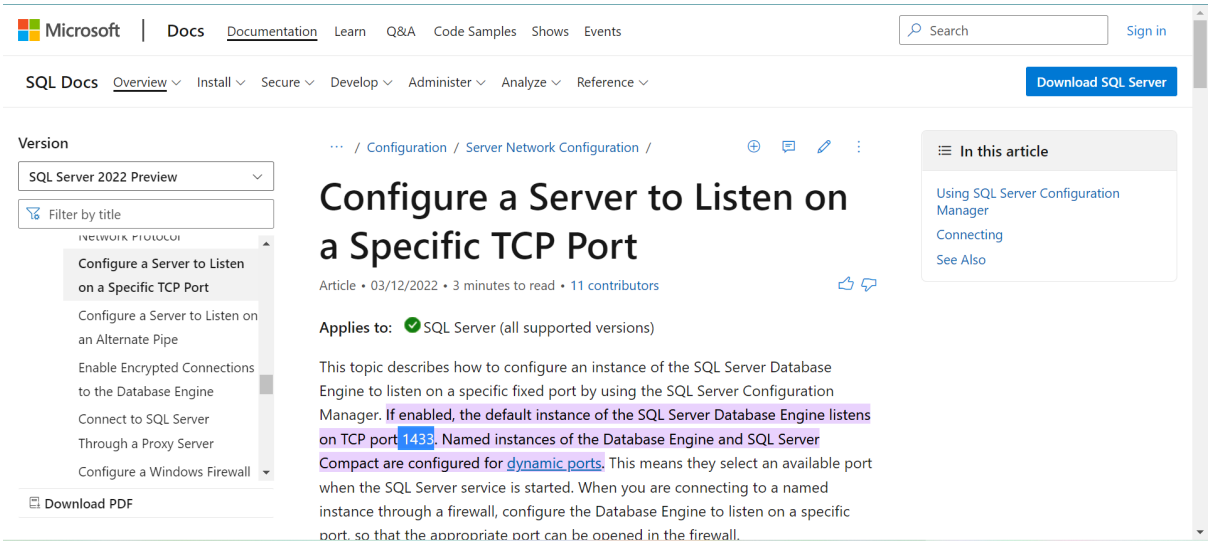
Firstly, refer to the wfuzz command given and change the local host part and add the parameter needed which is breed. Then, to find the possible directory, use GoBuster and insert Ip Address in the command and press enter. Open FireFox, search IpAddress/api/ and we found the file(site-log.php) inside the directory. Next, download the wordlist (link provided) and save in the download file. In the terminal, we insert the wfuzz command and paste the name of the wordlist file name in the command. Press enter and it starts working. After that, scroll down and find the specific id which contains 1 word and 13 characters. Go to Firefox, add the date from the terminal (1 word & 13 characters) in the URL and the flag is displayed on the site.

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

Tools used: Kali linux, Burpsuite, Terminal, Firefox

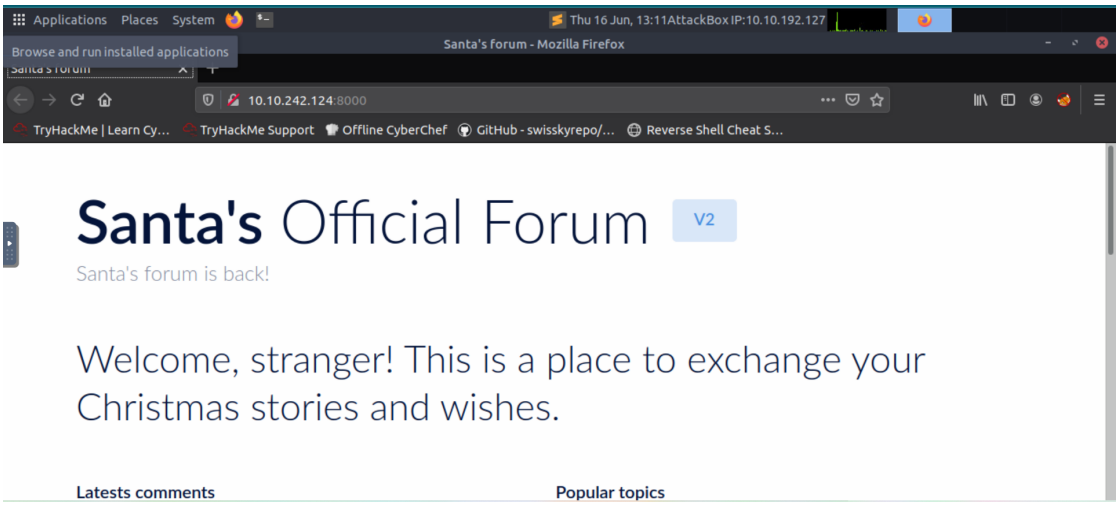
Solution/Walkthrough:

Question 1: What is the default port number for SQL Server running on TCP?
This is based on Microsoft's documentation found on google.com

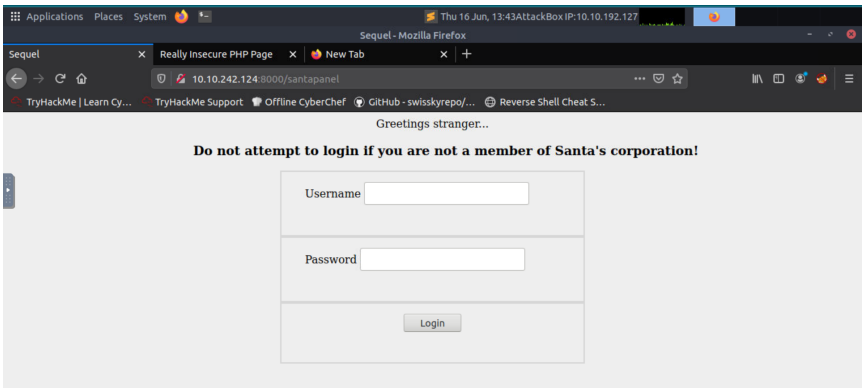


Question 2: Without using directory brute forcing, what's Santa's secret login panel?

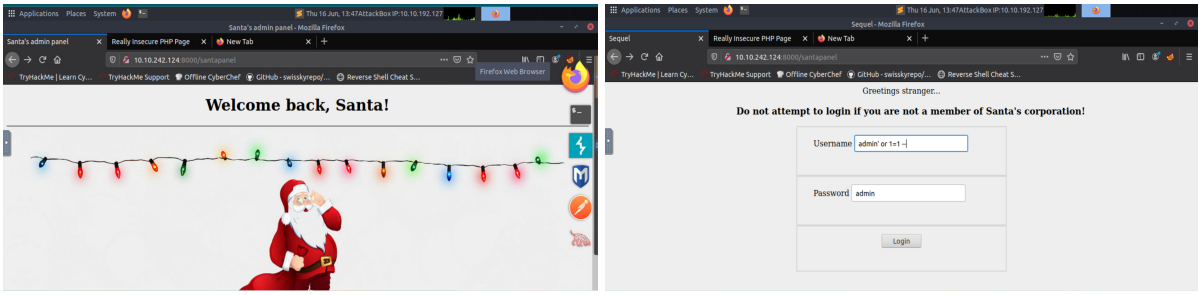
Typing in the ip address into firefox, we were directed to santa's official forum



So, from the ip address, we typed in “/santapanel” and discovered Santa’s secret login panel

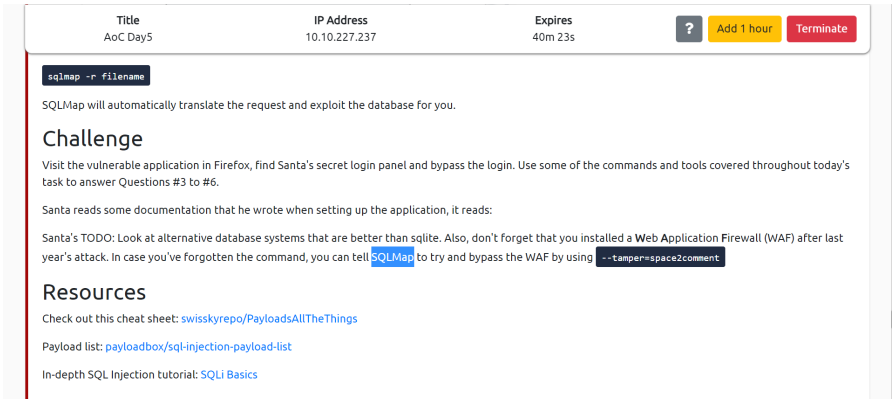


Then, by typing in [admin’ or 1=1 –] into username and [admin] into password, we were able to enter the secret panel



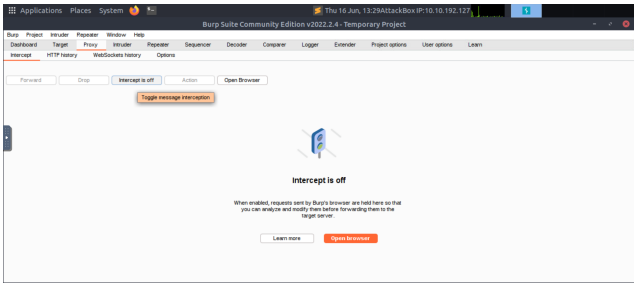
Question 3: What is the database used from the hint in Santa's TODO list?

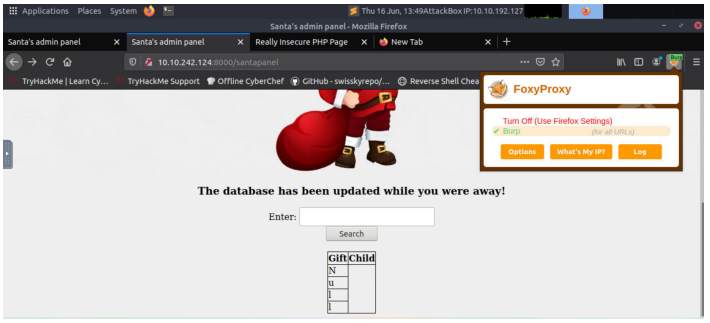
This is based on the instruction given where it instructed us to use sqlmap to try and bypass the web application firewall



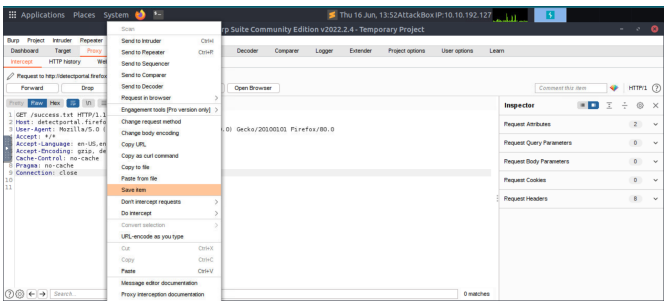
Question 4: How many entries are there in the gift database?

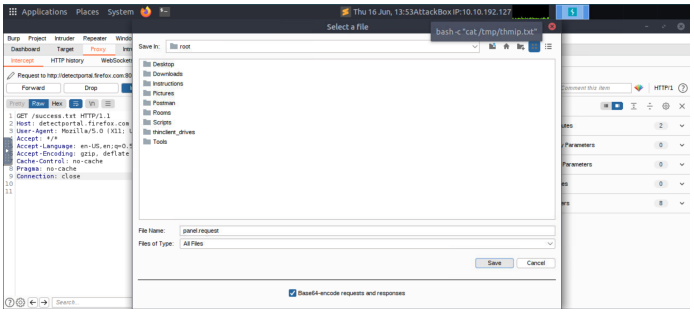
Open a temporary project on burpsuite community edition, and connect burp to foxyproxy on firefox. Then turn off intercept to avoid any disturbance



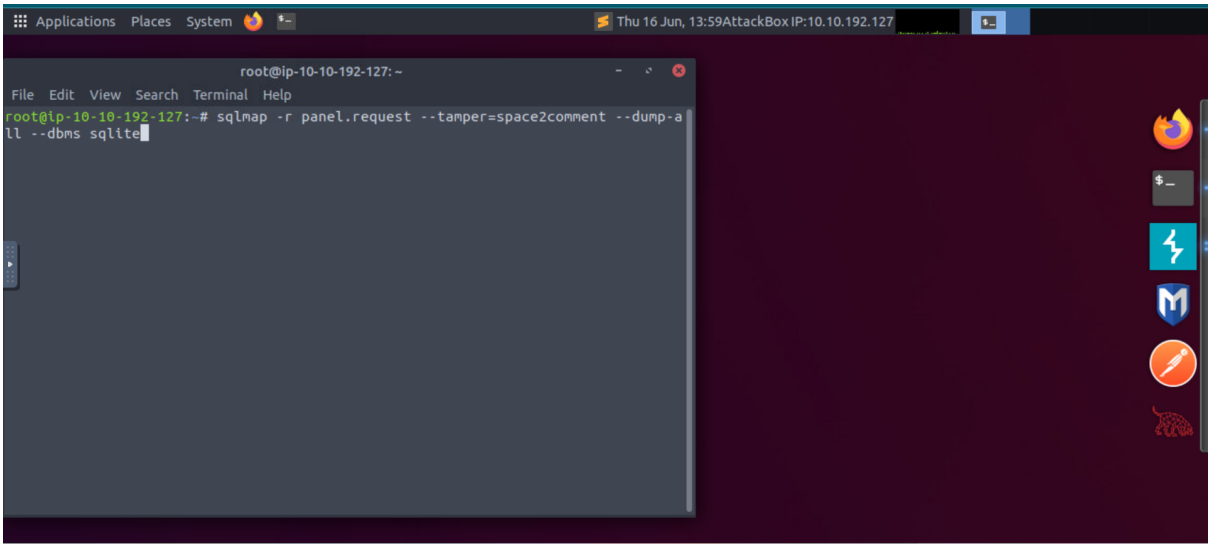


Then, type in “darkstar” into Santa’s search feature. Then, go to burpsuite, switch on the intercept, send it to the intruder and save the item as “panel.request”.

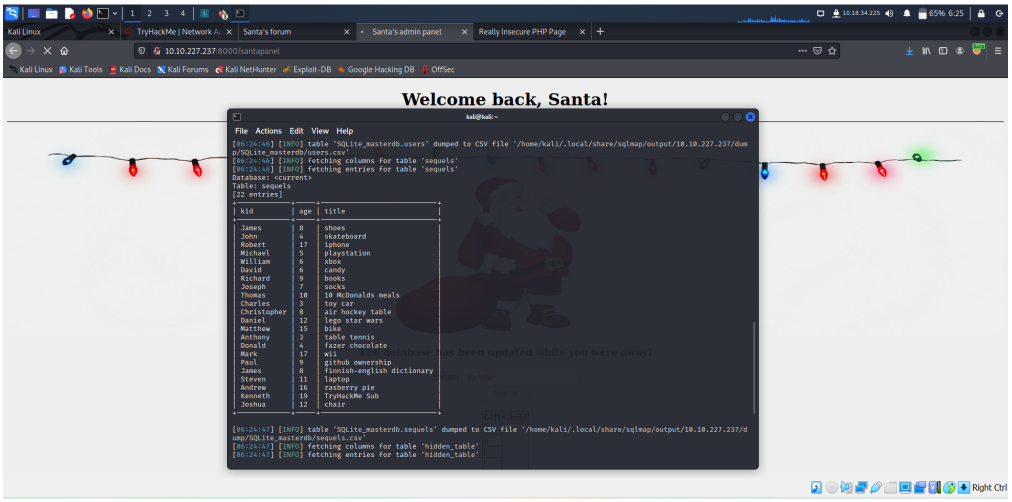




Next, open the terminal and use sqlmap [sqlmap -r panel.request –tamper=space2comment –dump-all –dbms sqlite] to enter Santa’s database using the item we had saved earlier

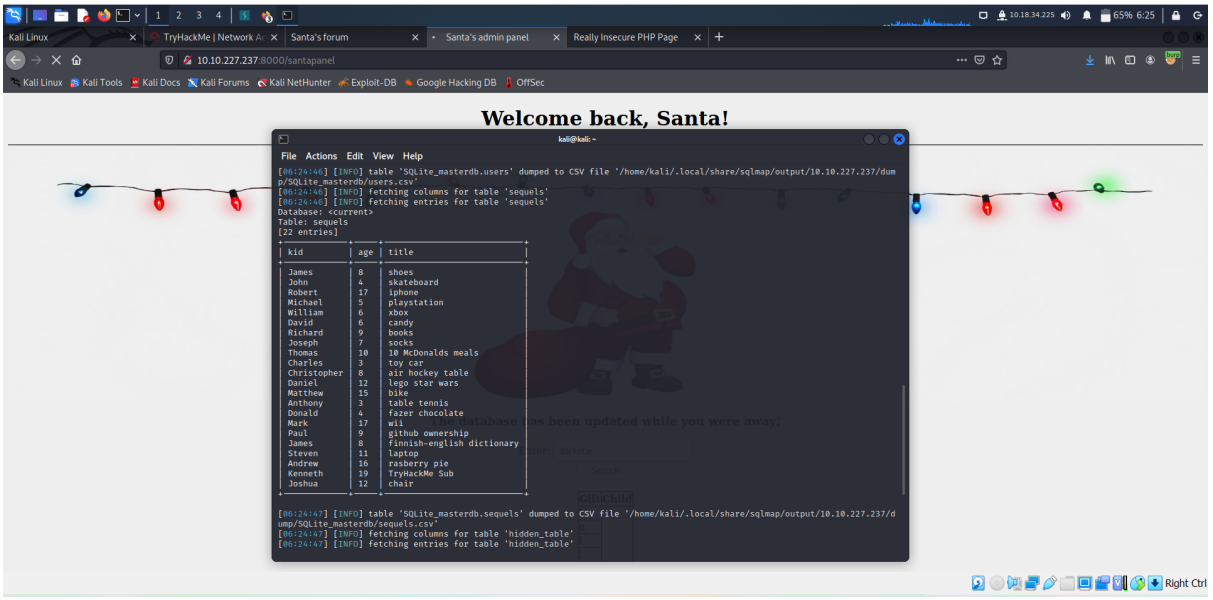


After accessing Santa's admin panel database through sqlmap, we found the gift database which has 22 entries



Question 5: What is James' age?

In the gift database, it stated each information which included the name of kids, age and title of what the kids asked for. So, from the database, we found that James is 8 years old

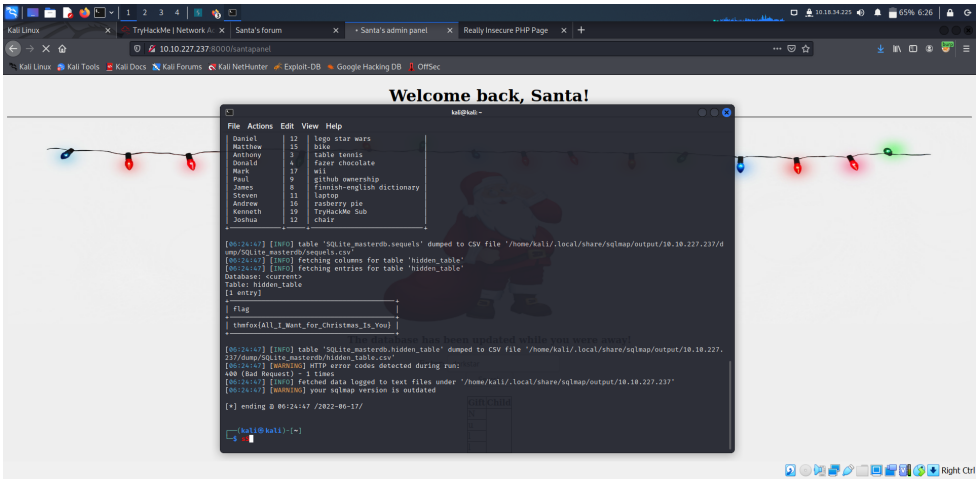


Question 6: What did Paul ask for?

From the database, it stated that Paul asked for a github ownership

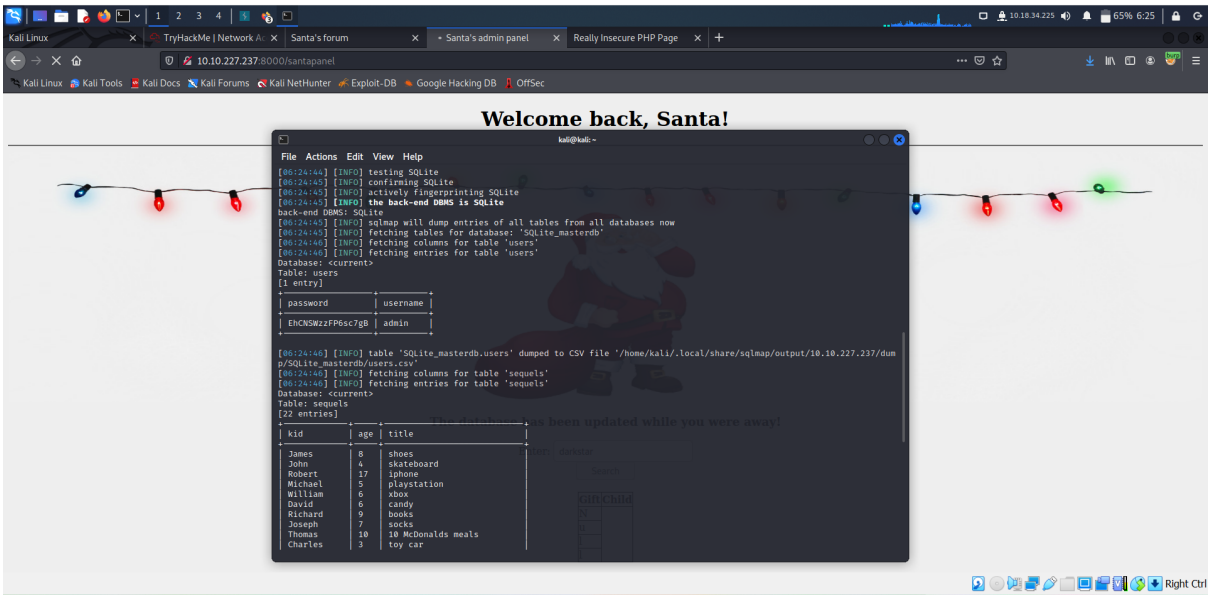
Question 7: What is the flag?

At the bottom of the database, the flag is given



Question 8: What is the admin's password?

In the same database, the username of admin and password is shared which is [EhCNSWzzFP6sc7gB]



Throughout process:

Firstly, we insert the ip address that was given into the search engine where we found Santa's official forum. Then, from the same ip address, we add "/santapanel" at the back to get into Santa's secret login panel. Put in [admin' or 1=1 –] into username and [admin] into password to enter the page. Next, add a temporary project into burpsuite and connect foxyproxy with burp. Make sure the intercept is off and type in "darkstar" into Santa's search feature. Then, go to burpsuite, switch on the intercept, send it to the intruder and save the item as "panel.request". Next, open the terminal and use sqlmap [sqlmap -r panel.request –tamper=space2comment –dump-all –dbms sqlite] to enter Santa's database using the item we had saved earlier. With that, all the information needed will be shown throughout the database.