PSP0201

Week 2

Writeup

Group Name: **Cyberteam**

Members

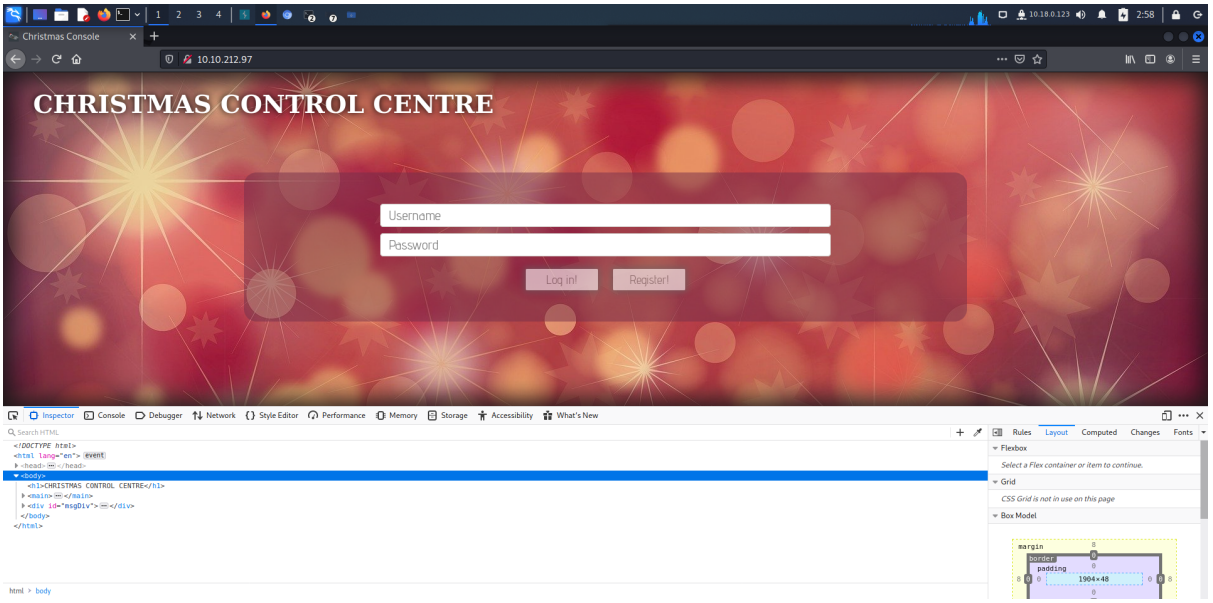
ID	Name	Role
1211101864	Julian Koh Chee Yong	Leader
1211103605	Danial Ierfan Bin Hazmi	Member
1211103281	Jievenesh Arvind Naidu A/L Uma Selvam	Member
1211103785	Brijhendhra A/L Saravanaraj	Member

Day 1: Web Exploitation – A Christmas Crisis

Tools used: Kali Linux, Firefox

Solution/walkthrough:

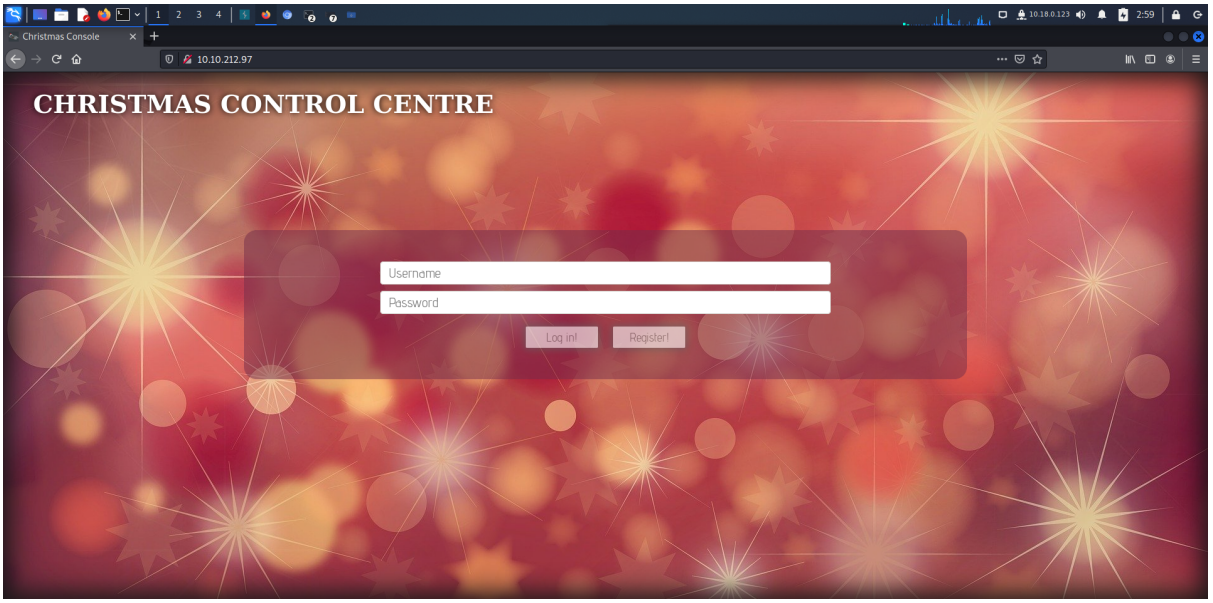
Question 1 - Inspect the website. What is the title of the website?

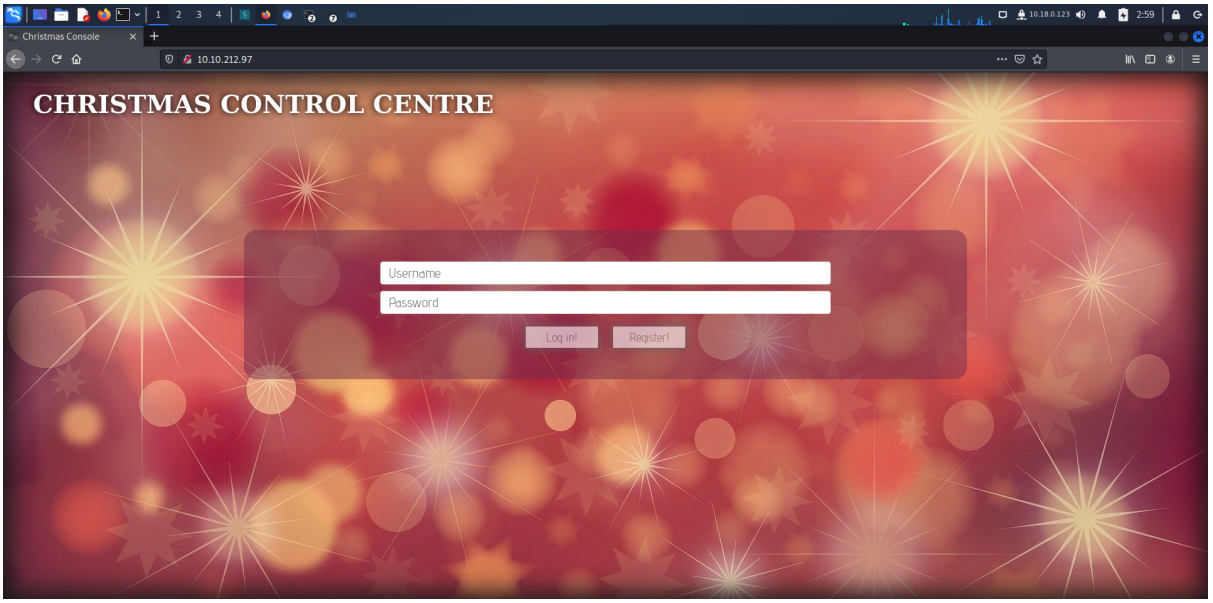


Answer: CHRISTMAS CONTROL CENTRE

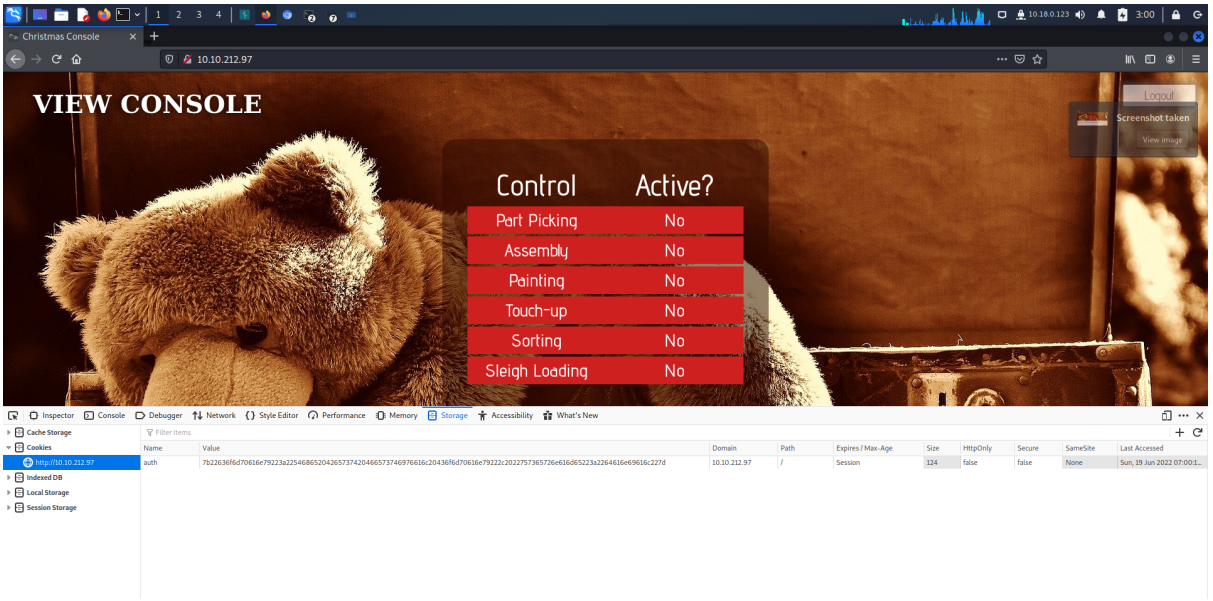
Question 2 - What is the name of the cookie used for authentication?

Registration and logging in to the Christmas Control Centre. No access to the control console.





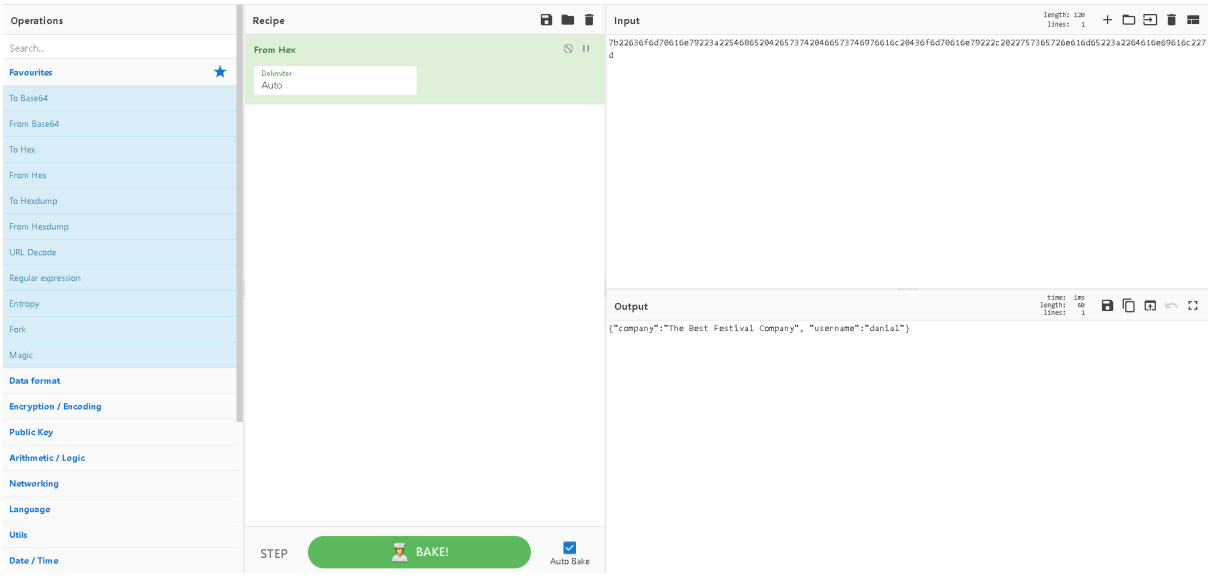
Opening up the browser developer tools to check on the cookie.



Answer: auth

Question 3 - In what format is the value of this cookie encoded?

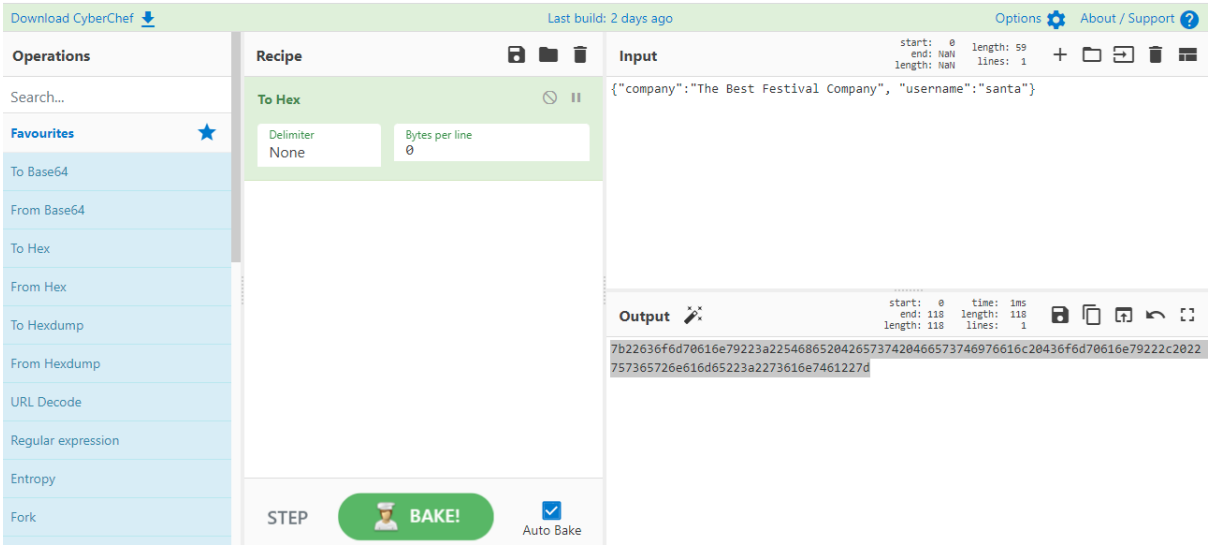
Using Cyberchef, convert the cookie value to string.



Answer: hexadecimal

Question 4 - Having decoded the cookie, what format is the data stored in?

Changing the username to 'santa', convert the JSON statement to hex.



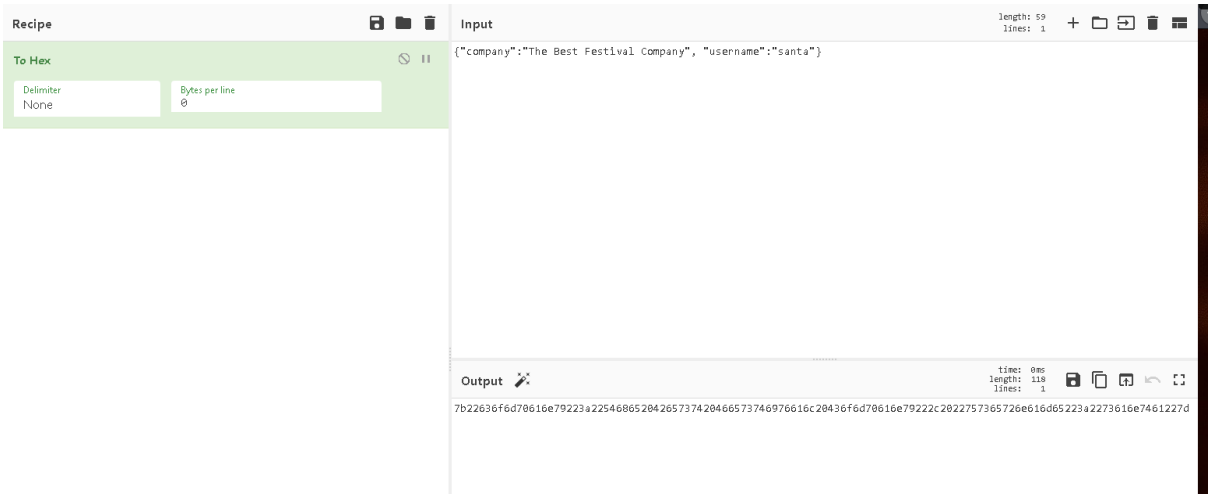
Answer: JSON

Question 5 - What is the value for the company field in the cookie?

Question 6- What is the other field found in the cookie?

Answer/walkthrough:

Decode the cookie by using CyberChef



Answer 5: The Best Festival Company

Answer 6: username

Question 7 - What is the value of Santa's cookie?

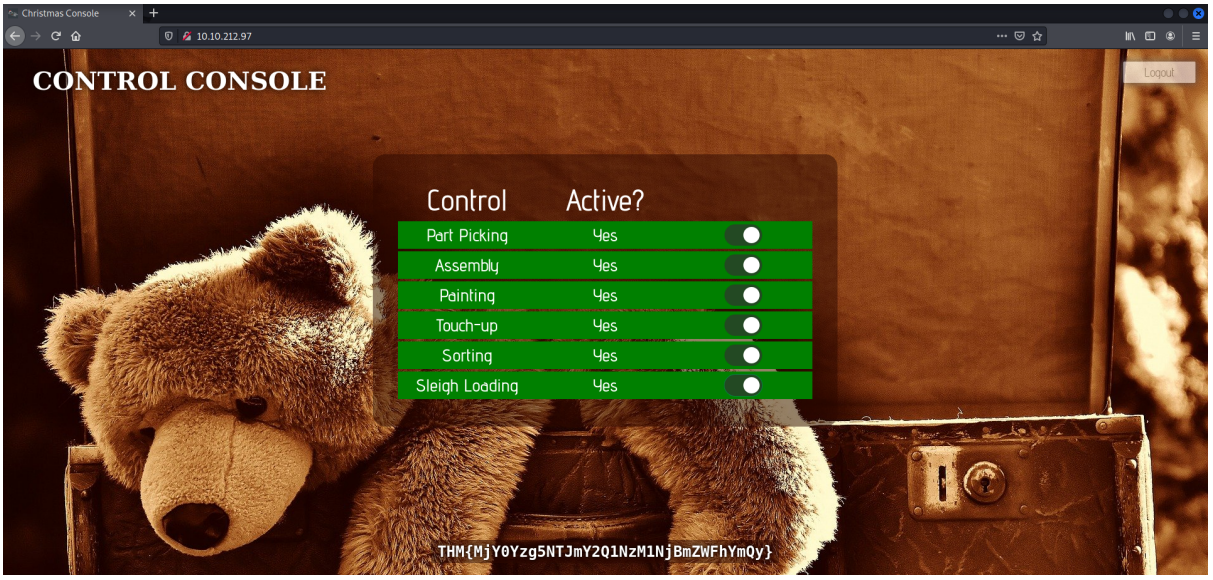
Obtain the value of the cookie.

Value
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2264616e69616c227d

Answer: 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d

Question 8 - What is the flag you're given when the line is fully active?

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



Answer: THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}

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 chose to view 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

Solution/Walkthrough:

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

?id=ODIzODI5MTNiYmYw

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

Image

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

/uploads/

Question 4:

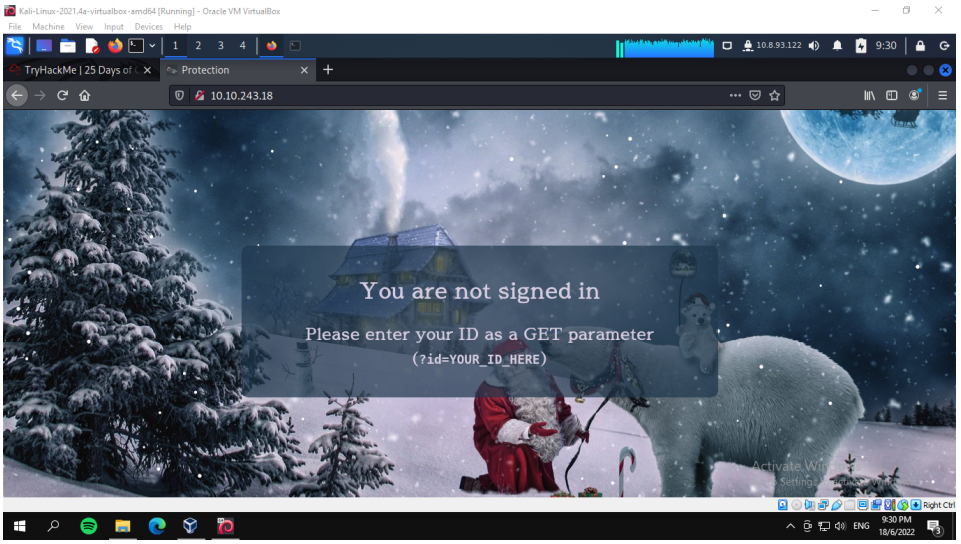
Q4: Read up on netcat's parameter explanations. Match the parameter with the explanation below. * 8 points

	l	v	n	p
Have nc give more verbose output.	○	○	◉	○
Used to specify that nc should listen for an incoming connection rather than initiate a connection to a remote host.	◉	○	○	○
Do not do any DNS or service lookups on any specified addresses, hostnames or ports.	○	◉	○	○
Specifies the source port nc should use, subject to privilege restrictions and	○	○	○	◉

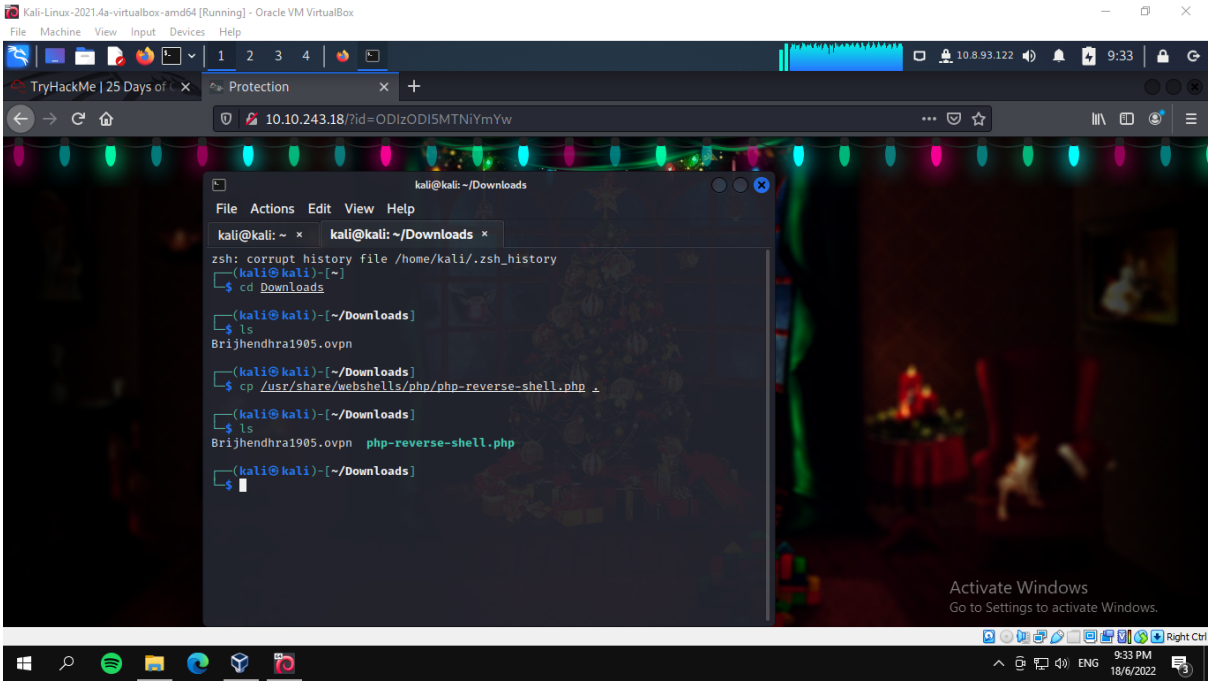
Question 5: What is the flag in /var/www/flag.txt?

THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}

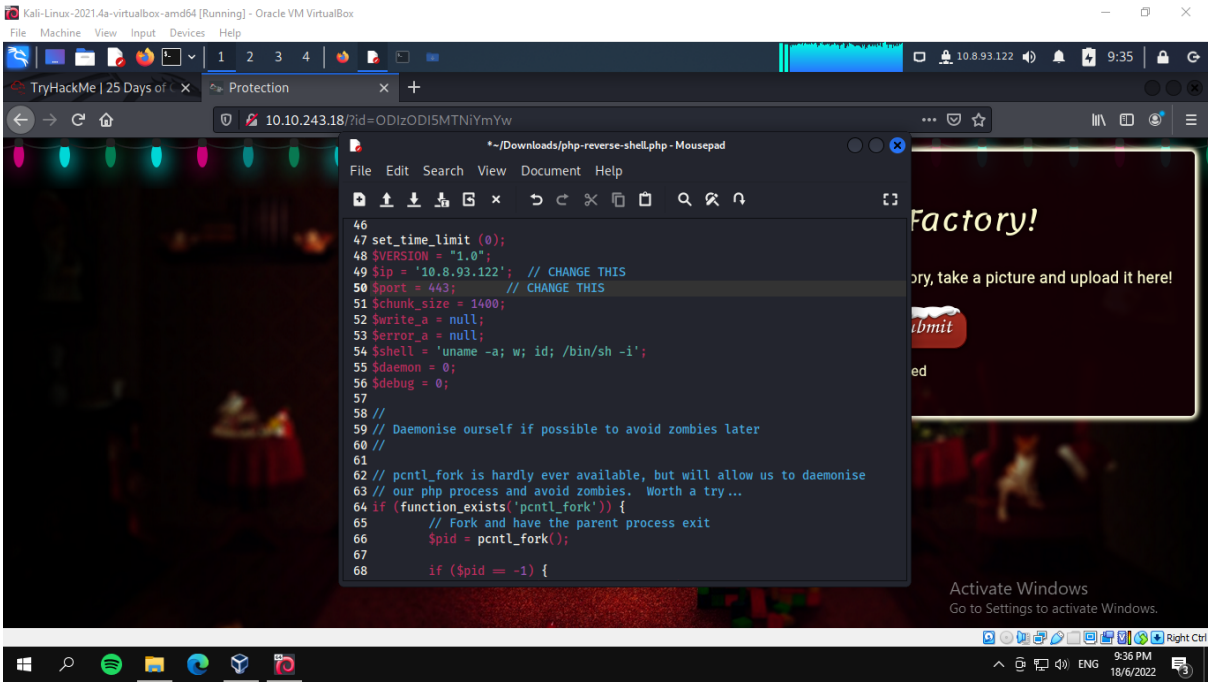
Not signed in without ID.



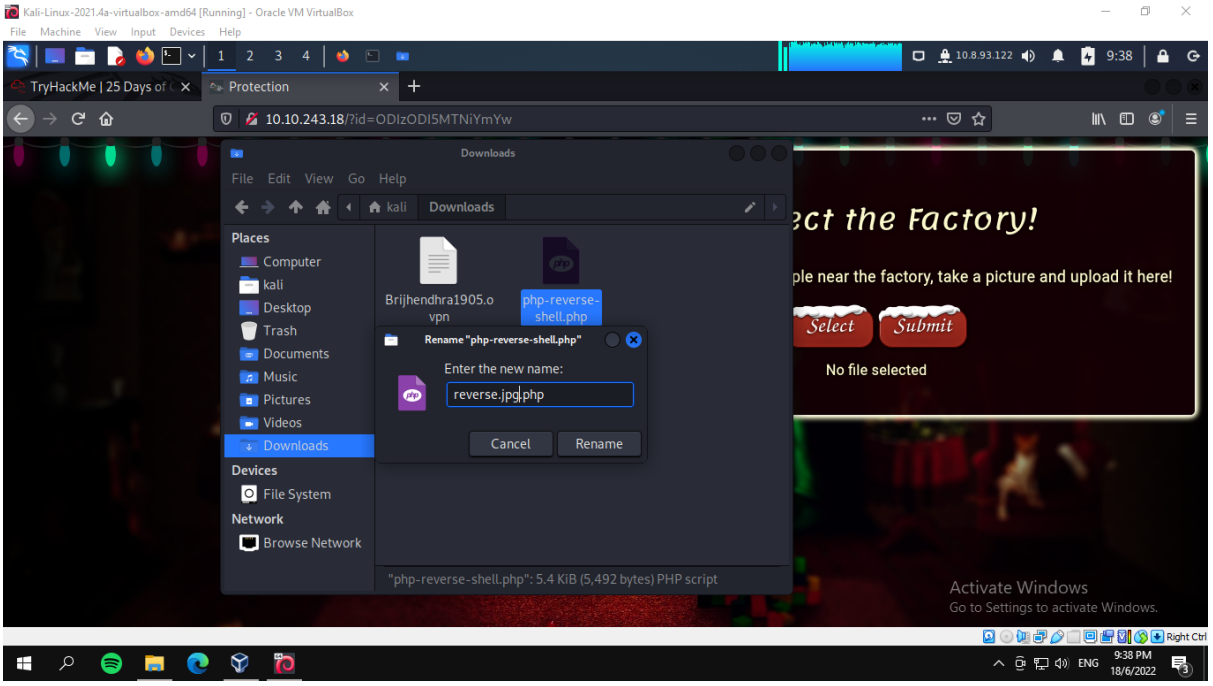
Once accessed into the page, copy the file into the current directory chosen which is downloads.



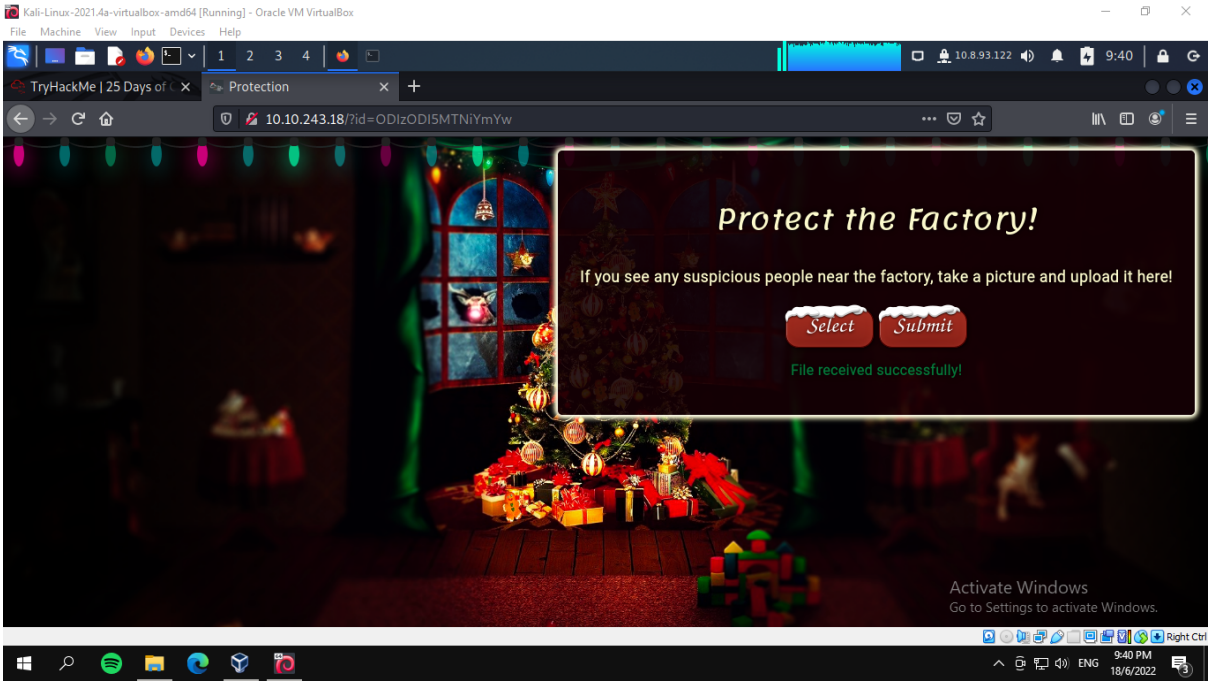
File is opened with mousepad and IP is changed to TryHackMe's current IP and port is changed to 443.

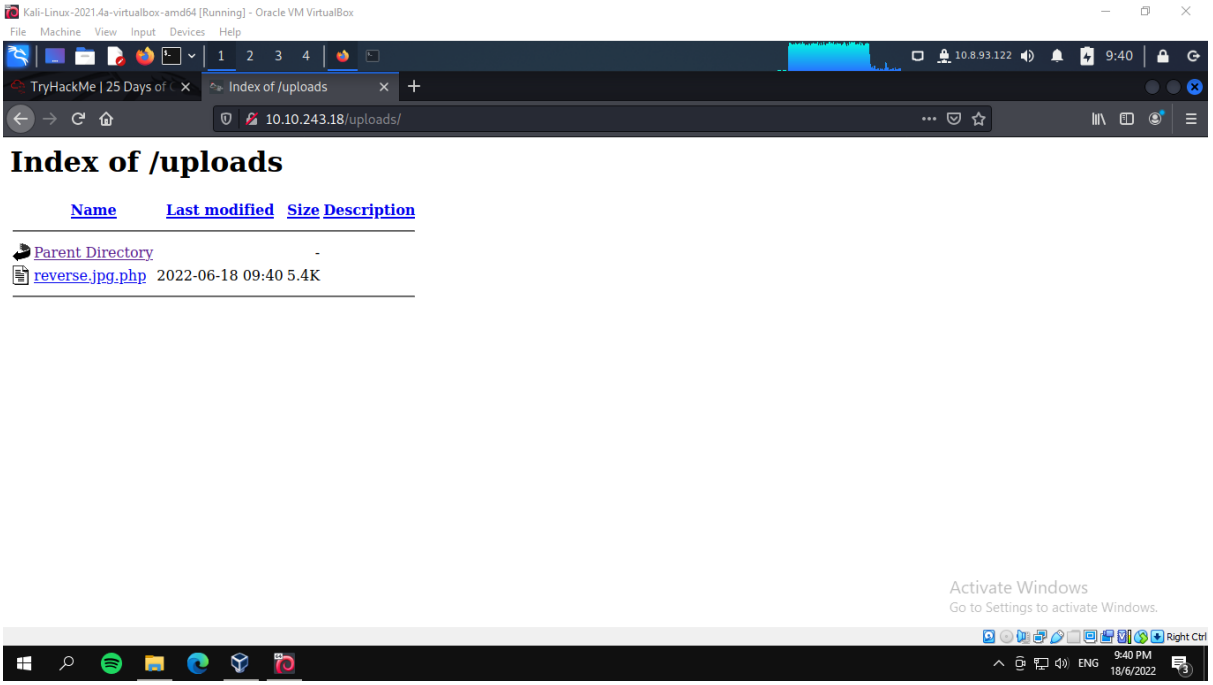


Php-reverse-shell.php is renamed to reverse.jpg.php



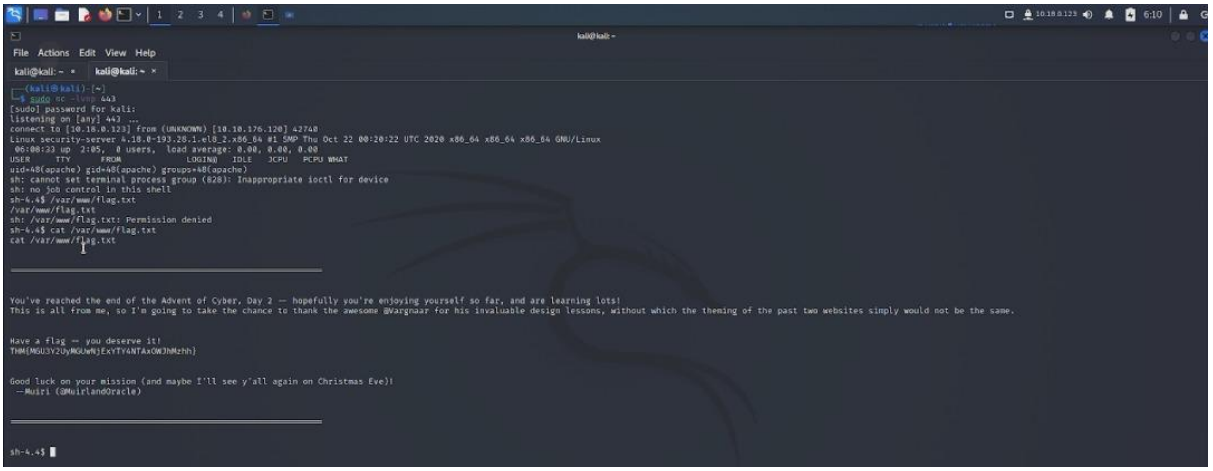
File is then chosen to submit.





We then create a netcat listener for port 443 for the uploaded reverse shell

We then locate the flag in the listener created.



Thought Process/Methadology:

Having accessed the target machine via ID given, we were shown a page with the buttons select and submit. We proceeded to copy the file in Linux to the current directory chosen which was downloads. That file is then opened with mousepad and the IP is changed to the TryHackMe's IP and the port is changed to 443. Later on, the file is renamed to a different name and is then selected and submitted. The file is then seen in the index of /uploads which shows that it has been submitted. After that, we create a netcat listener for the uploaded reverse shell and locate the flag in it.

Day 3: Web Exploitation – Christmas Chaos

Tools used : Kali Linux, Firefox, Burpsuite

Solution/Walkthrough :

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

Given from the text in THM

> What's even worse is that these devices are often exposed to the internet, potentially allowing anyone to access and control it. In 2018 it was reported that a botnet (a number of internet-connected devices controlled by an attacker to typically perform DDoS attacks) called Mirai took advantage of **I**nternet **o**f **T**hings (**IoT**) devices by remotely logging, configuring the device to perform malicious attacks at the control of the attackers; the Mirai botnet infected over 600,000 IoT devices mostly by scanning the internet and using default credentials to gain access.

Answer : Mirai

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

Given from the text in THM

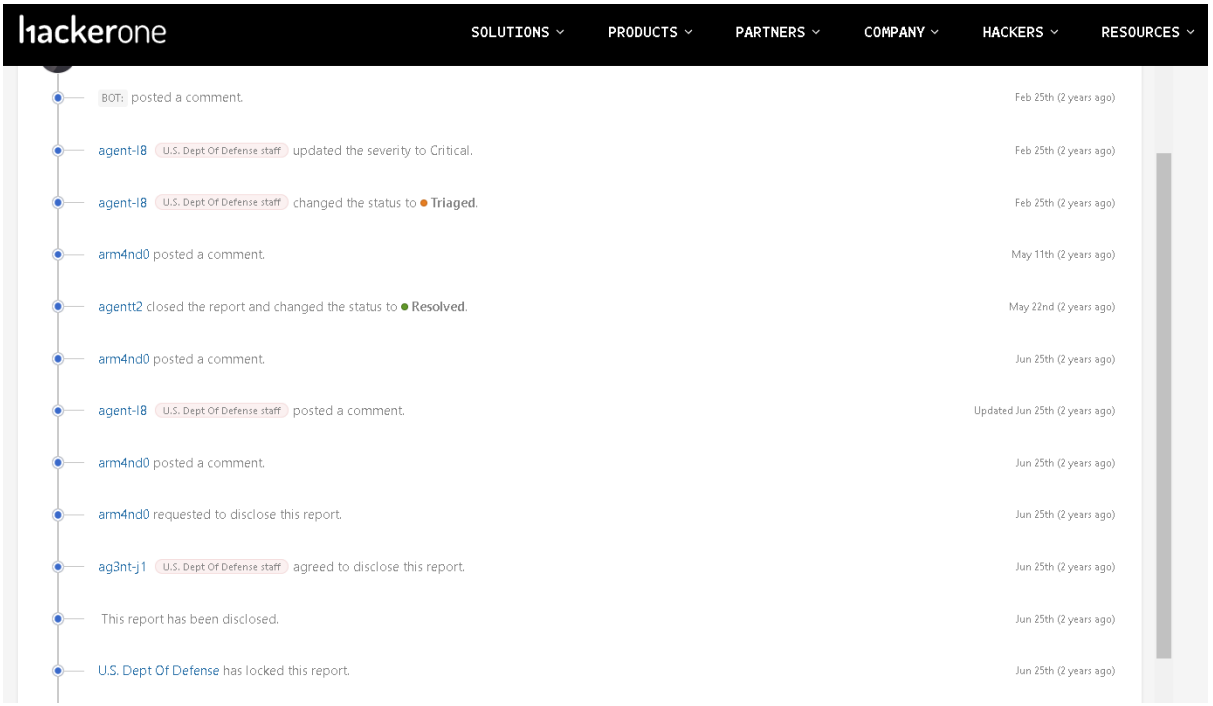
> In fact, companies such as Starbucks and the US Department of Defense have been victim to leaving services running with default credentials, and bug hunters have been rewarded for reporting these very simple issues responsibly (Starbucks paid $250 for the reported issue):

Answer : 250

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

Link of the file is provided at THM

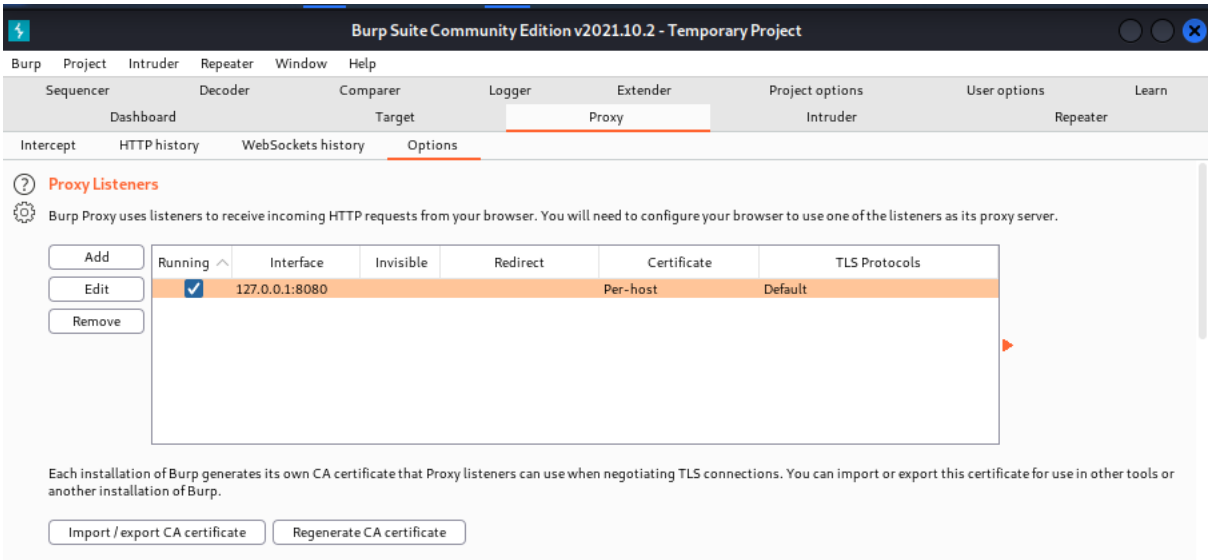
https://hackerone.com/reports/804548



Answer : agent-l8

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

Launch Burp Suite and navigate to Proxy. Then, go to Options and search under Proxy Listeners.



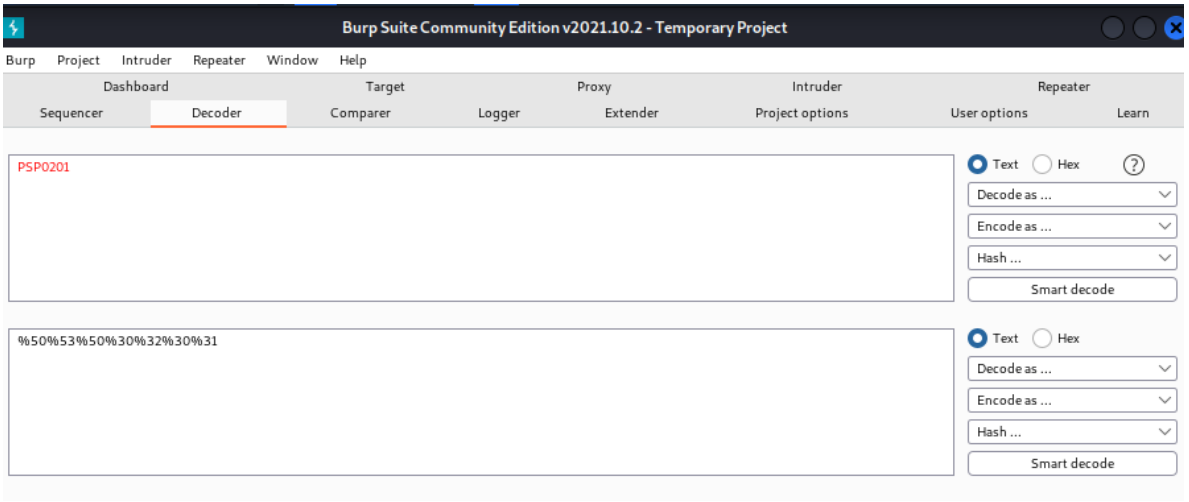
Answer : 8080

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

Answer : HTTP

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

Navigate to Decoder. Next, click on Text. Set the ‘Decode as…’ to Plain. Then, set the ‘Encode as…’ to URL. Fill in the box at the top with the text given.

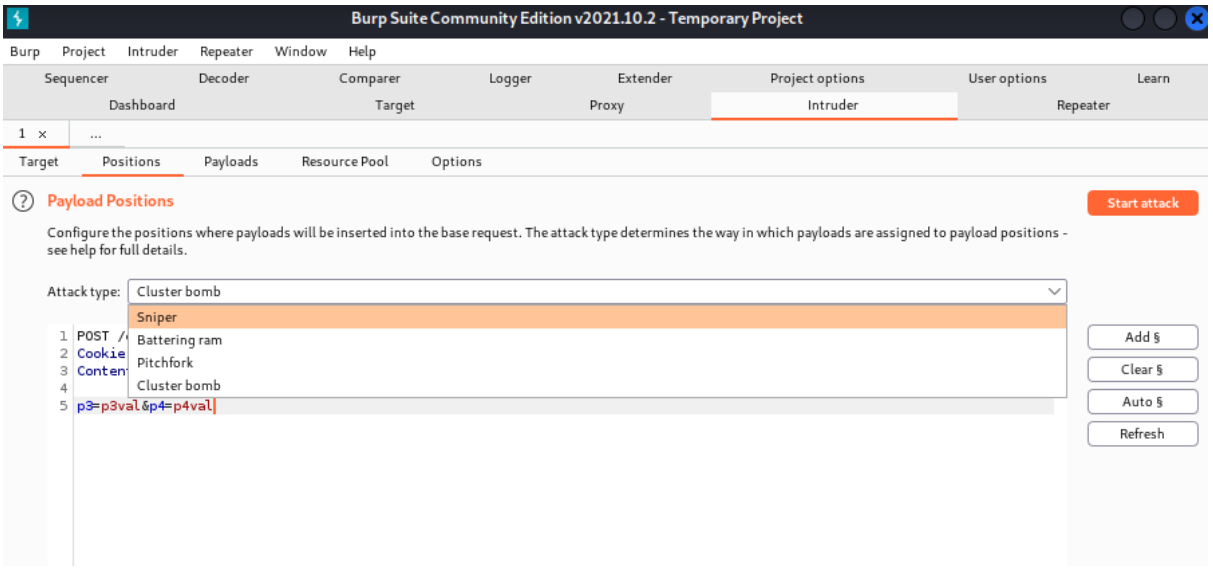


Answer : %50%53%50%30%32%30%31

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

Uses multiple payload sets. Different payload for each defined position up to maximum 20. Iterates through each payload set in turn, so all permutations of payload combinations are tested.

Navigate to Intruder and go to Positions. Look under Attack type.

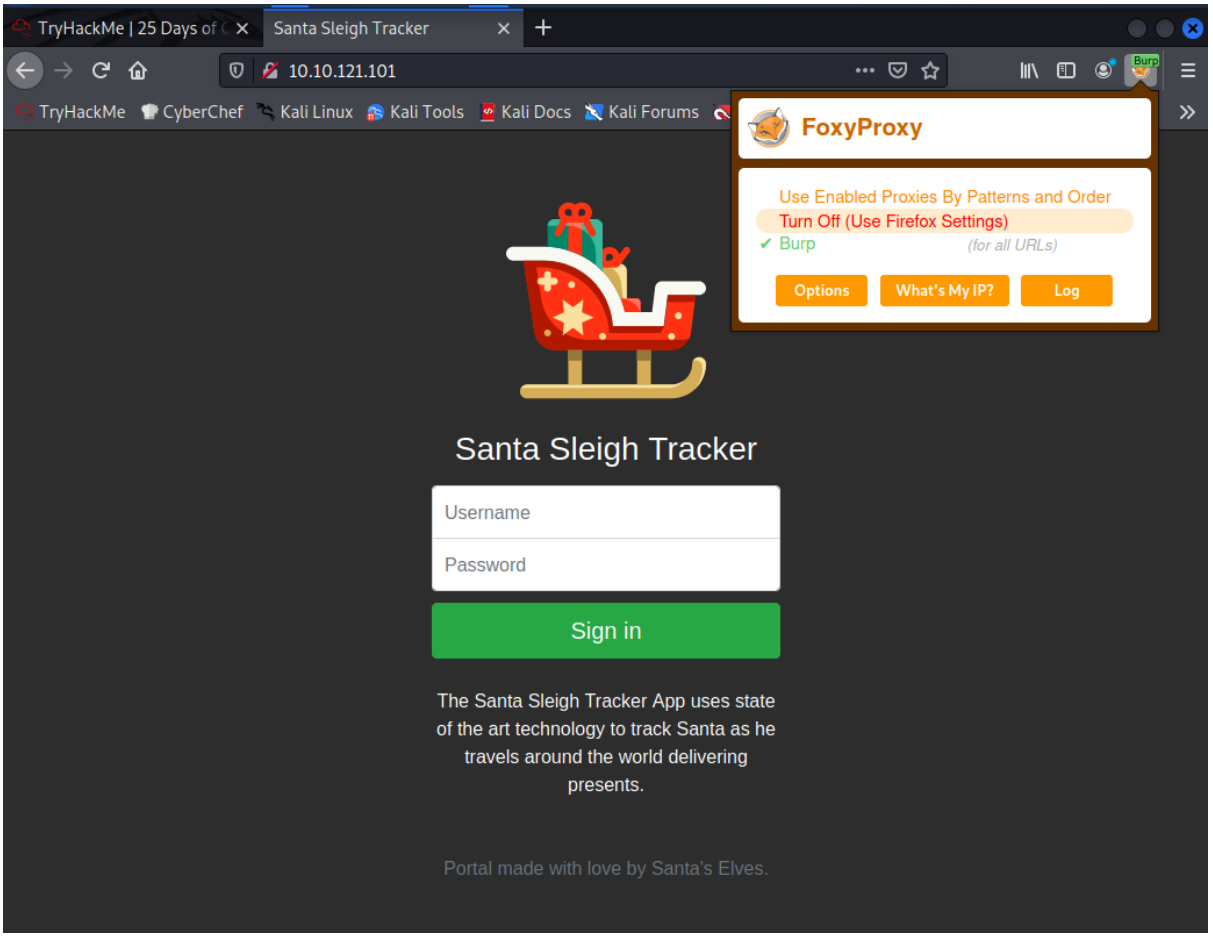


Answer : Cluster bomb

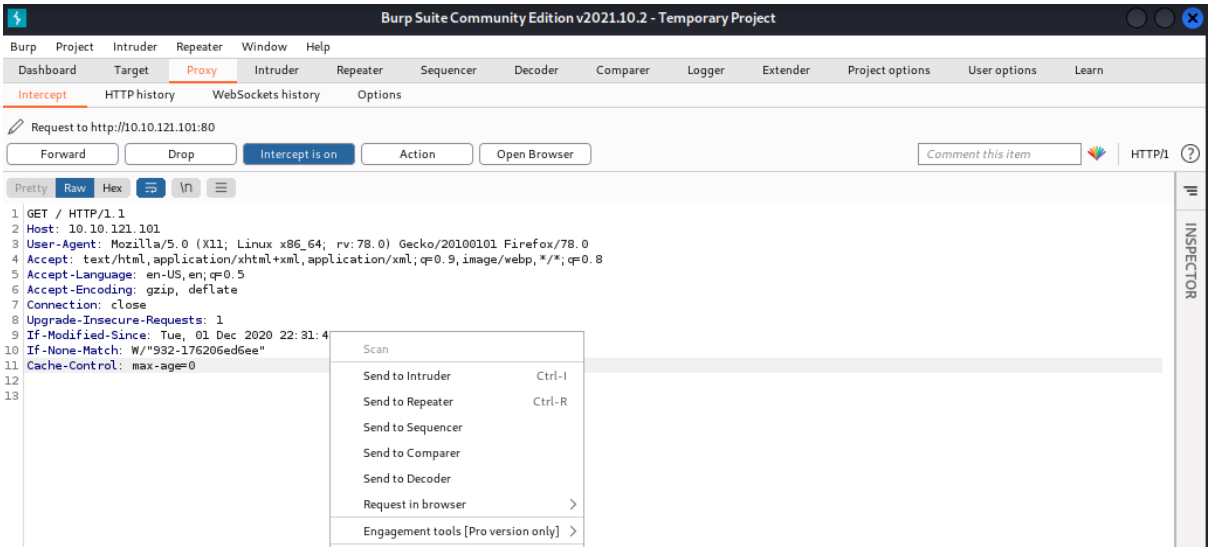
Question 8 : What is the flag?

Walkthrough :

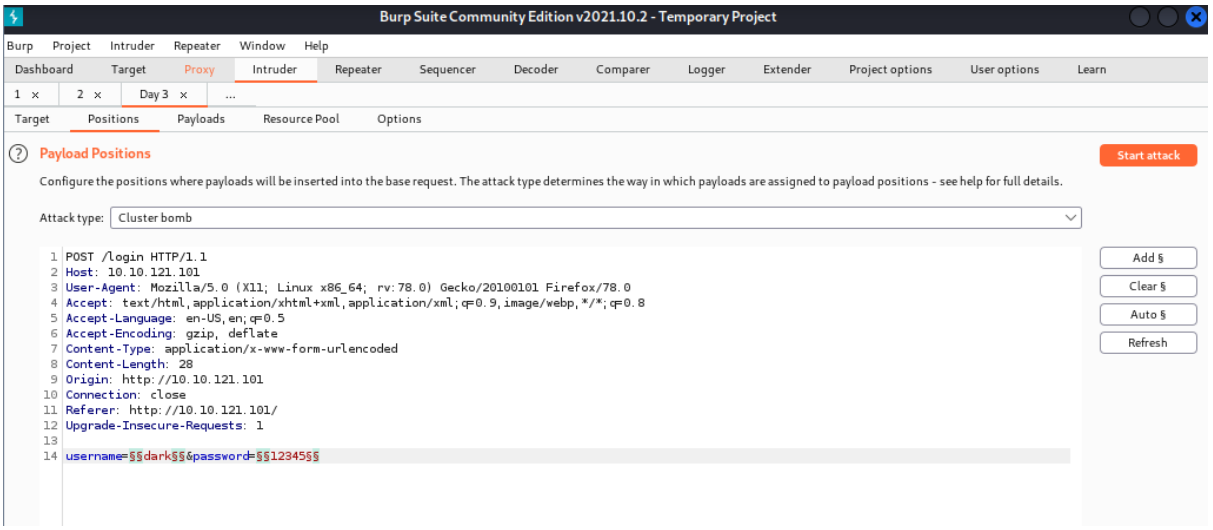
Copy the IP address given from THM and paste at the browser search bar. Select Burp on the FoxyProxy extension.



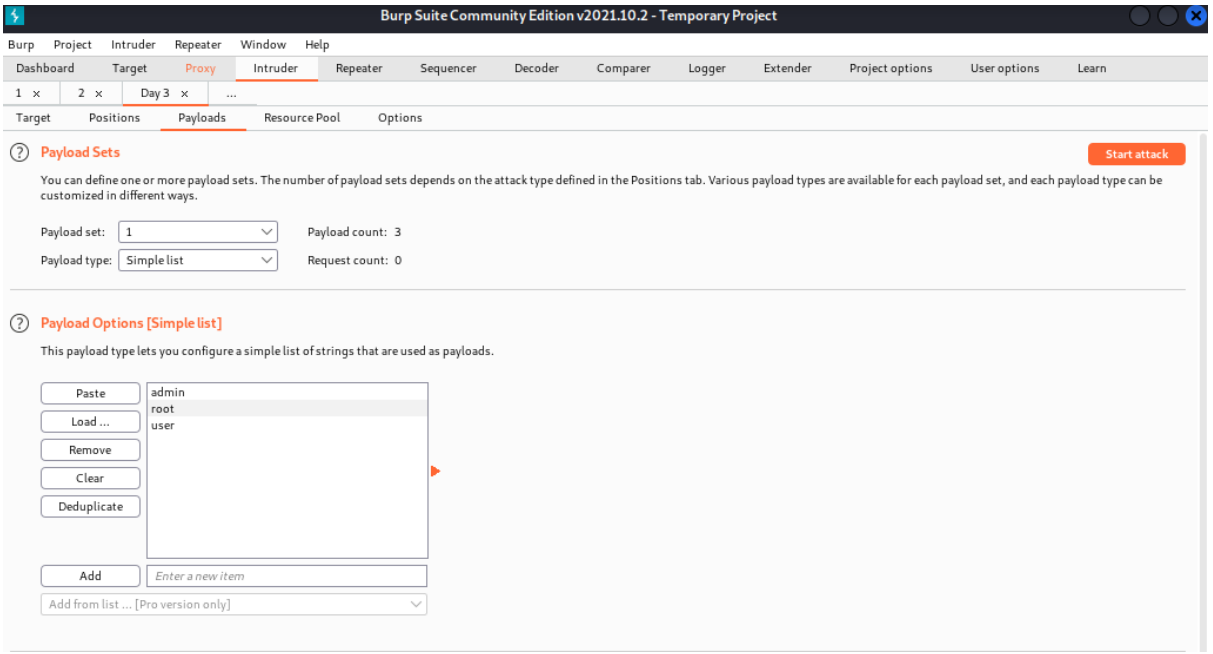
Enter any username and password and refresh the page. Go to Burp Suite. Navigate to Proxy and then to Intercept. Make sure the intercept is on. Forward the raw view result to Intruder.



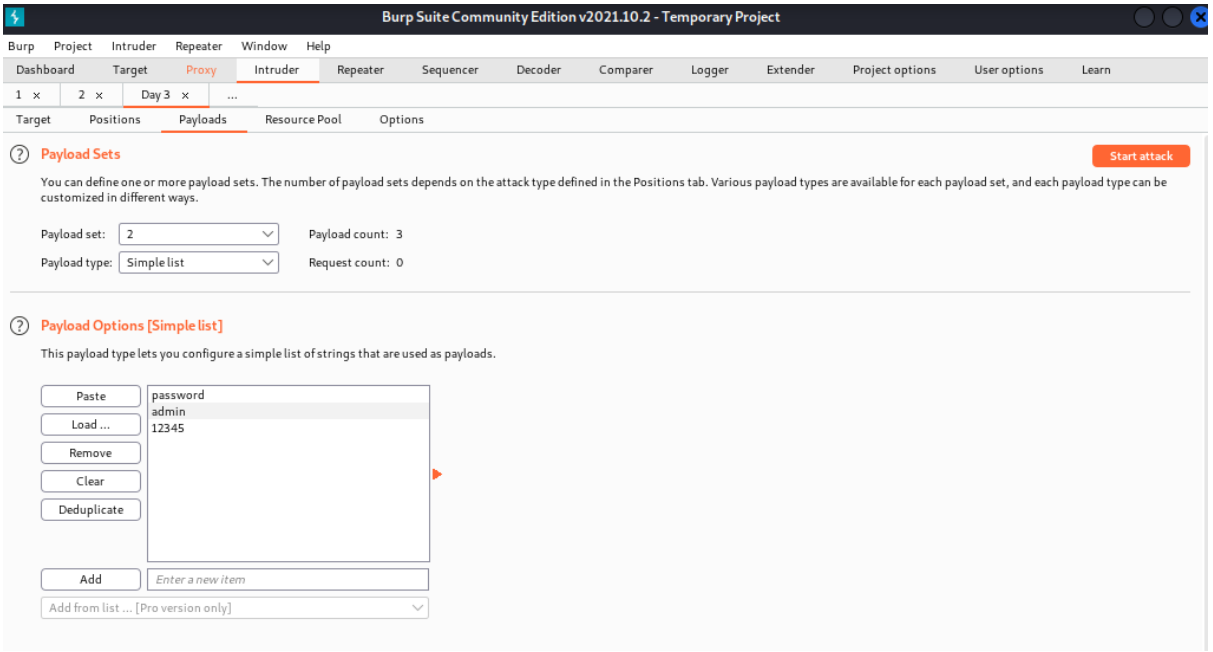
Highlight the inserted username and password and click on Add. Then, select Cluster Bomb to be the Attack type.



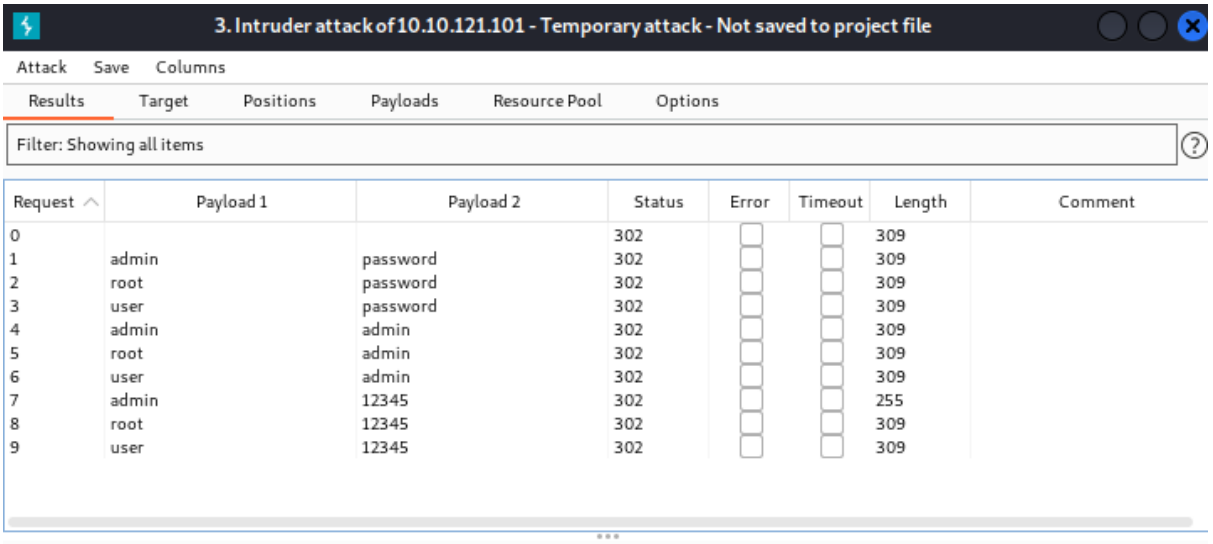
Go to Payloads. For Payload set 1, the options would be as below :



And as for Payload set 2, the options would be as below :

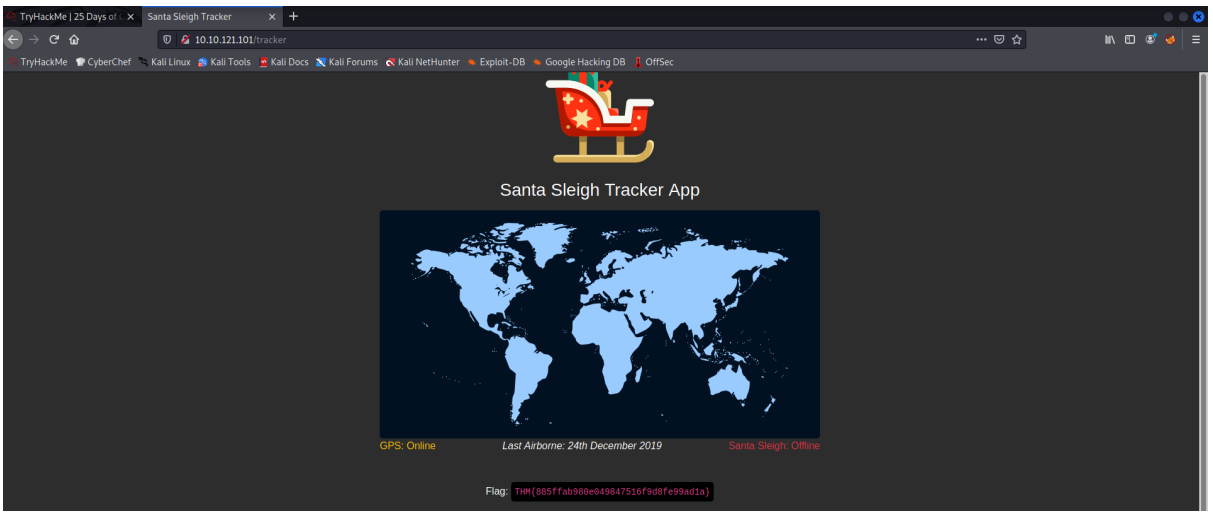


Start the attack. Observe the status or length of the results that differ which may be a successful request.



Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302			309	
1	admin	password	302			309	
2	root	password	302			309	
3	user	password	302			309	
4	admin	admin	302			309	
5	root	admin	302			309	
6	user	admin	302			309	
7	admin	12345	302			255	
8	root	12345	302			309	
9	user	12345	302			309	

Using the Payload 1 and Payload 2 that has different length, fill in the username and password at the website on the browser. Make sure to turn off Burp before submitting the details. Once done, click on Sign in and the flag will be shown.



Answer : THM{885ffab980e049847516f9d8fe99ad1a}

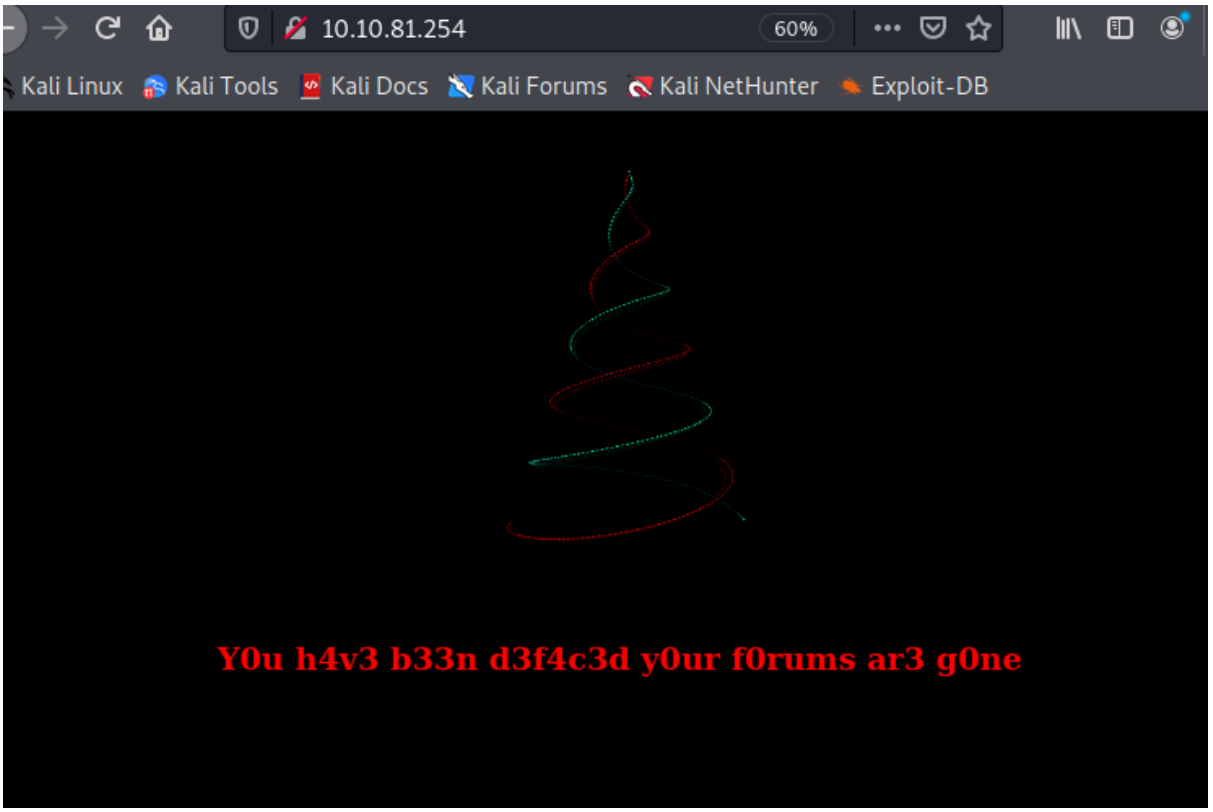
Thought Process/Methodology :

Upon accessing the target machine from the ID given, we were shown a page to sign in into Santa Sleigh Tracker. We inserted a random username and password and searched after turning on Burp on the browser extension. This recorded the request on Intercept at Proxy In Burp Suite. The record was then sent to Intruder to loop through the request. We highlighted the input of the username and password in Positions and click on Add to insert a new payload marker. At Payloads, we added a simple list of strings for both Set 1 and Set 2. Then, we start the attack. The results were shown and we identified the successful login by picking the login with either different status or length. We inserted the username and password back into the Santa Sleigh Tracker page. Before clicking Sign in, we turned off Burp on the browser extension. We were sent to the Santa Sleigh App page after successful login and were given the flag.

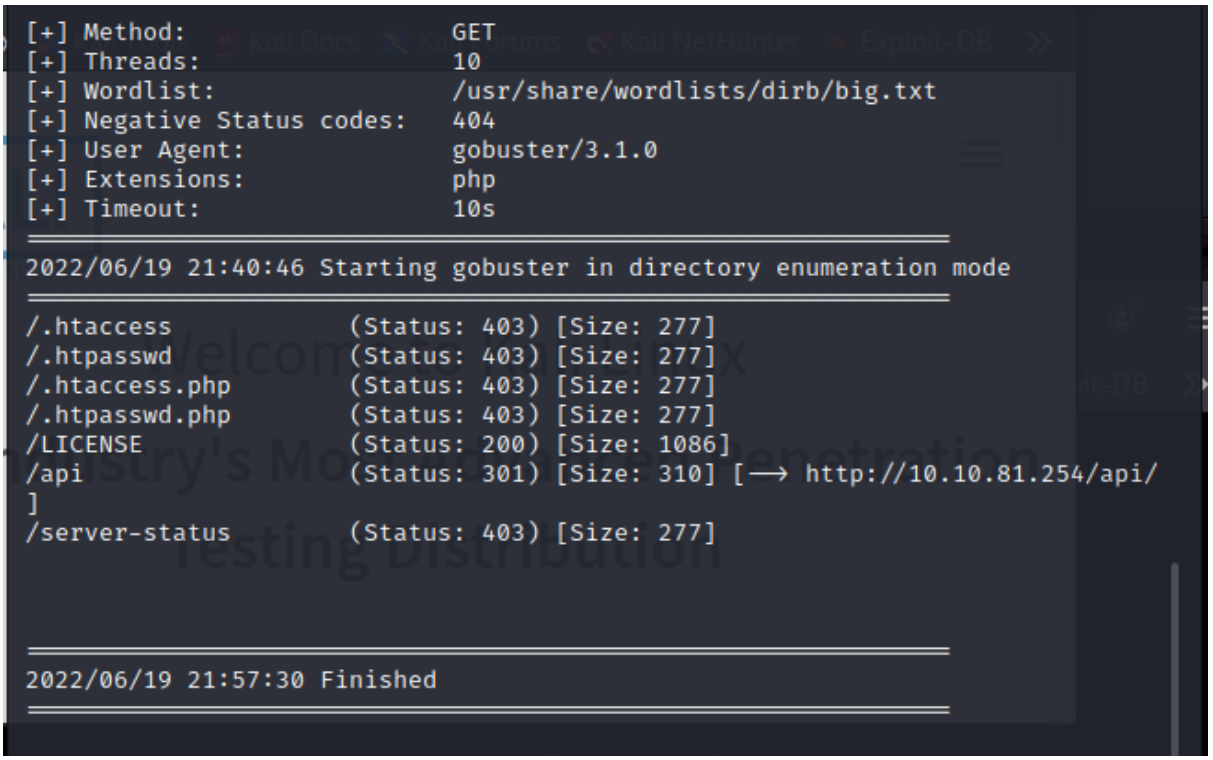
Day 4: Web Exploitation – Santa's watching

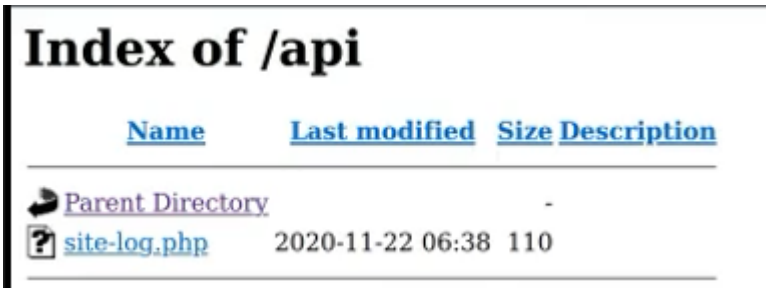
Tools used : Kali Linux, Firefox, gobuster

Deploy your AttackBox (the blue "Start AttackBox" button) and the tasks machine (green button on this task) if you haven't already. Once both have deployed, open FireFox on the AttackBox and copy/paste the machines IP (10.10.81.254) into the browser search bar.



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



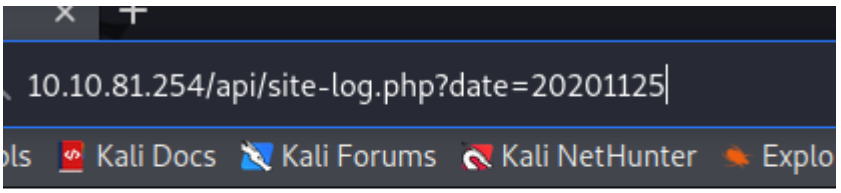


Site-log.php was found from fuzzing with ghostbuster

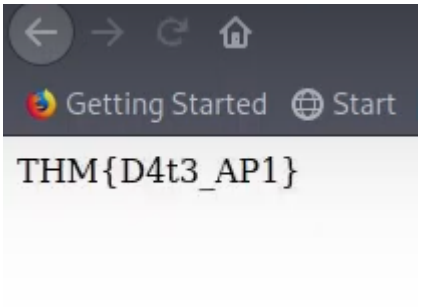
Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?

After entering "sudo wfuzz -c -z file,mywordlist.txt http://10.10.81.254/api.php?date=FUZZ" into the kali terminal, one result with the date "20201125" responded

Going back to the site.log.php and adding this date to the link



This flag was found



Thought Process/Methodology:

After finding the hidden api directory from fuzzing using ghost buster, I was able to find the date parameter. I then had to fuzz the list of dates using the command in the terminal to start the fuzzing process, i then found the date that I needed to gain access to the flag through the api directory

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

Tools used: Kali Linux, Burpsuite

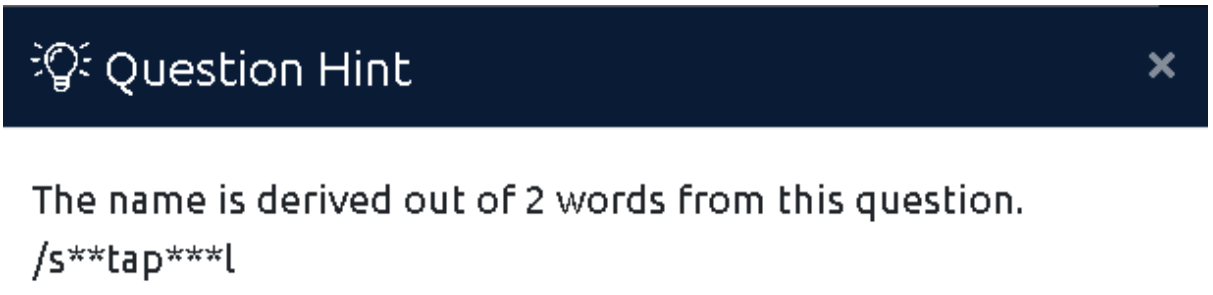
Solution/walkthrough:

Question 1: What is the default port number for SQL Server running on TCP?

Answer: 1433

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

Based on the hint from tryhackme:



Answer: /santapanel

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

Based on the paragraph:

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`

Answer: sqlite

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

Question 5: What is James' age?

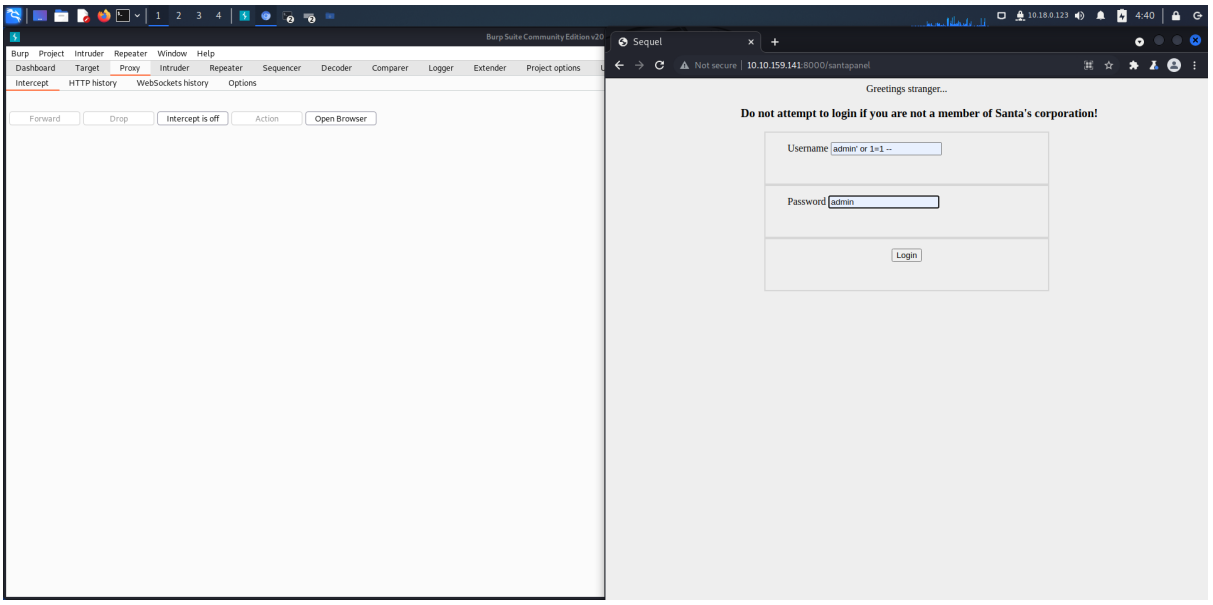
Question 6: What did Paul ask for?

Question 7: What is the flag?

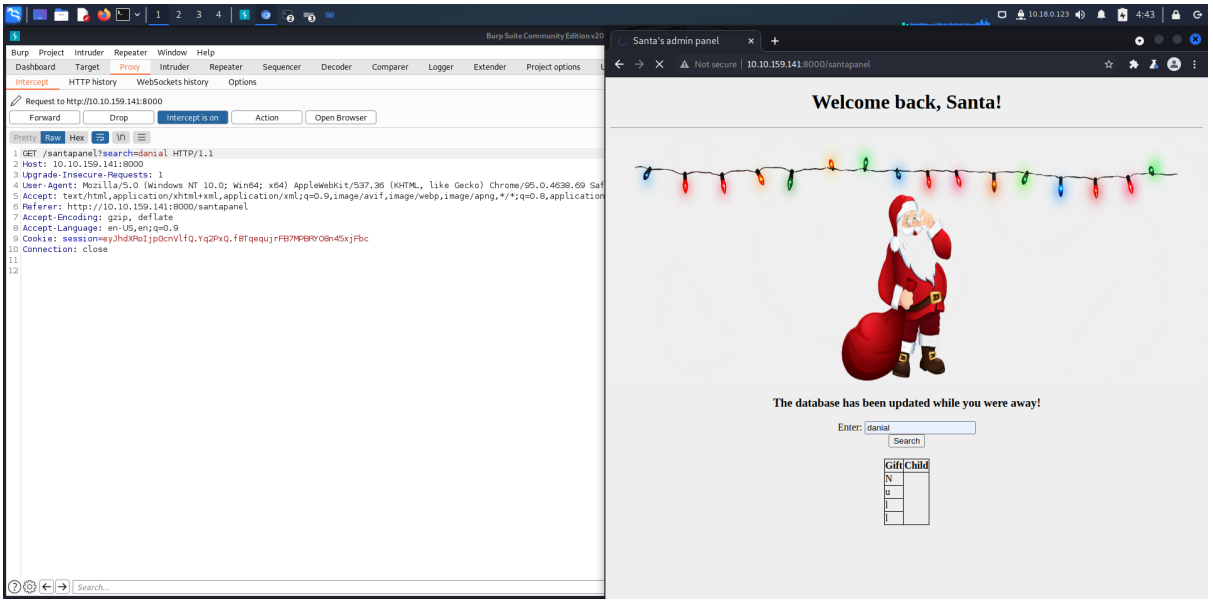
Question 8: What is admin's password?

Answer/walkthrough:

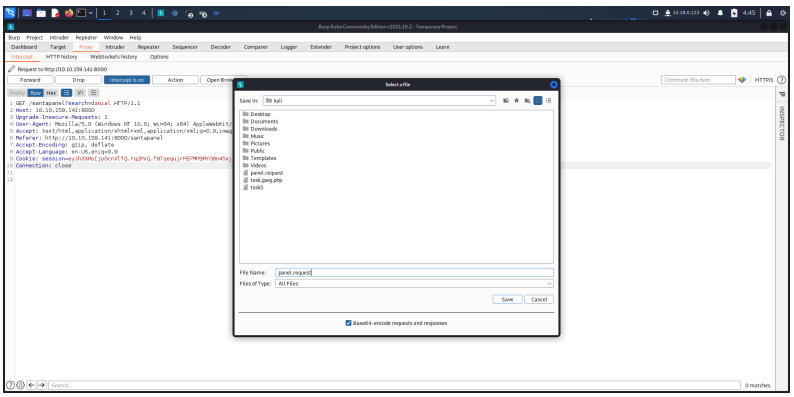
Firstly, I open the Burp suite and head to the proxy and turn off the intercepter. By using the browser from Burp suite I search for the access to Santa's secret login panel(http://10.10.159.141:8000/santapanel) . After that, I proceed to bypass the login using SQLi.



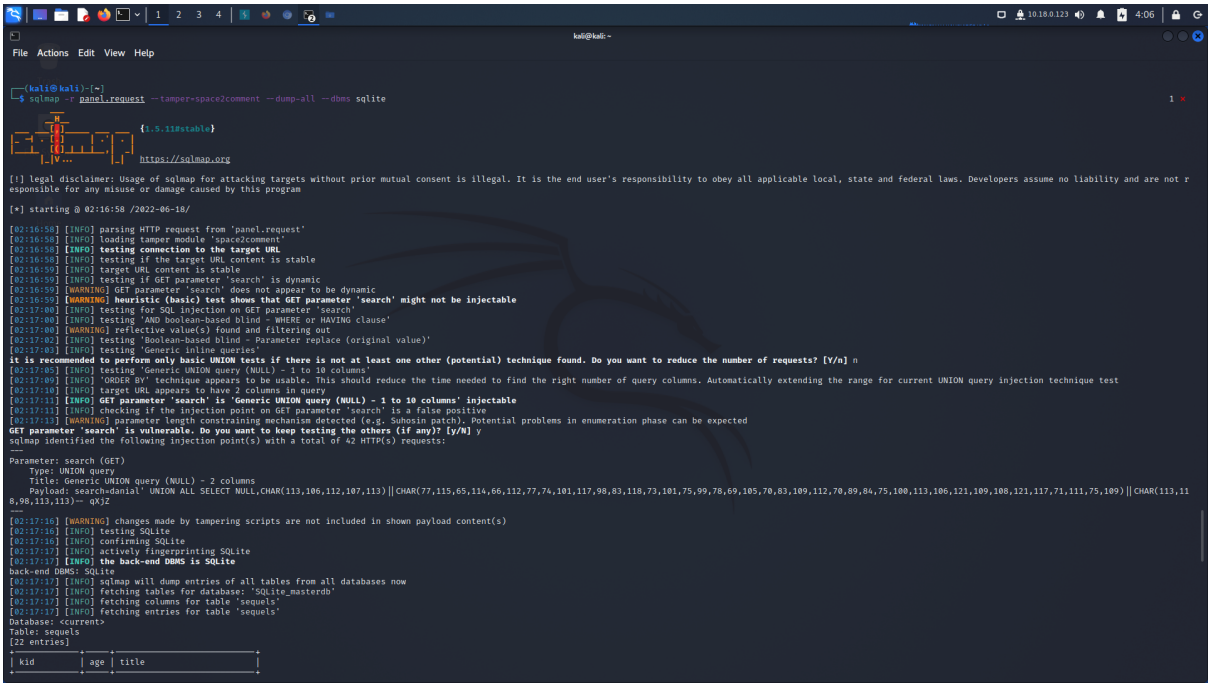
After that, I turn on the interceptor and search the database with a random name.

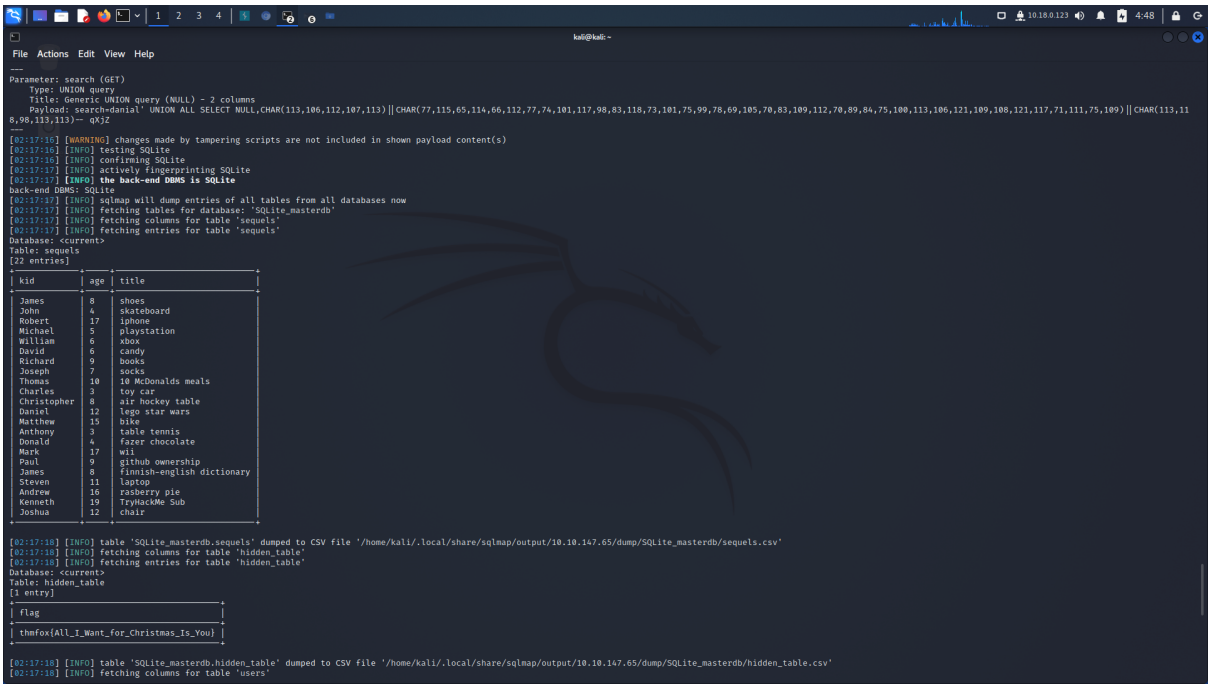


Then, I save the request as panel.request



Next, I open my kali terminal and run this command (sqlmap -r panel.request --tamper=space2comment --dump-all --dbms sqlite)





From that I got the access to the database and the answer for questions 4 to 8.

Answer 4: 22
Answer 5: 8
Answer 6: github ownership
Answer 7: thmfox{All_I_Want_for_Christmas_Is_You}
Answer 8: EhCNSWzzFP6sc7gB

Thought Process/Methodology:

After gaining the access to Santa's secret login panel, I was shown a login page for the member of Santa’s corporation. I proceed to bypass the login using SQLi. After logging in, I was shown a search

bar for the database. By turning on the interceptor on proxy, I proceed to search for a random name. Once the request had been shown in the proxy, I save the request. Consequently, I run my sql on the terminal. Then I was shown the database which include the flag.