PSP0201

Week 2

Writeup

Group Name: Hacktocrats

Members

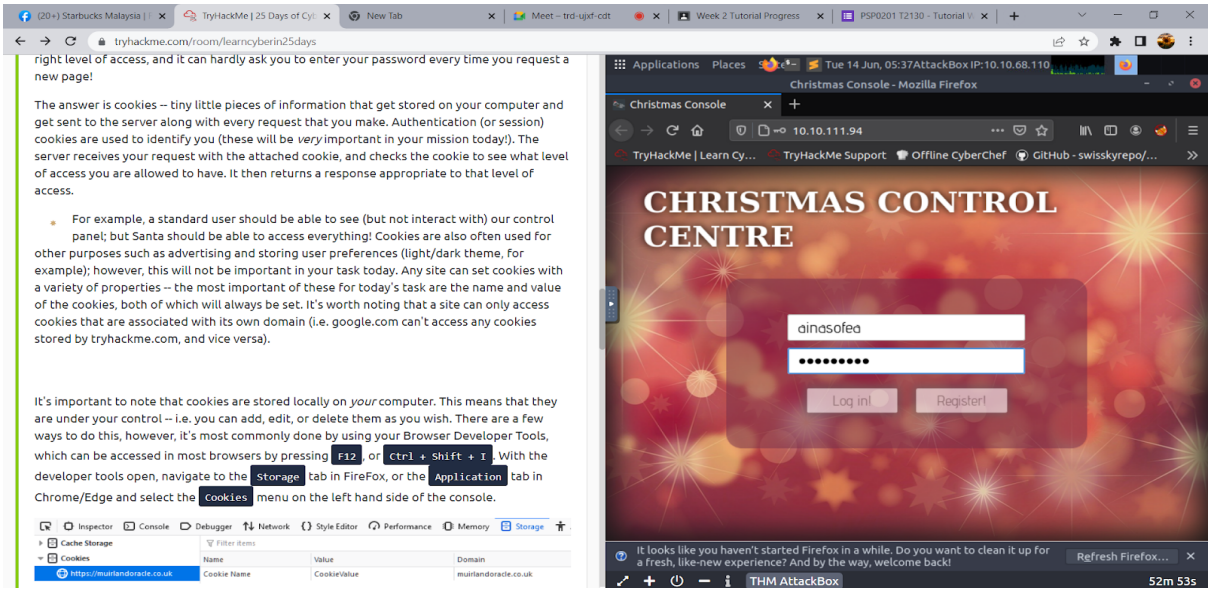
ID	Name	Role
12111 03194	NUR FARAHIYA AIDA BINTI ABD RAZAK	Leader
12111 03602	NUR ALIA AMELISA SYAZREEN BINTI MOHD SULEI	Member
12111 03430	AINA SOFEA BINTI AMIER HAMZAH	Member
12111 03237	NURUL AIN BINTI KAMARUDIN	Member

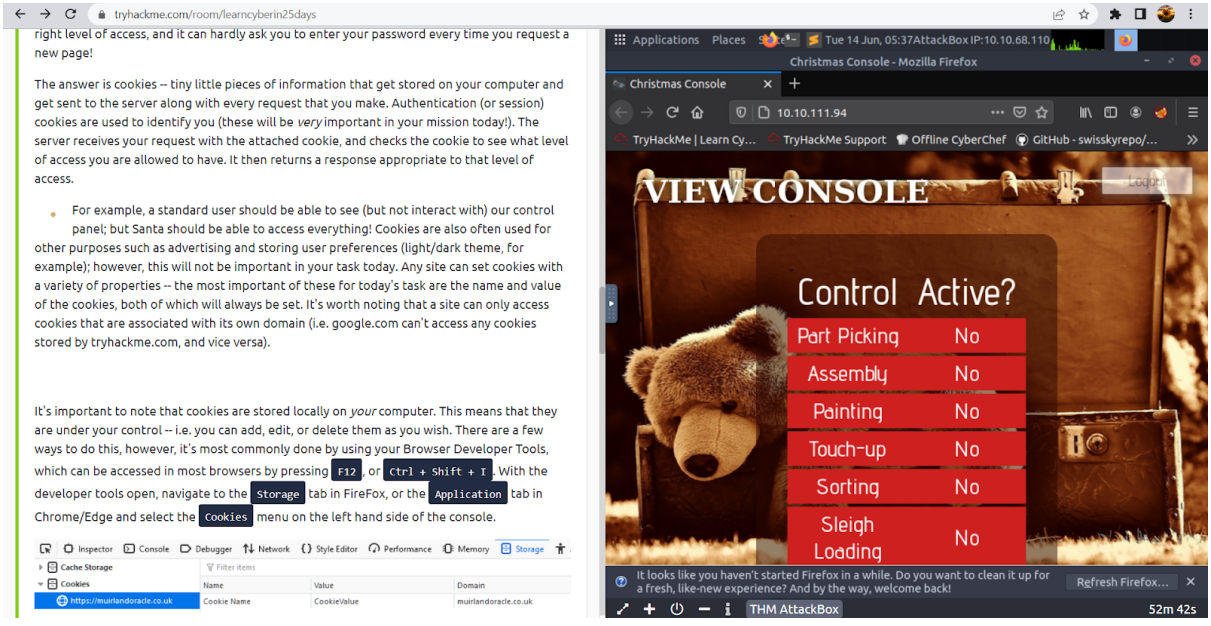
Day 1: Web Exploitation – A Christmas Crisis

Tools used: Kali Linux, Firefox

Solution/walkthrough:

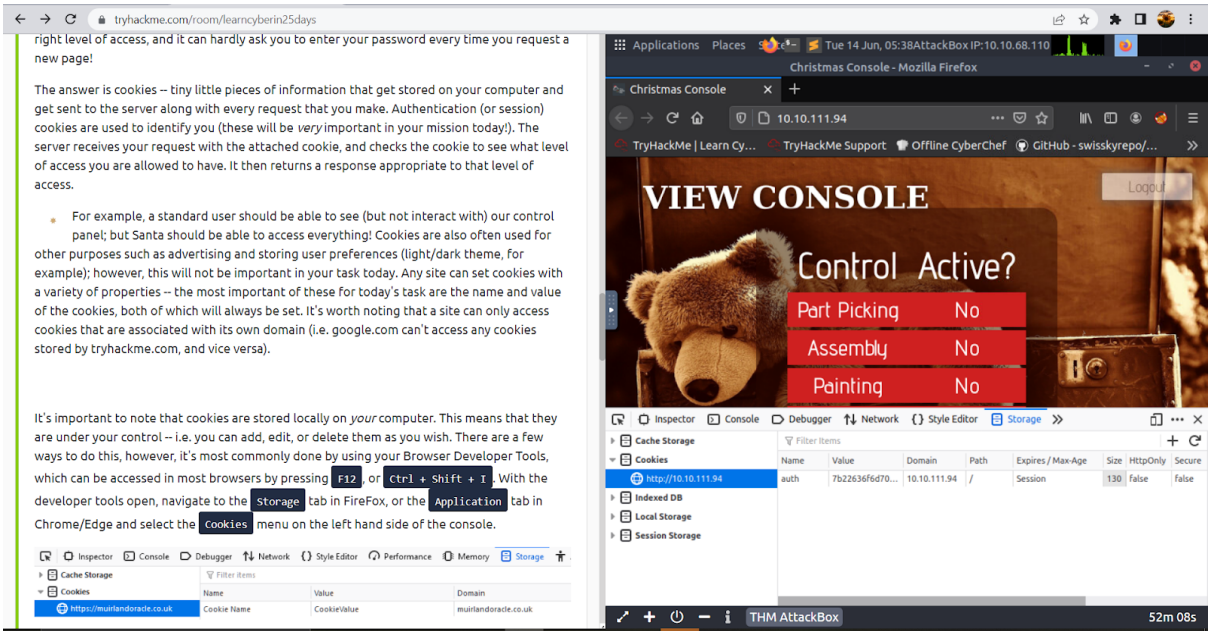
Question 1: Registration and logging to the Christmas Control Centre





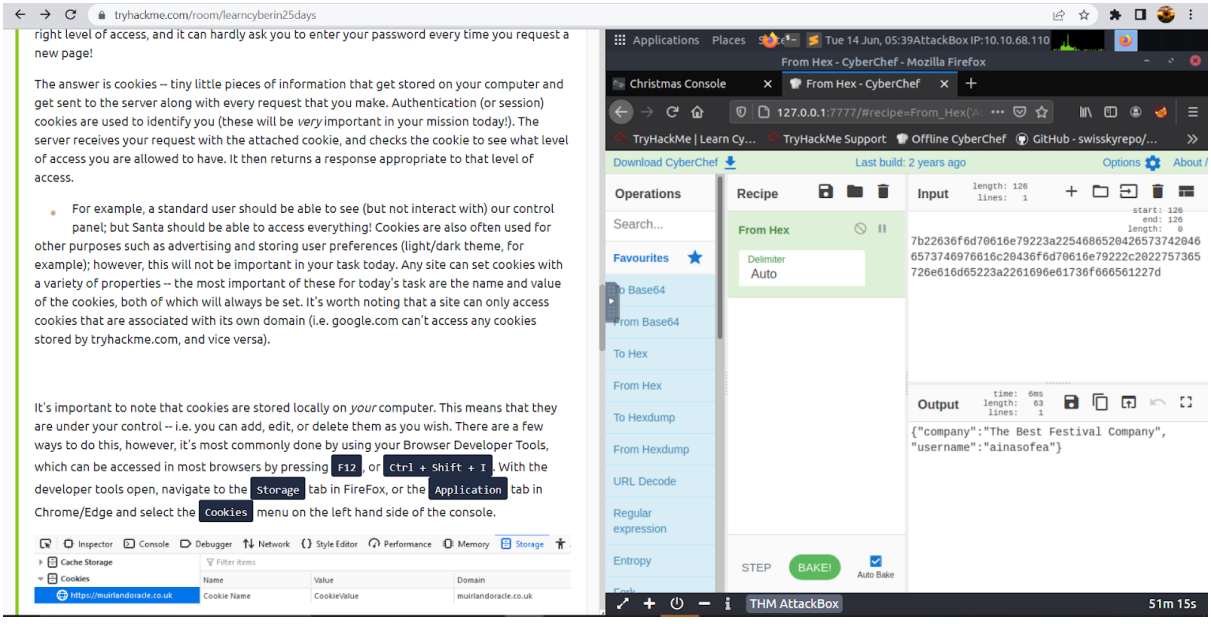
Question 2:

Open the browser tools to get the value and the name of the cookie



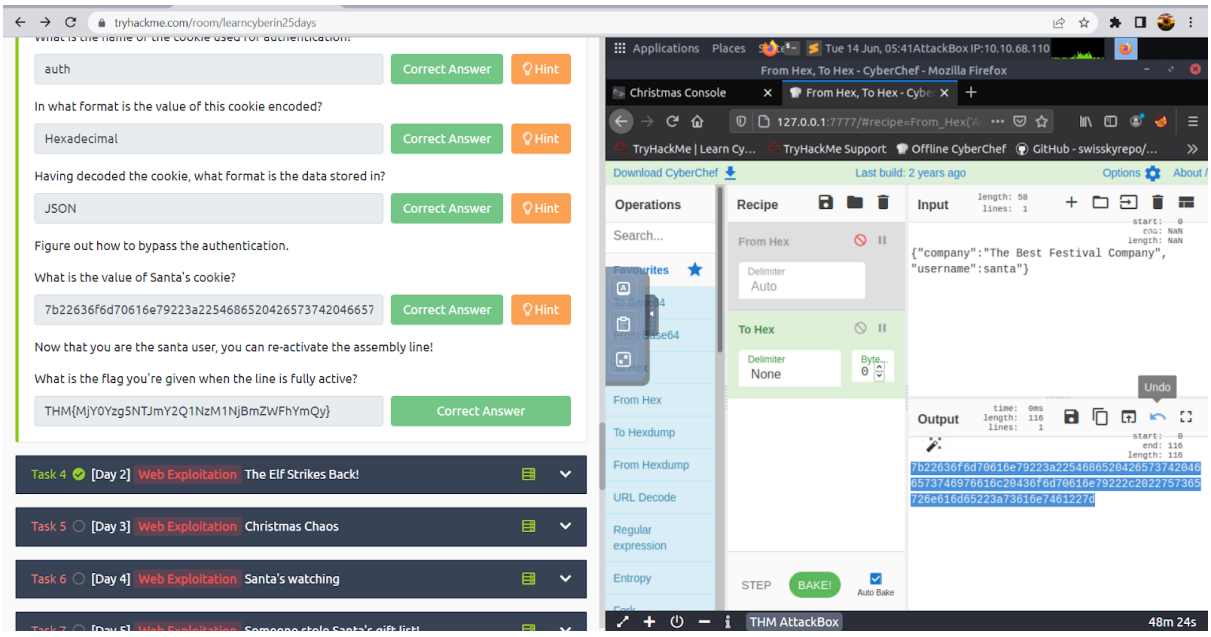
Question 3:

Change the value of the cookie to string by using cyberchef



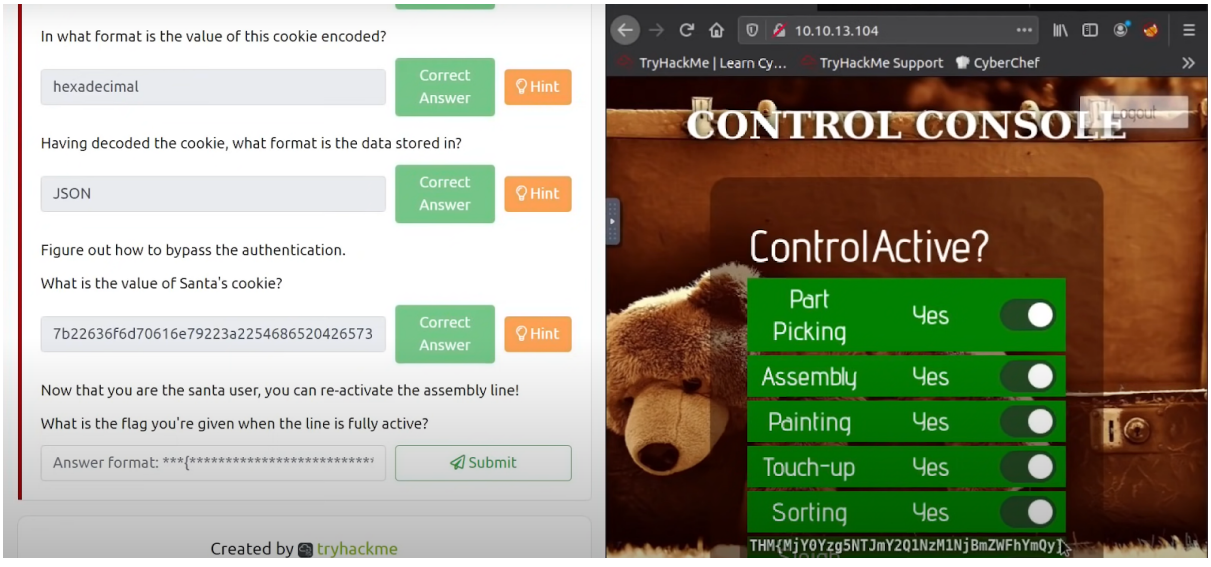
Question 4:

Changing the username to santa at the JSON files and returning to the value hexadecimal.



Question 5:

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



Thought Process/Methodology:

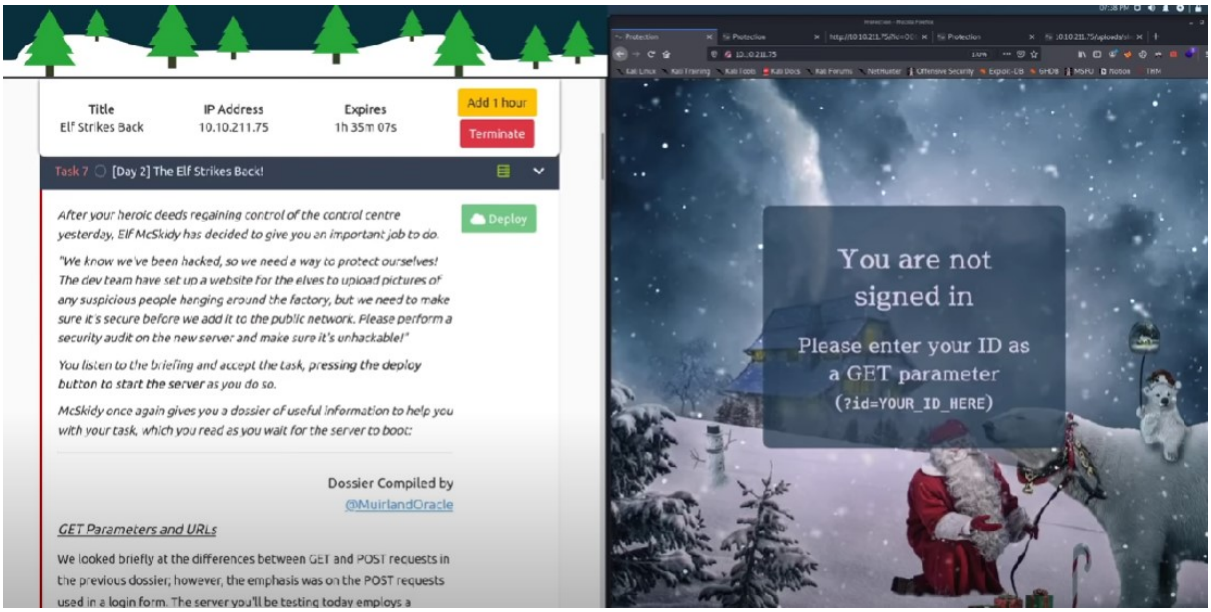
After we gained access to the target system, we were presented with a login/registration screen. We then created an account and logged in. After logging in, we opened the browser's developer tool and selected the Storage tab to examine the site cookie. We concluded from the cookie data that it was a hexadecimal number and used Cyberchef to convert it to text. We discovered a JSON statement containing the username element. We used Cyberchef to change the username to 'santa,' the administrator account, and then converted it back to hexadecimal. We updated the page after replacing the cookie value with the transformed one. We are now presented with an administrator page (Santa's) and proceeded to enable each control, which displayed the flag.

Day 2: Web Exploitation - The Elf Strikes Back!

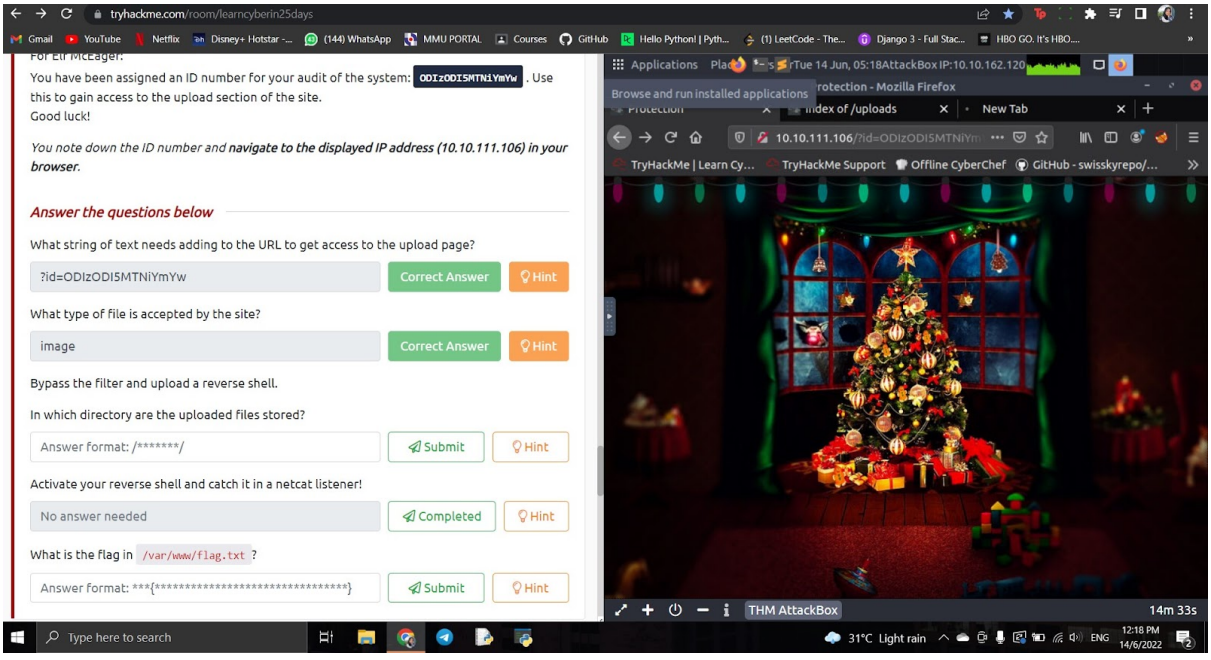
Tools used : Kali Linux & Firefox

Solution / Walkthrough :

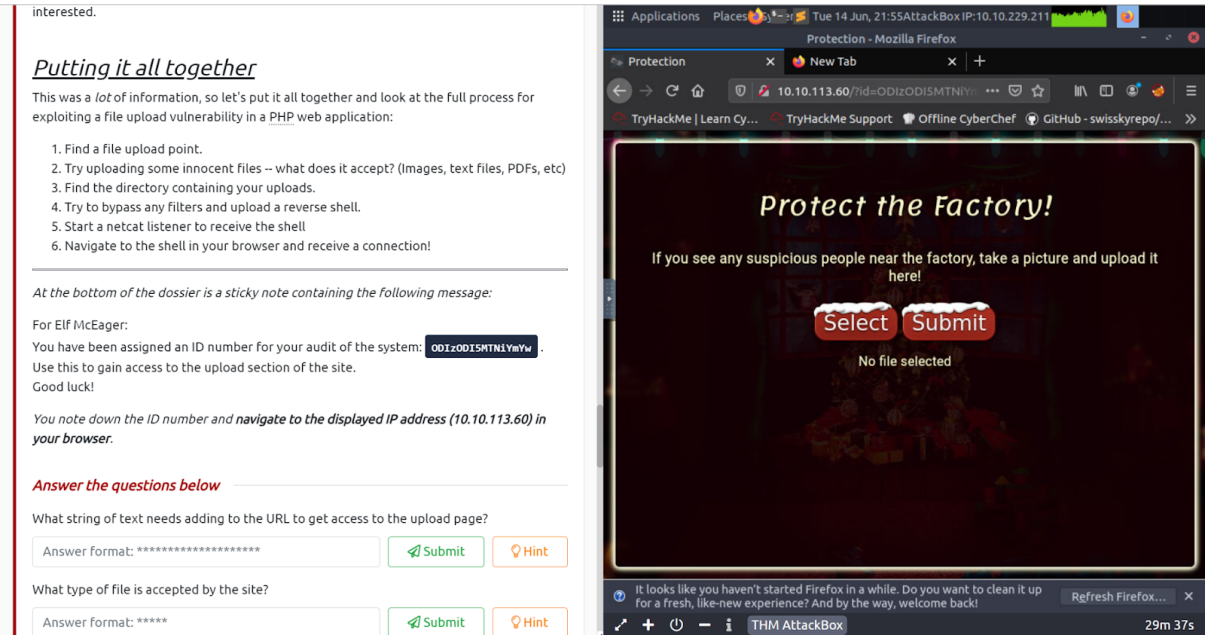
Question 1: the string of text that needed the url to be added to get the access to the upload page is detected.



Question 2: filter has been bypassed and reverse shell has been uploaded. Files have been uploaded in /uploads/ directory.



Question 3: Image is the type of file that has been accepted by the side



Question 4: The flag of /var/www/flag.txt is provided below the control console

Thought Process/Methodology:

After login, our ip address has been filled in the firefox. Then a file upload address has been located. We tried to upload a few unimpeachable files to figure out what it approves and what it does not. For example, files such as images, text files, PDFs, etc. Then we searched up the directory containing our uploads. After all of that has been done, we tried to bypass any filters in order to upload a reverse shell. After that, we started a netcat listener so that we could receive the shell. Last but not least, the shell in our browser has been navigated and the connection has been received!

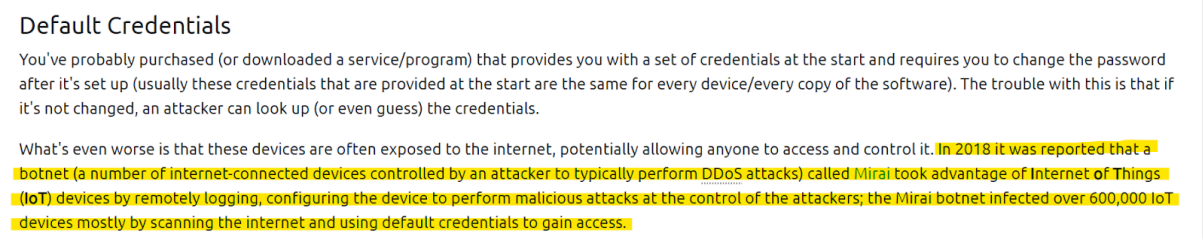
Day 3: Web Exploitation- Christmas Chaos

Tools used: Firefox, BurpSuite, FoxyProxy, Google

solutions/ walkthrough:

Question 1:

The name of the botnet that is mentioned in the text is Mirai botnet.



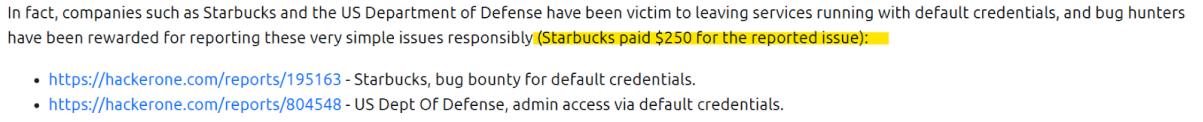
Default Credentials

You've probably purchased (or downloaded a service/program) that provides you with a set of credentials at the start and requires you to change the password after it's set up (usually these credentials that are provided at the start are the same for every device/every copy of the software). The trouble with this is that if it's not changed, an attacker can look up (or even guess) the credentials.

What's even worse is that these devices are often exposed to the internet, potentially allowing anyone to access and 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 Internet of Things (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 paid $250 for reporting default credentials according to the text.

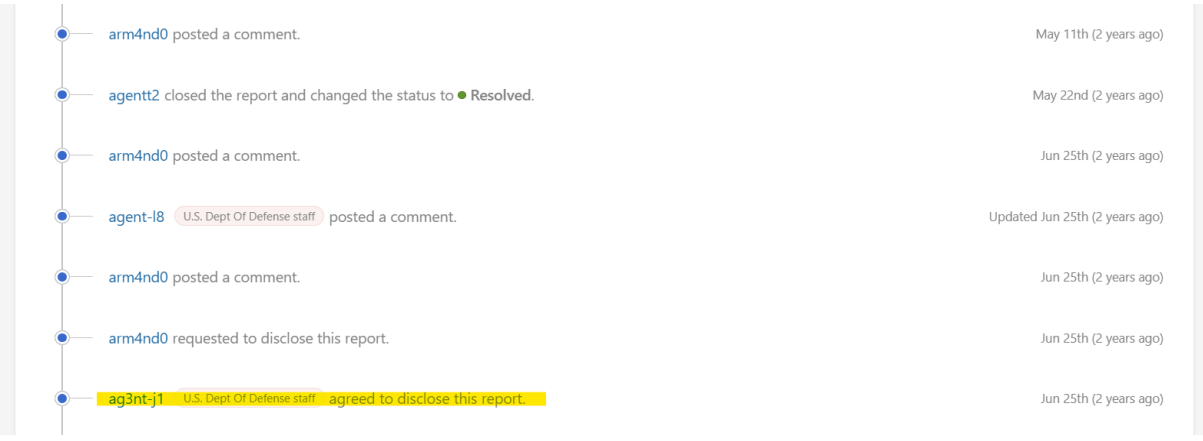


In fact, companies such as Starbucks and the US Department of Defense have been victim to leaving services running with default credentials, and bug hunters have been rewarded for reporting these very simple issues responsibly (Starbucks paid $250 for the reported issue):

- https://hackerone.com/reports/195163 - Starbucks, bug bounty for default credentials.
- https://hackerone.com/reports/804548 - US Dept Of Defense, admin access via default credentials.

Question 3:

The agent assigned from the Dept of Defense that disclosed the report on Jun 25th is ag3nt-j1.



arm4nd0 posted a comment. — May 11th (2 years ago)

agentt2 closed the report and changed the status to ● Resolved. — May 22nd (2 years ago)

arm4nd0 posted a comment. — Jun 25th (2 years ago)

agent-l8 U.S. Dept Of Defense staff posted a comment. — Updated Jun 25th (2 years ago)

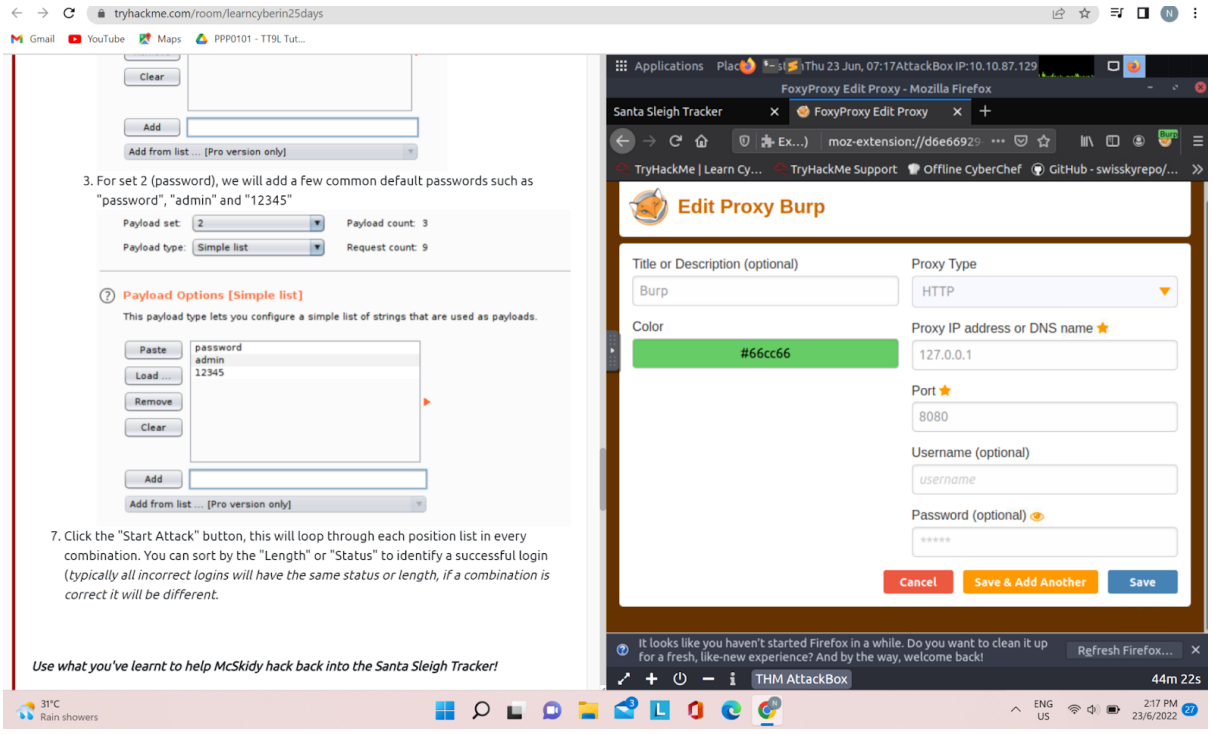
arm4nd0 posted a comment. — Jun 25th (2 years ago)

arm4nd0 requested to disclose this report. — Jun 25th (2 years ago)

ag3nt-j1 U.S. Dept Of Defense staff agreed to disclose this report. — Jun 25th (2 years ago)

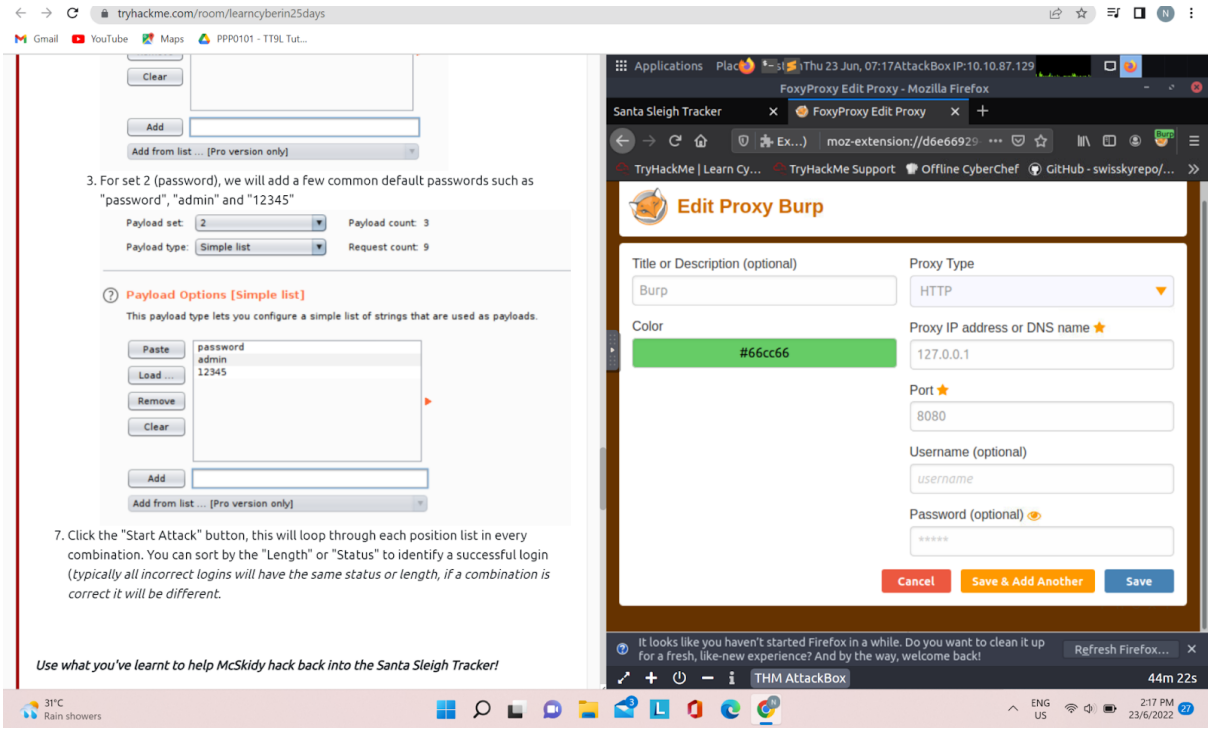
Question 4:

We can look for the port number on Burp by clicking the options on Burp and select edit Proxy Burp. The port number is 8080.



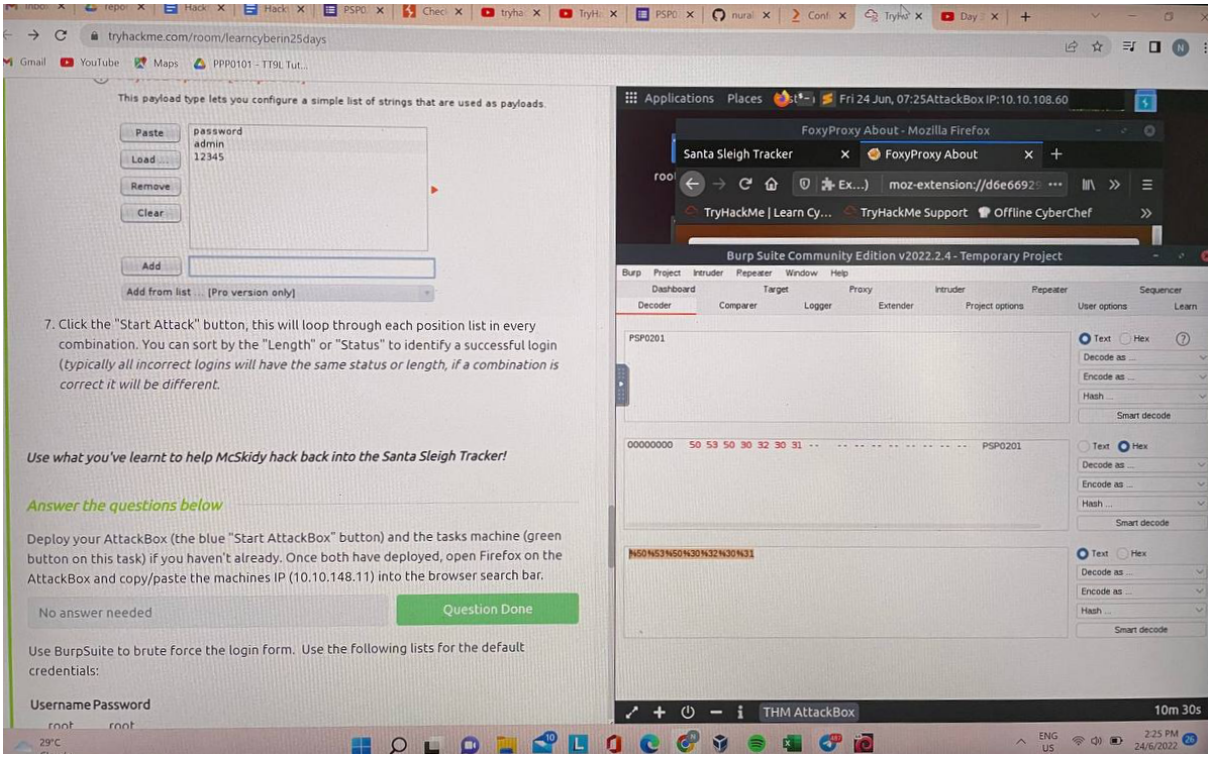
Question 5:

The proxy type can be found in the same section as the port number. The proxy type is HTTP.



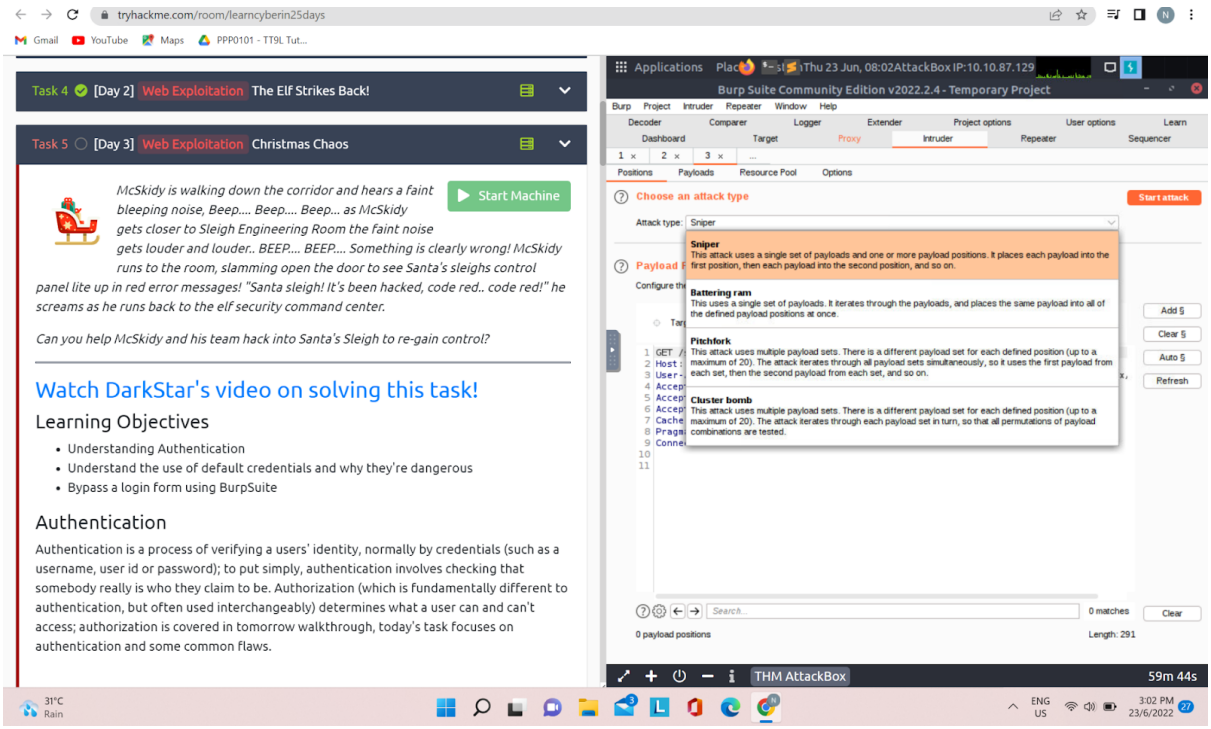
Question 6:

In BurpSuite, select the decoder tab. Insert the word “PSP0201” and encode the text as URL. The value obtained is the one we are looking for which is %50%53%50%30%32%30%31.



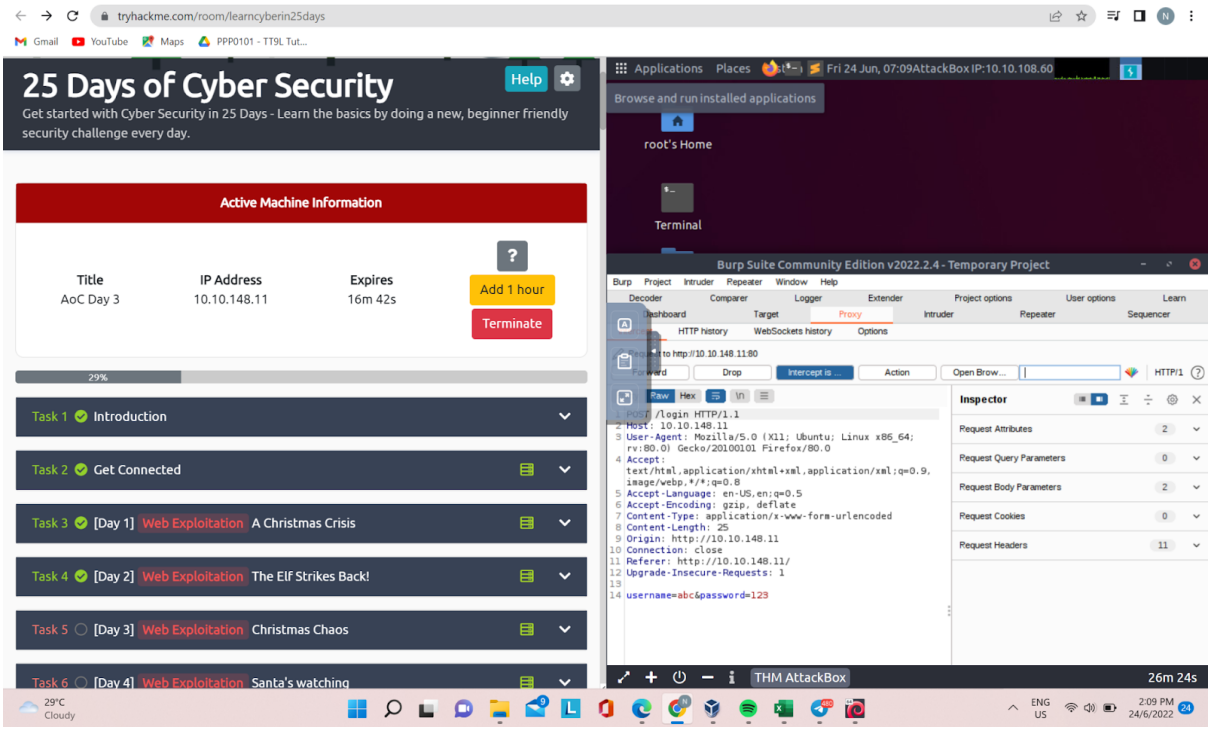
Question 7:

In the attack type section from the intruder tab, the one that matches the description in the google form which is “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” is Cluster Bomb.

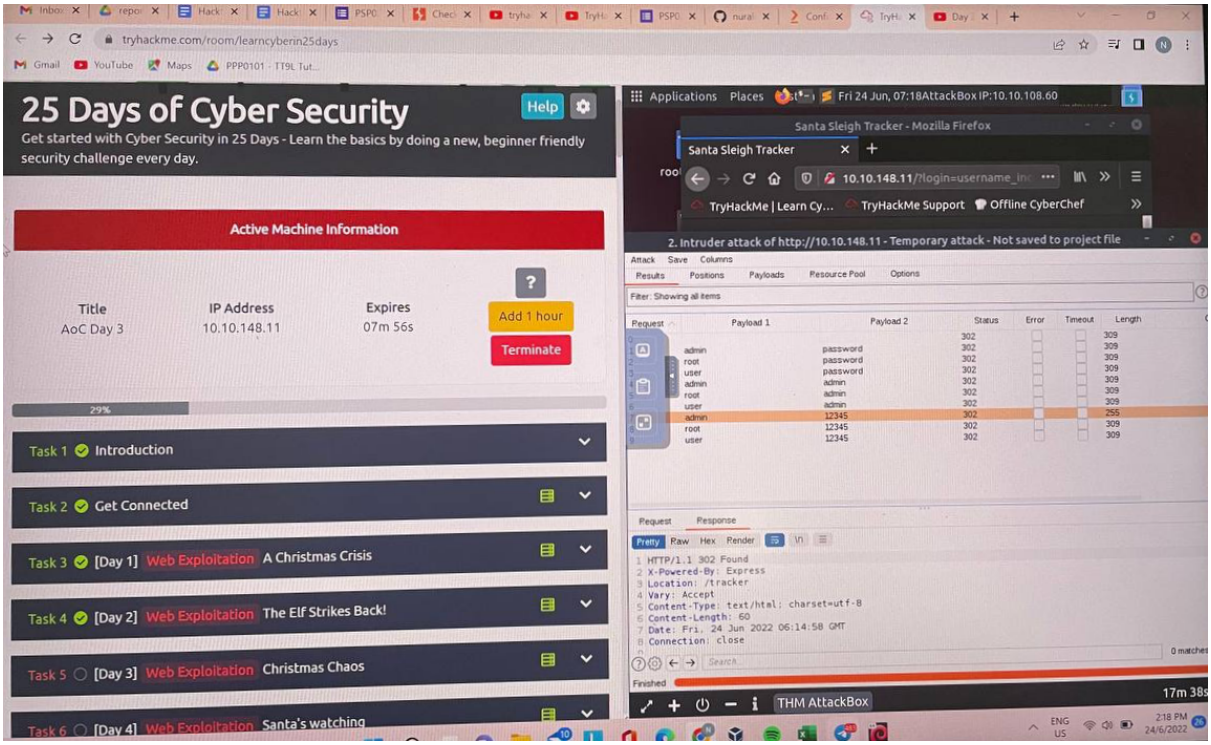


Question 8:

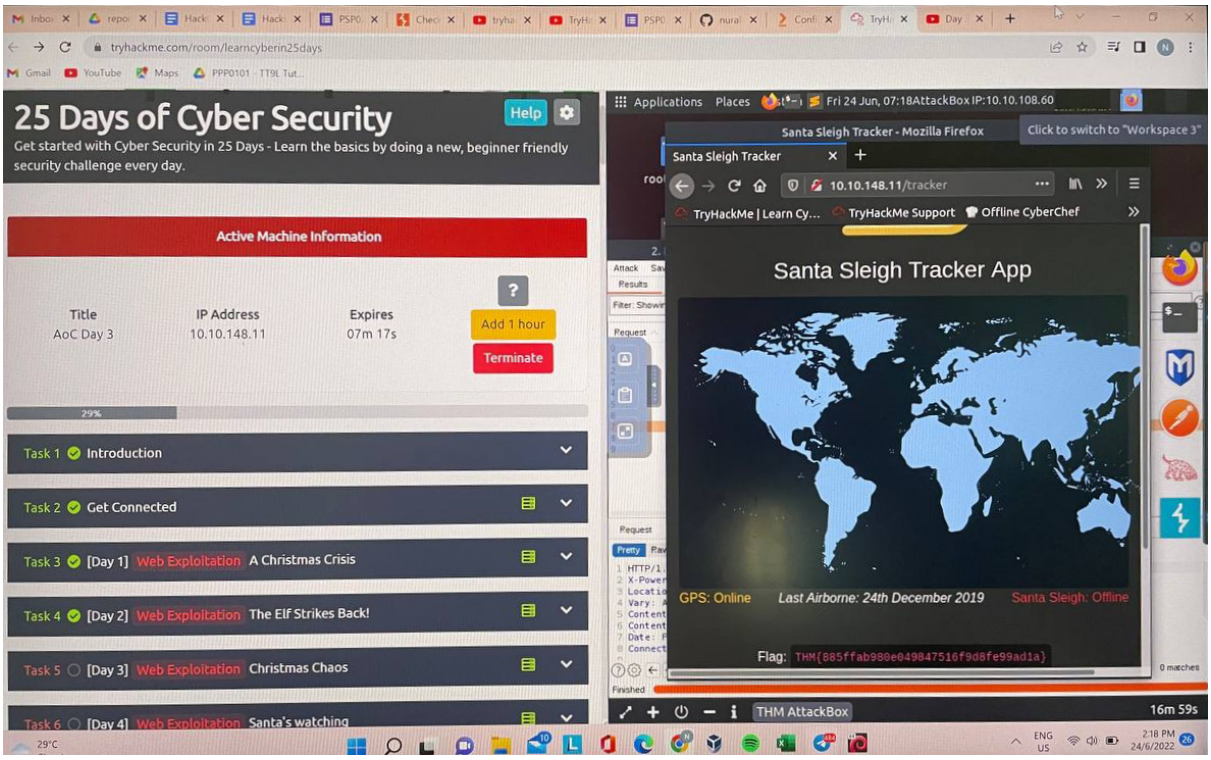
To obtain the flag, go to BurpSuite and enter the port number 8080 and change the specific address to 127.0.0.1. We need to ensure the intercept is on, turn on ‘Burp’ on FoxyProxy and now we can see that BurpSuite has held our request. Go to Santa’s portal and login using any random username and password. This captured request will be shown in the proxy tab. Right click and choose ‘send to intruder’ . In the intruder tab, we can now see our request. Select “Cluster Bomb” in the Attack type dropdown menu. As we want to tell each “Position” which payload to use, we will choose a list of usernames and passwords to be used. In this case, for Payload 1 which is the username, we use: “admin”, “root”, “user”. For Payload 2 which is the password, we use: “password”, “admin”, and “12345”.



Click the “Start Attack” button to loop through each position list in every combination. We can sort the “Length” and “Status” to look for a successful login. In our case, we identified that the correct username and password would be “admin” and “12345”.



Direct back to Santa's Portal and enter the correct username and password. The flag is now shown on the screen!!



Thought Process/Methodology:

Day 4: Web Exploitation - Santa's watching

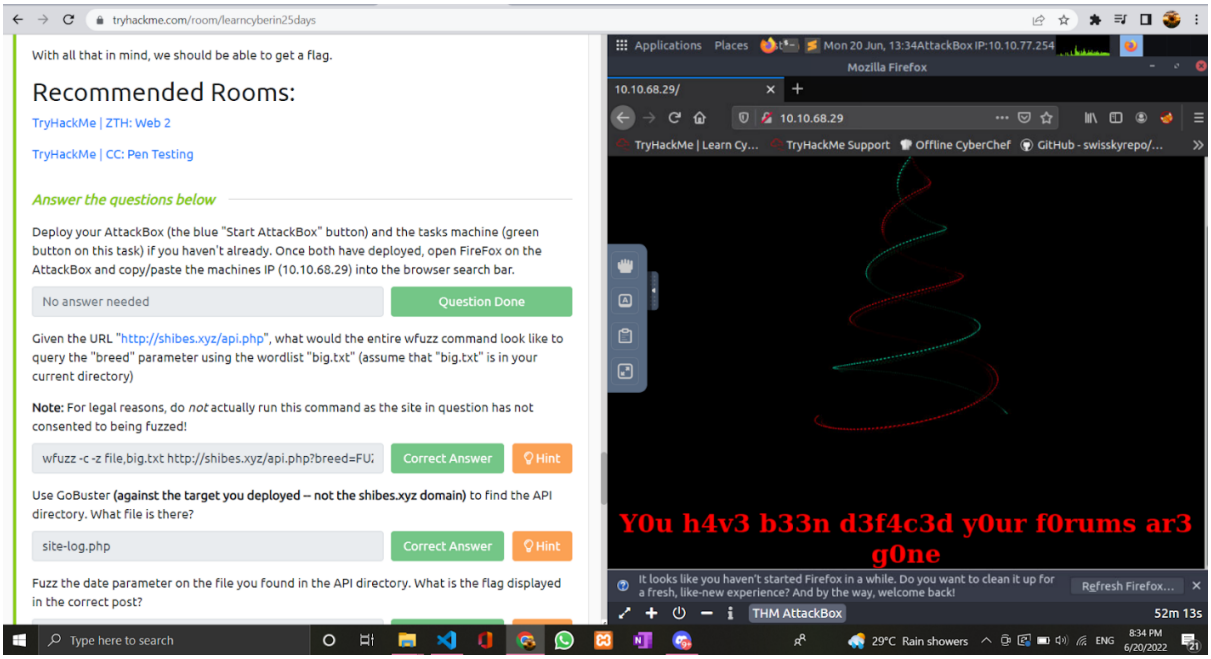
Tools used: Attackbox, mozilla firefox, terminal

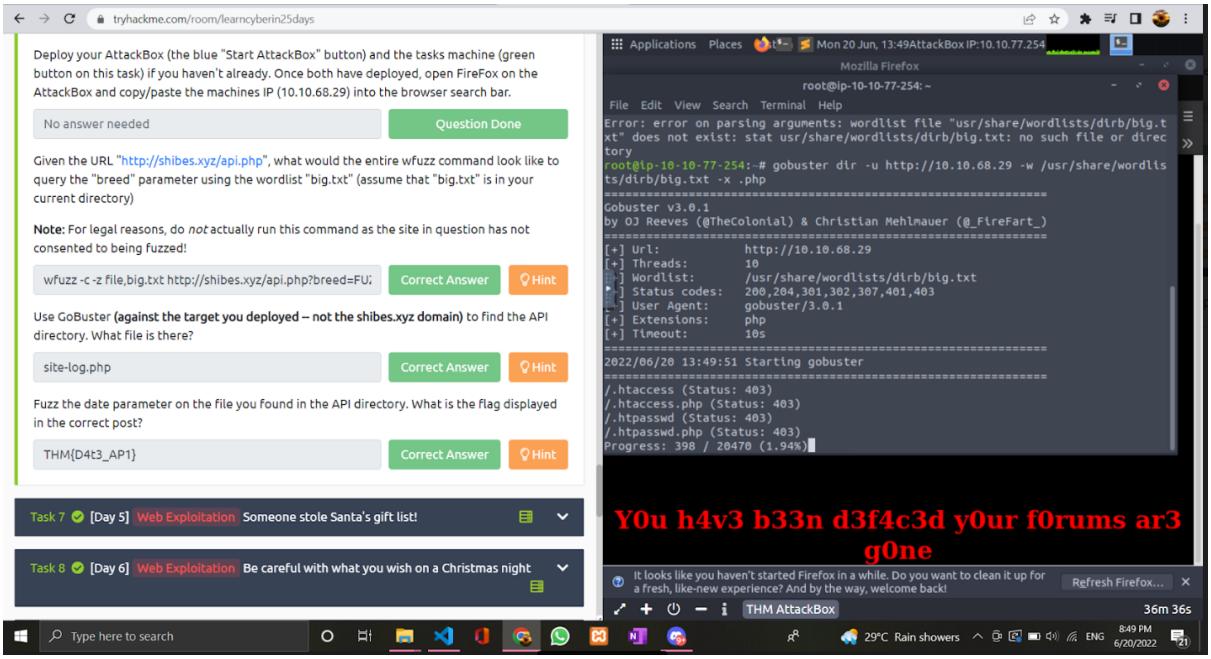
Solution/walkthrough:

Question 1:

Open the IP addresses given in the firefox.
Then find the accurate parameter and command.

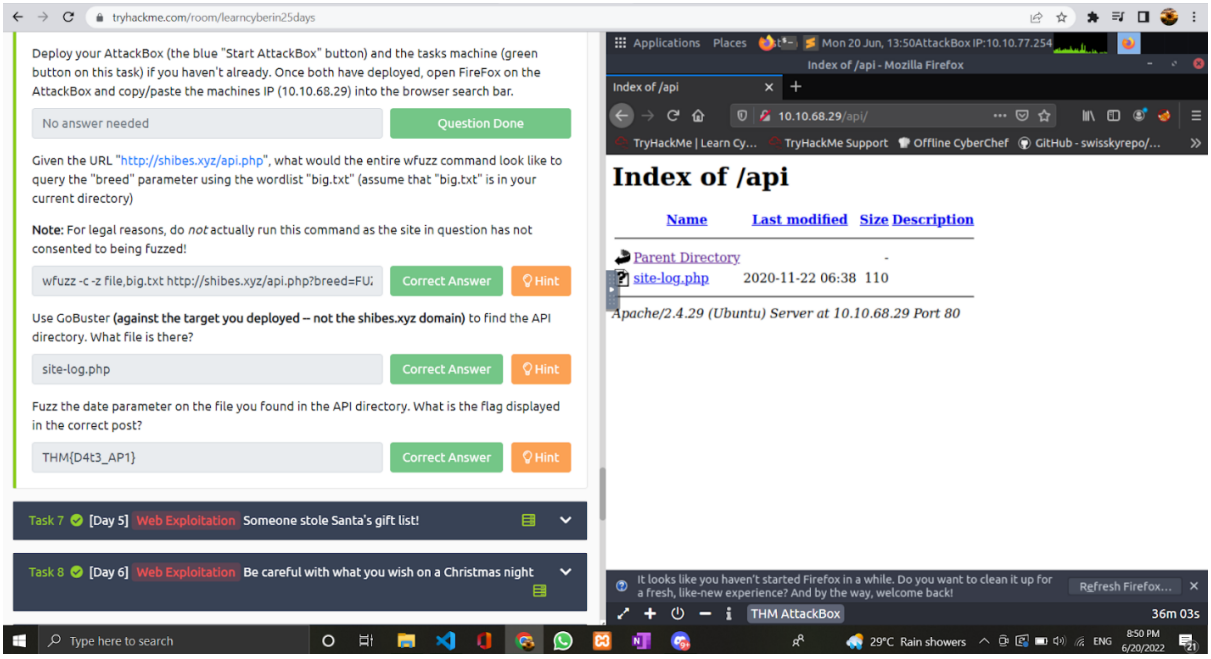
Common wfuzz dash c to get the colour output, dash z to select that we are going to use a file. Then we want the big.txt and we put the url which is 'https://shibes.xyz/api.php' and breed for FUZZ at the end.





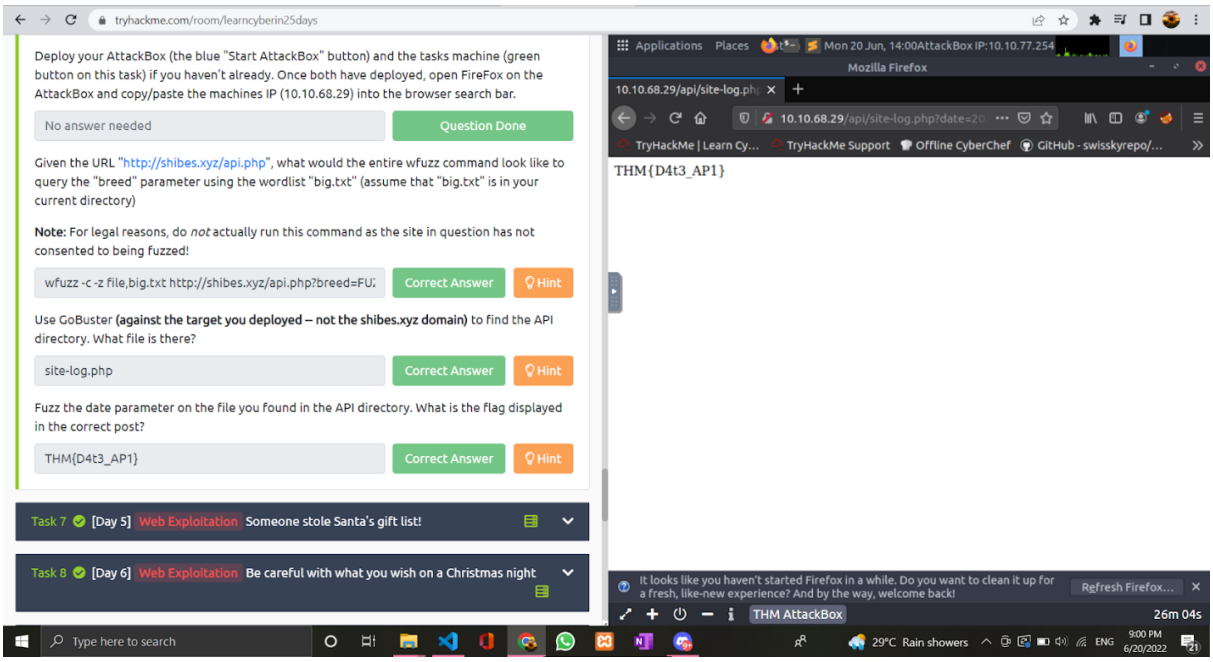
Question 2:

We enter the IP addresses and navigate with the api directory and find the file site-log.php



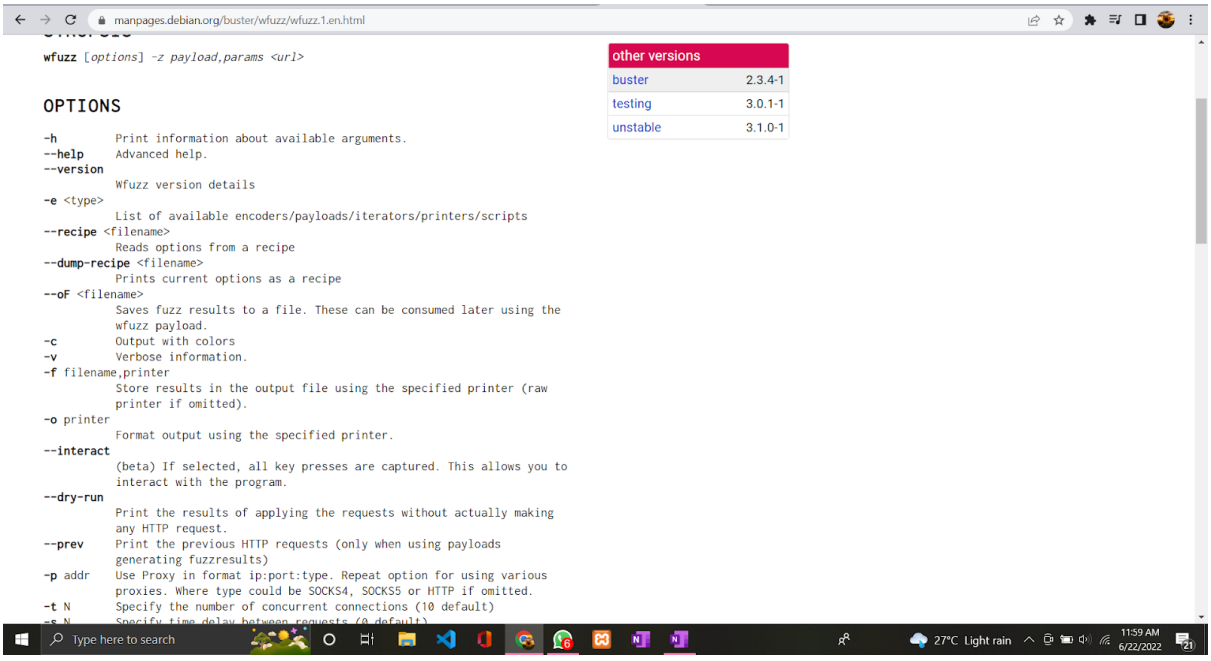
Question 3:

Search the IP address, the file and the date of the file using the command date=YYYYMMDD.



Question 4:

-f parameter store results to printer and filenames.



Thought process and methodology:

We have to understand the parameter in the WFUZZ and handle it in the terminal. In the terminal, we use the gobuster directory to discover the valuable directories if they exist. We use -u to specify which url to enumerate, -w as path to the wordlist and lastly, -x to specify file extension. We also use the API directory to navigate the files in the Mozilla Firefox's search. To find the flag, we navigate with the api directory and use the file name which is site-log.php and the date command. The date of the file we can see beside the file on the screen is 2020-11-22. With the date format, YYYYMMDD. Then, we get the secret flag.

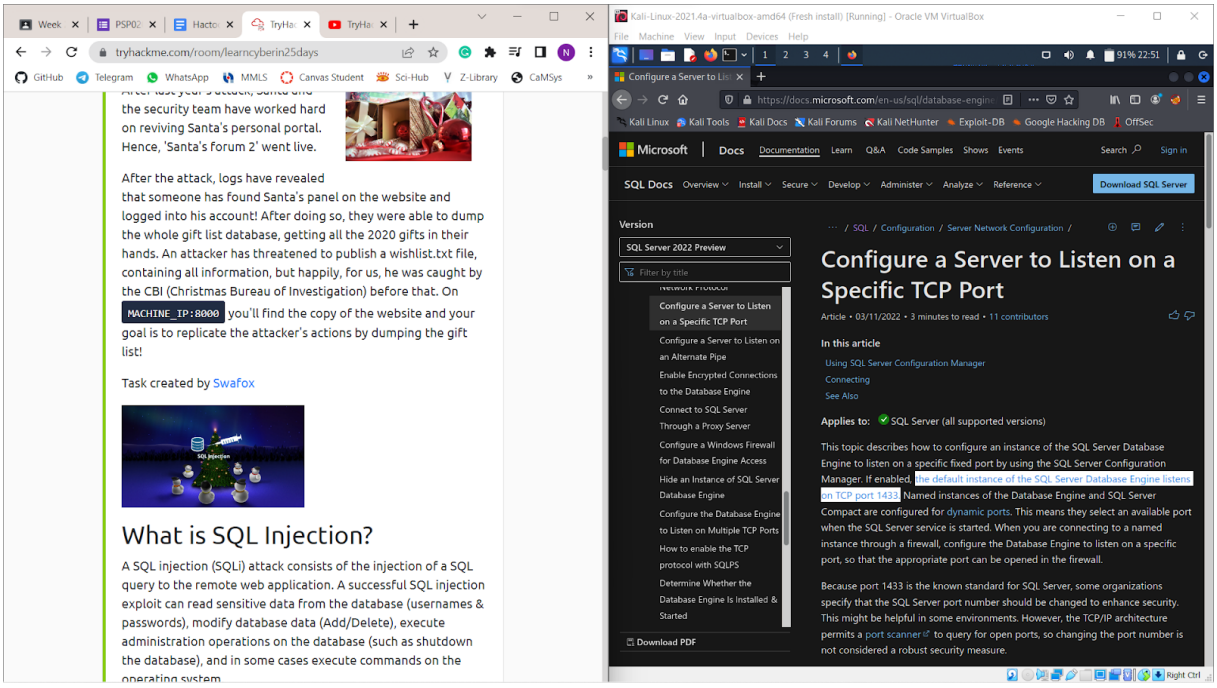
Day 5: Web Exploitation - Someone stole Santa's Gift List

Tools used: Kali linux, Firefox, Burp Suite, FoxyProxy

Solution/walkthrough:

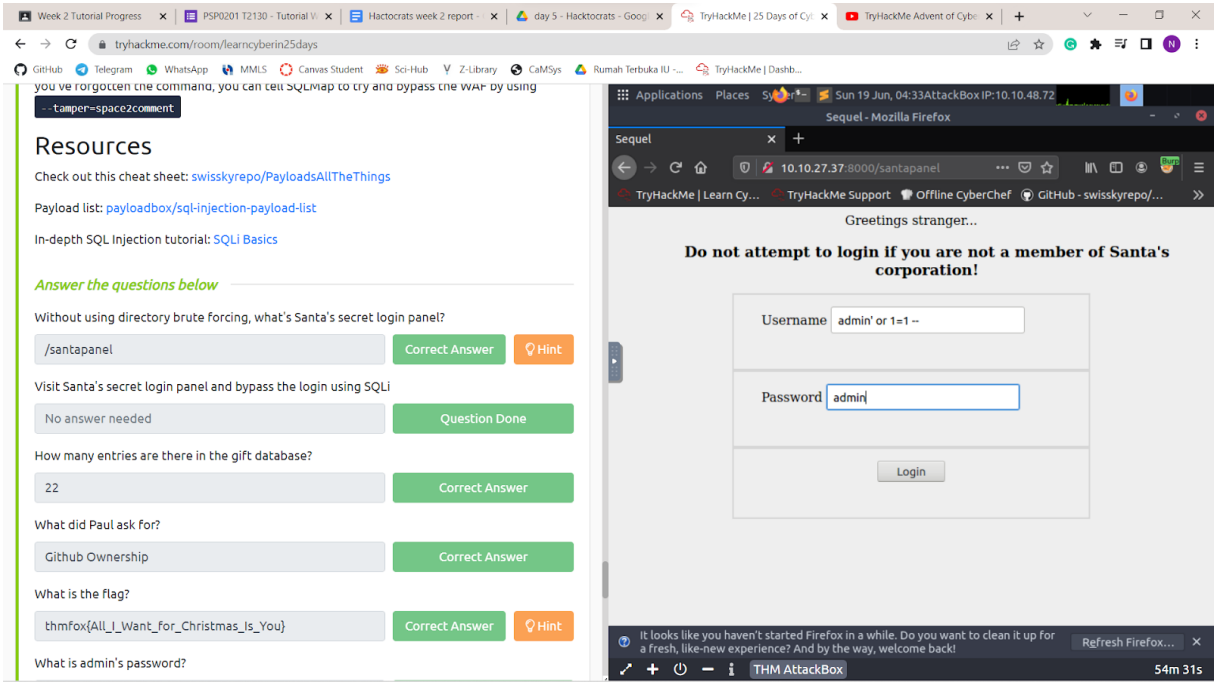
Question 1

Open microsoft documentation on firefox to obtain default port number for SQL server running on TCP



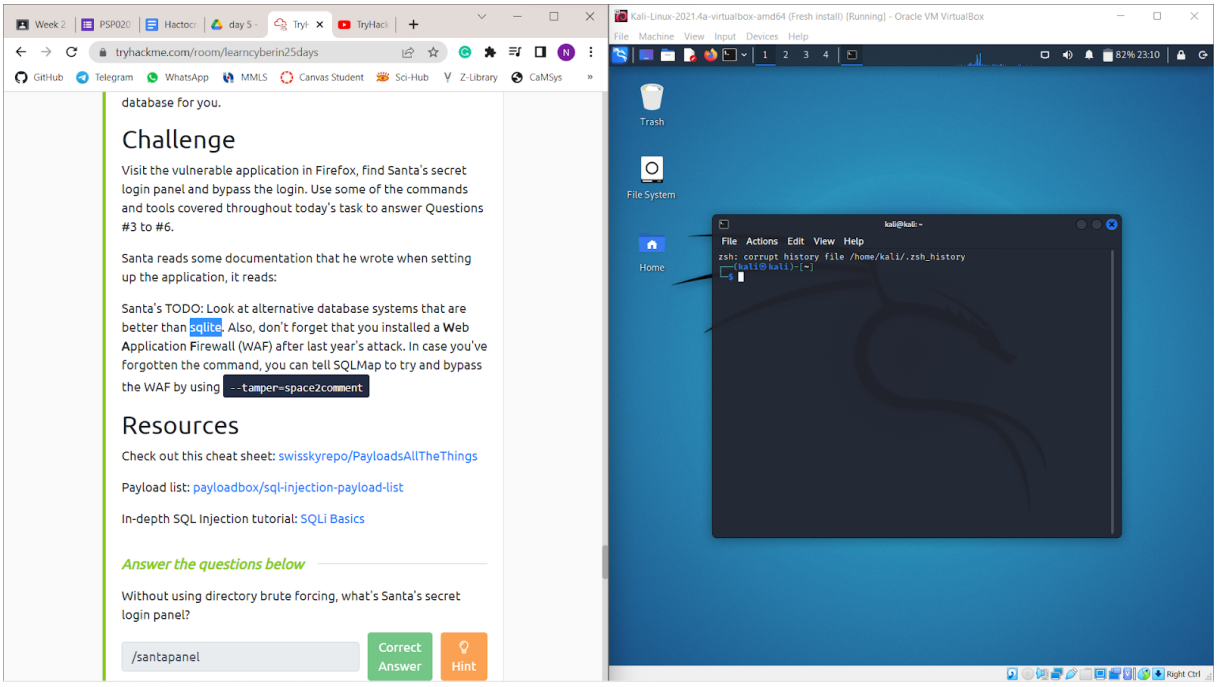
Question 2

Bypassing through santa's login panel by inserting username and comment the rest of the query



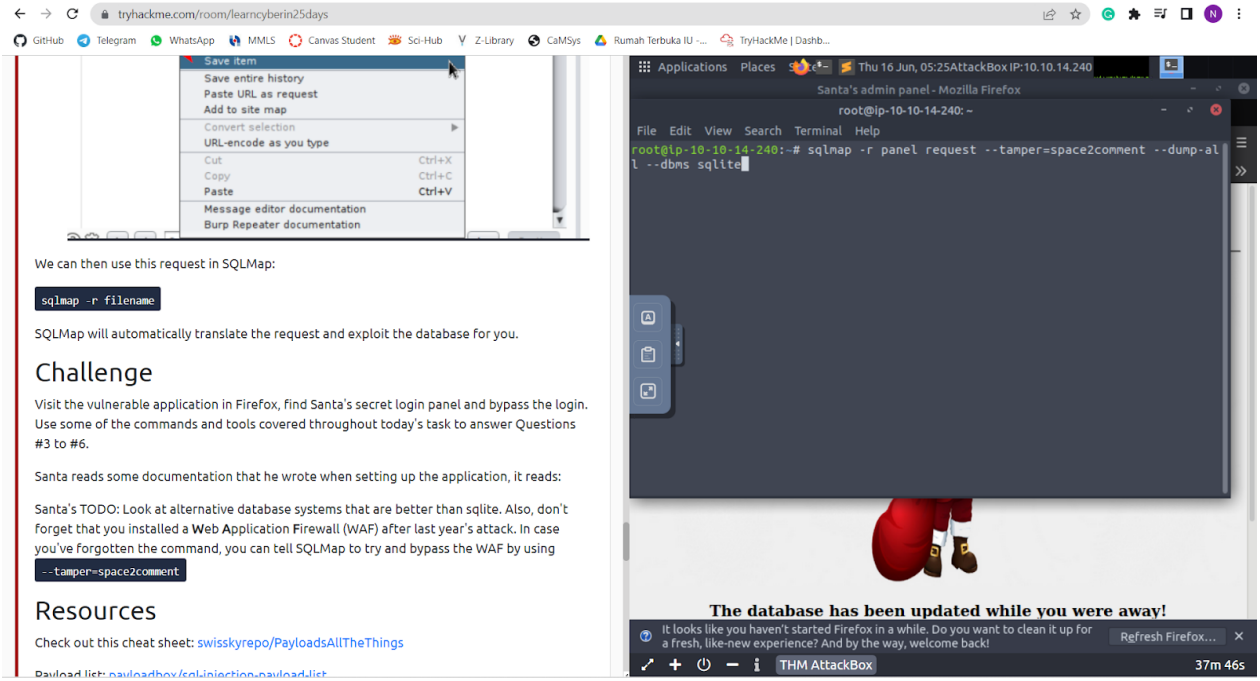
Question 3

Obtaining database used in Santa's TODO list

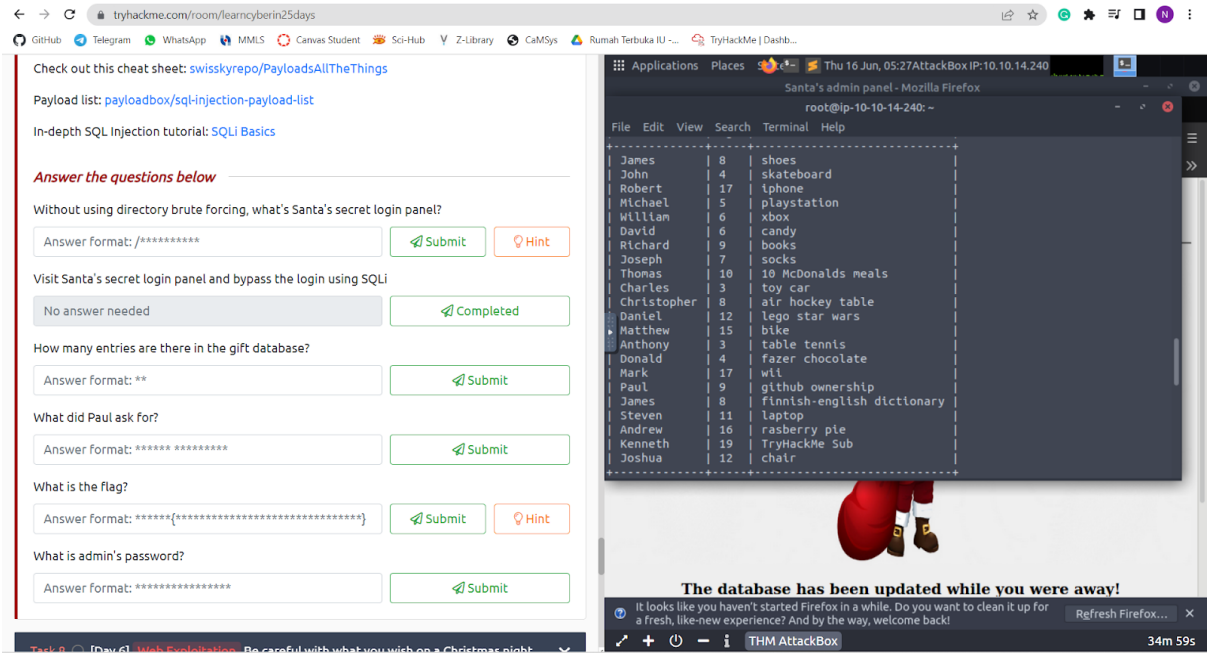


Question 4

Insert burp suite saved request into SQL commands and successfully obtained the wishlist from the database.

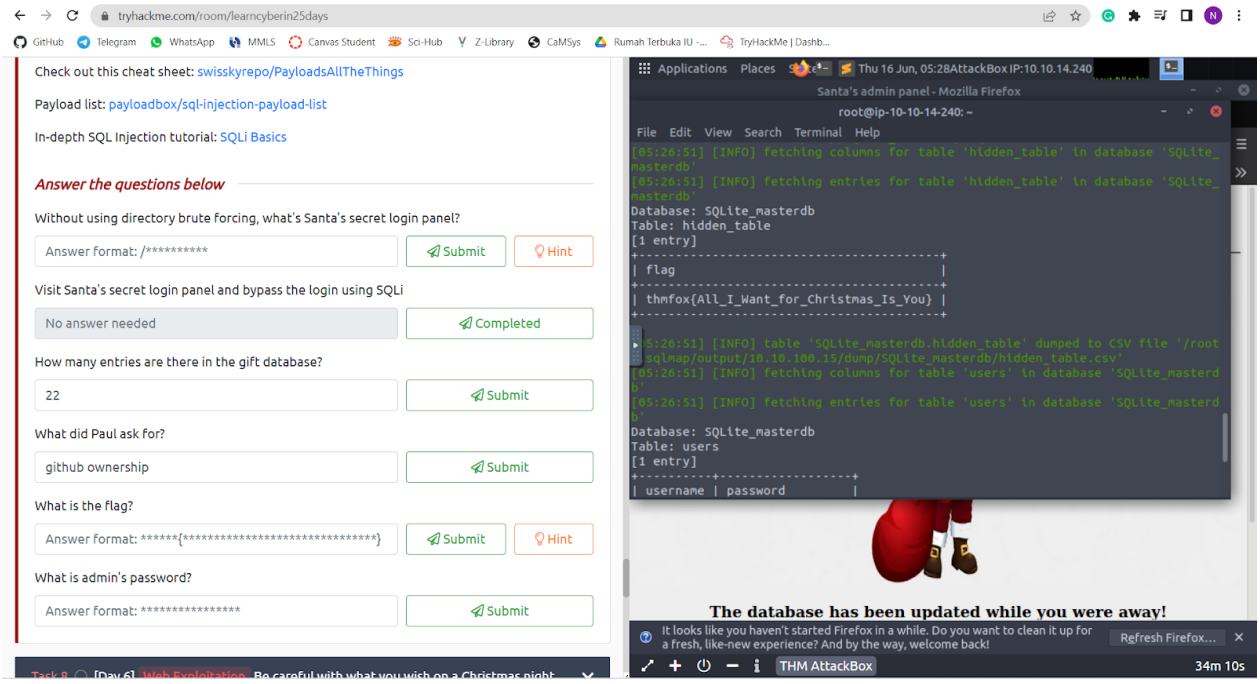


Get number of entries, Paul's christmas gift and James' age.



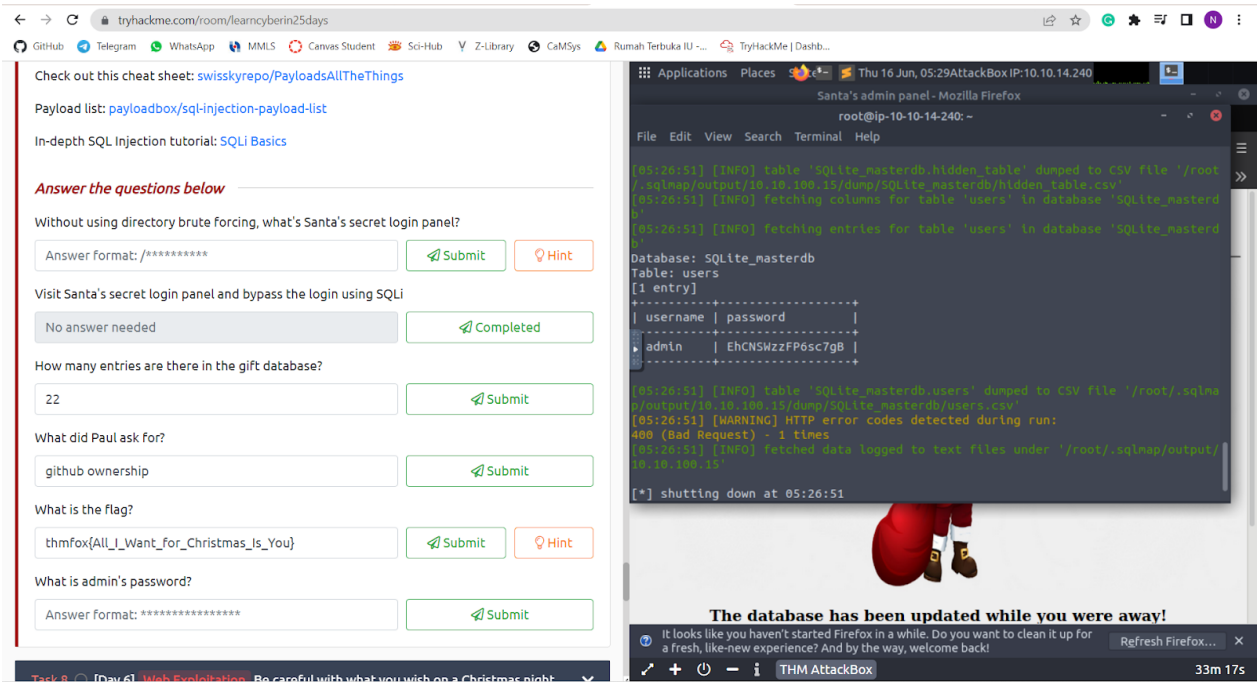
Question 5

Scroll down to see THM flag



Question 6

Scroll down further to see admin's password



Thought process/methodology:

We browsed to the copy of the website and managed to access santa's secret login panel using try and error method. We tried inserting a few names after the ip address and found out that the name for santa's secret login panel is santapanel. After that, we used burpsuite to intersect request from the webpage and save the request to our local machine. We then use sqlmap in the terminal to get the data in the gift list database. Sql commands that we used includes "--tamper=space2comment" to bypass the firewall, "--dump-all" to show the entire database and "--dbms" to specify the type of database that is running. We successfully obtain the gift list, THM flag and admin's password.