PSP0201
WEEKLY WRITE UP
WEEK 2
GROUP 7

Group Name : Sang Haekeo (The Hackers)

Sang
- Taken from a Malay word , sang , meaning ‘the’

Haekeo
- Taken from a Korean word , 해커 , meaning ‘hacker’
-

ID	NAME	ROLE	TASK
1211102162	AMILIA NADZEERA BINTI BAHARUDIN	Leader	- Day 1 & 2 write up
1211100930	KU NAJWA SYAUQINA BINTI KU AZRIN	Member	
1211101693	SAVITHA MURUGUMUNISEGARAN	Member	- Day 3 & 4 write up

TASK 3 ; DAY 1 : WEB EXPLOITATION - A CHRISTMAS CRISIS

Tools used : Attackbox , Firefox

Solution/walkthrough:

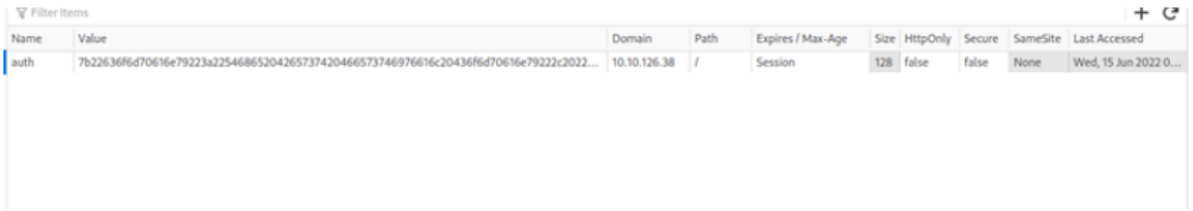
Question 1

The title of the website is <title>Christmas Console</title>.

```
<!DOCTYPE html>
<html lang=en>
    <head>
        <title>Christmas Console</title>
        <meta charset=utf-8>
        <meta name=viewport content="width=device-width, initial-scale=1.0">
        <script src="assets/js/login.js"></script>
        <script src="assets/js/userfuncs.js"></script>
        <link rel=stylesheet type=text/css href="/assets/css/style.css">
```

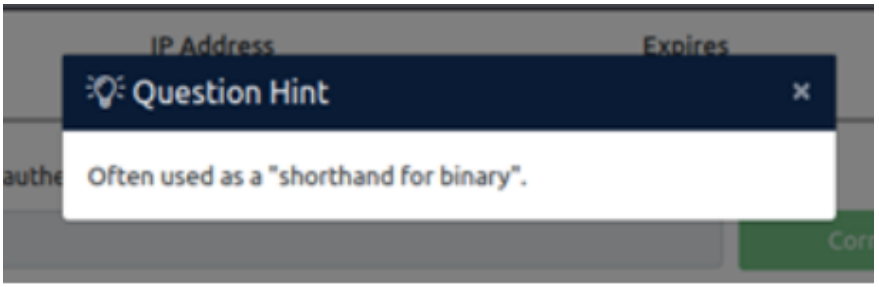
Question 2

The name of the cookie used for authentication is auth.



Question 3

Value of cookie encoded is format in hexadecimal



Question 4

The data is stored in JSON format. JSON is a text-based data format that is used to store and transfer data. In JSON, the data are in key/value pairs separated by a comma , .

Question 5

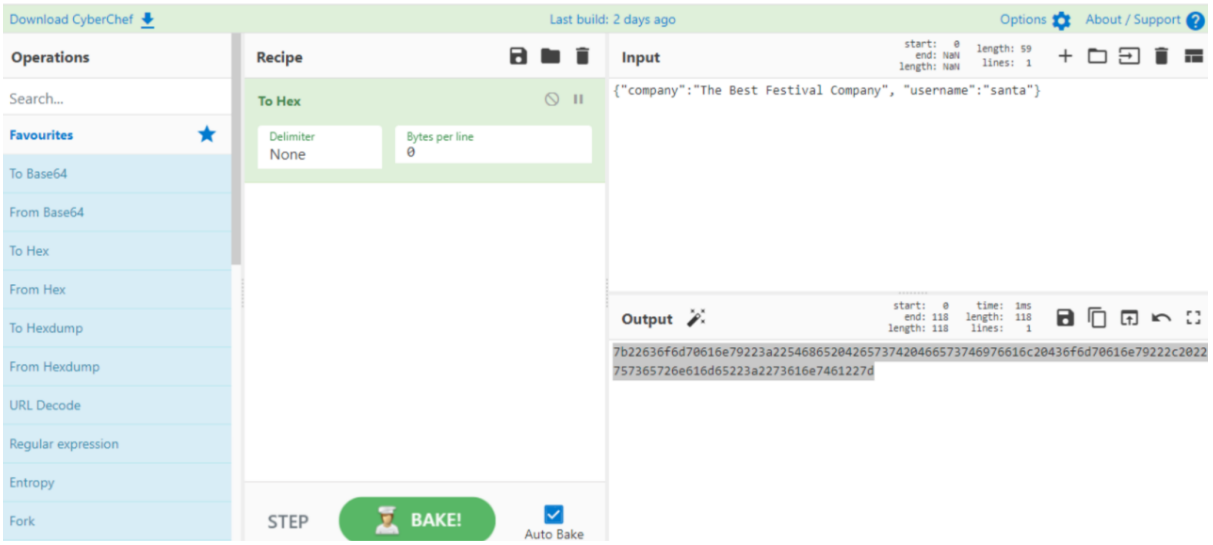
The value for the company field in the cookie is The Best Festival Company.

Question 6

Username is the other field found in the cookie.

Question 7

After change the username to santa, the value of Santa's cookie is 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022 757365726e616d65223a2273616e7461227d.



Question 8

We now have access to the controls, switched on every control shows the flag. The flag is THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}.

Thought Process/Methodology:

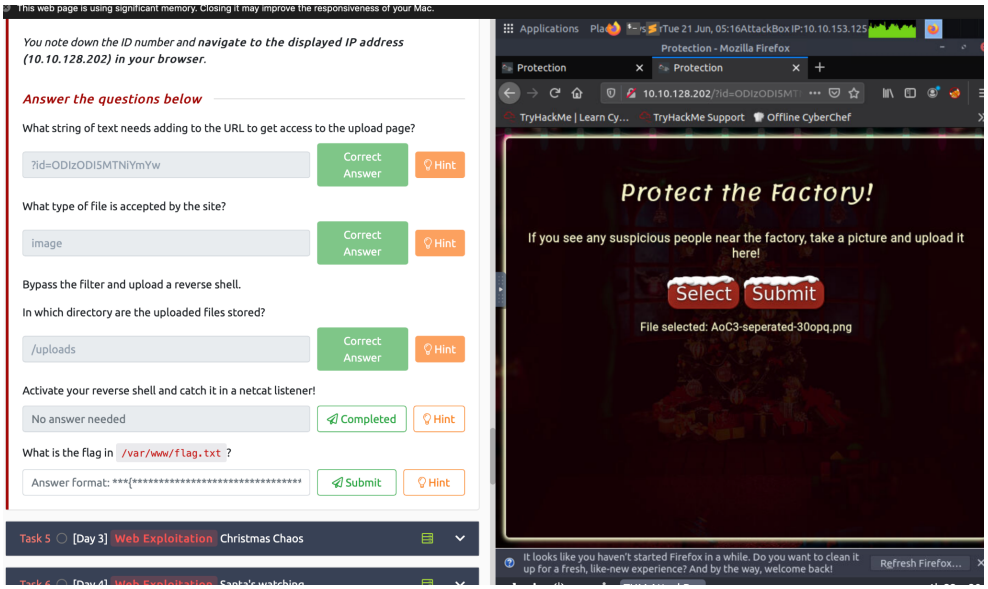
We connected to the network via AttackBox. After succeeding, we copied the IP address and pasted it in our own browser.A login/registration page appeared. We proceeded to register an account and login. After logging in, we opened the browser's developer tool and chose to view the site cookie from the 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 had changed 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.

TASK 4 ; DAY 2 : WEB EXPLOITATION - THE ELF STRIKES BACK

Tools used : AttackBox , Firefox , Terminal Emulator

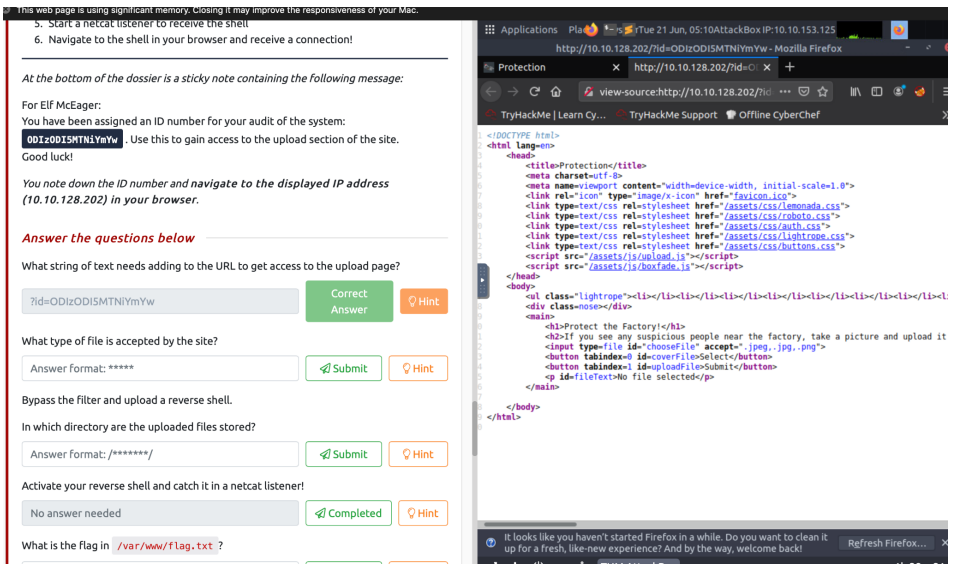
Question 1

?id=ODIzODI5MTNiYmYw is added to the URL to get access to the upload page



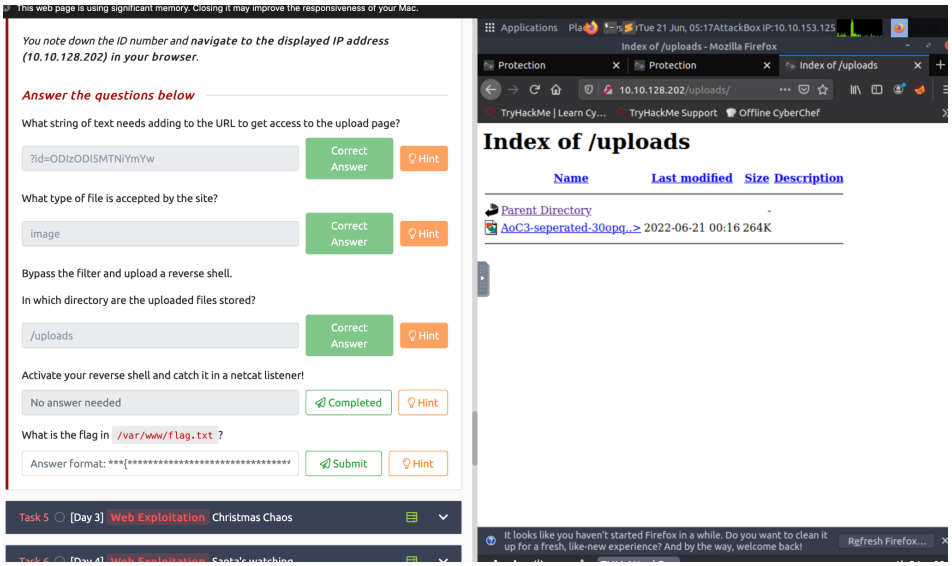
Question 2

files with extensions: .jpeg, .jpg, and .png are allowed. Image is the type of file that is accepted by the site.



Question 3

/uploads/ is the directory that uploads files stored.



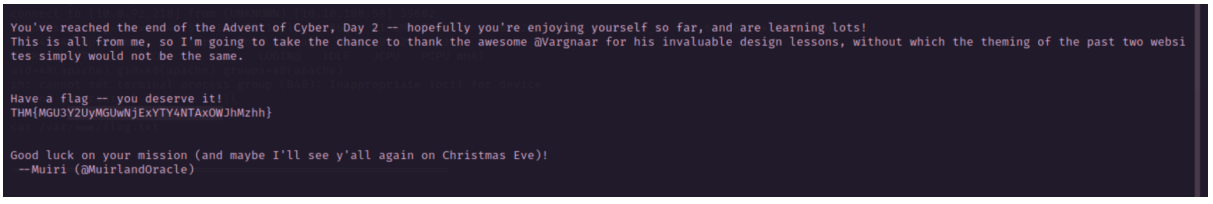
Question 4

Netcat parameter explanations :

- -v Has nc give more verbose output.
- -p Specifies the source port nc should use, subject to privilege restrictions and availability.
- -l Used to specify that nc should listen for an incoming connection rather than initiate a connection to a remote host.
- -n Does not do any DNS or service lookups on any specified addresses, hostnames or ports.

Question 5

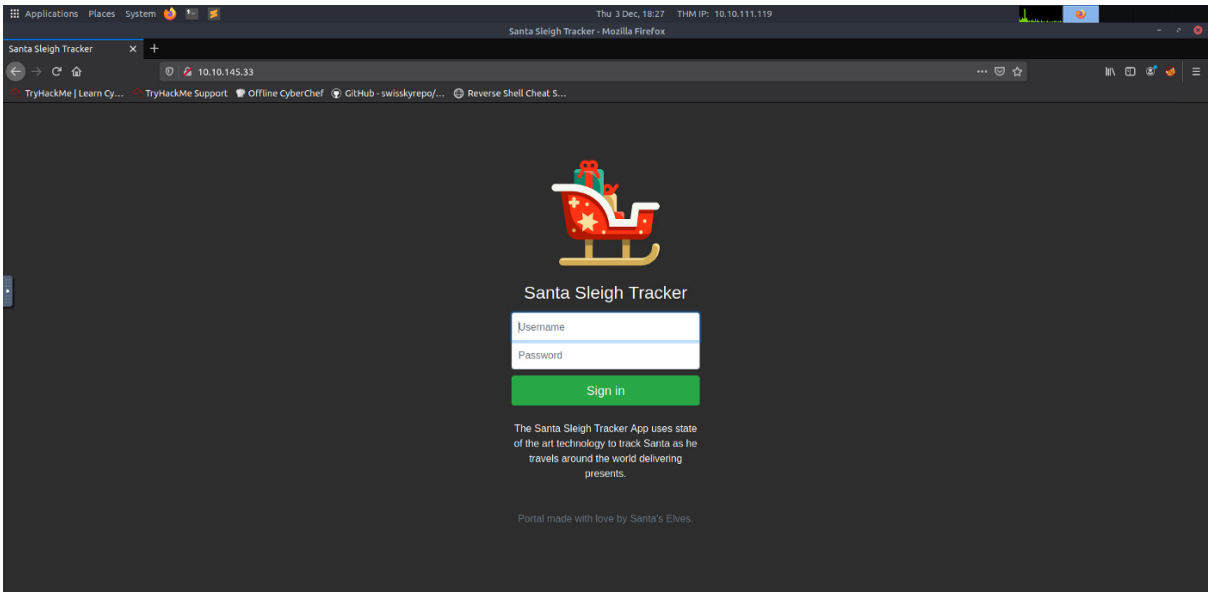
In the netcat terminal windows, we can see a shell and can find the flag: cat /var/www/flag.txt THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}



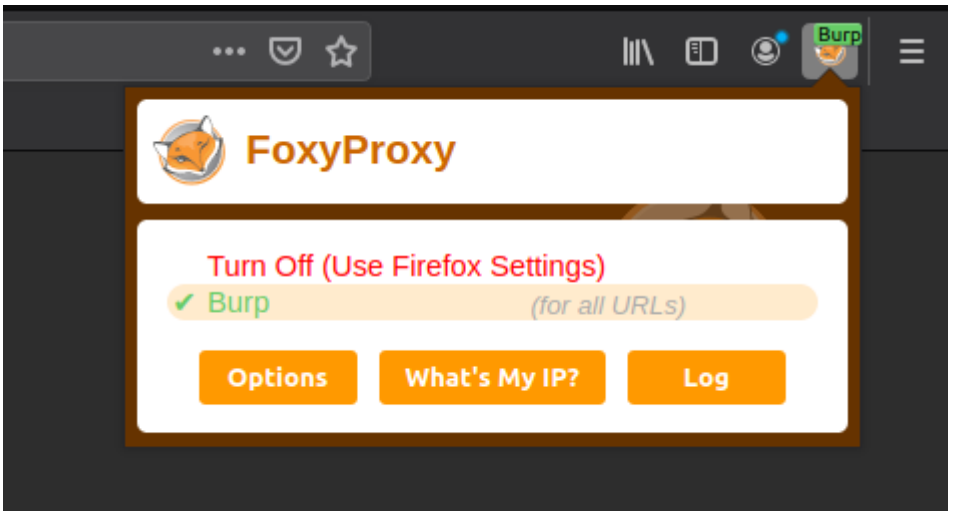
Thought Process/Methodology:
Firstly we copied the IP address and pasted it in our own browser. We were shown a page that said ‘You are not signed in Please enter your ID as a GET parameter (?id=YOUR_ID_HERE)’. The id that we received was ODIzODI5MTNiYmYw. We added ?id=ODIzODI5MTNiYmYw to our URL. After hitting enter , we were directed to the upload page. To find the type of file that is accepted by the site, we right-clicked on it and chose the ‘view page sources’ option. Then, it showed the source code. It allows files with extensions of .jpeg, .jpg, and .png. From that, we know the type of file that is accepted by the site is image. For this section, we need to get a reverse shell script ready. To use this script, we copy ‘cp usr/share/webshells/php/php-reverse-shell.php ./shell.jpeg.php’ to our terminal. Next, we need to edit the script in nano. There are two lines of code with comments //CHANGE THIS after them, the ip and port variables. For the IP address we entered the IP of our machine ‘10.8.92.218’ and for the port we put ‘443’. Next, we run netcat with the command sudo nc -lvpn 443 in order to listen on port 443. We came back to page uploads and submitted the script we just created. In the 'select' button, we entered the shell.jpeg.php script then clicked 'submit’. We need to find the directory that any uploaded files are saved in. This can be done by taking a guess at what the directory may be. It can be found with /uploads. Click on the file to execute the shell! In our netcat terminal windows, we see a shell and can find the flag.

Day 3: Christmas Chaos

The challenge's webpage can be found here:



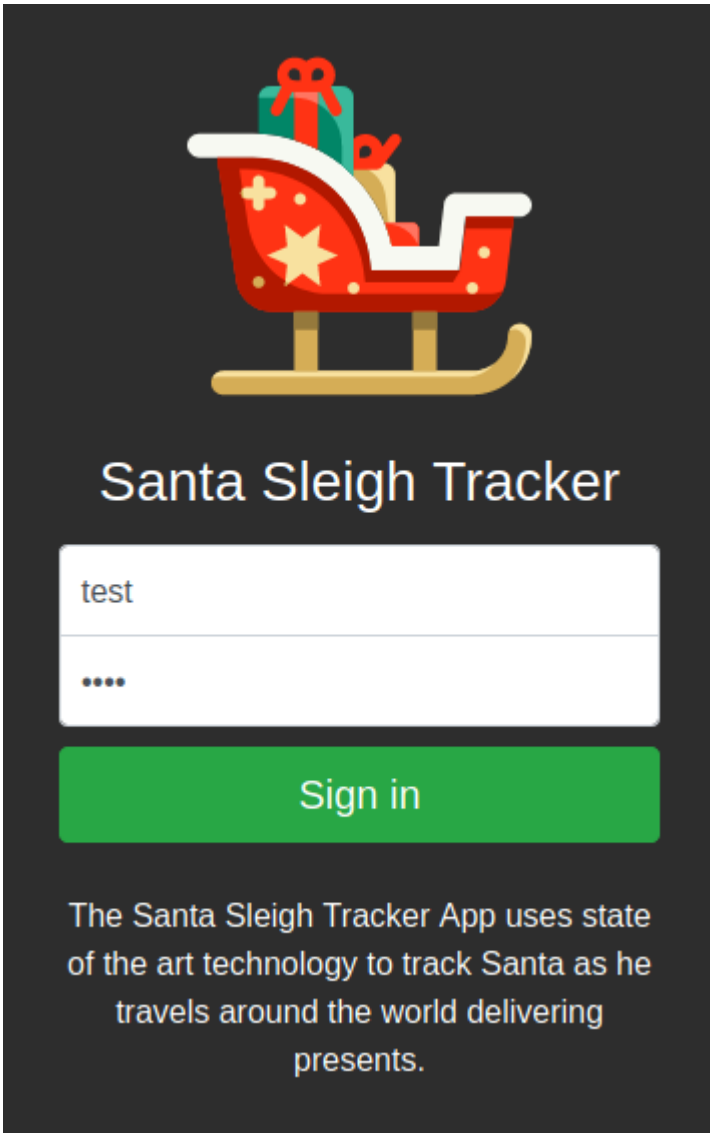
It seems that Burp Suite is being used to try every possible combination on the login form. In order to begin traffic intercepting, We first launched Burp Suite and then activated Foxy Proxy:



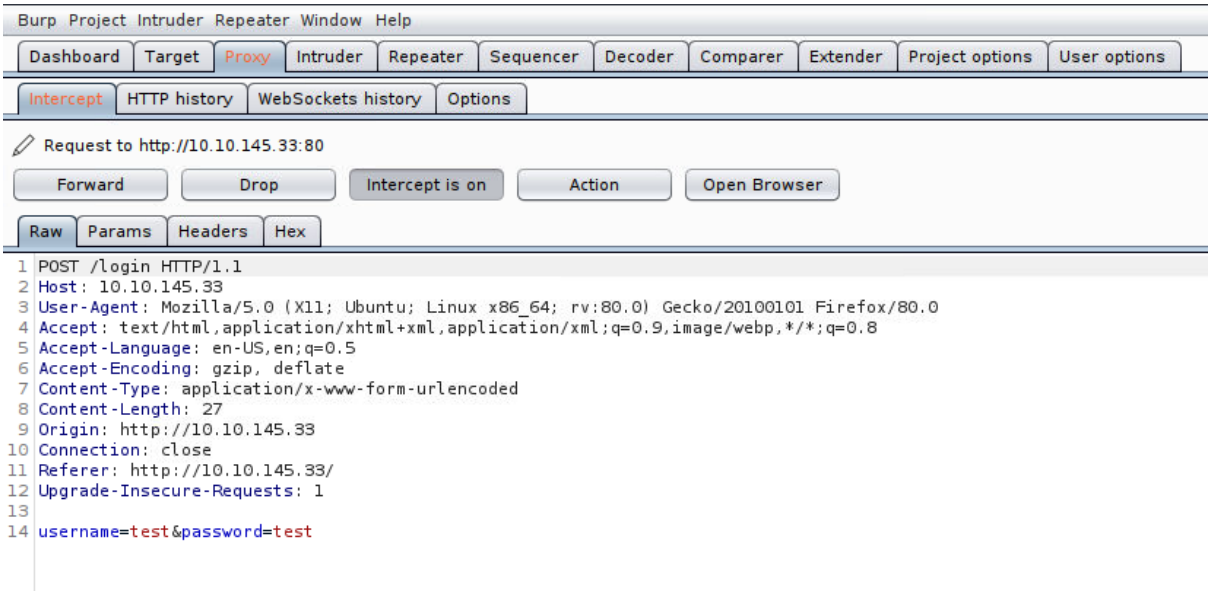
We're going to utilise the list of default credentials to try to log in, using each one one at a time:

Username	Password
root	root
admin	password
user	12345

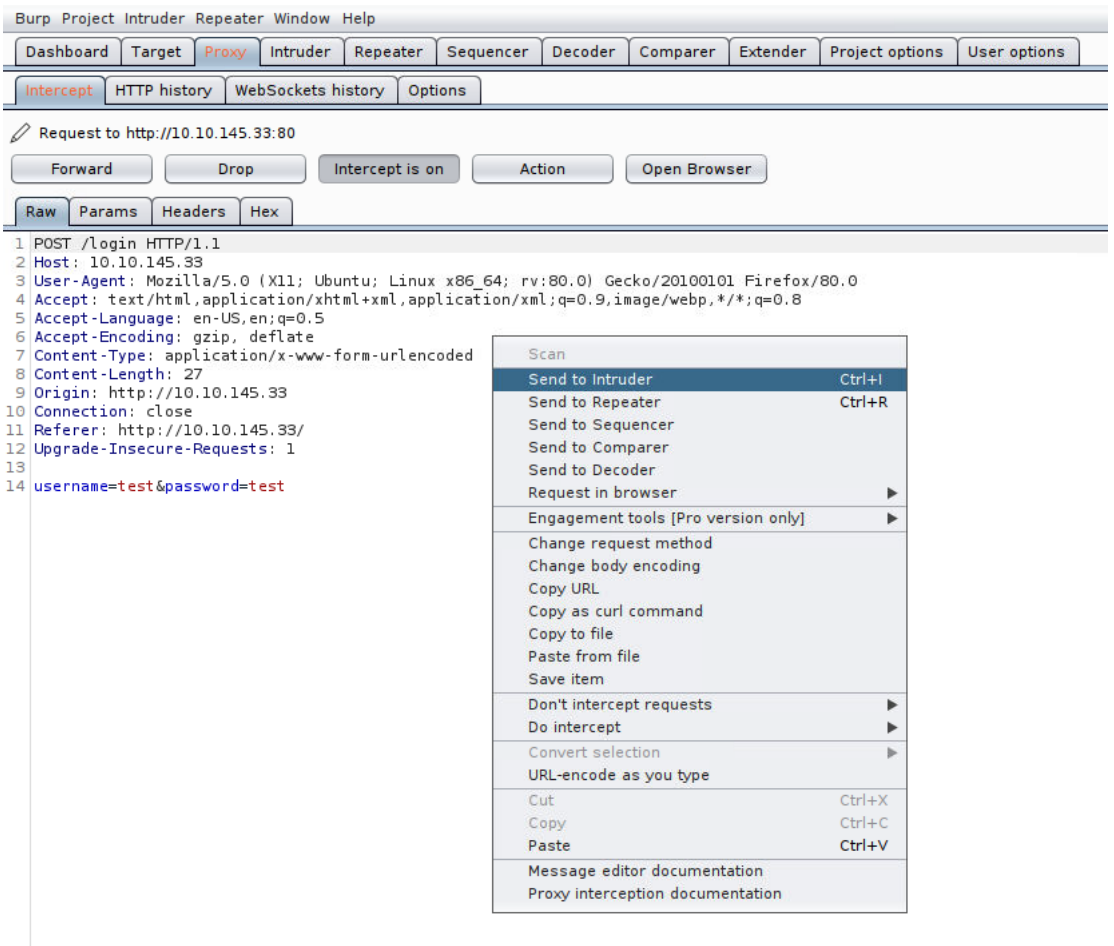
We first conducted a test:



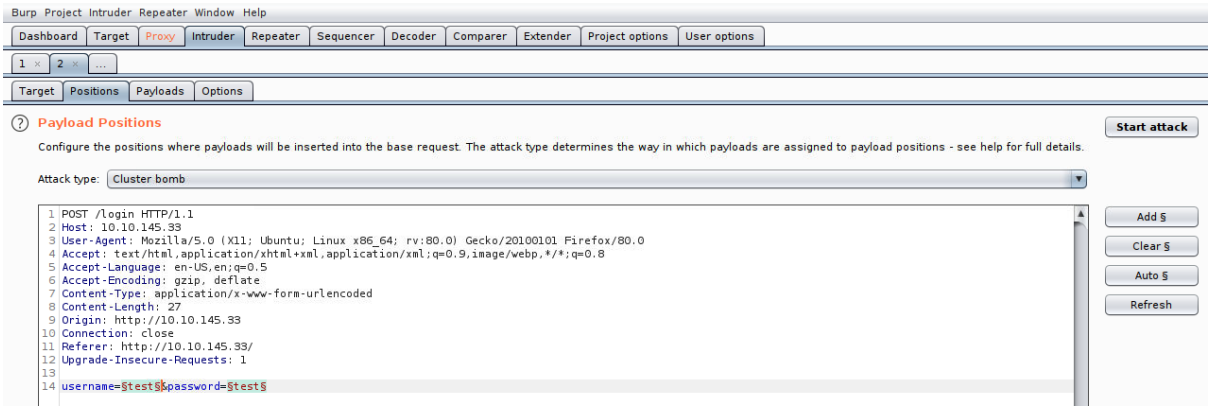
We went back to Burp Suite to review the request after that:



After that, we can choose "send to invader" by right-clicking anywhere in that section:



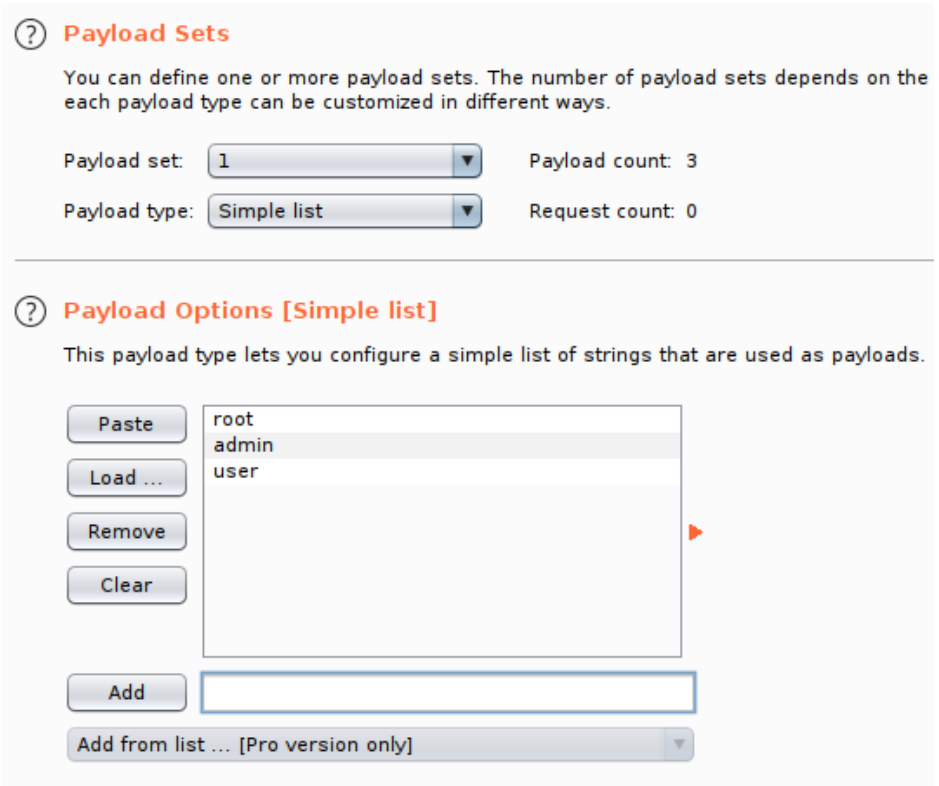
Look at the positions tab from the Intruder:



You can see that it has already set a few positions as defaults for you (highlighted in green). Burp Suite will use brute force in certain places.

To ensure that each payload supplied rotates in and out in turn, change the assault type to "Cluster Bomb."

Add all the usernames to payload 1 (the first green highlight):



Add all the passwords for payload 2:

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the each payload type can be customized in different ways.

Payload set: 2 Payload count: 3

Payload type: Simple list Request count: 9

Payload Options [Simple list]

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

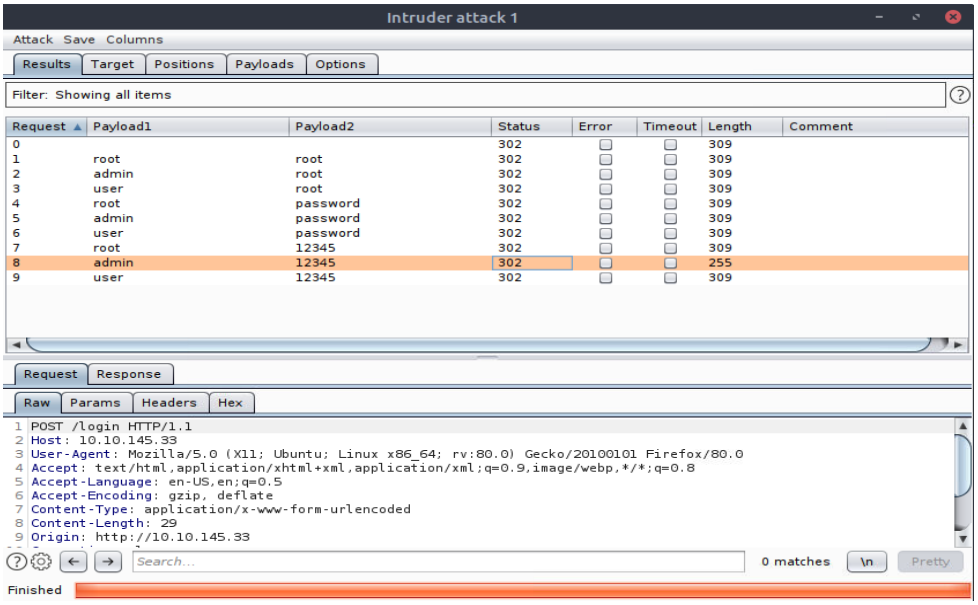
Paste
Load ...
Remove
Clear

root
password
12345

Add

Add from list ... [Pro version only]

The automated attack will now begin when we click the "Start Attack" button in the top right corner.



The combination that has a different length is typically the right one. So we try logging in with the credentials admin and 12345.

Don't forget to deactivate FoxyProxy before attempting to log in.

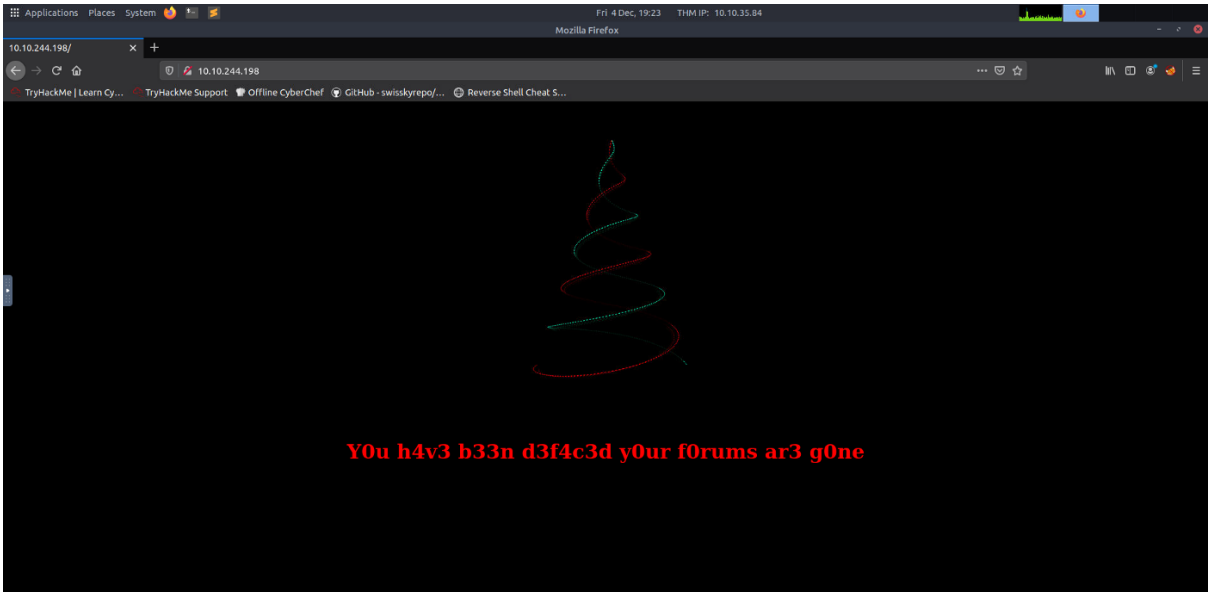
We're in!

Day 4: 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)

The website linked to the IP address is located here:



However, the first query actually asks us to check out http://shibes.xyz/api.php, which is a distinct domain.

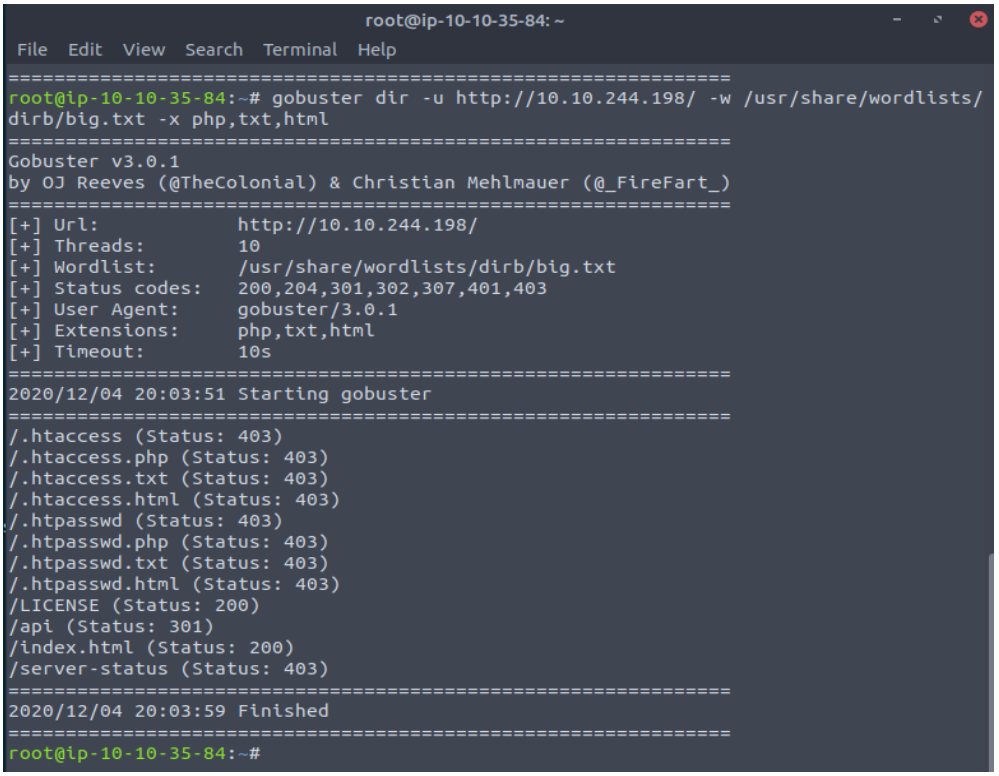
Since it's bogus, you can't actually perform it, but just visualise how your command would appear if you used the challenge materials:

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

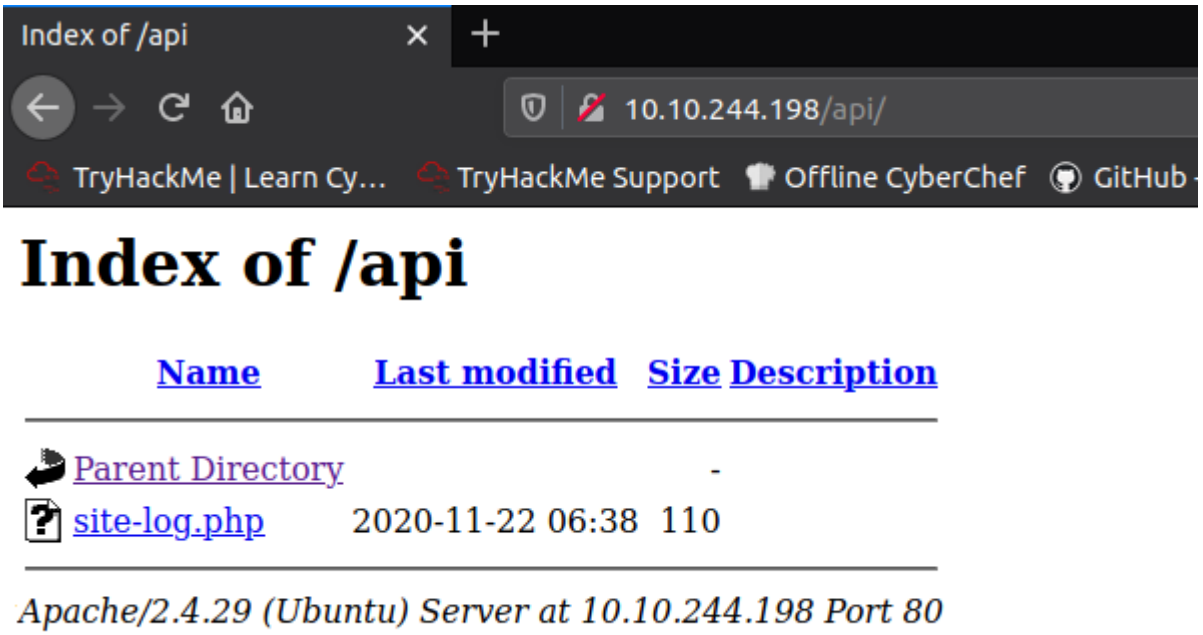
Question 2

Use GoBuster to find the API directory. What file is there?

We ran GoBuster on the main page:



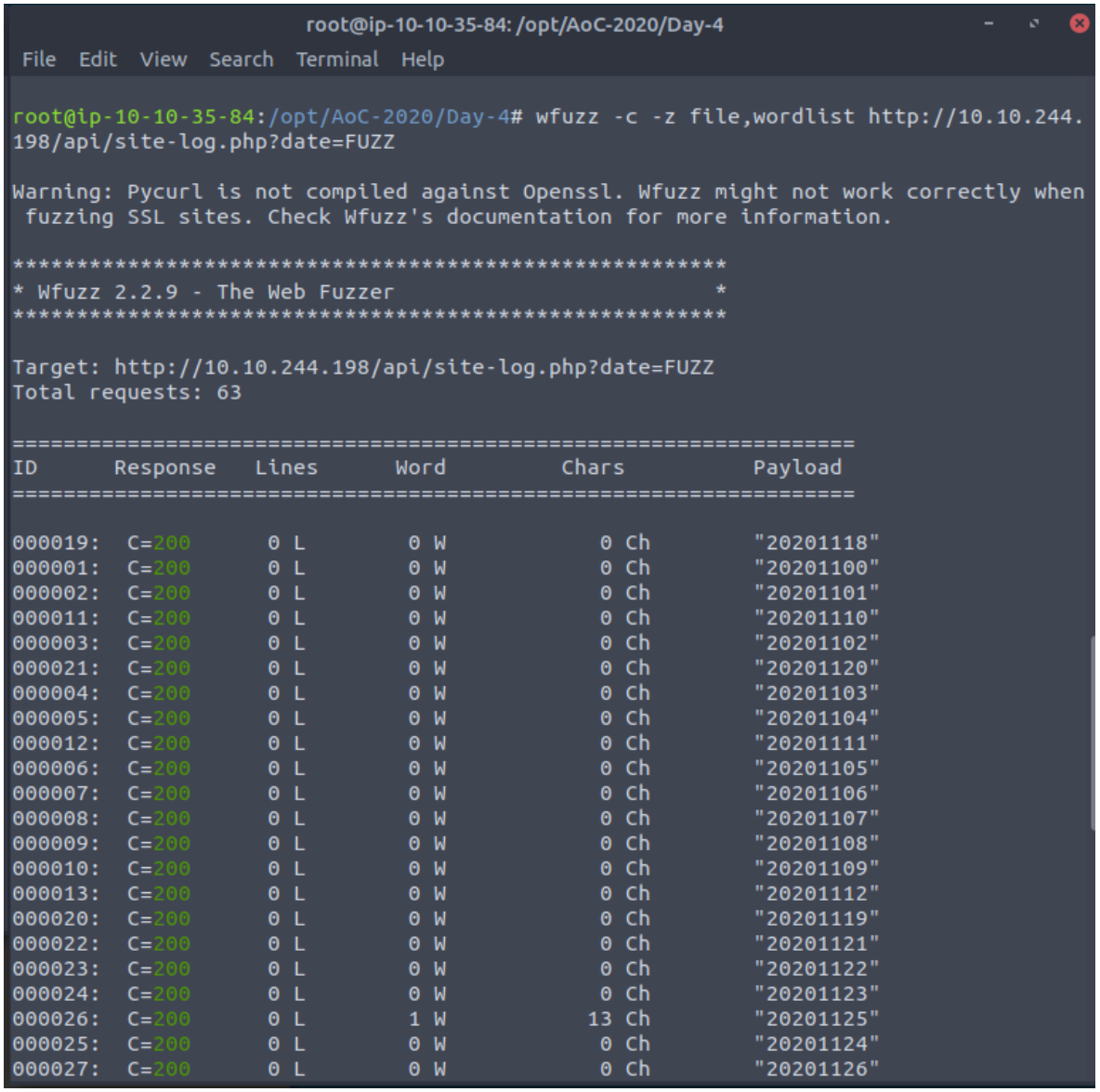
We then went to /api and discovered site-log.php, which was the file we needed.



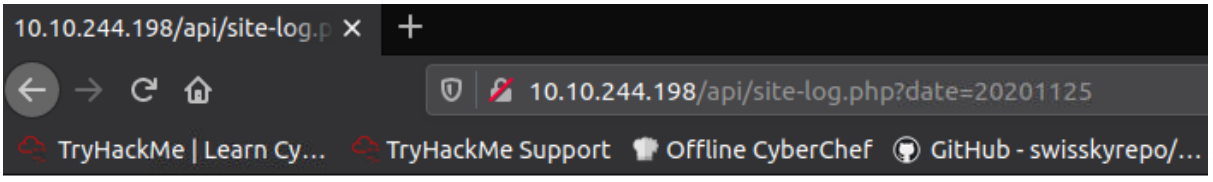
Question 3

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

We used the wfuzz command to find one that stood out from the others. We can determine that the date 20201125 is not empty because it has 13 characters and not just zeros like the rest:



We may see the flag by going there in our web browser.



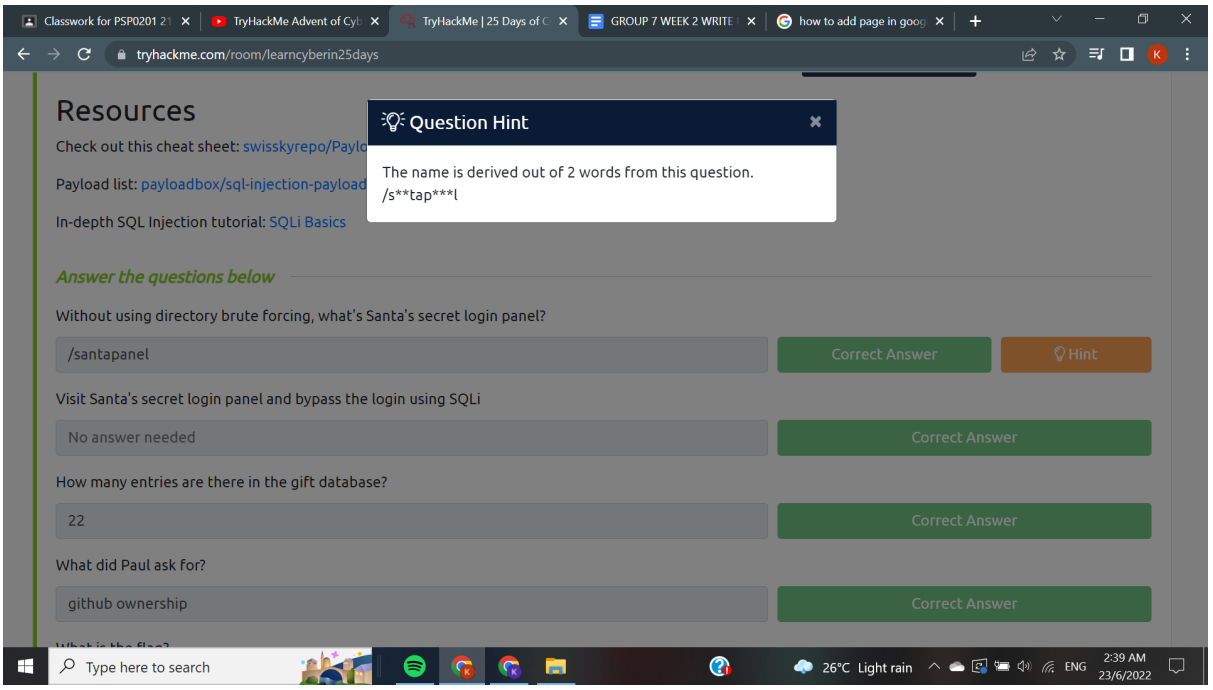
THM{D4t3_AP1}

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

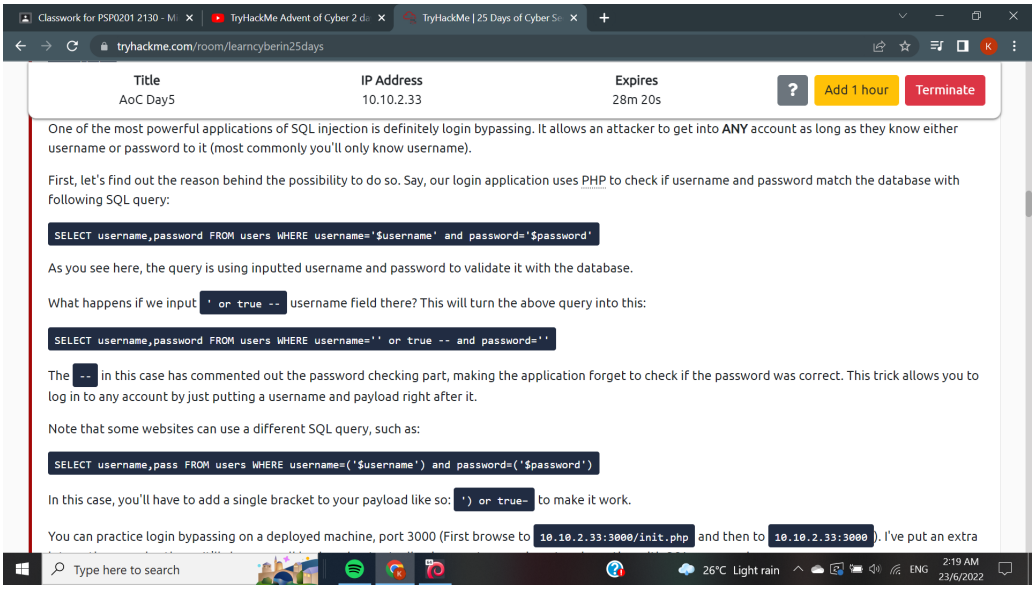
Tool used : Kali linux, firefox

Solution :

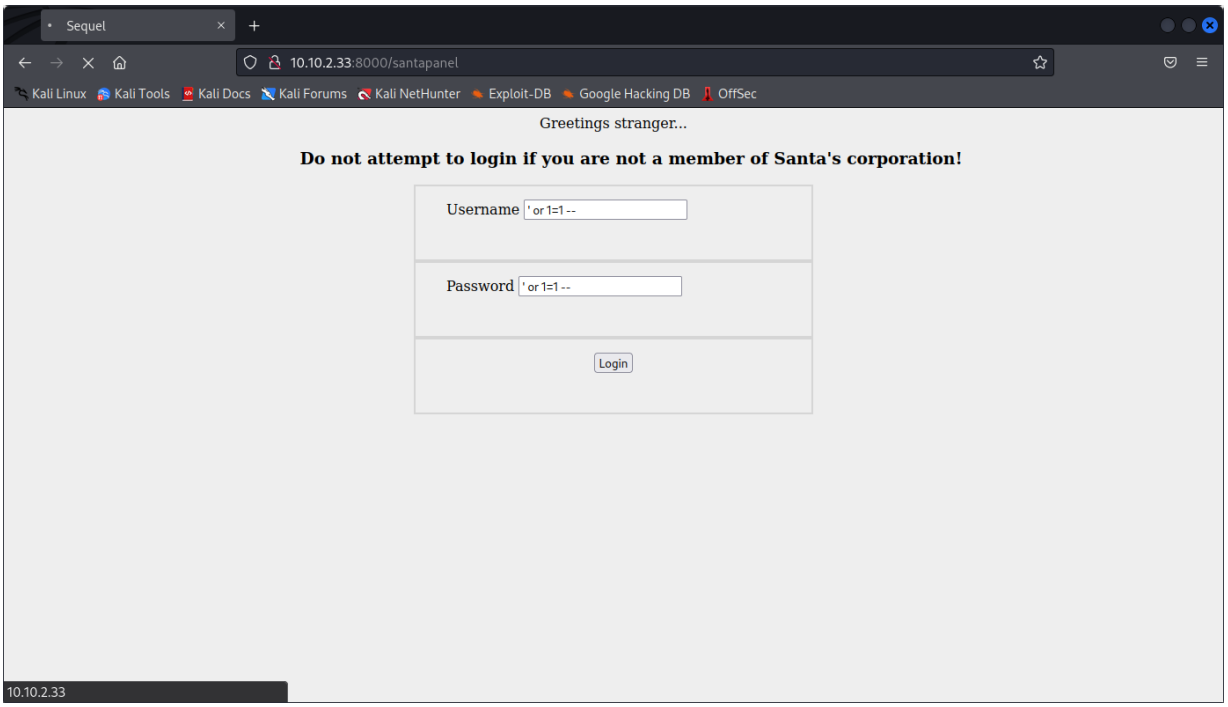
Question 1 : `Without using directory brute forcing, what's Santa's secret login panel?`

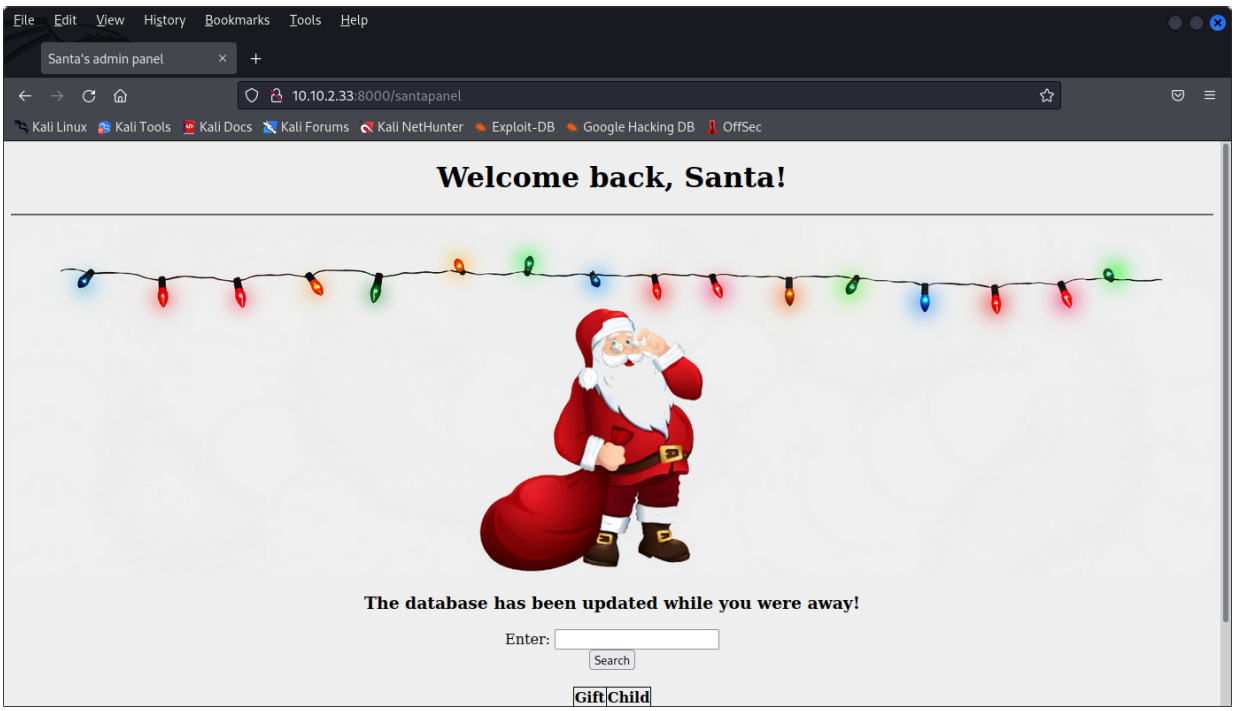


Question 2 :
`Visit Santa's secret login panel and bypass the login using SQLi`

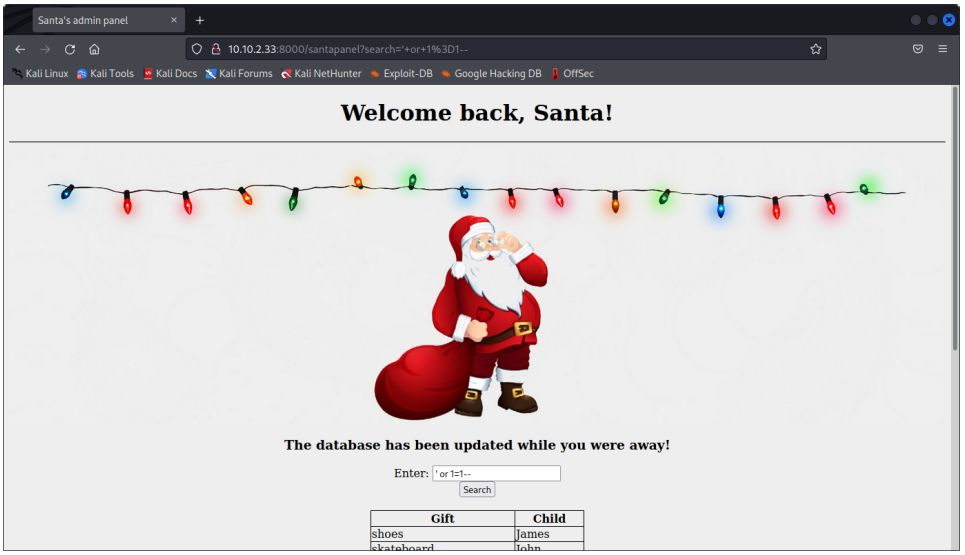


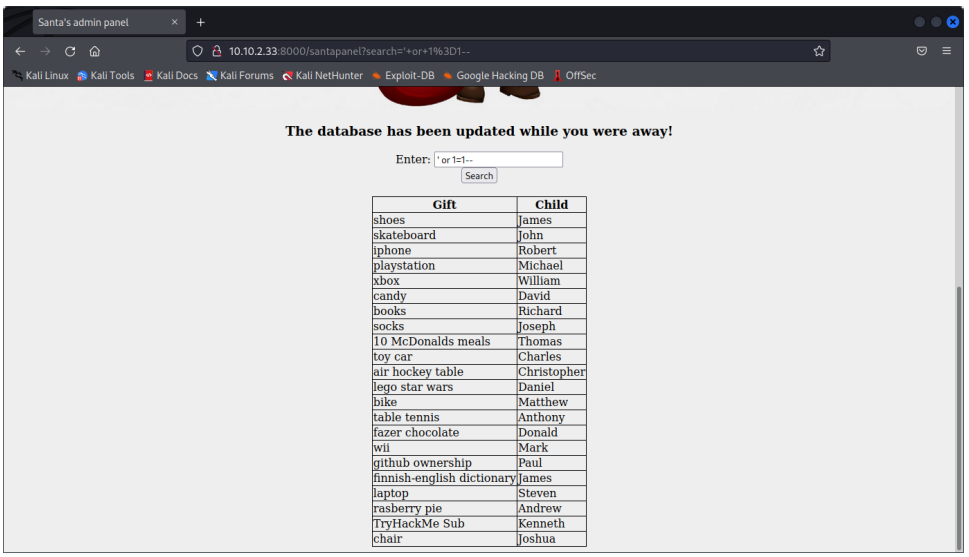
Using the ‘ or 1=1– to log in.



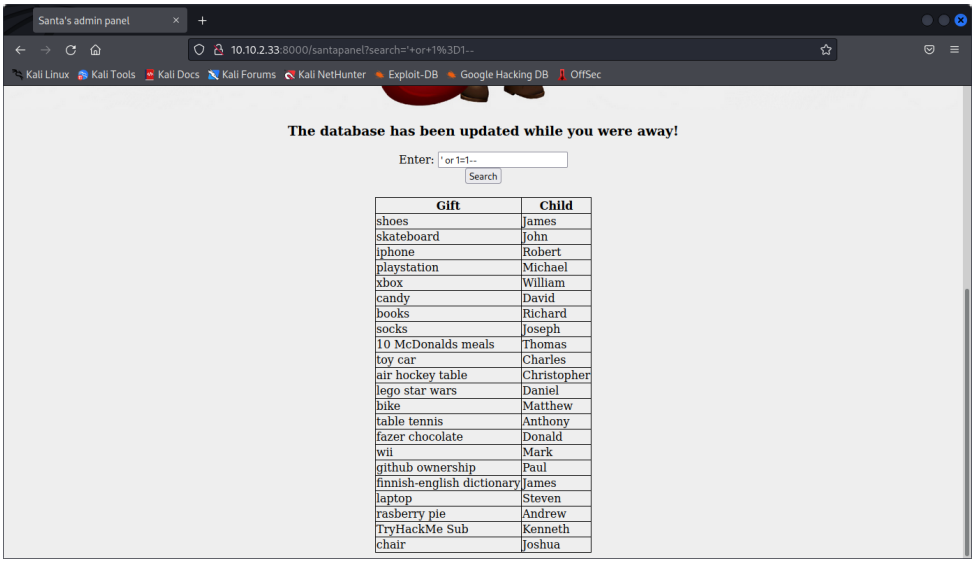


Question 3 : How many entries are there in the gift database?



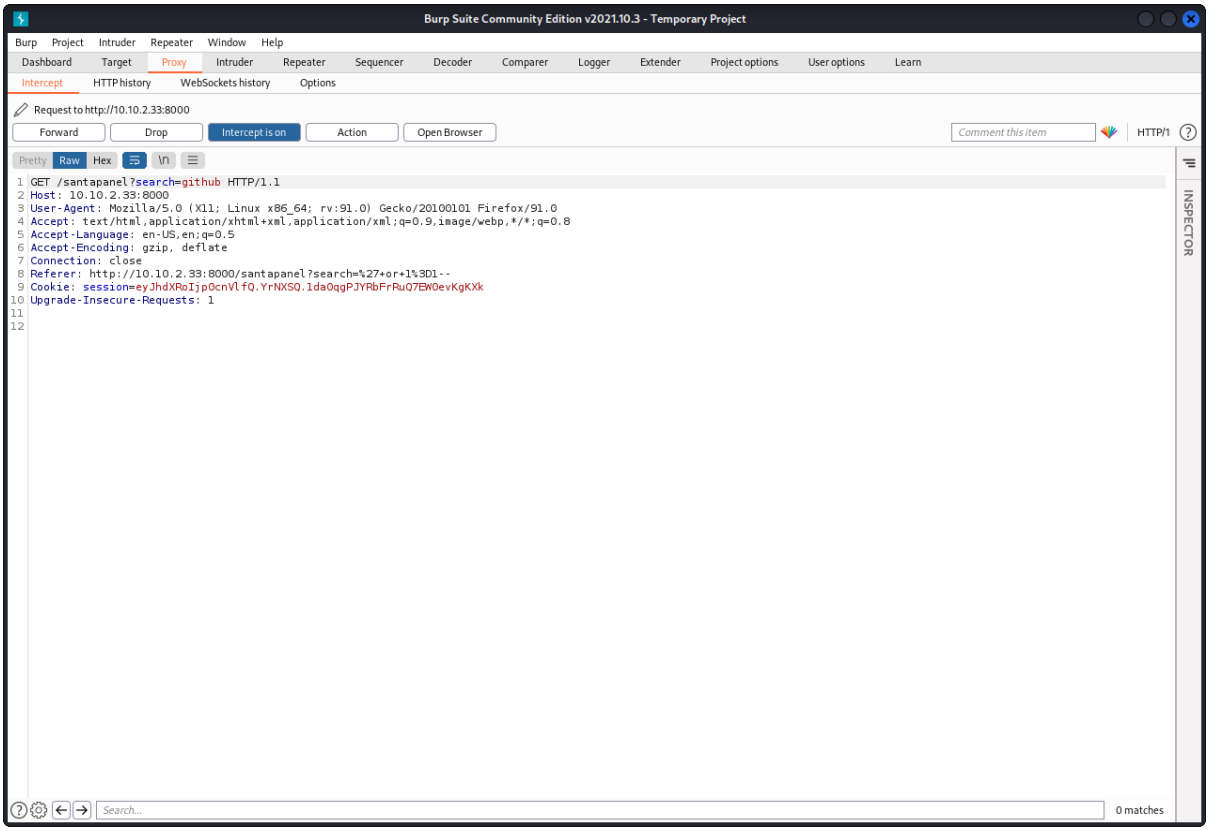


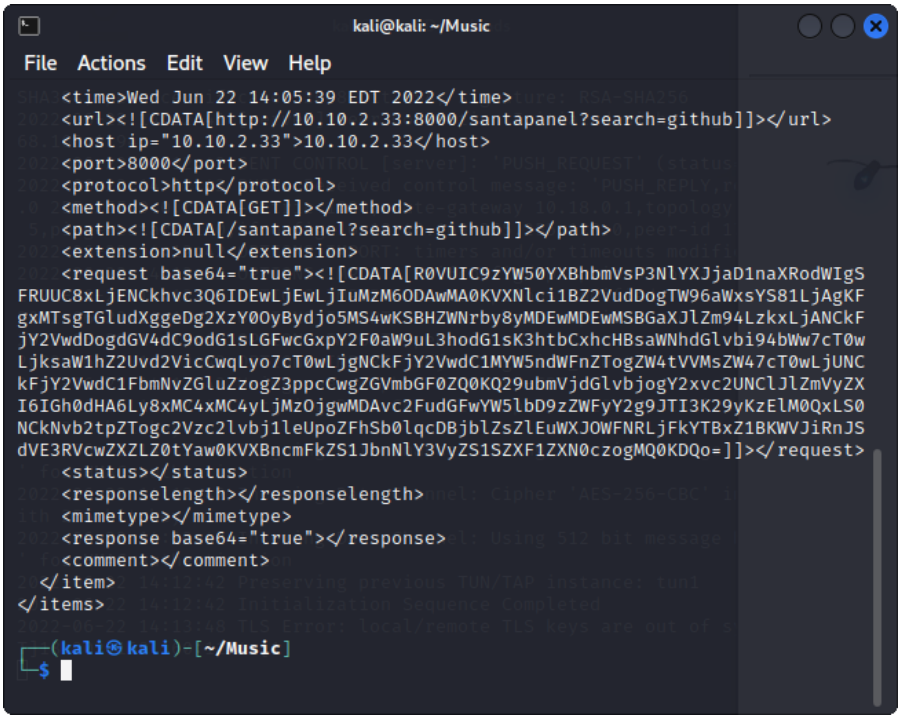
Question 4 : What did Paul ask for?

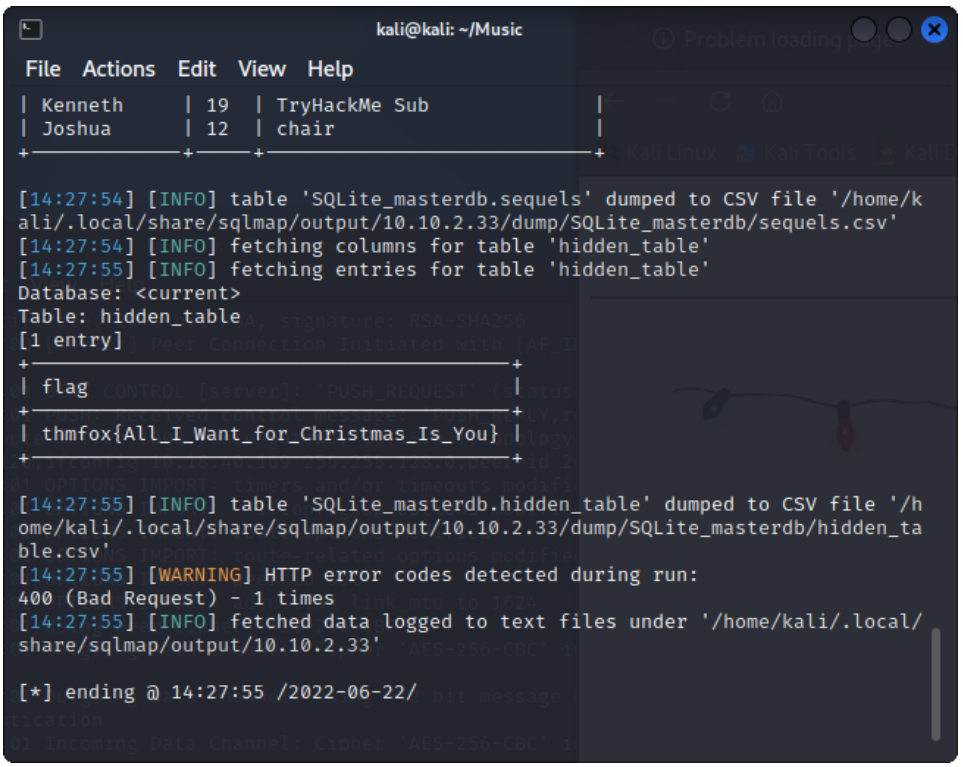


Question 5 : What is the flag?

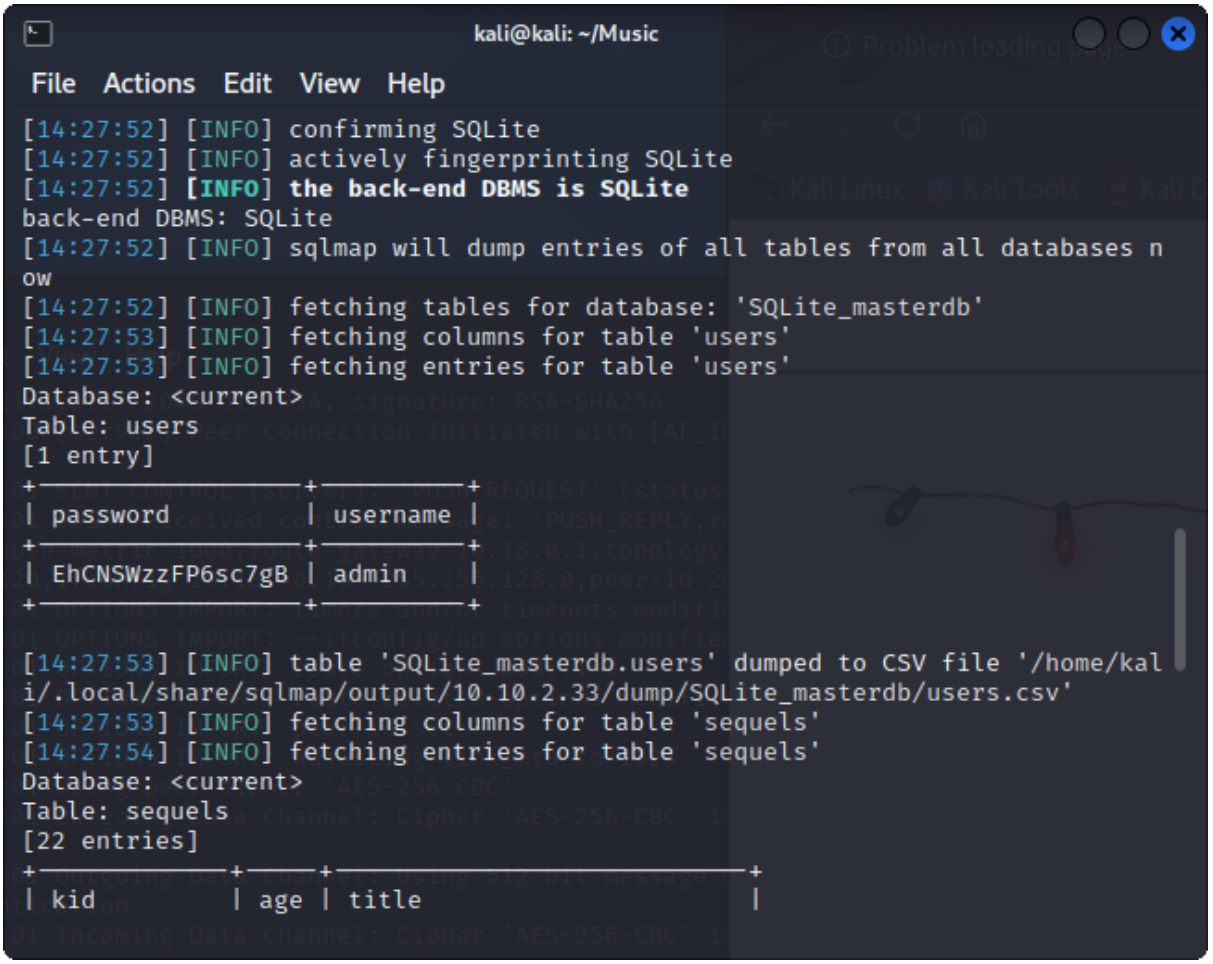
Using burpsuite to to receive request from the search. And then save the item to your file.


Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://10.10.2.33:8000
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex \n
1 GET /santapanel?search=github HTTP/1.1
2 Host: 10.10.2.33:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.2.33:8000/santapanel?search=%27+or+1%3D1--
9 Cookie: session=eyJhdXRoIjp0cnVlfQ.YrNXSQ.1da0qgPJYRbFrRuQ7EW0evKgKXk
10 Upgrade-Insecure-Requests: 1
11
12
INSPECTOR
Search...
0 matches


kali@kali: ~/Music
File Actions Edit View Help
<time>Wed Jun 22 14:05:39 EDT 2022</time>
<url><![CDATA[http://10.10.2.33:8000/santapanel?search=github]]></url>
<host ip="10.10.2.33">10.10.2.33</host>
<port>8000</port>
<protocol>http</protocol>
<method><![CDATA[GET]]></method>
<path><![CDATA[/santapanel?search=github]]></path>
<extension>null</extension>
<request base64="true"><![CDATA[R0VUIC9zYW50YXBhbmVsP3NlYXJjaD1naXRodWIgSFRUUC8xLjENCkhvc3Q6IDEwLjEwLjIuMzM6ODAwMA0KVXNlci1BZ2VudDogTW96aWxsYS81LjAgKFgxMTsgTGludXggeDg2XzY0OyBydjo5MS4wKSBHZWNrby8yMDEwMDEwMSBGaXJlZm94LzkxLjANCkFjY2VwdDogdGV4dC9odG1sLGFwcGxpY2F0aW9uL3htbCt4bWwsYXBwbGljYXRpb24veG1sO3E9MC45LGltYWdlL3dlYnAsKi8qO3E9MC44DQpBY2NlcHQtTGFuZ3VhZ2U6IGVuLVVTLGVuO3E9MC41DQpBY2NlcHQtRW5jb2RpbmcgOiBnemlwLCBkZWZsYXRlDQpDb25uZWN0aW9uOiBjbG9zZQ0KUmVmZXJlcjogaHR0cDovLzEwLjEwLjIuMzM6ODAwMC9zYW50YXBhbmVsP3NlYXJjaD0lMjclMjBvciUyMDElM0QxLS0NCkNvb2tpZTogc2Vzc2lvbj1leUpoZFhSb0lqcDBjblZsZlEuWXJOWFNRLjFkYTBxZ1BKWVJiRnJSdVE3RVcwZXZLZ0tYaw0KVXBncmFkZS1JbnNlY3VyZS1SZXF1ZXN0czogMQ0KDQo=]]></request>
<status></status>
<responselength></responselength>
<mimetype></mimetype>
<response base64="true"></response>
<comment></comment>
</item>
</items>
(kali㉿kali)-[~/Music]
$



Question 6 : What is admin's password?



Thought Process/Methodology: