PSP0201 Week 2 Writeup

GROUP NAME:GLHF

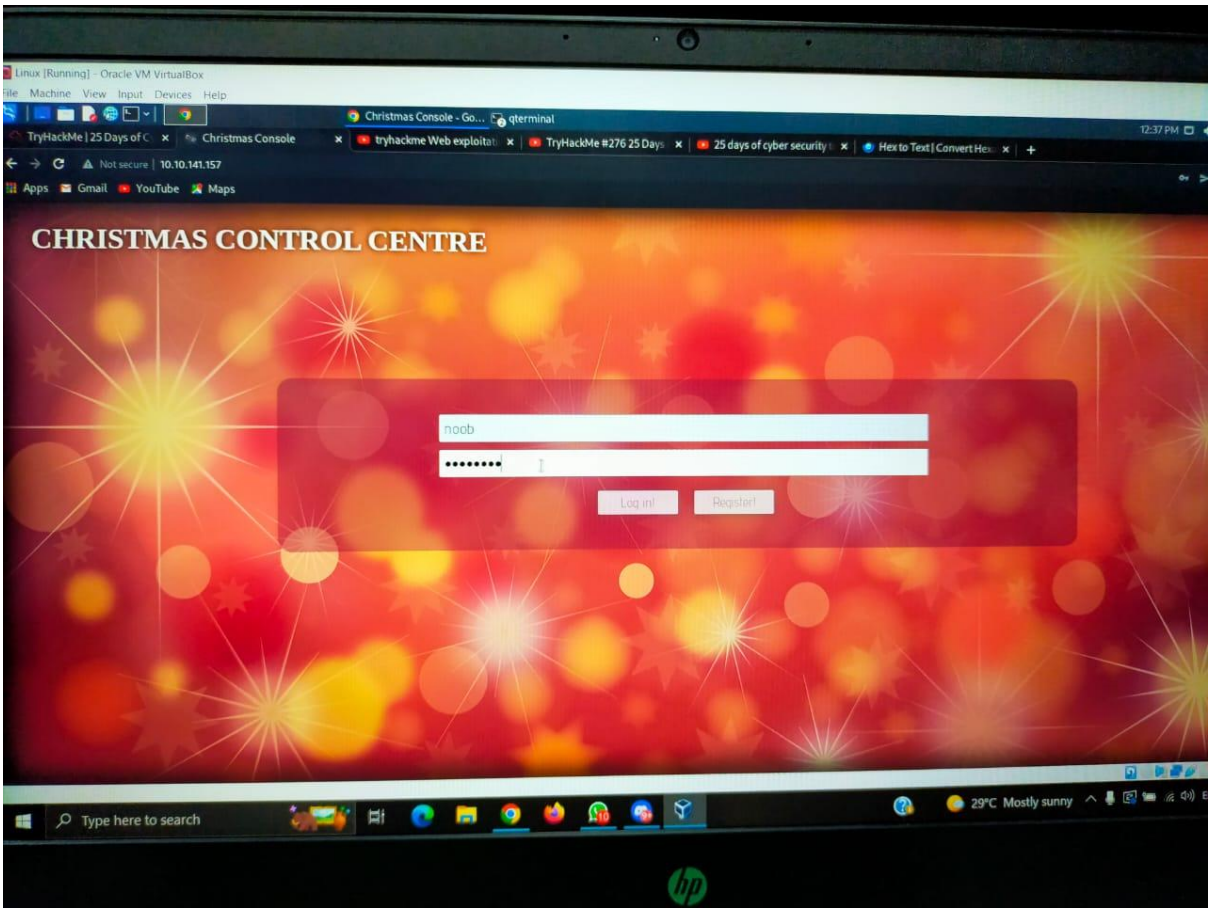
ID	NAME	ROLE
1211103400	Rohit	Leader
1211103299	Shuuban	Member
1211101214	Muhammad Syafiq Bin Ahmad Ghazali	Member

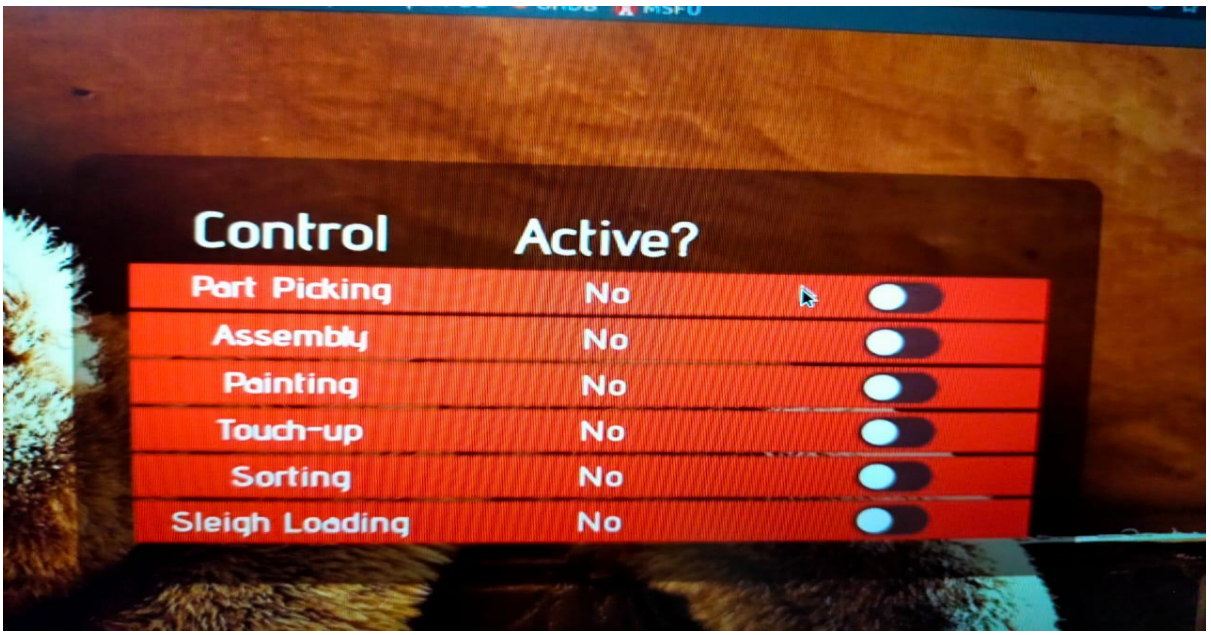
Day 1: Web Exploitation – A Christmas Crisis

Tools used: Kali Linux, Chrome / Attackbox

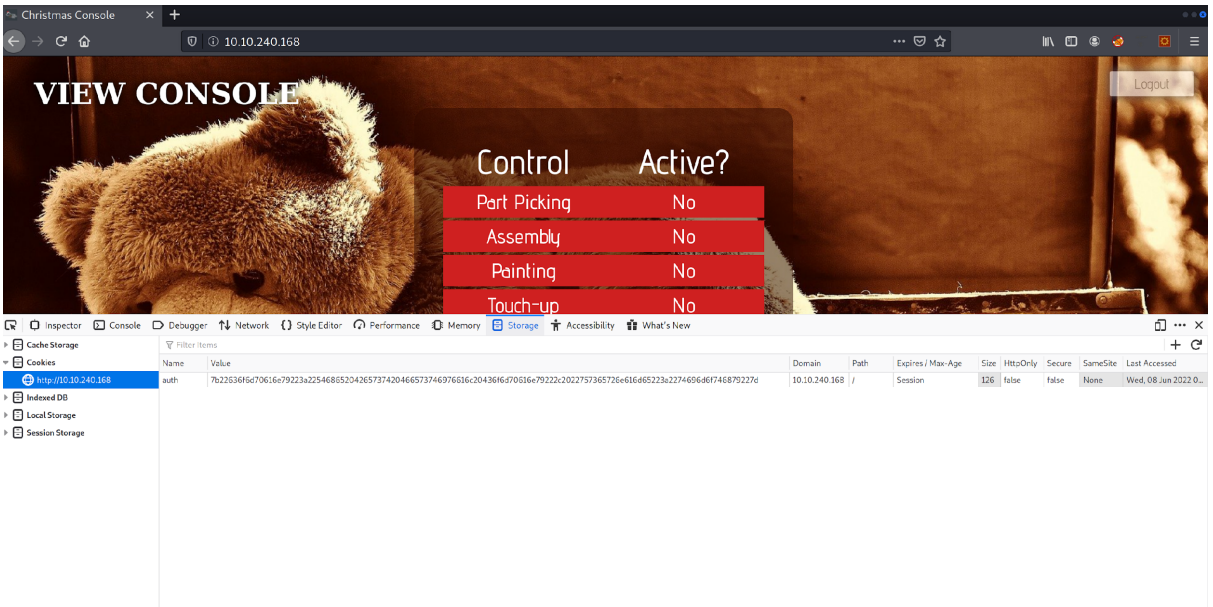
Question 1

Register and login page.No access





Inspect Element/Applications/Cookie to get the cookies



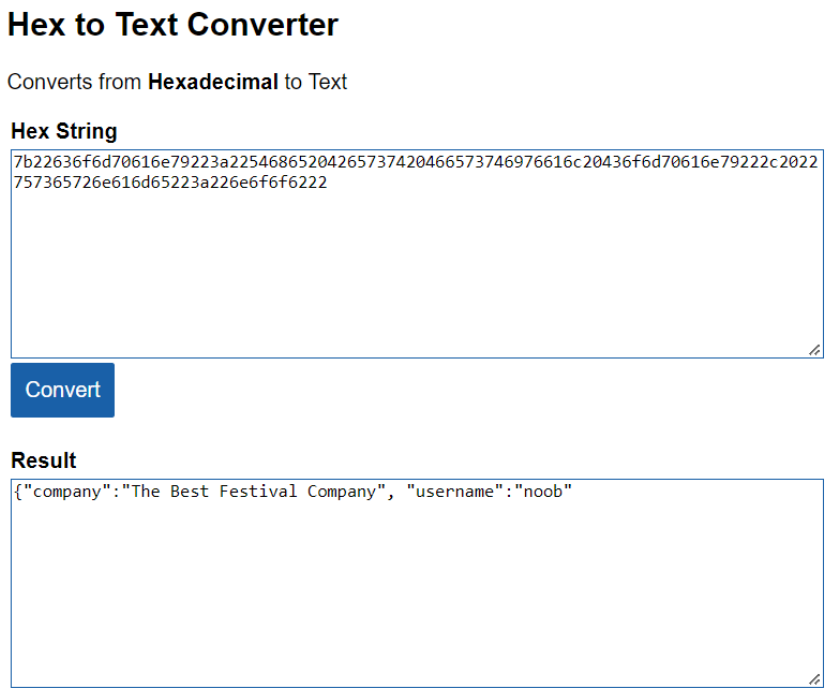
Question 2

Obtaining the cookies

Value
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2274696d6f746879227d

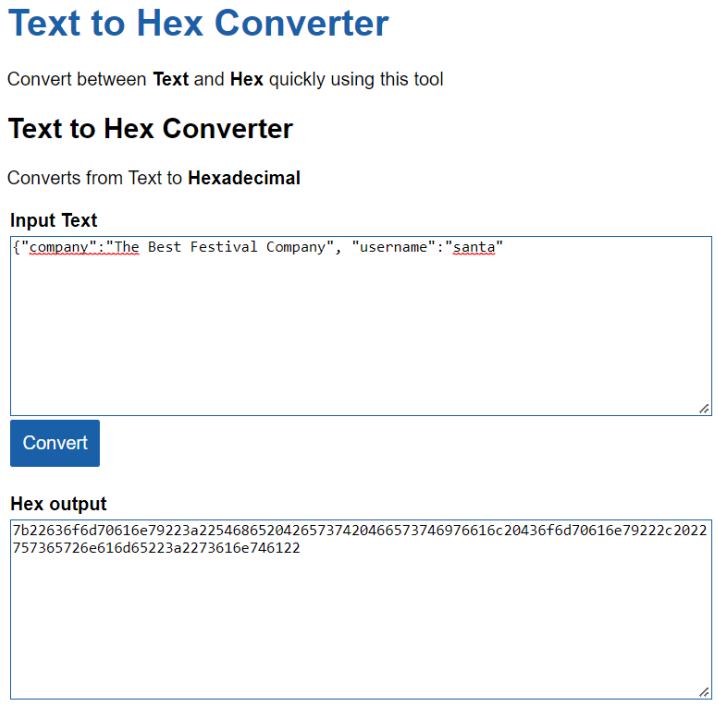
Question 3

Used a random hex converter to convert hex to text.(note: I was unable to open cyberchef.)



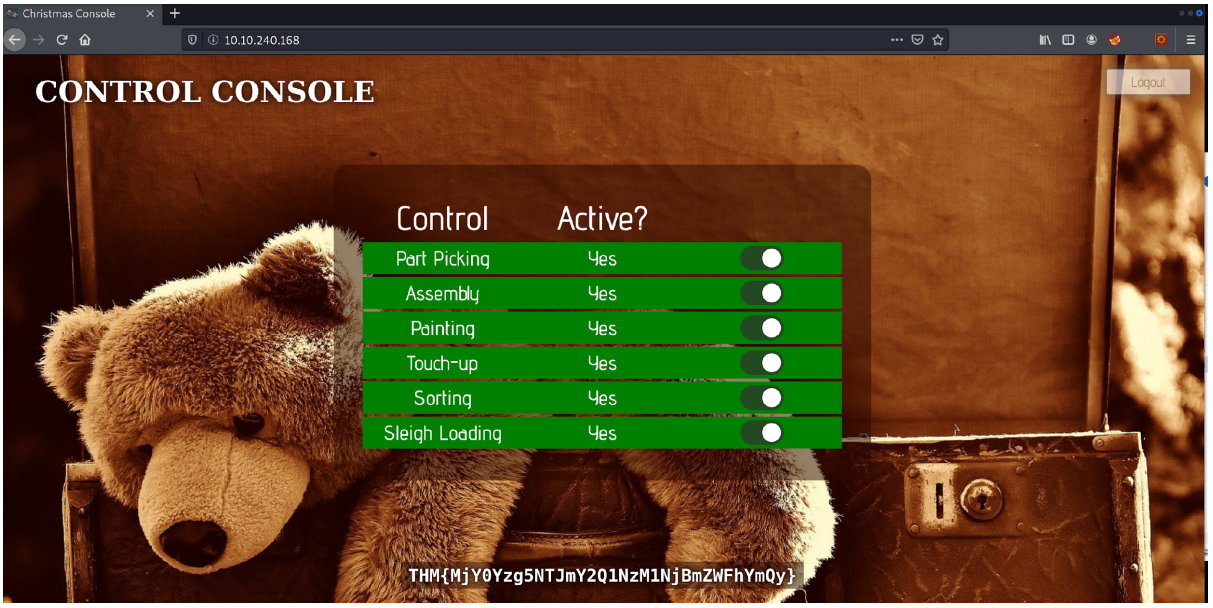
Question 4

Changed the username to ‘santa’ to obtain the cookies.



Question 5

Access available and controls can be used



Thoughts:

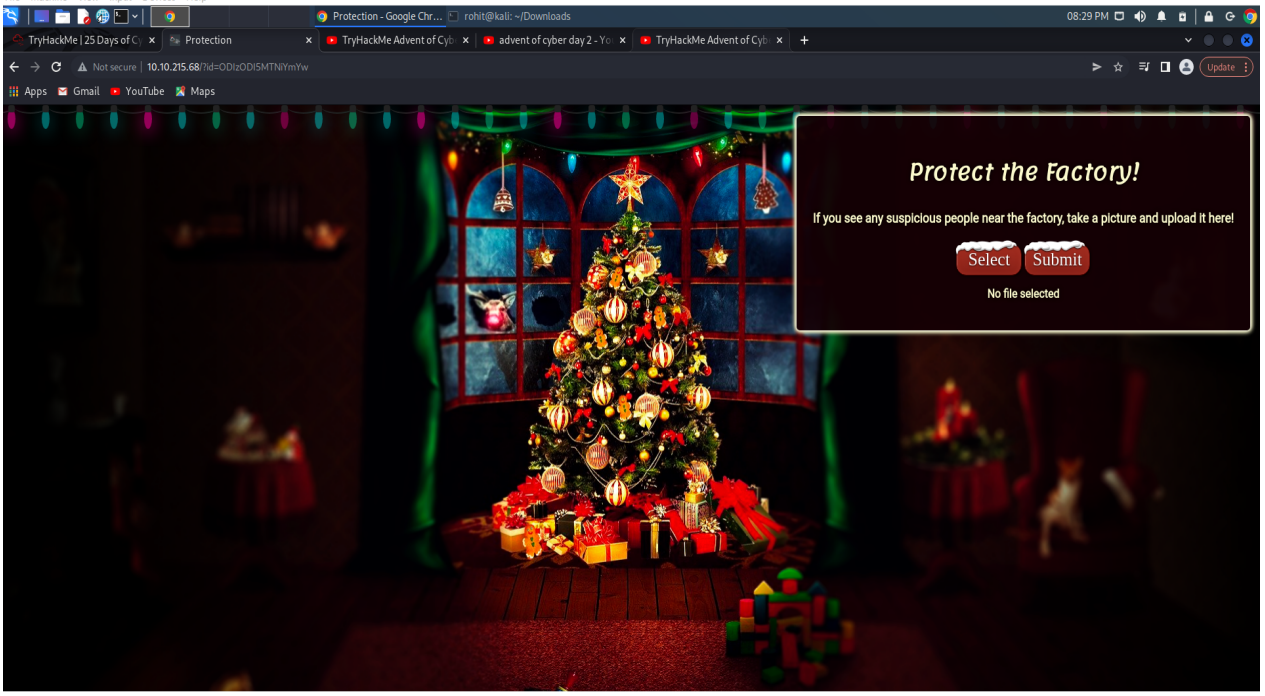
Once the machine is accessed,We saw a login page and we registered an account.After that we accessed the developer tools by clicking on the inspect element and then applications and the cookies tab.then we took the cookie value and converted it to a json text and changed the json text's username to 'santa' and converted it back to hex.once we pasted the new cookie value we managed to gain access to the admin page.

DAY 2 - The elf stikes back

Tools used: Linux

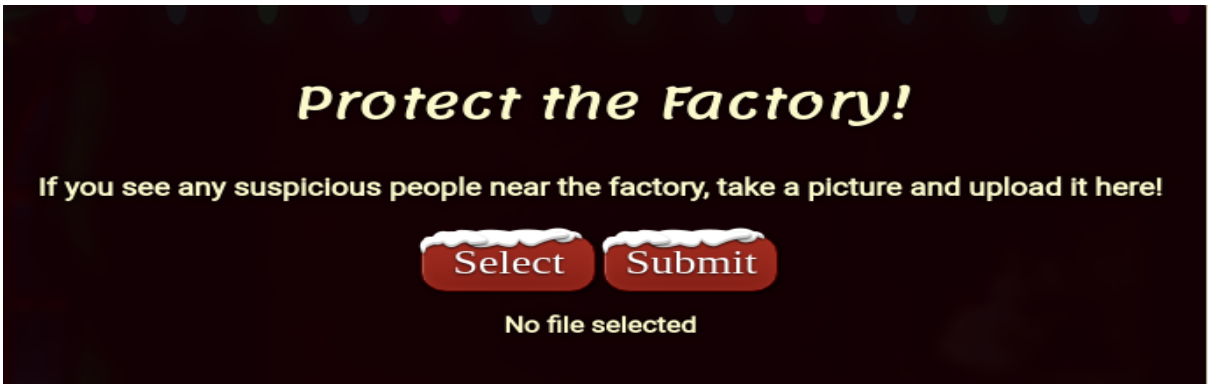
Question 1

Getting to the id page using the id given

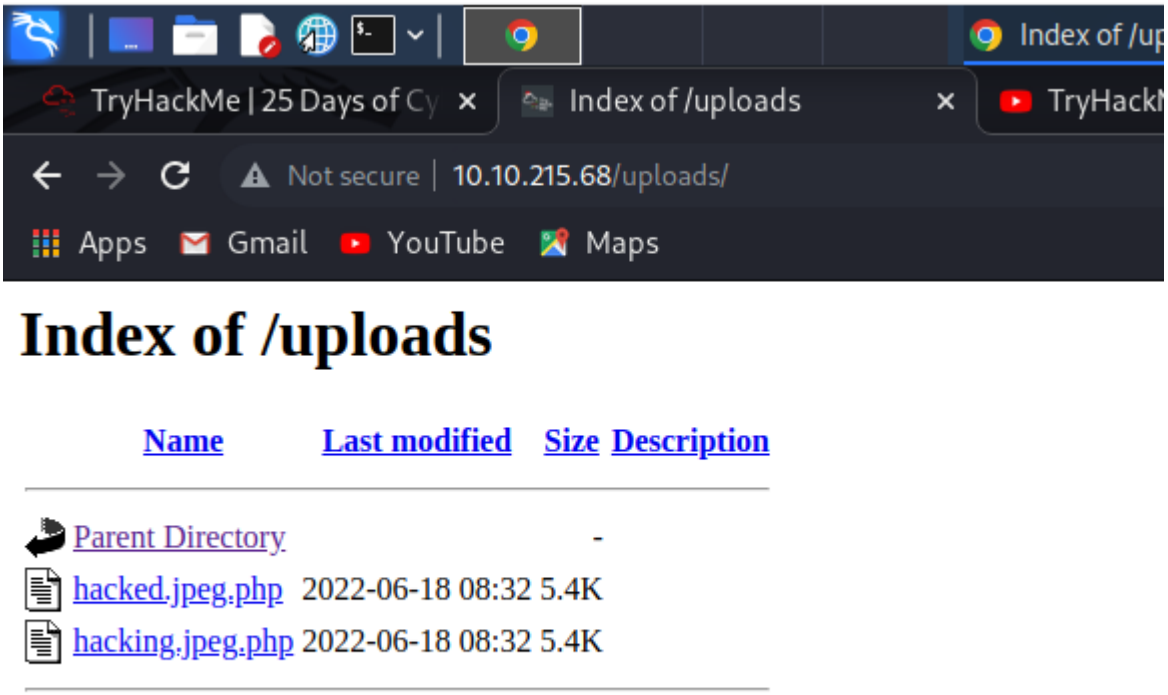


Question 2

It only accepts an image as stated

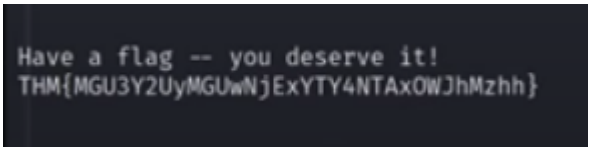


Question 3



Question 5

Getting the flag



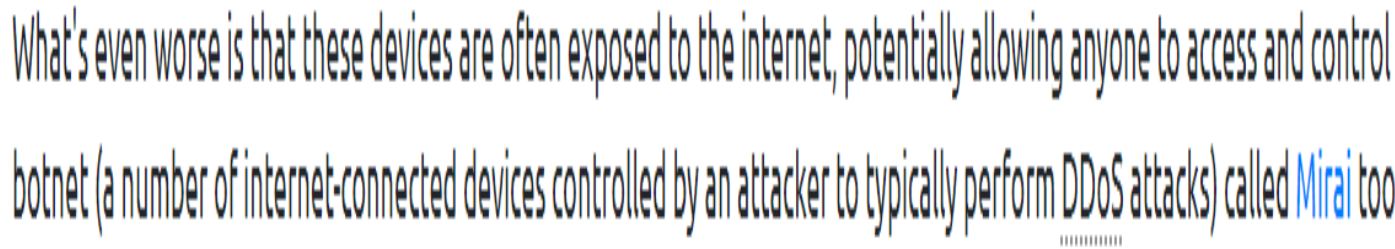
Thoughts:

We went to the machine, entered the given id on the taskbar, and used php to alter the script by changing the ip and port number to reverse shell and then changed the php file to a jpg file and uploaded it to the upload page and we managed to crack it down.

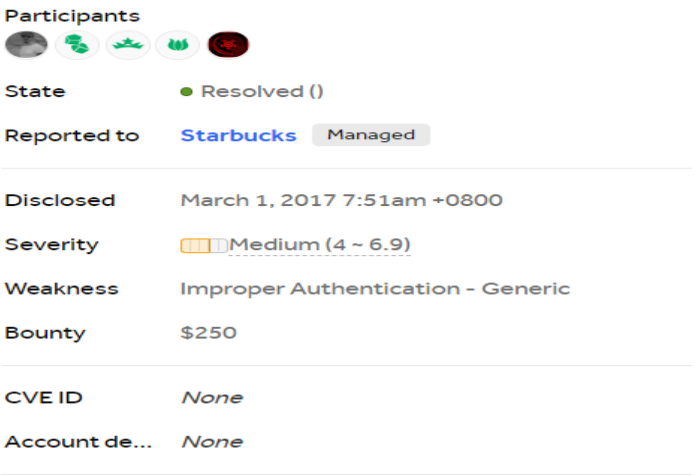
Day 3 Christmas Chaos

Tools used: Linux

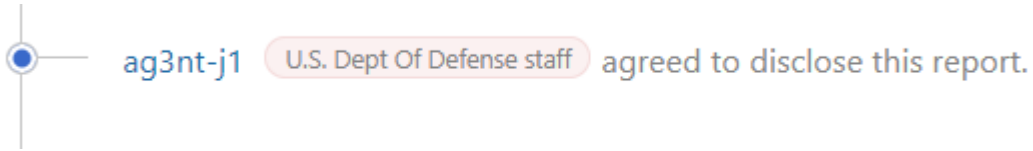
Question 1



Question 2



Question 3



Question 4

Proxy is 8080

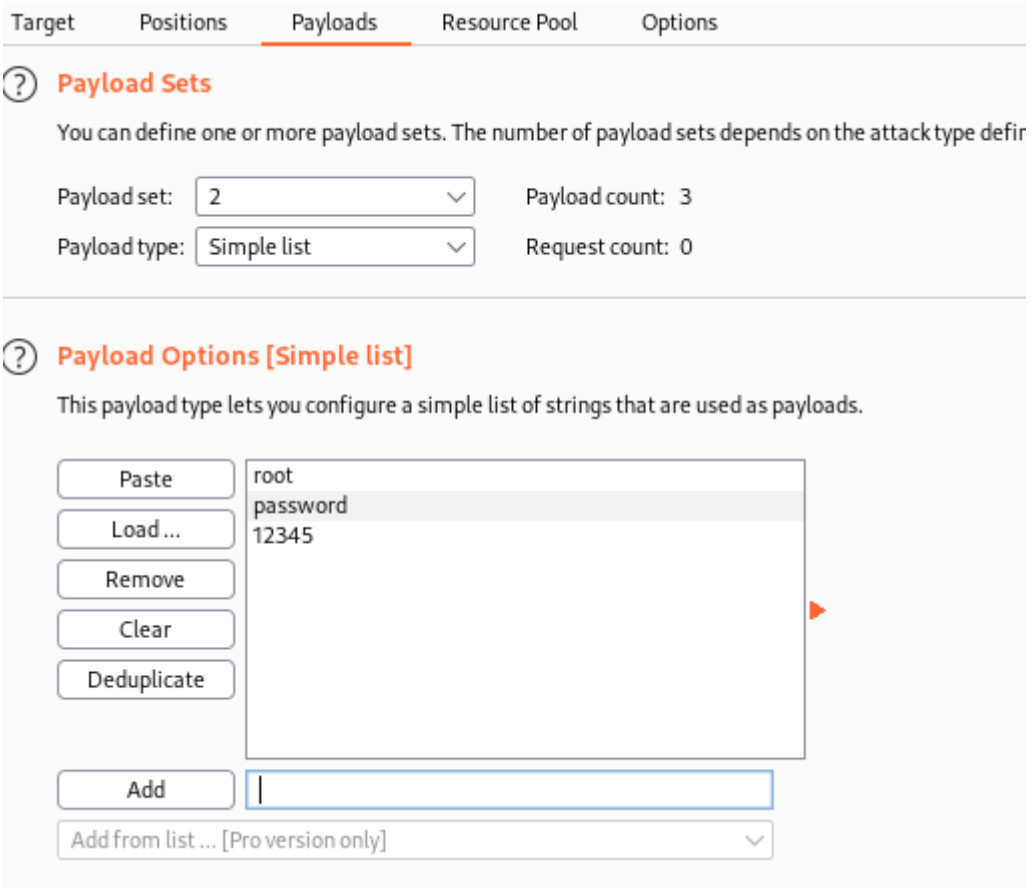
Info	Suite	This version of Burp Suite was released over three months ago. Please consider updating to benefit from enhance...
Info	Proxy	Proxy service started on 127.0.0.1:8080

Question 6

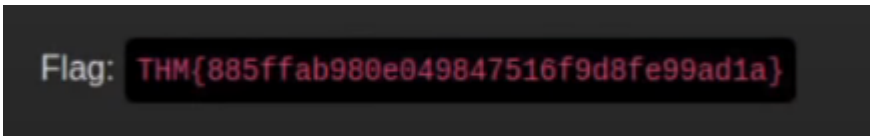
Using decoder in burpsuite

Question 7

Cluster Bomb



Question 8



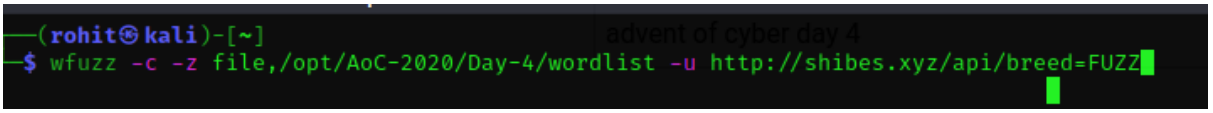
Thoughts:

We accessed the machine and turned on the foxy proxy and turned the intercept on.We entered a random username and password and we got it in burpsuite.We forwarded it to the intruder and repeater. We then went to the intruder tab and selected cluster bomb and we went to the payloads and entered the given options of usernames and passwords.Once we started the attack we got the username and password.

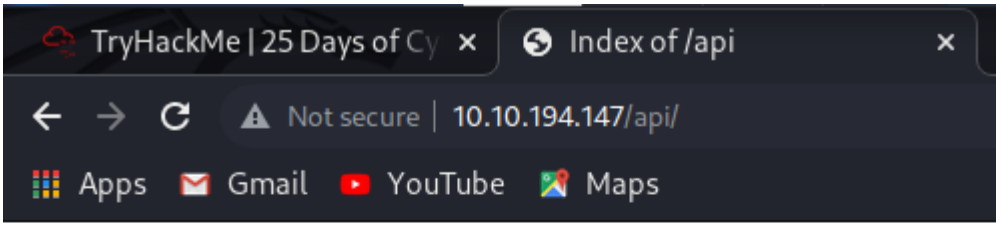
Day 4- Santa's Watching

Tools used: linux

Question 1



Question 2

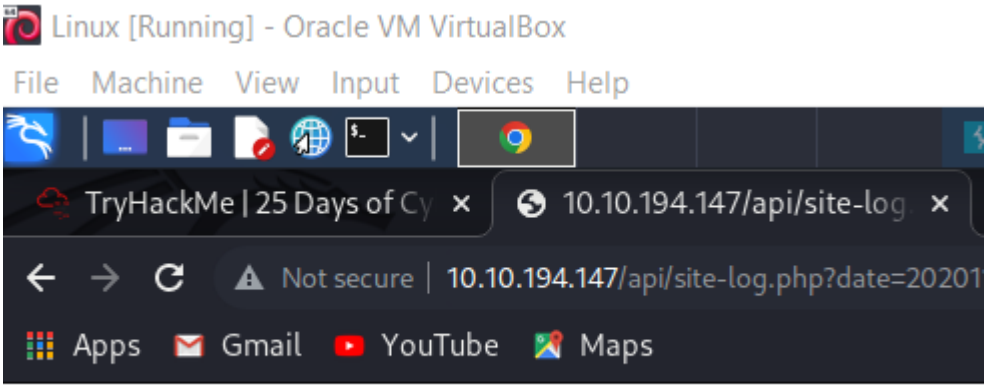


Index of /api

Name	Last modified	Size	Description
Parent Directory		-	
site-log.php	2020-11-22 06:38	110	

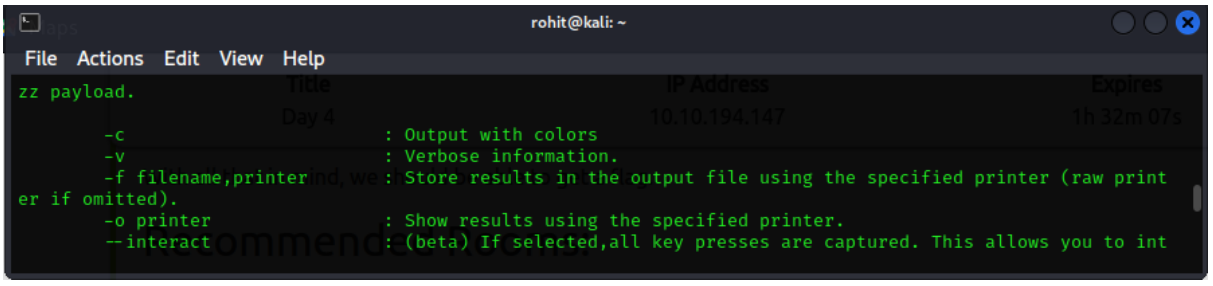
Apache/2.4.29 (Ubuntu) Server at 10.10.194.147 Port 80

Question 3



THM{D4t3_AP1}

Question 4



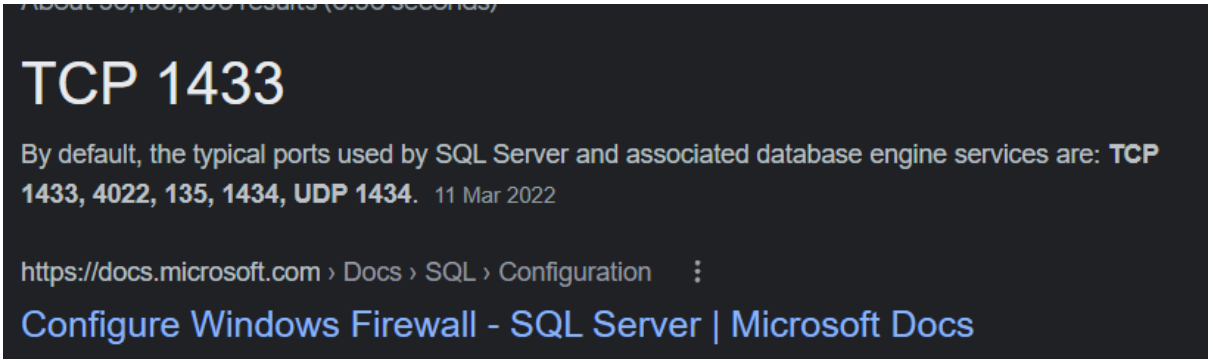
Thoughts:

We accessed the machine. And then we used gobuster to find the api page directory.once we have found the api directory, we used wfuzz to get the value.

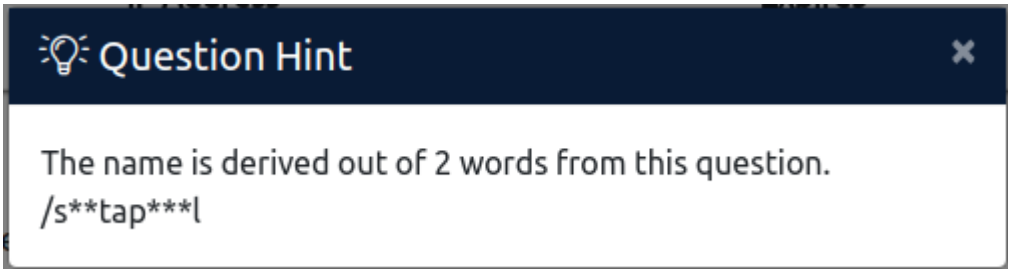
Day 5- Someone Stole Santa's Gift List

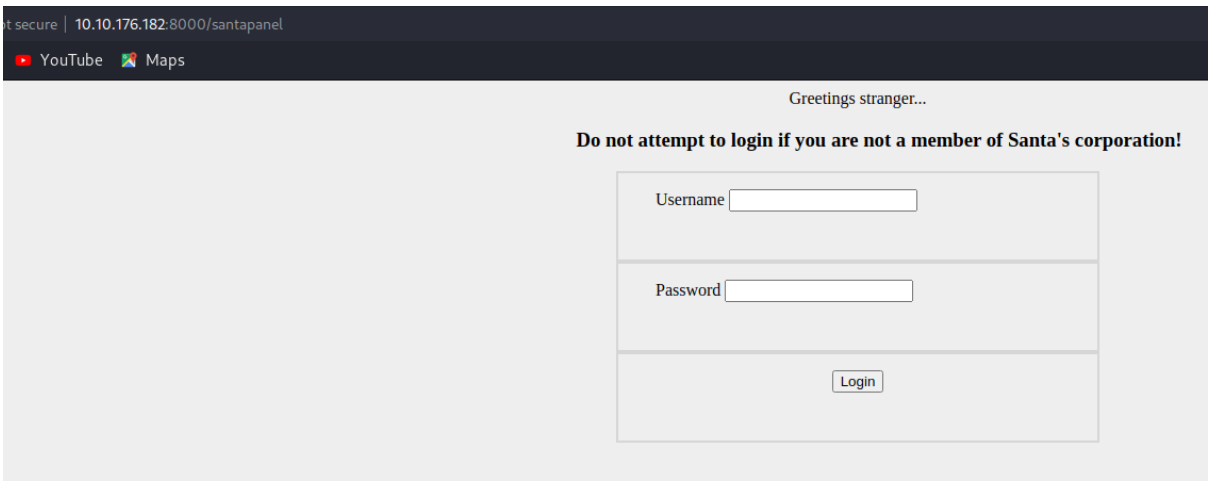
Tools used: linux

Question 1



Question 2





Question 3

Question 4

There's a total of 22 entries

```
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
Kenneth     | 19  | TryHackMe Sub
Joshua      | 12  | chair
```

Question 5

James' age is 8

```
James       | 8   | shoes
```

Question 6

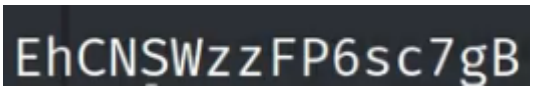
Github Ownership

```
Paul        | 9   | github ownership
```

Question 7

```
thmfox{All_I_Want_for_Christmas_Is_You}
```

Question 8



Thoughts:

We accessed the machine, and guessed santa's admin page which is santapanel,bypassed the login page.And once we've entered the page we used burpsuite to intercept and did a sql injection to get all the information.