PSP0201
Week 2
Report

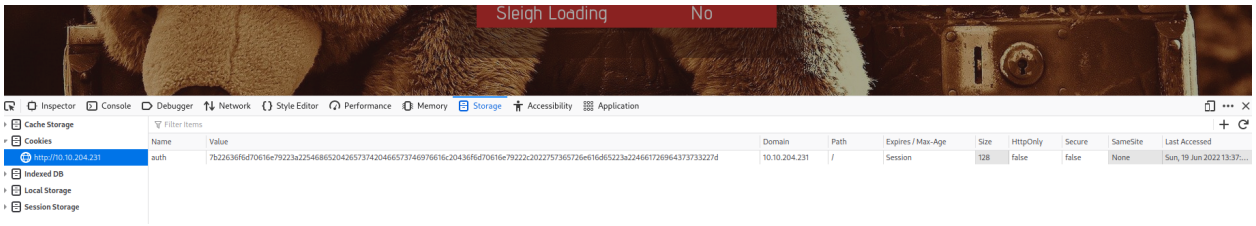
Group Name : Cipher
Members :

ID	Name	Role
1211103064	MUHAMAD AIMAN BIN MOHD EHWAL	Leader
1211103085	MUHAMMAD FARID BIN JAYATAN	Member
1211103373	MUHAMMAD ALIF BIN KHABALI	Member
1211103451	ARIF MUHRIZ BIN SYAMSUL FOZY	Member

Day 1: Web Exploitation – A Christmas Crisis

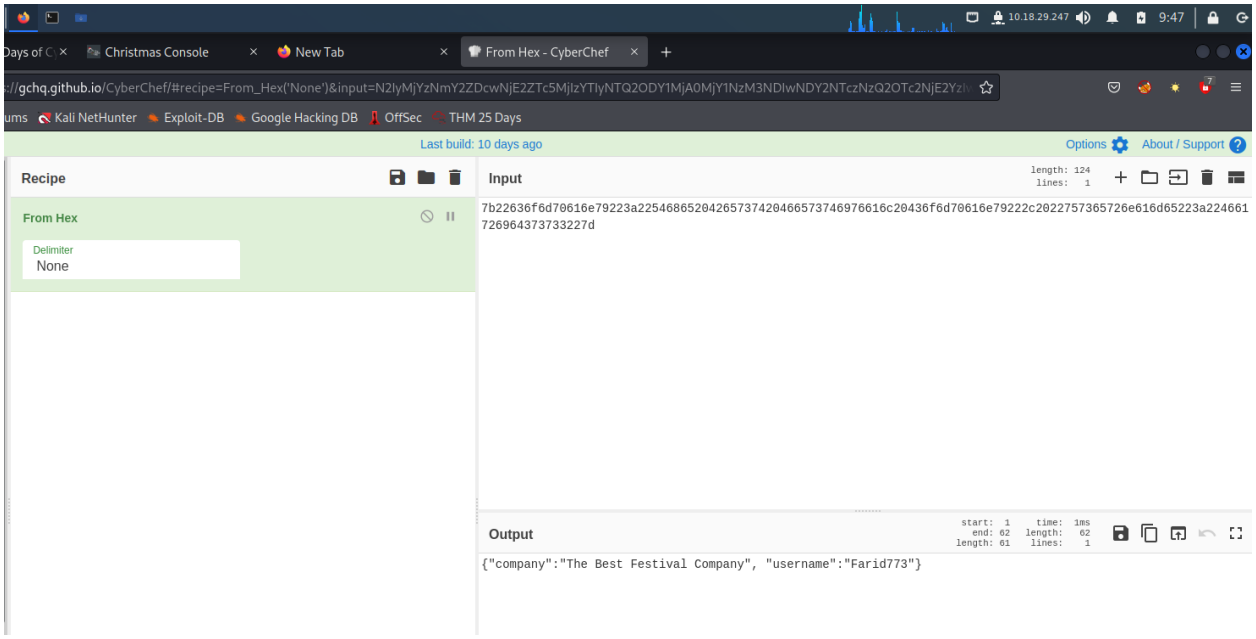
Tool Used : Kali Linux, Firefox
Solution / Walkthrough :

Question 1 & 2



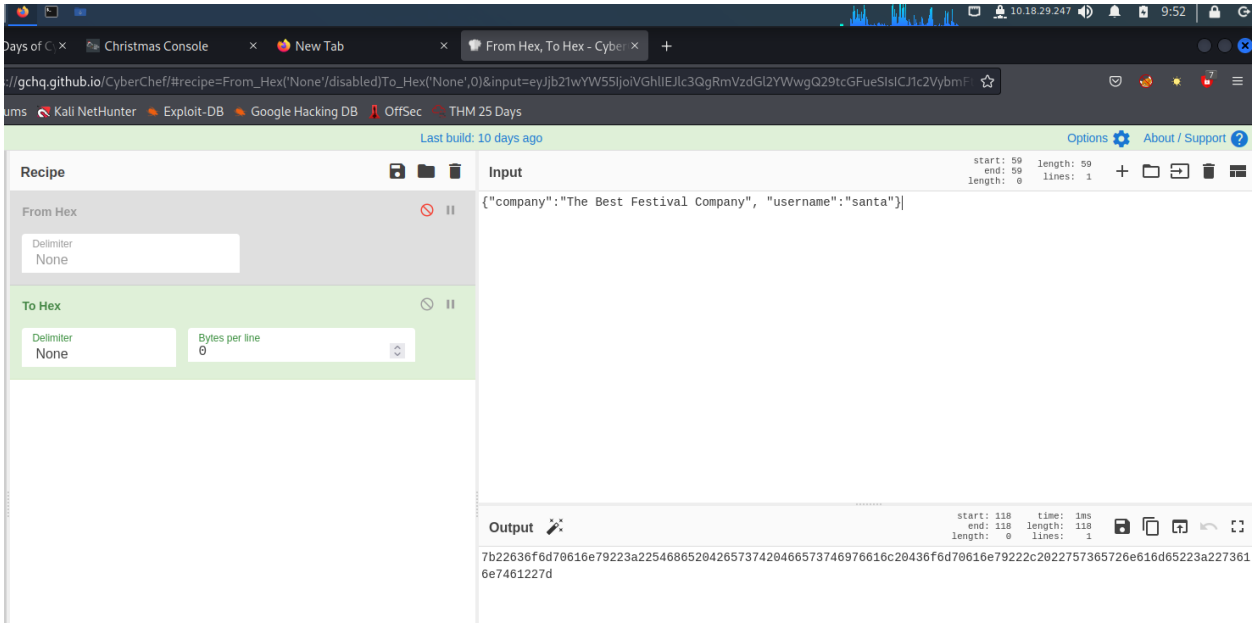
After successfully logged in, by using the F12 key, a new mini-tab will be opened which displays the information needed in the storage section. The information displayed are the name of the cookie, and the value format of the cookie.

Question 3



By taking the cookie value, we can go to the CyberChef website to decrypt the value and change it into a different translation. The hexadecimal values that we copied can be translated into a text format for us to manipulate easily.

Question 4



Question 5

From the translated value that we got, we can change the username to “santa” for us to get different hexadecimal values. With this new value, we can then put it into the cookie value in the mini-tab and update it.

After refreshing the page, we now have the access to manipulate Santa's control panel and activate every control to acquire the flag.

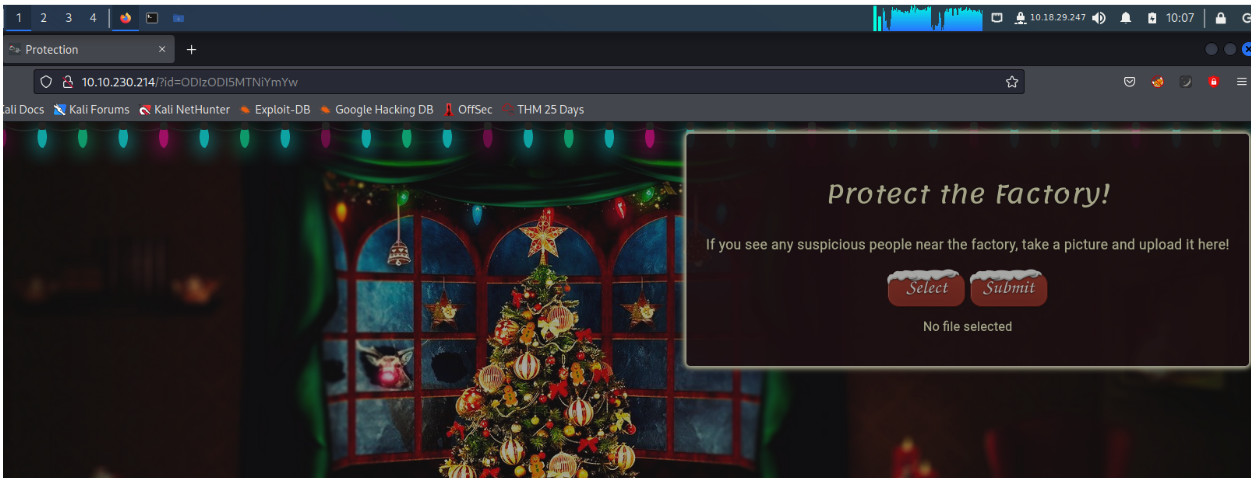
Thought Process / Methodology :

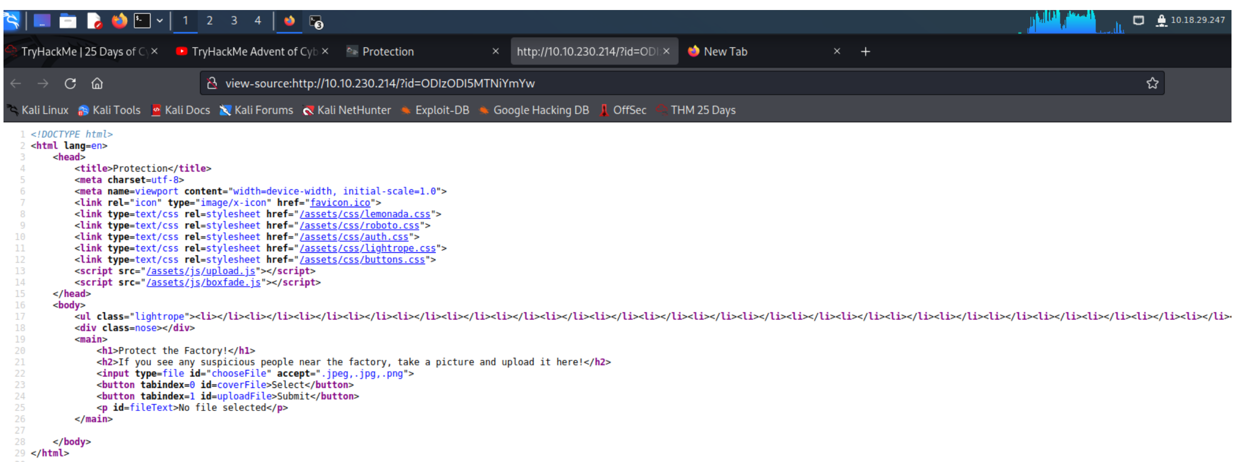
After we have successfully accessed the target machine, we are directed to a login and registration page. We then proceed to register an account and login. After we logged in, we opened the browser's developer tool and chose to view the site cookie at the 'Storage' tab. Checking the cookie value, we can identify that the value is hexadecimal and we can use that to convert it to text format using Cyberchef. We found out that it was in a JSON statement with the username element. By using Cyberchef, we can change the username to 'santa', the administrator account, and convert it back to hexadecimal using Cyberchef. We replaced the cookie value with the one that we acquired earlier and refreshed the page. We now have access to the administrator Santa's page and enable every control to make it display the flag.

Day 2: Web Exploitation – The Elfs Strikes Back!

Tool Used : Kali Linux, Firefox
Solution / Walkthrough :

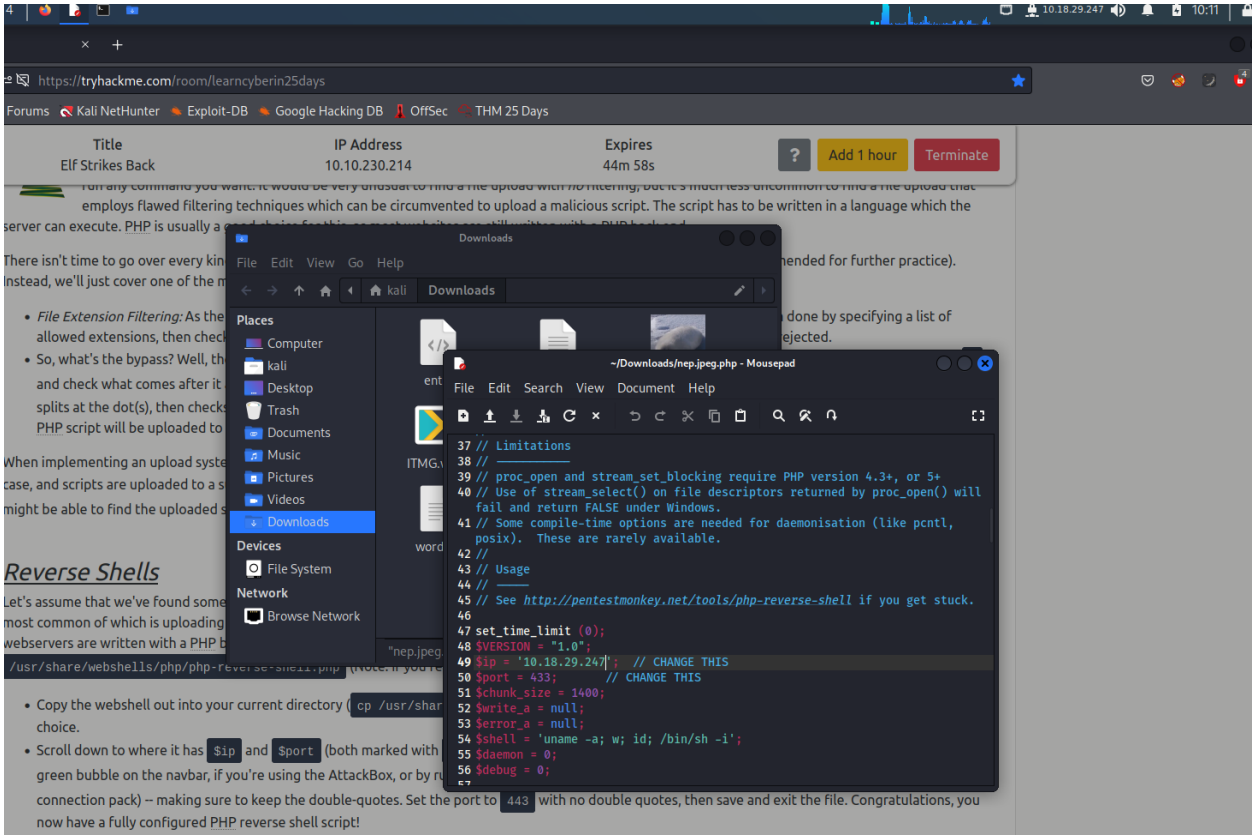
<u>Question 1 & 2</u>

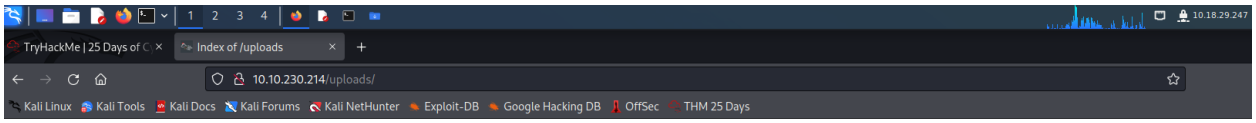




With the given ID number, we can use it to go into this page. The page only accepted an image file.

Question 3



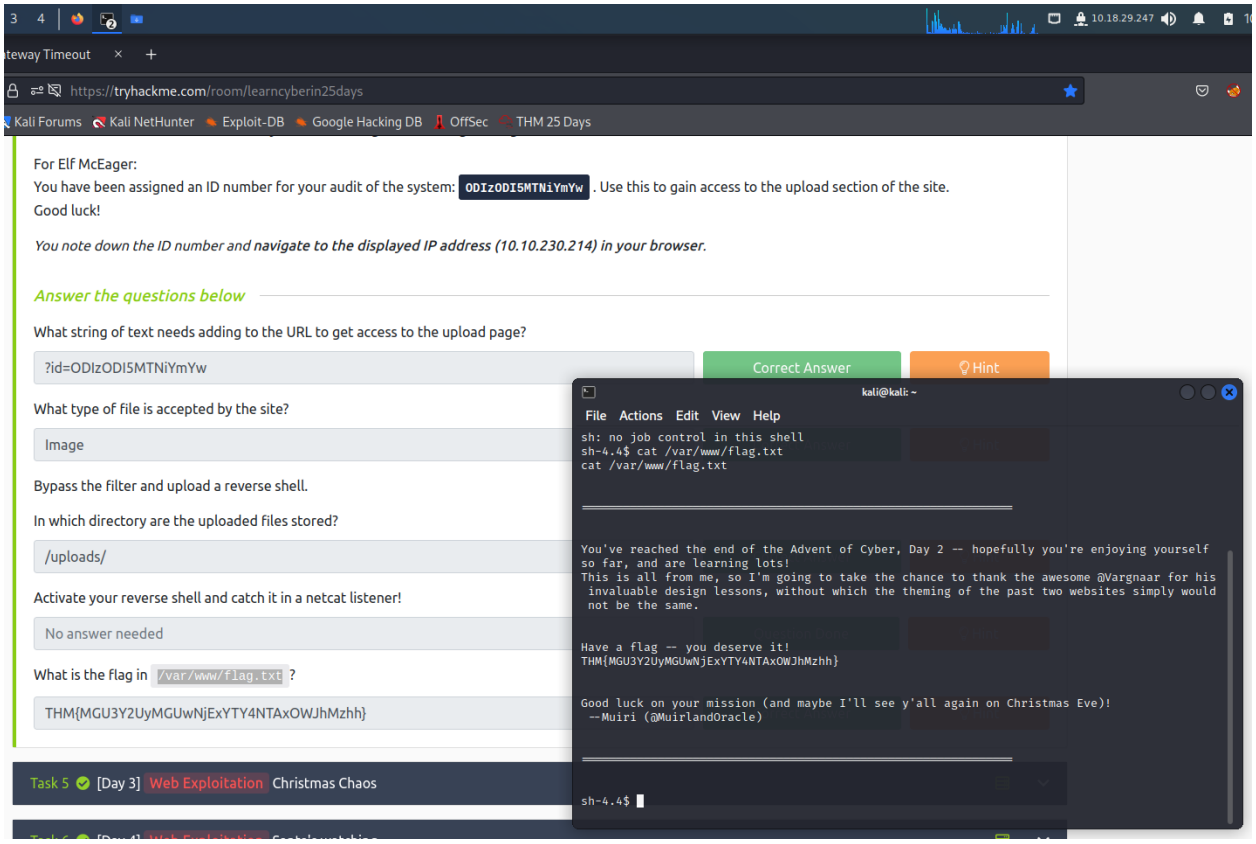


Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
nep.jpeg.php	2022-06-19 10:15	5.4K	

We can acquire the shell file in the statements. With this, we also have to change the IP and Port. From the statement we know that /uploads/ is one of the ways for us to indicate where our stored image is stored.

Question 4



After running the **sudo nc -lvnp 443** command in the terminal, we can go ahead and open the file in the /uploads/ address directory. By clicking the file while the terminal is listening, it will detect a request and will do its process. After that, we can put in the command **/var/www/flag.txt** and the terminal will process and reveal the flag.

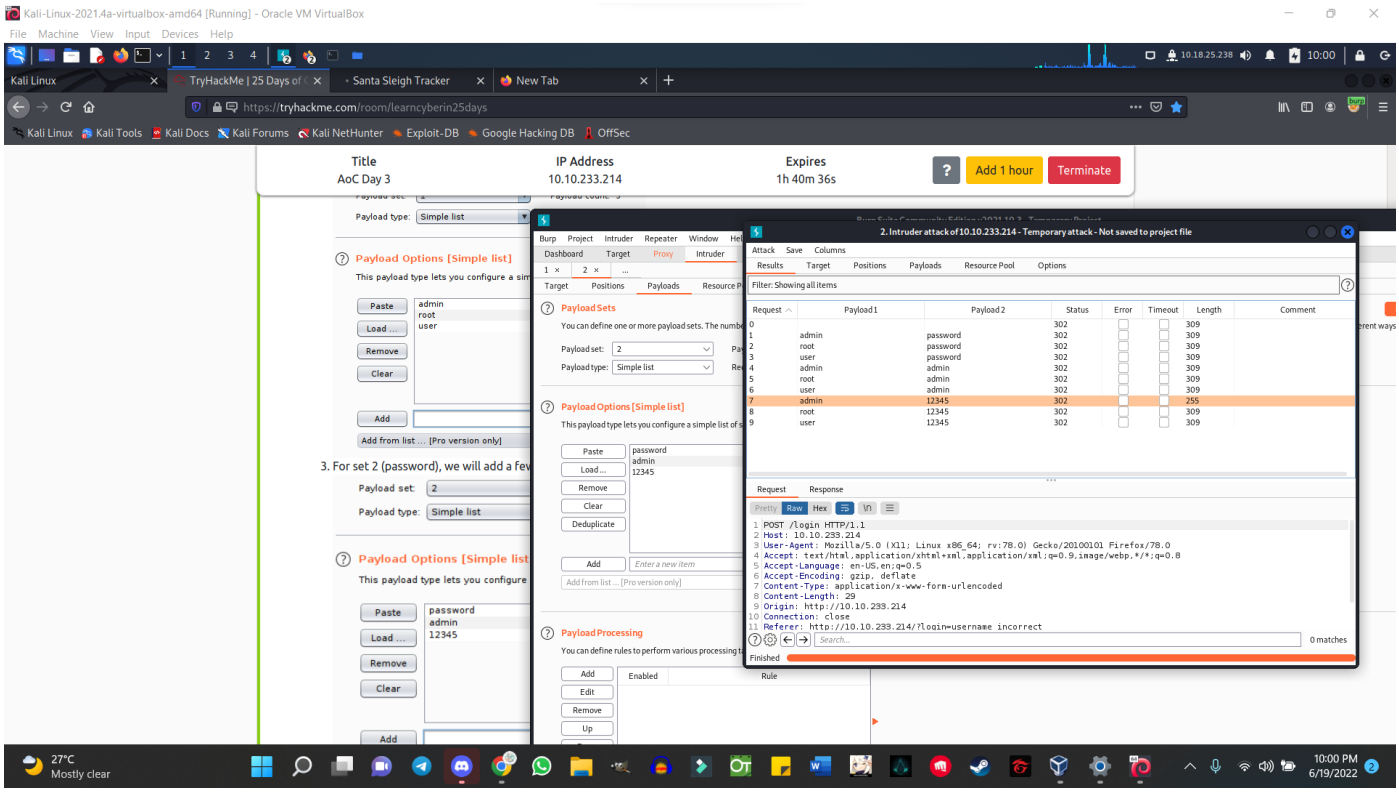
Thought Process / Methodology :

By using the ID given in the statement, we can use it to direct us into a new interactable page. By right clicking the page, we can inspect the page details which can show us the format that it requires. (in this case it was an image). Downloading the shell file given in the statement, we must also manipulate the IP and Port and then save it. This saved jpeg.php file will then be uploaded to the page. To identify where the file was stored in, we used the **/uploads/** subdirectory. This new upload page will enable us to open/check the image file that was uploaded. Opening a new terminal, we typed in the command **sudo nc -lvnp 443** to enable it to listen to our request when opening the image. After that we open the image and a request will be detected. In the same terminal we will then type in **cat /var/www/flag.txt.** This will then show us the flag we needed.

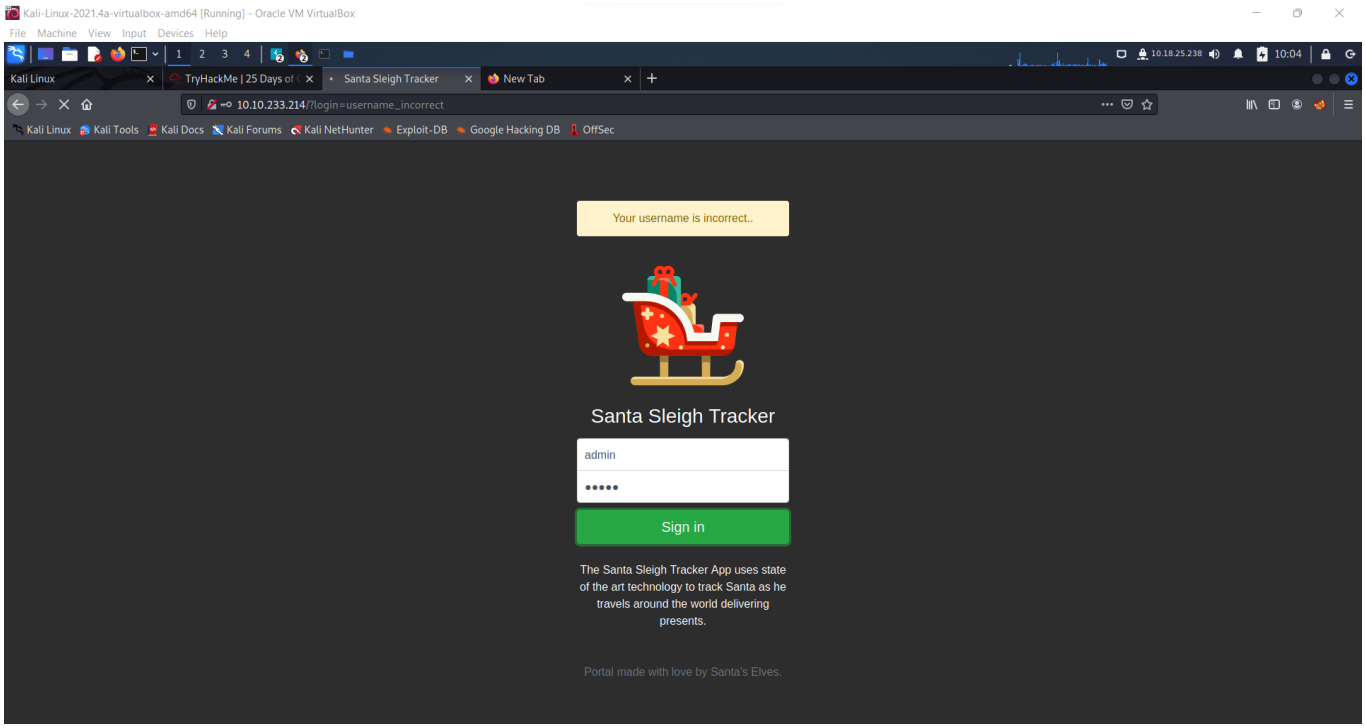
Day 3: Web Exploitation – Christmas Chaos

Tool Used : Kali Linux, Firefox, BurpSuite, FoxyProxy
Solution / Walkthrough :

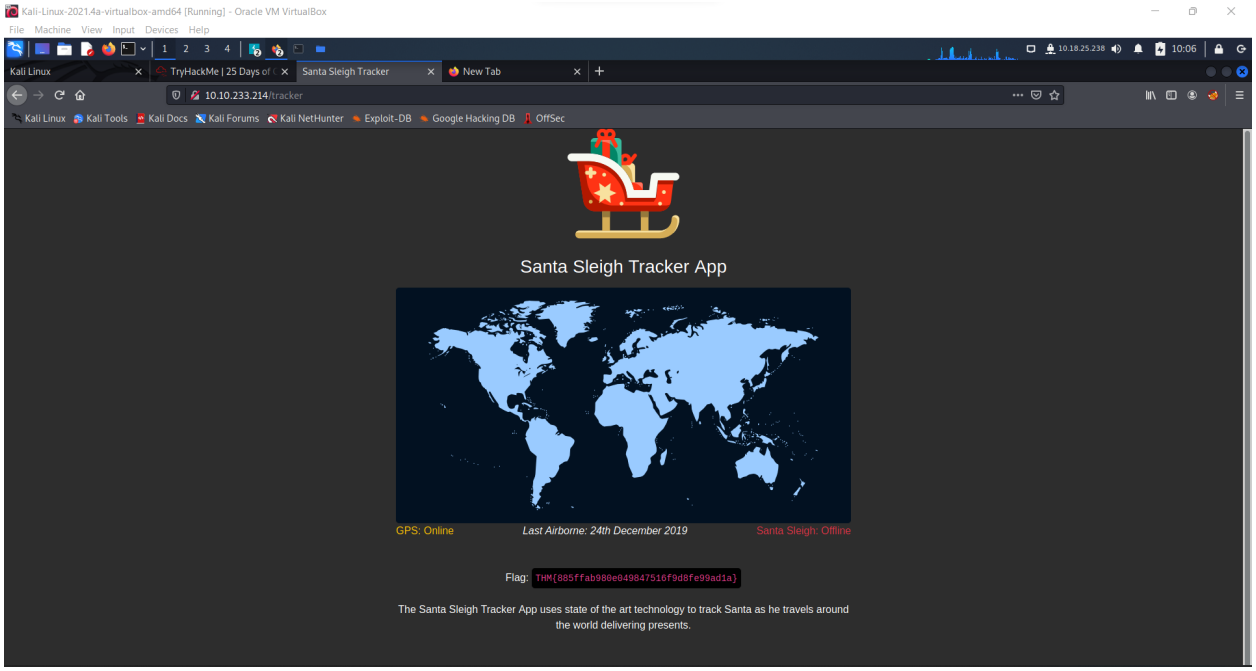
Question 1



After utilising Burpsuite as well as FoxyProxy, the system will detect the correct username and password which is in the different length column (in the orange highlight).



Enter the username and password from the highlight into boxes.



3. Flag *THM{885ffab980e049847516f9d8fe99ad1a}* is captured.

Thought Process / Methodology :

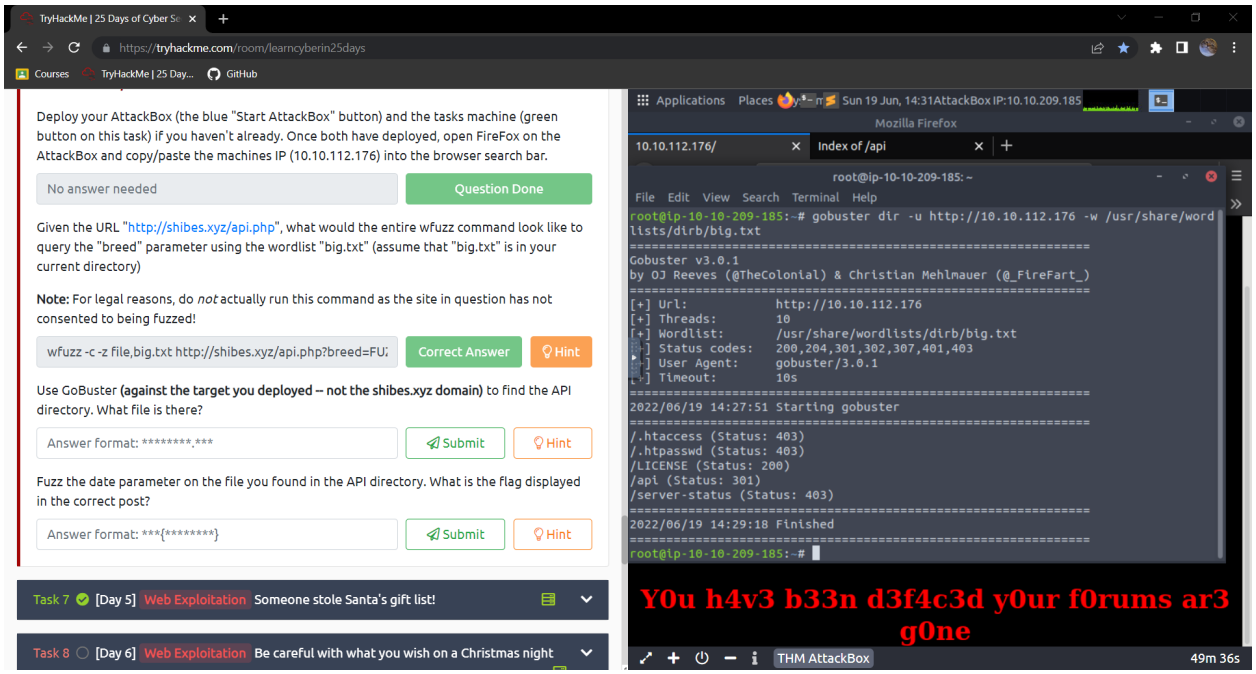
After connecting to OpenVPN , we copy the IP address from the Active Machine Information and open the Santa Sleigh Tracker. Open BurpSuite and make sure the intercept is on as well as turn on the FoxyProxy . Then, in the Santa Sleigh Tracker there are two boxes named “Username” and “Password”. We just type anything into these two boxes. After that, the BurpSuite will show the words we typed earlier in the section.Right click on the section then we click “Send to intruder”. Next, we go the Positions section and change “Sniper” to “Cluster Bomb”. We moved to the Payloads section then we add “admin” , “root” , “user” in the Payload set 1, then we add “password” , “admin” , “12345” in the Payload set 2. Hit start attack. We waited for a few seconds then found a line with a different length. It should be the right combination of username and password for the Santa Sleigh Tracker.We return to the Santa page then turn off FoxyProxy and change BurpSuite to intercept off . Put the username and password which are “admin” and “12345” respectively. We can enter the page then we found the flag *THM{885ffab980e049847516f9d8fe99ad1a}.*

Day 4: Web Exploitation - Santa's watching

Tool Used : Kali Linux, Firefox, Attackbox

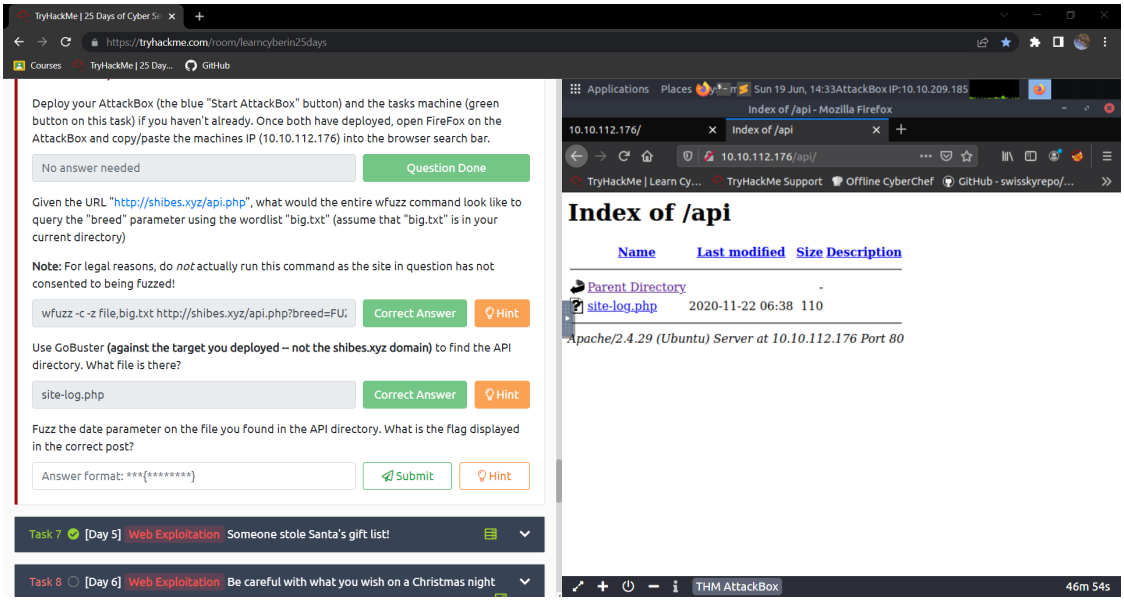
Solution / Walkthrough :

Question 1:



Question 2:

We use GoBuster command **gobuster dir -u ip -w /usr/share/worlists/dirb/big.txt** to find the API directory and then we get the file from there. The file name is **site-log.php**



Question 3:

We got the flag by using the command shown below. We changed **Fuzz** to **20201125** to get the flag.

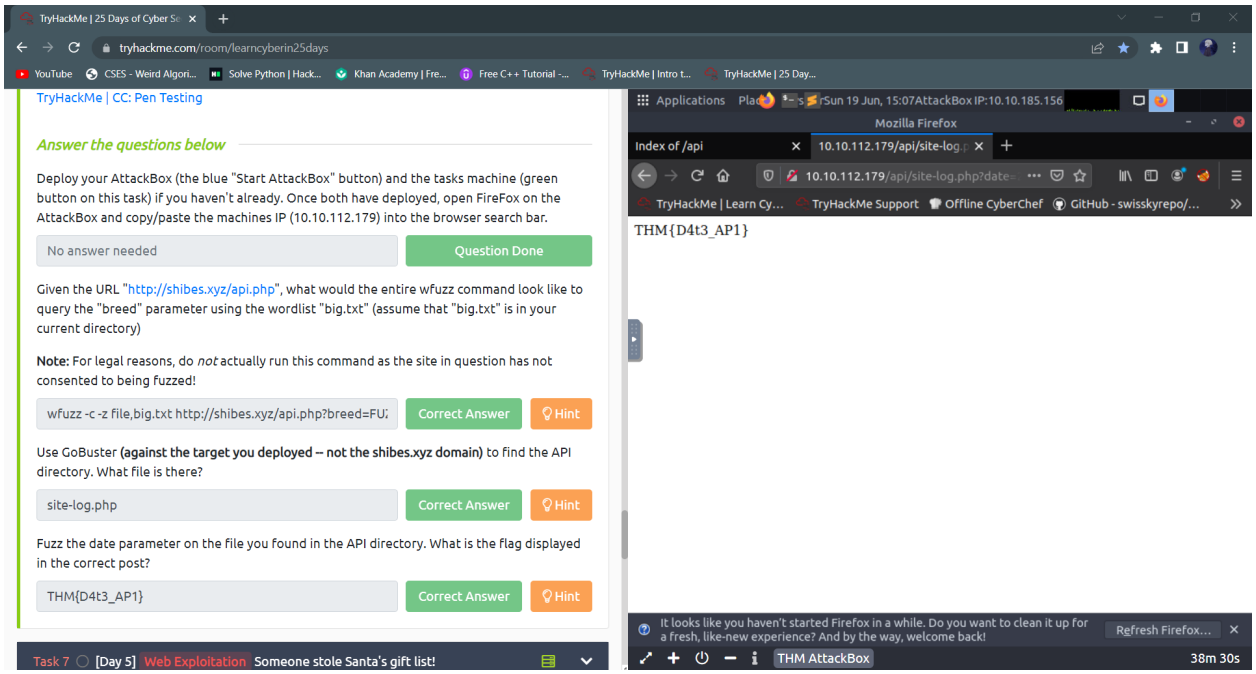
```
┌──(kali㉿kali)-[~]
└─$ wfuzz -c -z file,/home/kali/Downloads/wordlist -u http://10.10.203.172/api/site-log.php
?date=FUZZ
```

kali@kali: ~

File Actions Edit View Help

```
000000002:   200        0 L      0 W        0 Ch        "20201101"
000000004:   200        0 L      0 W        0 Ch        "20201103"
000000013:   200        0 L      0 W        0 Ch        "20201112"
000000015:   200        0 L      0 W        0 Ch        "20201114"
000000019:   200        0 L      0 W        0 Ch        "20201118"
000000042:   200        0 L      0 W        0 Ch        "20201211"
000000040:   200        0 L      0 W        0 Ch        "20201209"
000000027:   200        0 L      0 W        0 Ch        "20201126"
000000041:   200        0 L      0 W        0 Ch        "20201210"
000000039:   200        0 L      0 W        0 Ch        "20201208"
000000036:   200        0 L      0 W        0 Ch        "20201205"
000000035:   200        0 L      0 W        0 Ch        "20201204"
000000038:   200        0 L      0 W        0 Ch        "20201207"
000000037:   200        0 L      0 W        0 Ch        "20201206"
000000030:   200        0 L      0 W        0 Ch        "20201129"
000000029:   200        0 L      0 W        0 Ch        "20201128"
000000034:   200        0 L      0 W        0 Ch        "20201203"
000000033:   200        0 L      0 W        0 Ch        "20201202"
000000032:   200        0 L      0 W        0 Ch        "20201201"
000000031:   200        0 L      0 W        0 Ch        "20201130"
000000028:   200        0 L      0 W        0 Ch        "20201127"
000000025:   200        0 L      0 W        0 Ch        "20201124"
000000024:   200        0 L      0 W        0 Ch        "20201123"
000000026:   200        0 L      1 W       13 Ch        "20201125"
000000023:   200        0 L      0 W        0 Ch        "20201122"
000000022:   200        0 L      0 W        0 Ch        "20201121"
000000020:   200        0 L      0 W        0 Ch        "20201119"
000000017:   200        0 L      0 W        0 Ch        "20201116"
000000021:   200        0 L      0 W        0 Ch        "20201120"
000000018:   200        0 L      0 W        0 Ch        "20201117"
000000016:   200        0 L      0 W        0 Ch        "20201115"
000000043:   200        0 L      0 W        0 Ch        "20201212"
000000014:   200        0 L      0 W        0 Ch        "20201113"
000000045:   200        0 L      0 W        0 Ch        "20201214"
000000058:   200        0 L      0 W        0 Ch        "20201227"
000000055:   200        0 L      0 W        0 Ch        "20201224"
000000049:   200        0 L      0 W        0 Ch        "20201218"
000000057:   200        0 L      0 W        0 Ch        "20201226"
000000059:   200        0 L      0 W        0 Ch        "20201228"
000000056:   200        0 L      0 W        0 Ch        "20201225"
000000051:   200        0 L      0 W        0 Ch        "20201220"
000000054:   200        0 L      0 W        0 Ch        "20201223"
000000053:   200        0 L      0 W        0 Ch        "20201222"
000000052:   200        0 L      0 W        0 Ch        "20201221"
000000050:   200        0 L      0 W        0 Ch        "20201219"
000000047:   200        0 L      0 W        0 Ch        "20201216"
000000060:   200        0 L      0 W        0 Ch        "20201229"
000000048:   200        0 L      0 W        0 Ch        "20201217"
000000044:   200        0 L      0 W        0 Ch        "20201213"
000000046:   200        0 L      0 W        0 Ch        "20201215"
000000061:   200        0 L      0 W        0 Ch        "20201230"
000000063:   200        0 L      0 W        0 Ch        "http://10.10.203.172/api/
                                                        site-log.php?date="
000000062:   200        0 L      0 W        0 Ch        "20201231"

Total time: 0
```



Thought Process / Methodology :

We used the example to get the command for the first question. For question 2, we used gobuster to get the API directory and visited the website API to get the file inside of the API. Lastly, we used the command shown in the picture above to get the date and changed FUZZ to the correct date which is 20201125.

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

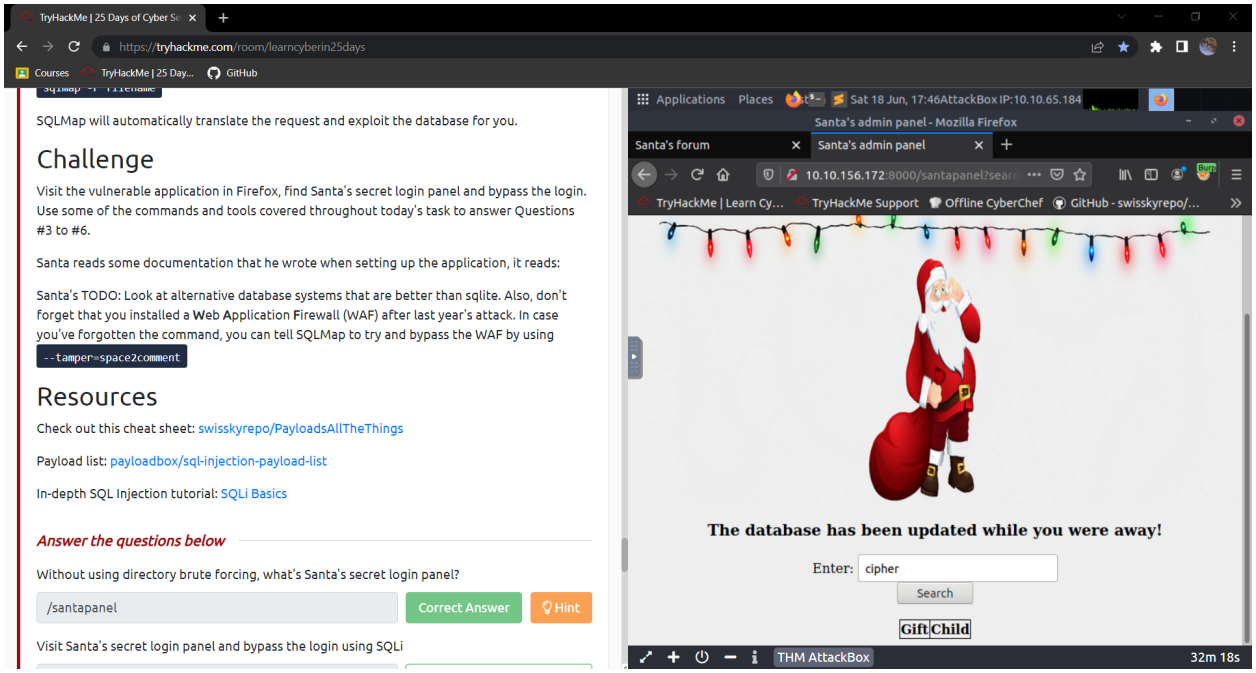
Tool Used : Attackbox, Firefox, BurpSuite
Solution / Walkthrough :

Question 1:

We just guessed the secret panel by using the hint given

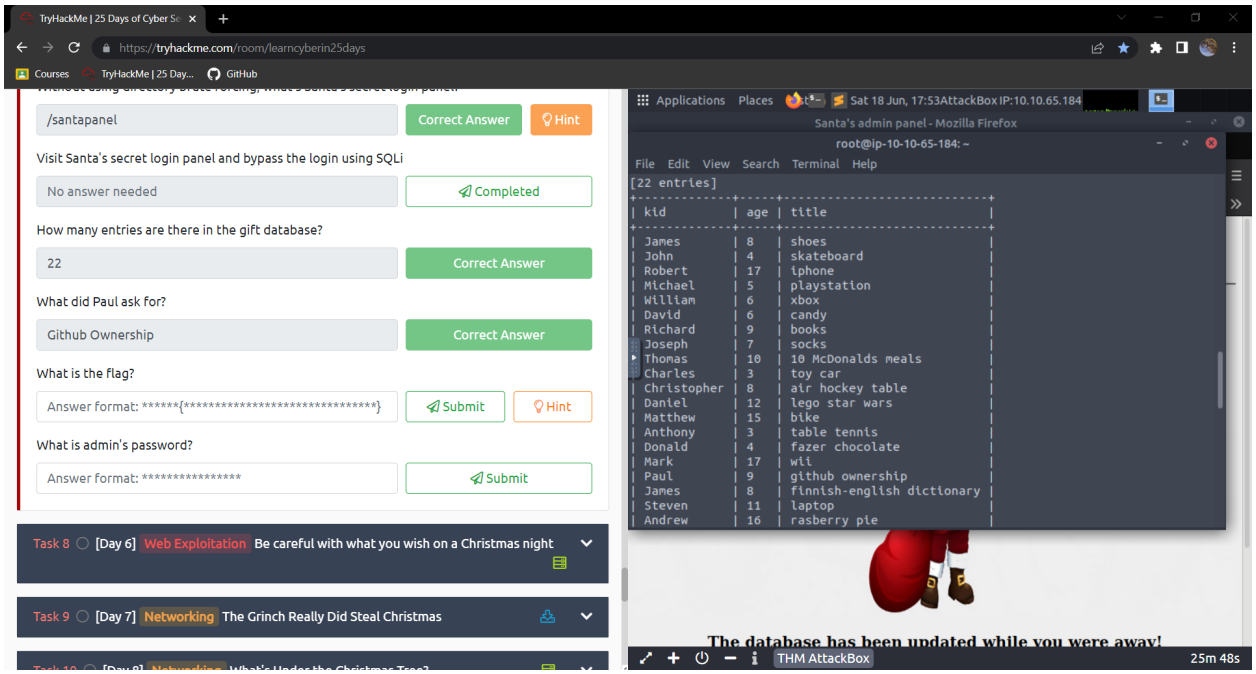
Question 2:

We just bypass the login by using admin' or true -- as the username.



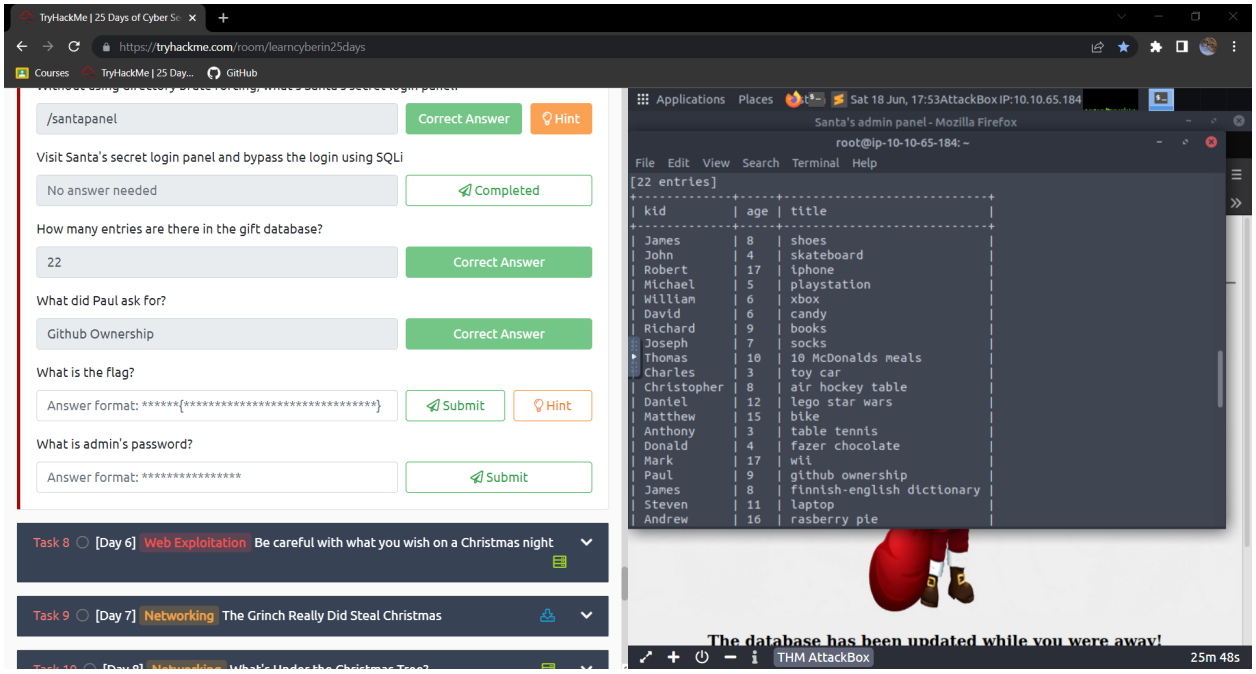
Question 3:

We saved the panel request on burp and use command **sqlmap -r file --tamper=space2comment --dump-all --dbms sqlite** to get all the information.



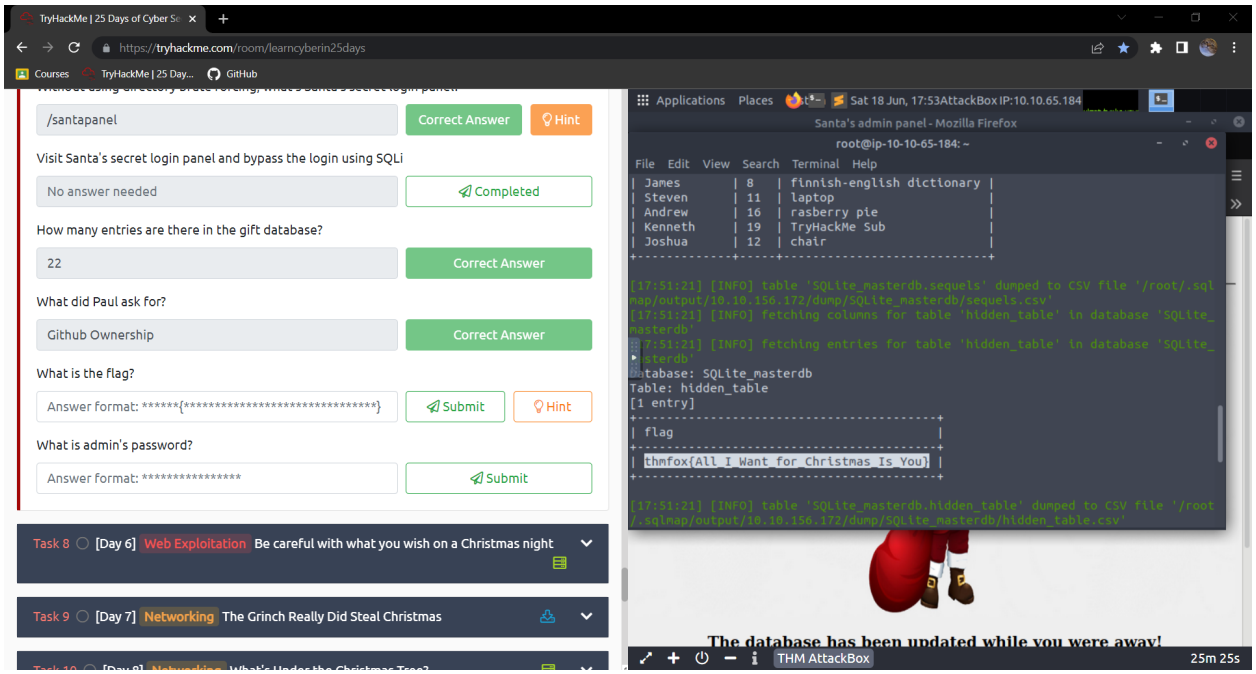
Question 4:

We used the same command.



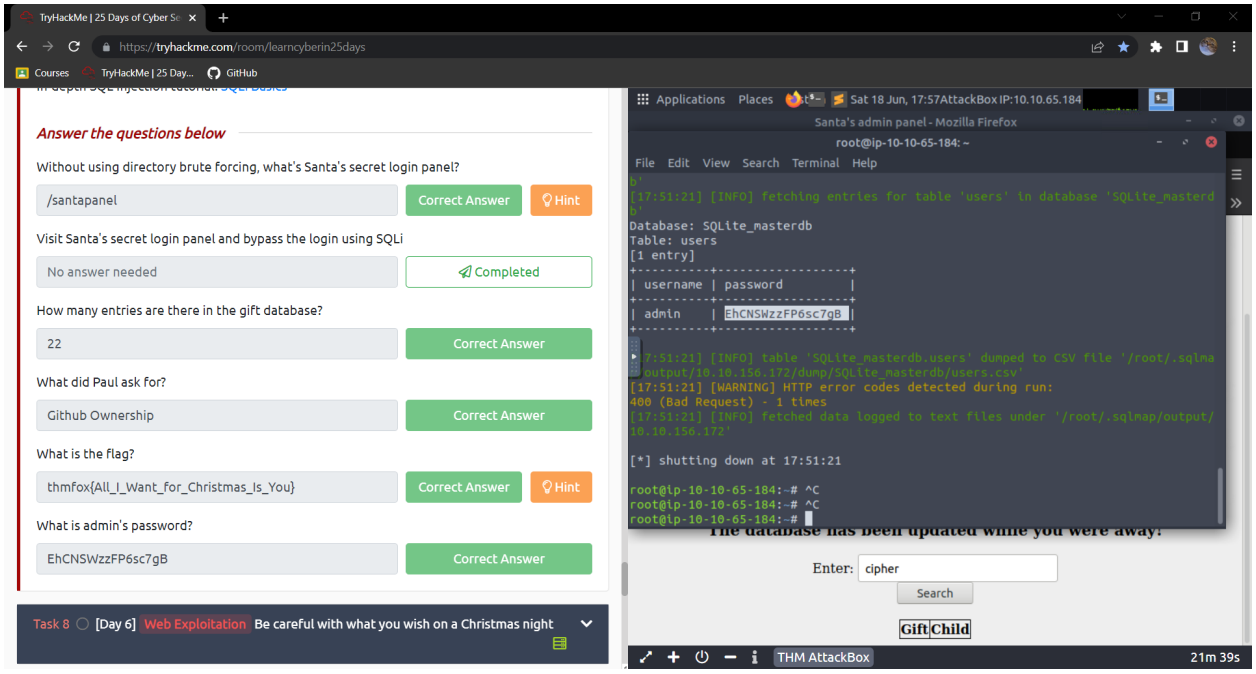
Question 5:

We got the flag from the same command.



Question 6:

We got the password from the same command.



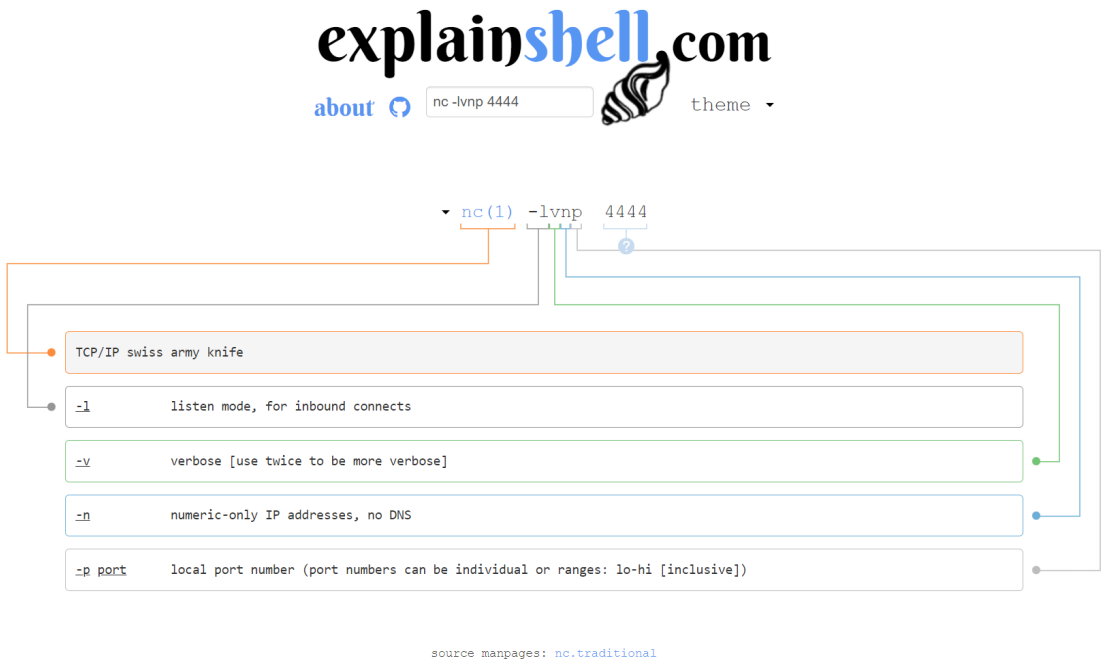
Thought Process / Methodology :

We were shown the Santa's forum. After getting the santa's secret panel directory, we visited the secret panel and bypassed the login by using admin' or true -- as the username. After that we saved the panel request on burpsuite and use the command **sqlmap -r file --tamper=space2comment --dump-all --dbms sqlite** to get all the necessary information.

Extra Questions :

Day 2:

Question 4



Day 3:

Question 1

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 **I**nternet **o**f **T**hings (**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.

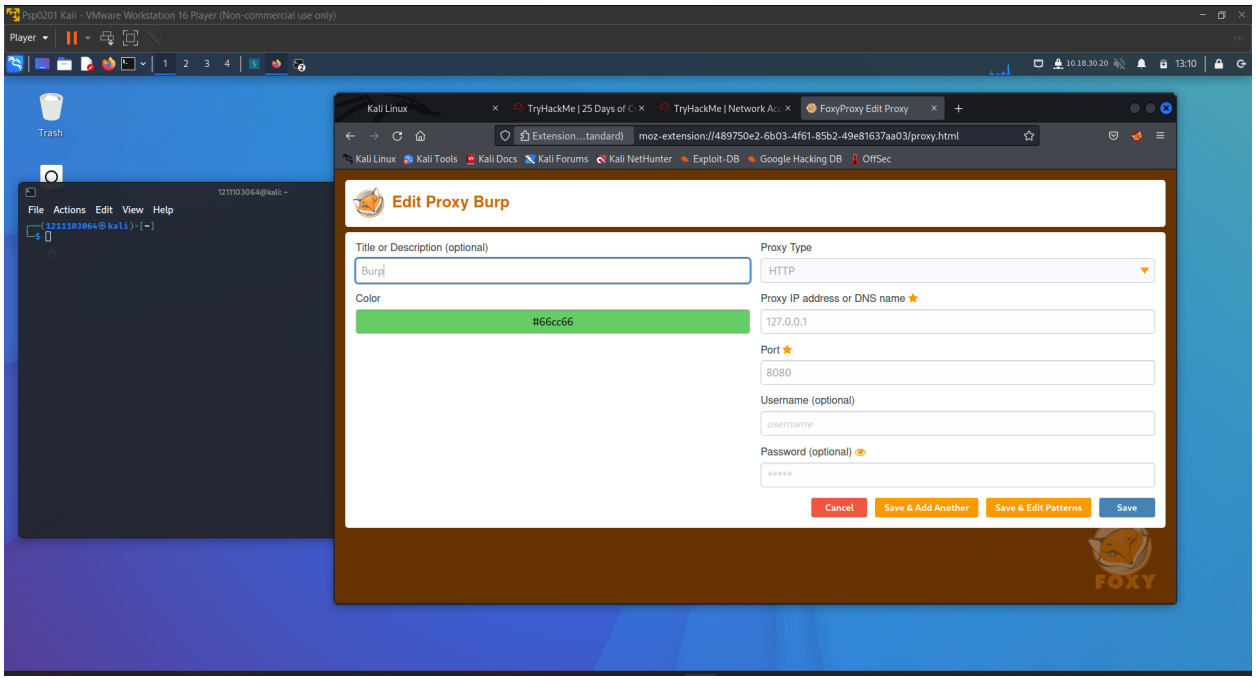
Question 2

Bounty $250

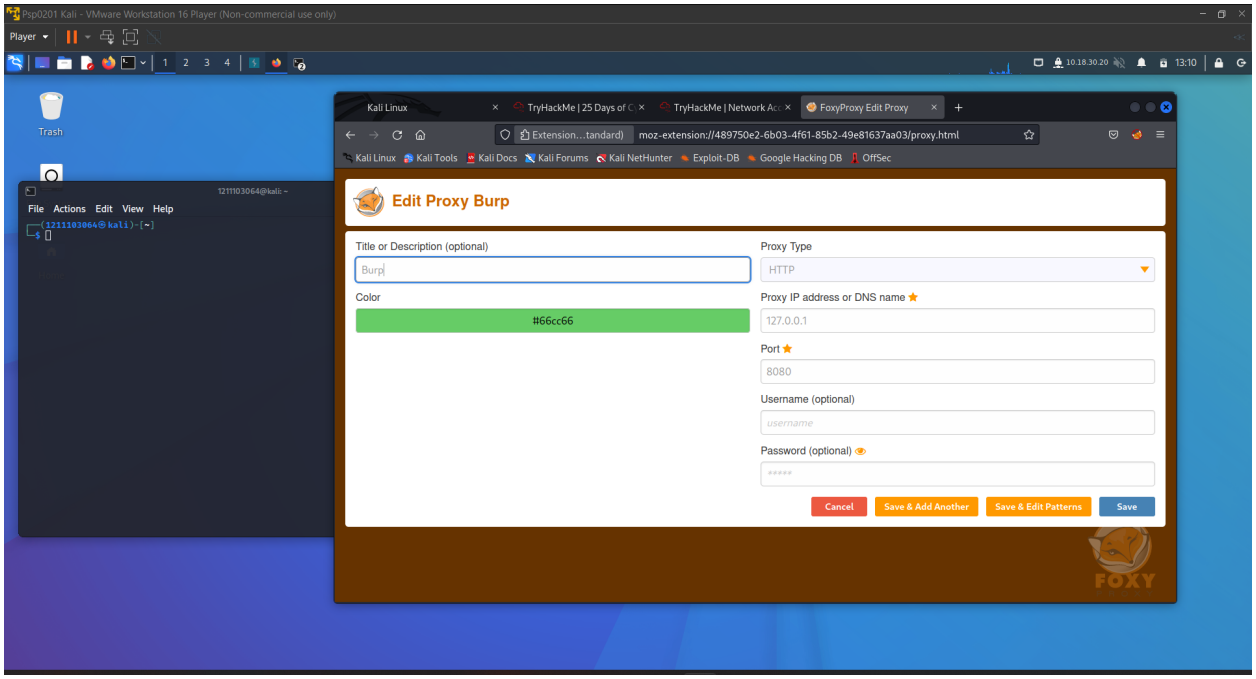
Question 3

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

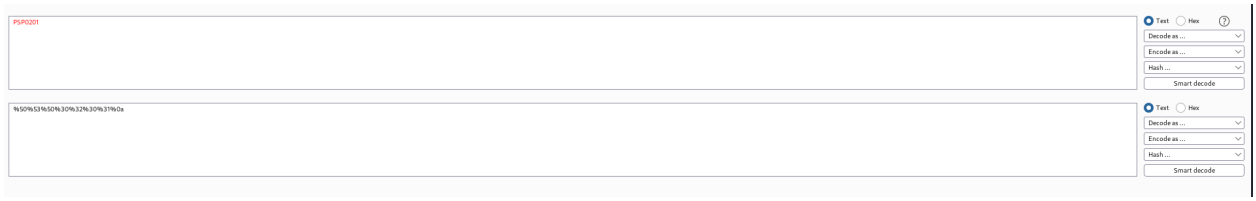
Question 4



Question 5

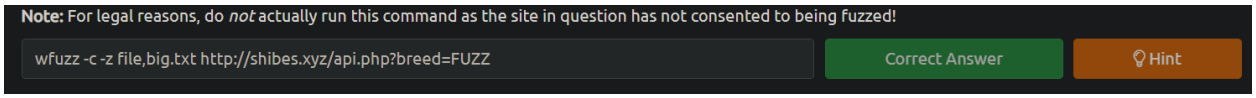


Question 6



Day 4:

Question 1

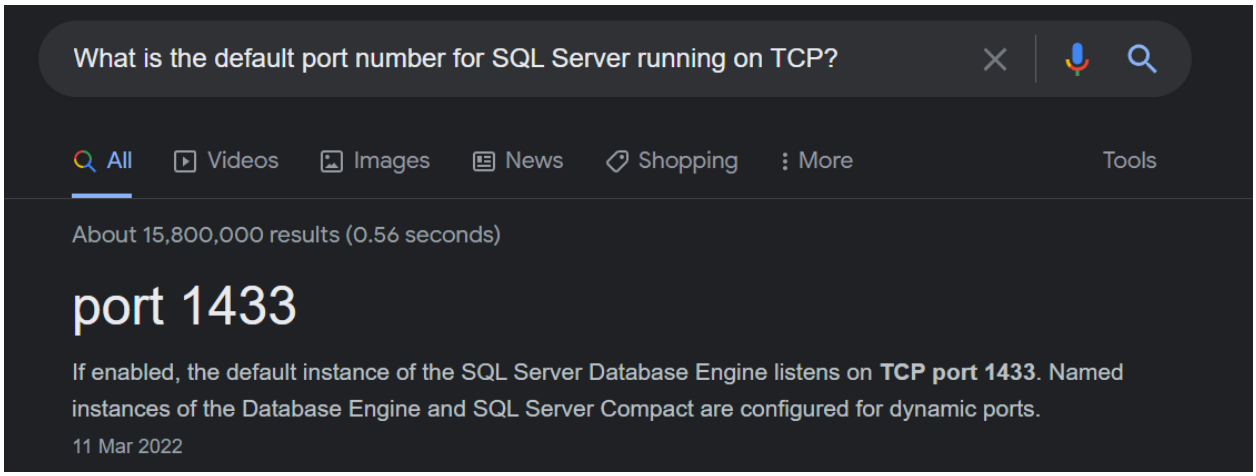


Question 4

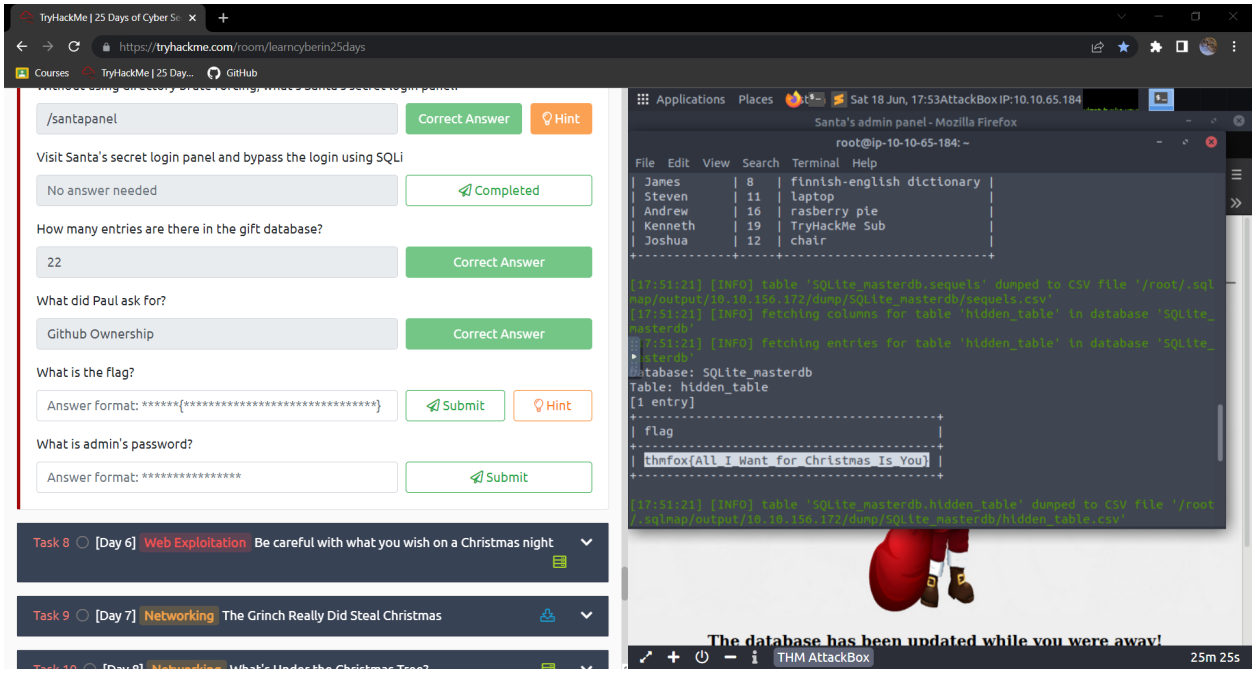
```
-f filename,printer      : Store results in the output file using the specifie
```

Day 5:

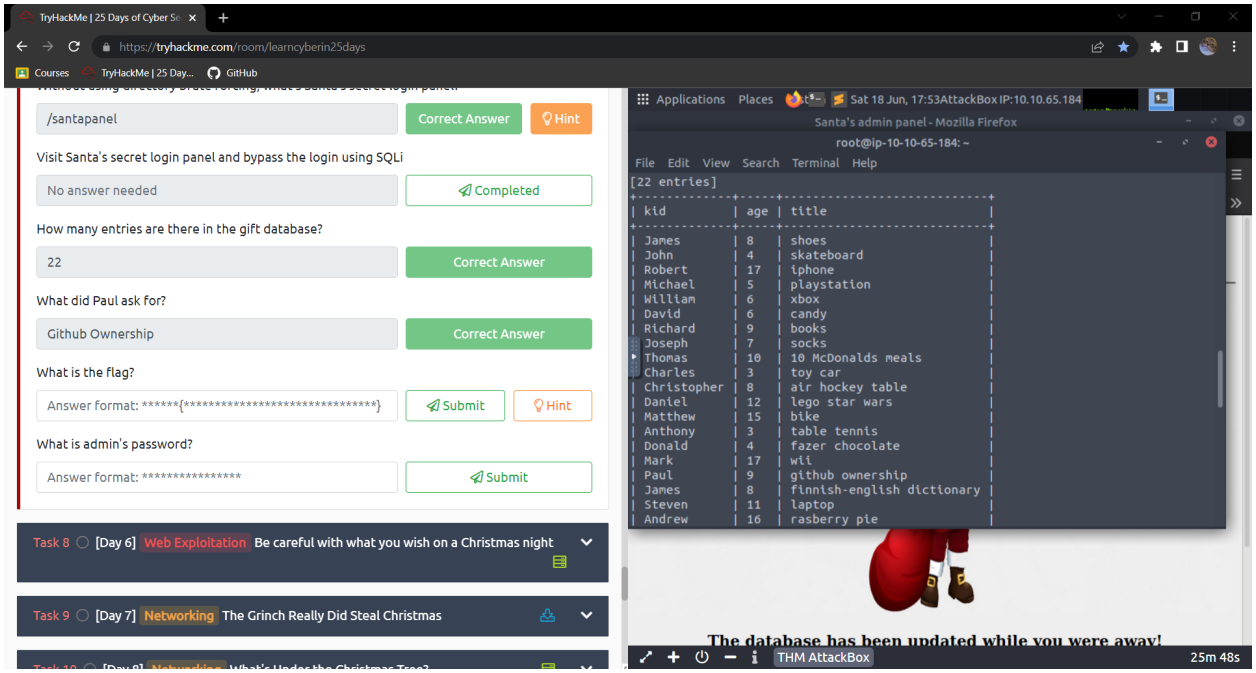
Question 1



Question 3



Question 5


TryHackMe | 25 Days of Cyber Se
https://tryhackme.com/room/learncyberin25days
Courses
TryHackMe | 25 Day...
GitHub
/santapanel
Correct Answer
Hint
Visit Santa's secret login panel and bypass the login using SQLi
No answer needed
Completed
How many entries are there in the gift database?
22
Correct Answer
What did Paul ask for?
Github Ownership
Correct Answer
What is the flag?
Answer format: ******{**********}
Submit
Hint
What is admin's password?
Answer format: **********
Submit
Task 8 [Day 6] Web Exploitation Be careful with what you wish on a Christmas night
Task 9 [Day 7] Networking The Grinch Really Did Steal Christmas
Applications
Places
Sat 18 Jun, 17:53
AttackBox IP:10.10.65.184
Santa's admin panel - Mozilla Firefox
root@ip-10-10-65-184: ~
File Edit View Search Terminal Help
[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	rasberry pie
The database has been updated while you were away!
THM AttackBox
25m 48s