PSP0201

Week 2

Writeup

Group Name: Haxon

Members

ID	Name	Role
1211102370	Lau Zi Thao	Leader
1211102797	Teng Wei Joe	Member
1211103142	Wong Khai King	Member
1211101029	Garrison Goh Zen Ken	Member

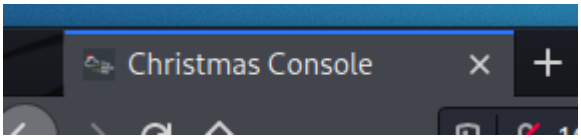
Day 1: Web Exploitation – A Christmas Crisis

Tools used: Kali Linux, Firefox, CyberChef

Solution/walkthrough:

Question 1

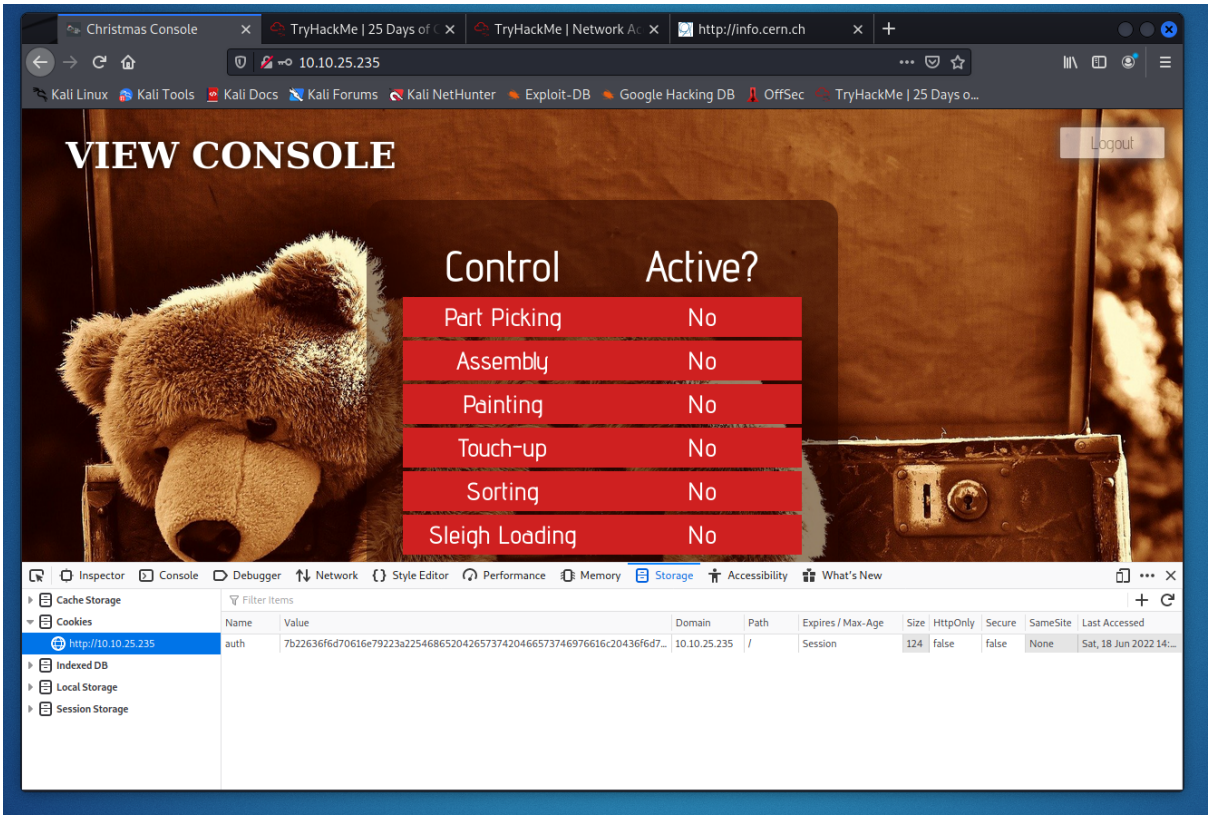
Inspect the website. What is the title of the website?



The title of the website is shown in the browser tab.

Question 2

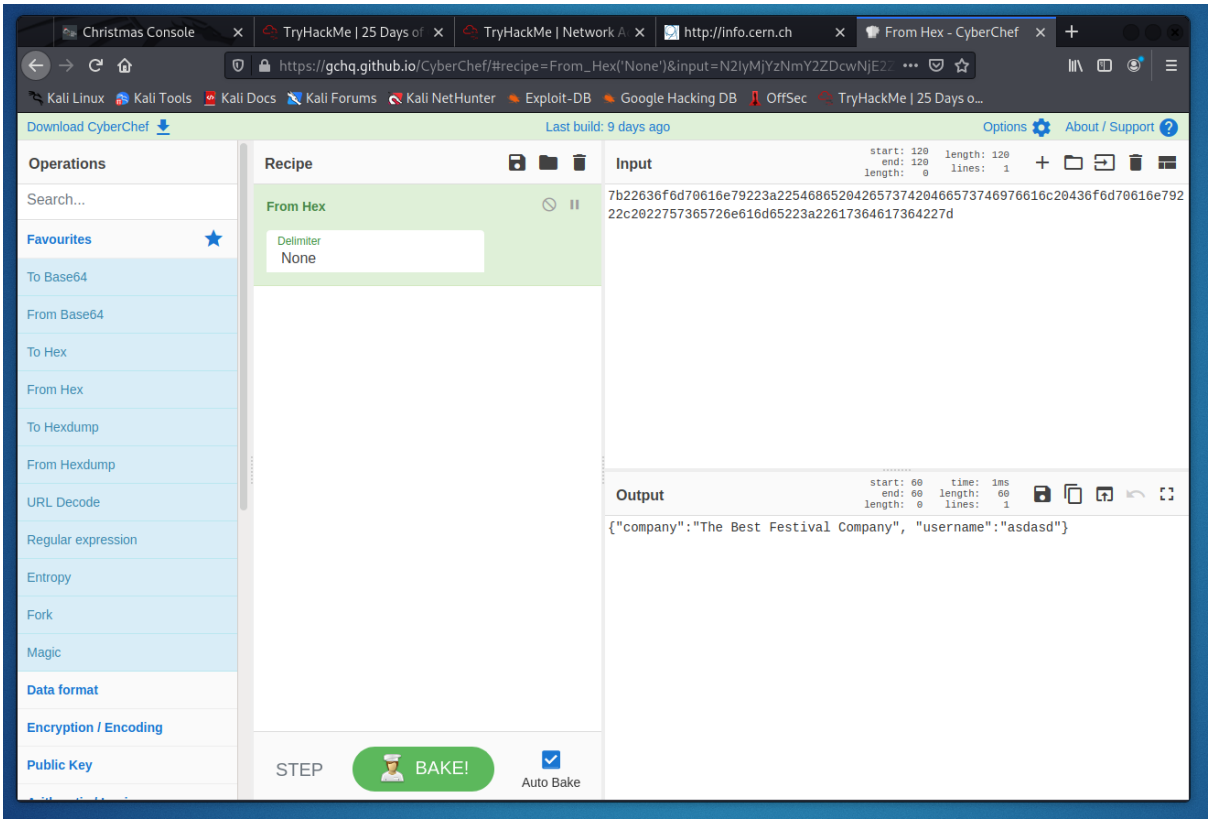
What is the name of the cookie used for authentication?



Press the shortcut keys Ctrl + Shift + I or F12 key to access the browser's developer tools. The cookies of the website are located in the storage tab. The name of the cookie that is used for authentication is auth as shown in the image above.

Question 3

In what format is the value of this cookie encoded?



The value of the cookie is in the format of Hexadecimal because its value is able to be decoded by CyberChef by using the "From Hex'' option.

Question 4

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

```
{"company":"The Best Festival Company", "username":"asdasd"}
```

The data is stored in JSON format as it includes curly brackets and quotation marks.

Question 5

What is the value for the company field in the cookie?

```
["company":"The Best Festival Company",
```

The value for the company field in the cookie is The Best Festival Company, as shown in the decoded hex value in CyberChef.

Question 6

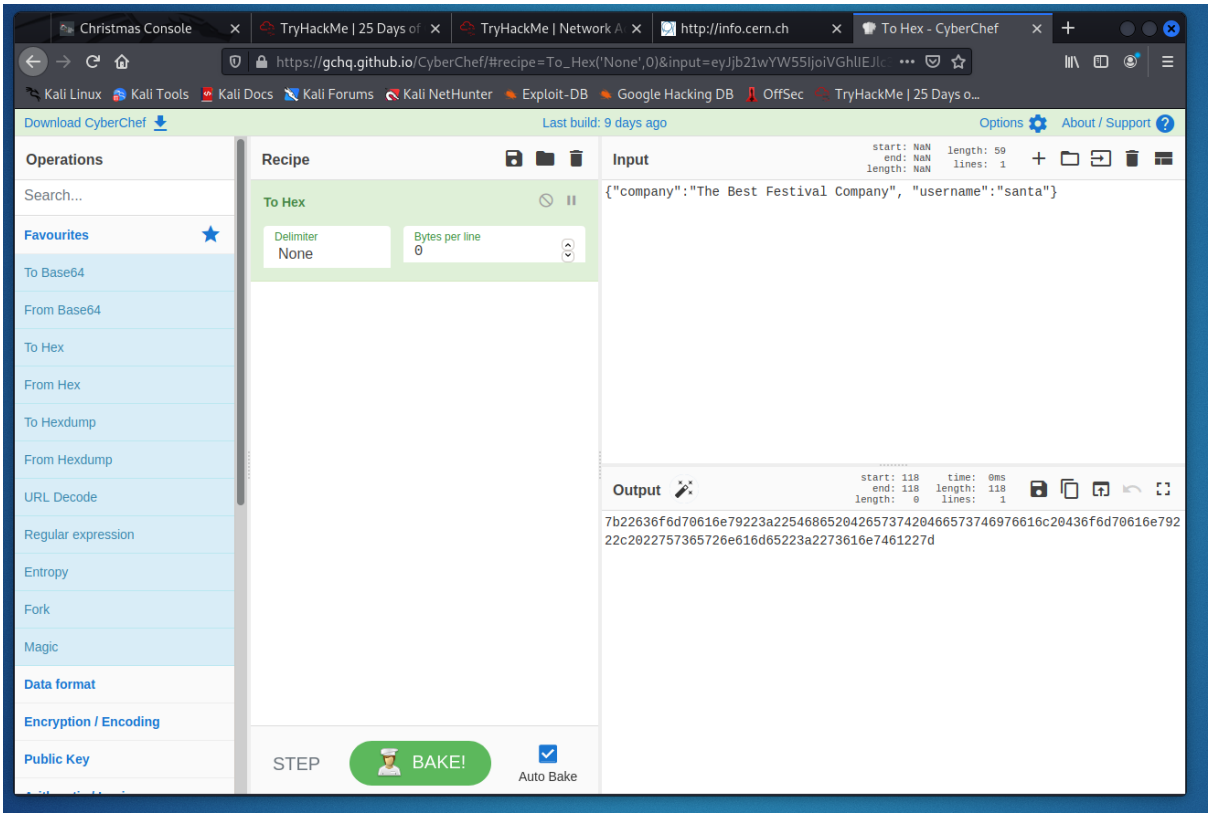
What is the other field found in the cookie?

```
"username":"asdasd"}
```

The other field found in the cookie is username. It is also shown in the decoded hex value in CyberChef.

Question 7

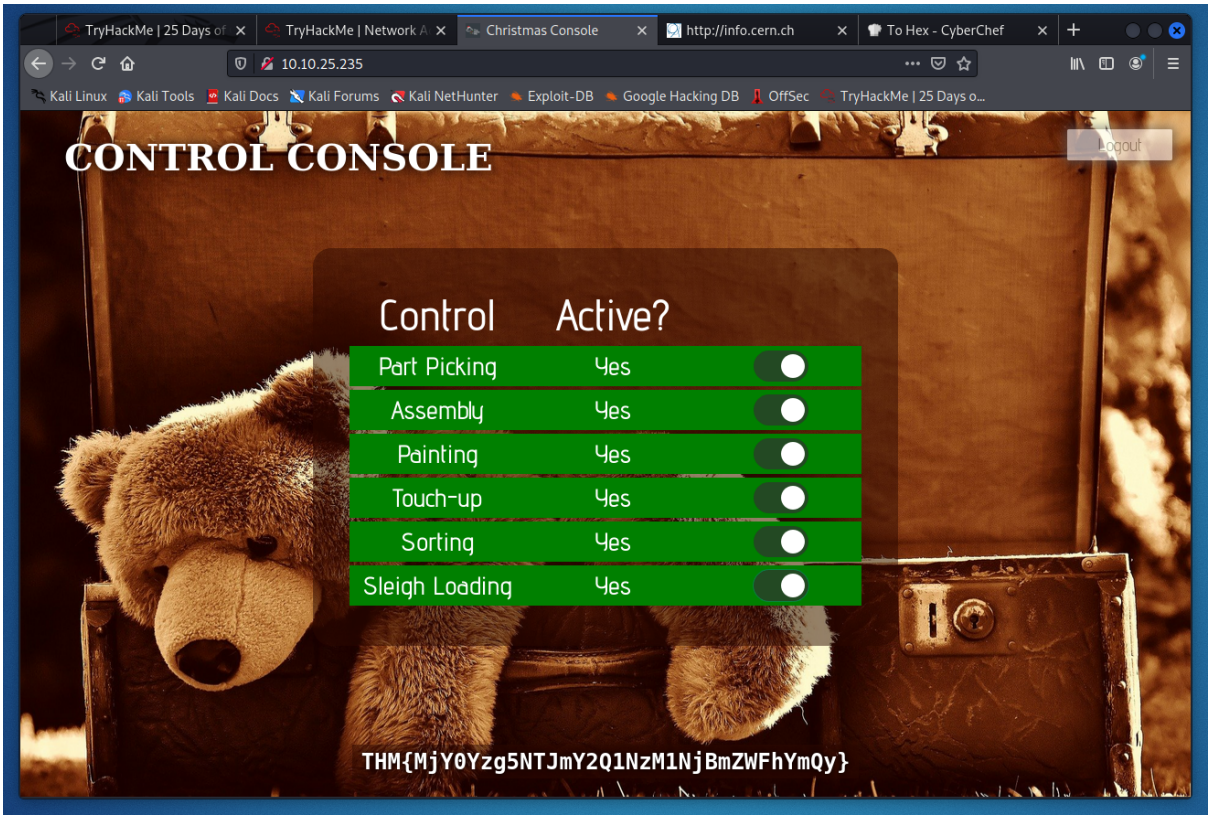
What is the value of Santa's cookie?



In CyberChef, the "To Hex" option is used and the JSON format from the previous cookie value is copied and pasted into the blank space. But instead of having our username in the username field, we replaced it with the word santa. This way, when we encode it back to hex, it will show us the value of Santa's cookie.

Question 8

What is the flag you're given when the line is fully active?



When refreshing the page using Santa's cookie, a control prompt is shown. The flag is acquired by activating all the controls.

Thought Process/Methodology:

When entering the target machine's IP address in the browser, an authentication page is shown. We registered an account and logged in into the website. After logging in, we opened up the browser's developer tools by using the hotkey shortcut Ctrl + Shift + I. We explored the Storage tab in the developer's tools and found the authentication cookie for the website. We inserted the cookie value into CyberChef to find out it was a hexadecimal value. When decoding the hexadecimal value, the result is a line of text showing the company and the username used to login. We deduced that it is in JSON format because of the curly brackets and quotation marks. Using CyberChef, we reused the JSON line and encoded it back to hexadecimal but instead of using our username, we replaced it with santa. We replaced the hexadecimal value with the new one and proceeded to refresh the page. We are now logged in as Santa and have administrator privileges. We activated all the controls and the flag was shown.

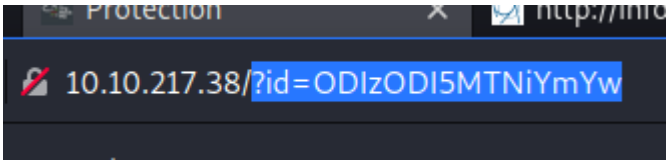
Day 2: Web Exploitation – The Elf Strikes Back!

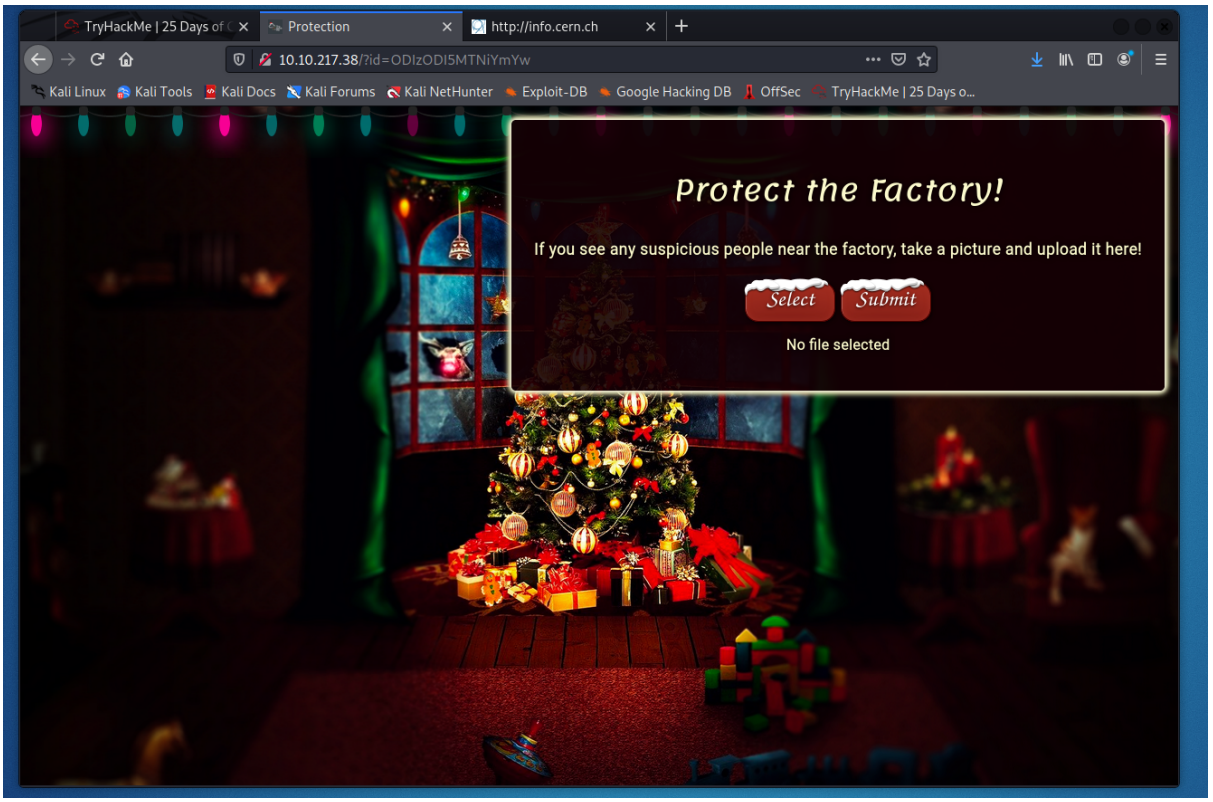
Tools used: Kali Linux, Firefox, Terminal, Nano

Solution/walkthrough:

Question 1

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





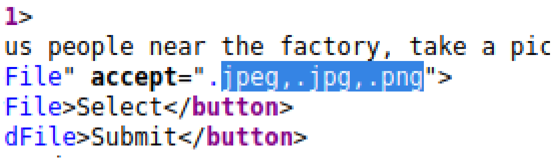
TryHackMe has provided an ID for us. We used a GET Parameter by putting a question mark in the URL with the parameter name of "id" with the value of the ID given after it. So it goes like this:

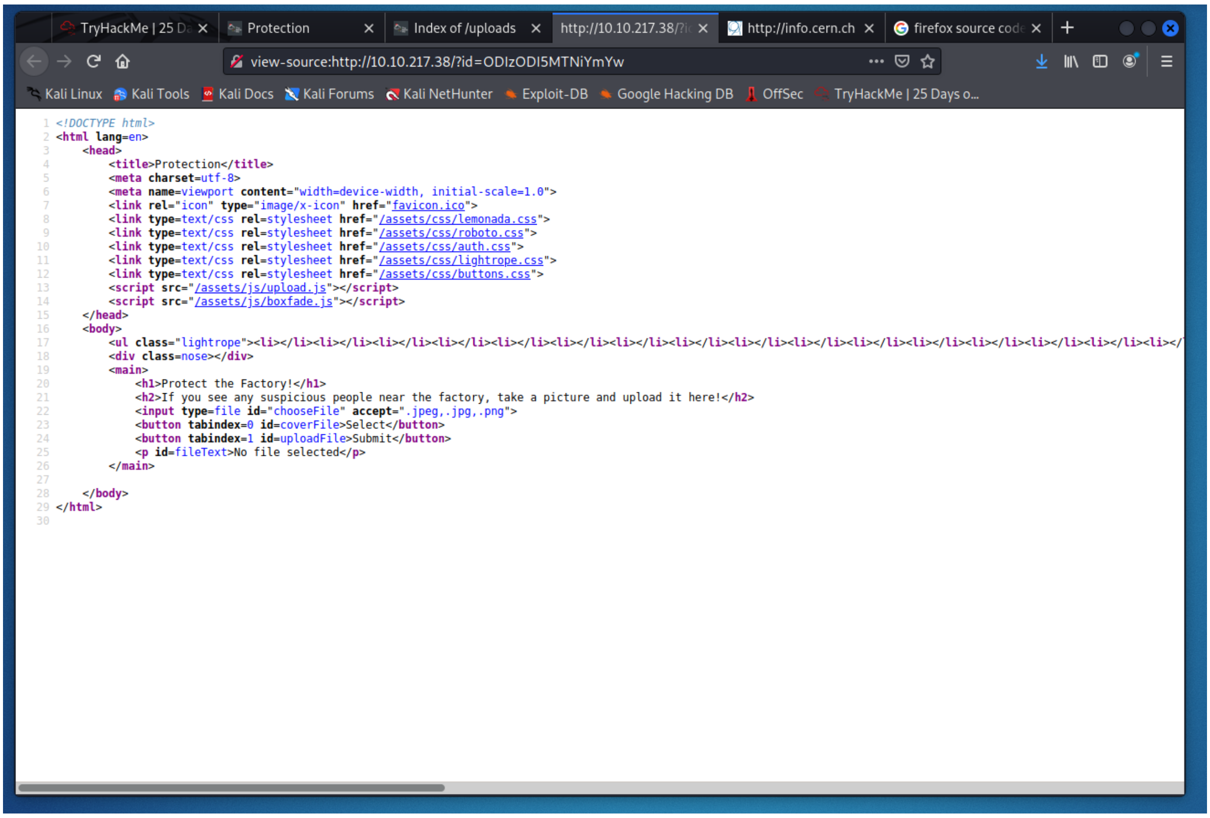
?=ODIz0DI5MTNiYmYw

which allows us to access the website.

Question 2

What type of file is accepted by the site?

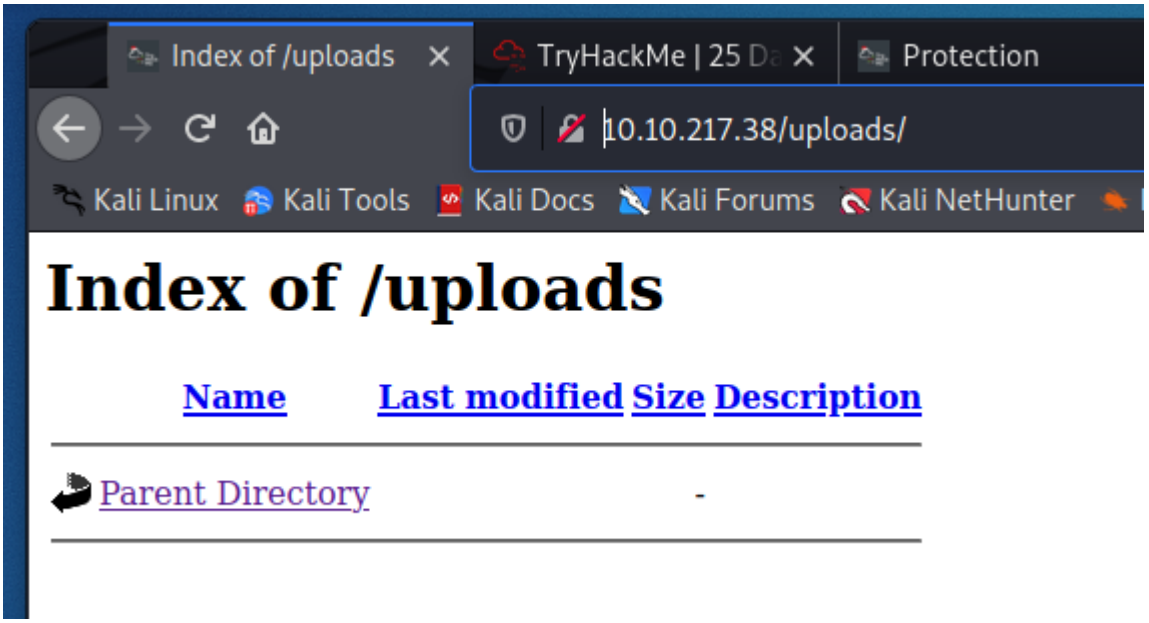




By right clicking on the website, we are able to view the page source. With this, we are able to note that the website only accepts files with ".jpeg", ".jpg" and ".png" in their names which means that the website only accepts images.

Question 3

In which directory are the uploaded files stored?



We tried a trial and error method by trying many different common directories: /images, /resources, /uploads, etc. and /uploads was the correct directory for the storage of uploaded files.

Question 4

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

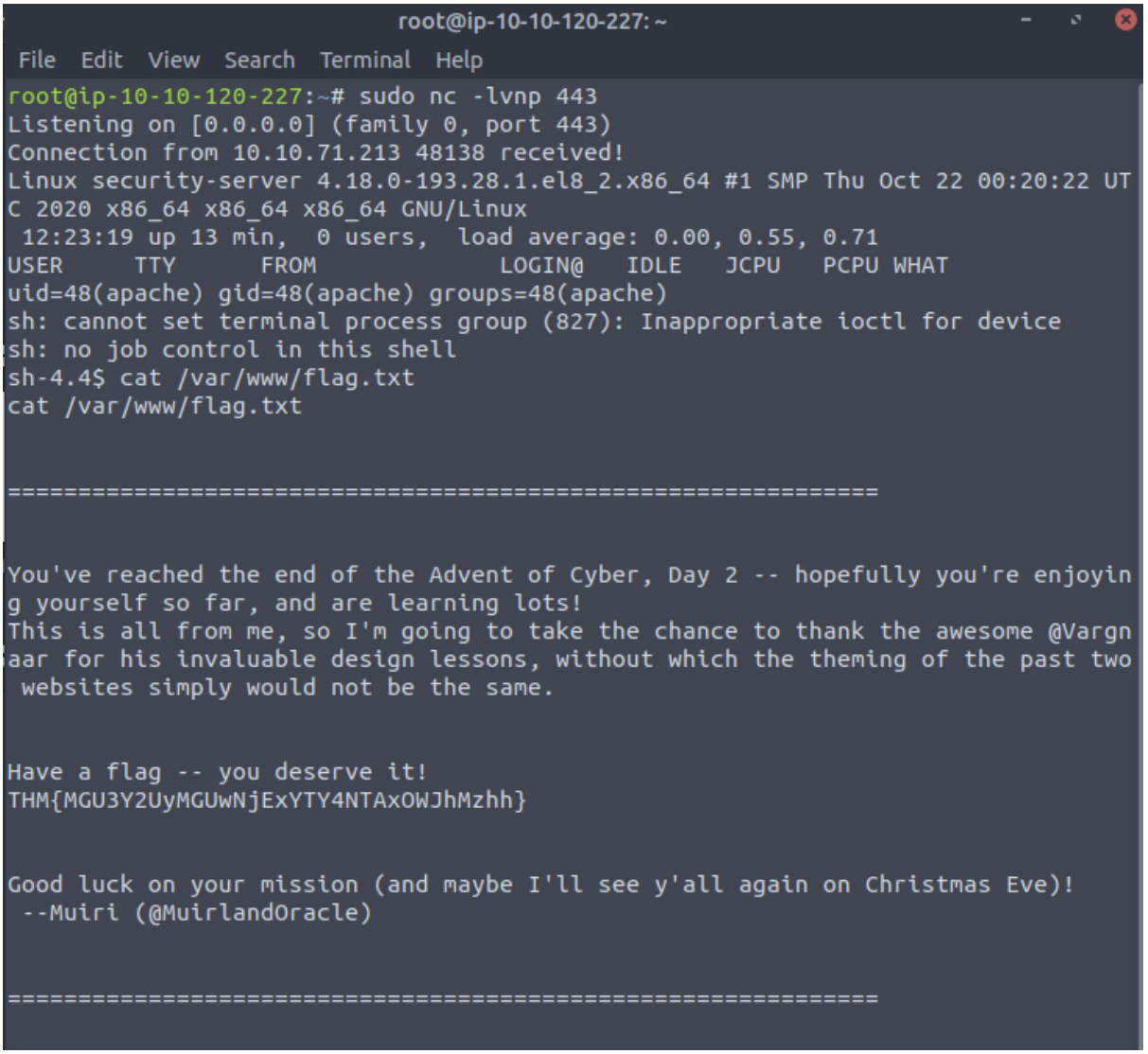
	l	v	n	p
Used to specify that nc should listen for an incoming connection rather than initiate a connection to a remote host.	◉	○	○	○
Specifies the source port nc should use, subject to privilege restrictions and availability.	○	○	○	◉
Do not do any DNS or service lookups on any specified addresses, hostnames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

We read up about the parameters for netcat online and obtained information regarding the use of many different netcat parameters which are -l, -v, -n and -p.

Information from: https://www.varonis.com/blog/netcat-commands/

Question 5

What is the flag in /var/www/flag.txt?



We used a reverse shell provided in the AttackBox. We changed the IP address and the port of the reverse shell to the IP address of the AttackBox and the port 443. We renamed the reverse shell file from php-reverse-shell.php to php-reverse-shell.jpeg.php so it is accepted by the website as there is ".jpeg" in the file name. After that, we opened the terminal and used netcat to listen to the reverse shell at port 443. The command line we typed was "sudo nc -lvnp 443". We then clicked on the reverse shell in the uploads directory of the website. We are now able to read the contents of the flag.txt file by using the command line "cat /var/www/flag.txt". The flag shown was

THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}

Thought Process/Methodology:

We used the ID given by THM in a GET Parameter in the URL of the website to access the website and we are prompted with a screen to upload files. We tried many different directories by putting common ones in the URL and we found out that it is /uploads. We viewed the page source and found out that the website only accepts image file types. With that information, we used a reverse shell and edited the IP address similar to the AttackBox's and changed the port to 443. After that, we renamed the reverse shell to include .jpeg in the file name so it is accepted by the website. After uploading the reverse shell, we opened up the terminal to activate the netcat listener. We then opened the uploads directory and clicked on the reverse shell. The netcat listener in the terminal then received a response from the reverse shell from the website. We are then able to read the contents of the flag by using the cat command line which was "cat /var/www/flag.txt".

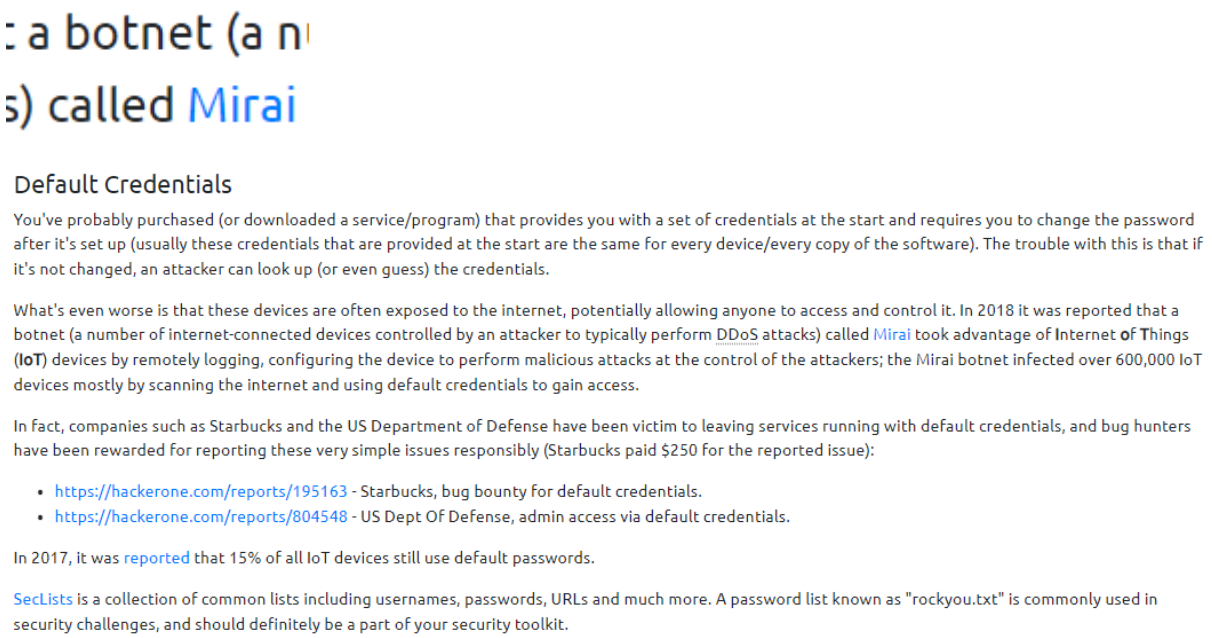
Day 3: Web Exploitation – Christmas Chaos

Tools used: Kali Linux, Firefox, FoxyProxy, Burpsuite

Solution/walkthrough:

Question 1

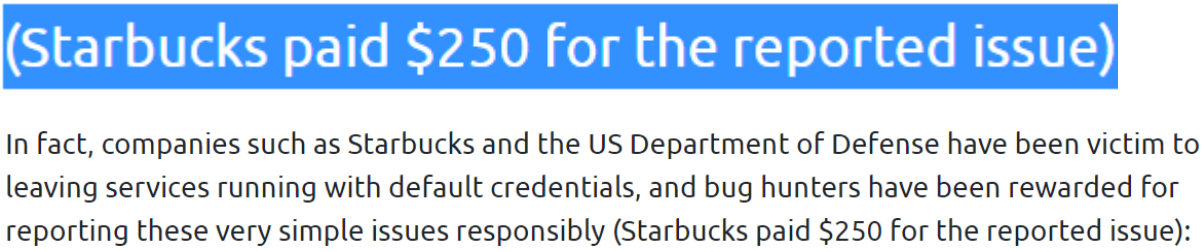
What is the name of the botnet mentioned in the text that was reported in 2018?



The name of the botnet mentioned in the text is called Mirai as shown in the image above.

Question 2

How much did Starbucks pay in USD for reporting default credentials according to the text?



Starbucks paid 250 USD for reporting default credentials according to the text as shown in the image above.

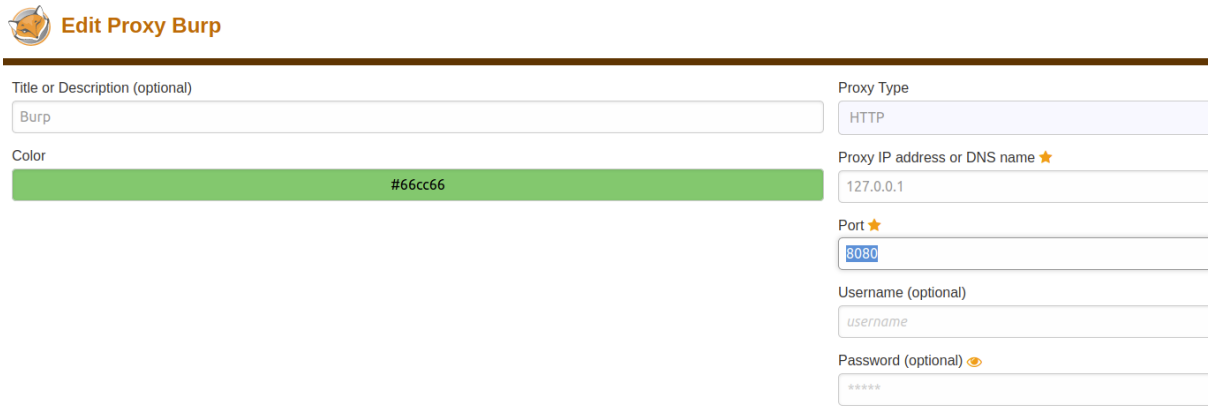
Question 3

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

The name of the agent that disclosed the report on June 25th is ag3nt-j1 as shown in the image above.

Question 4

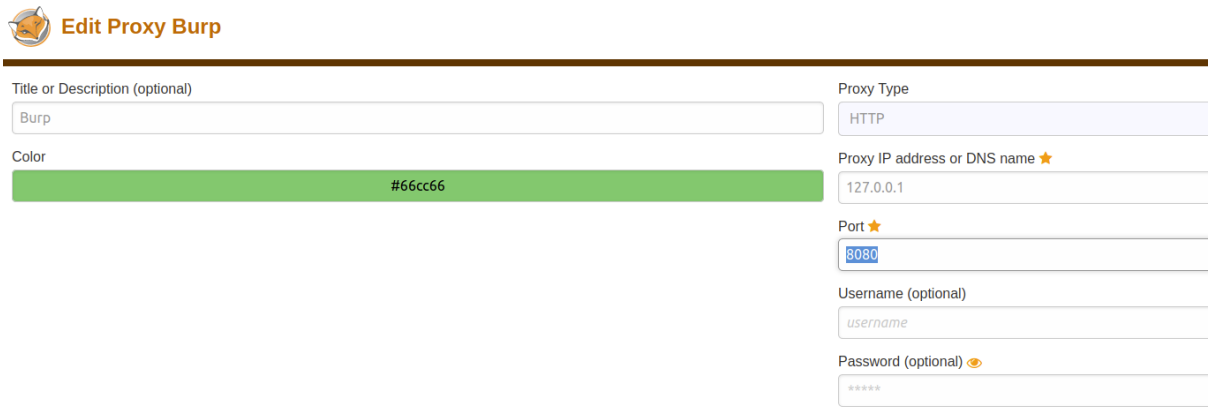
Examine the options on FoxyProxy on Burp. What is the port number for Burp?



Press Edit Proxy Burp in FoxyProxy. The port number for Burp is 8080.

Question 5

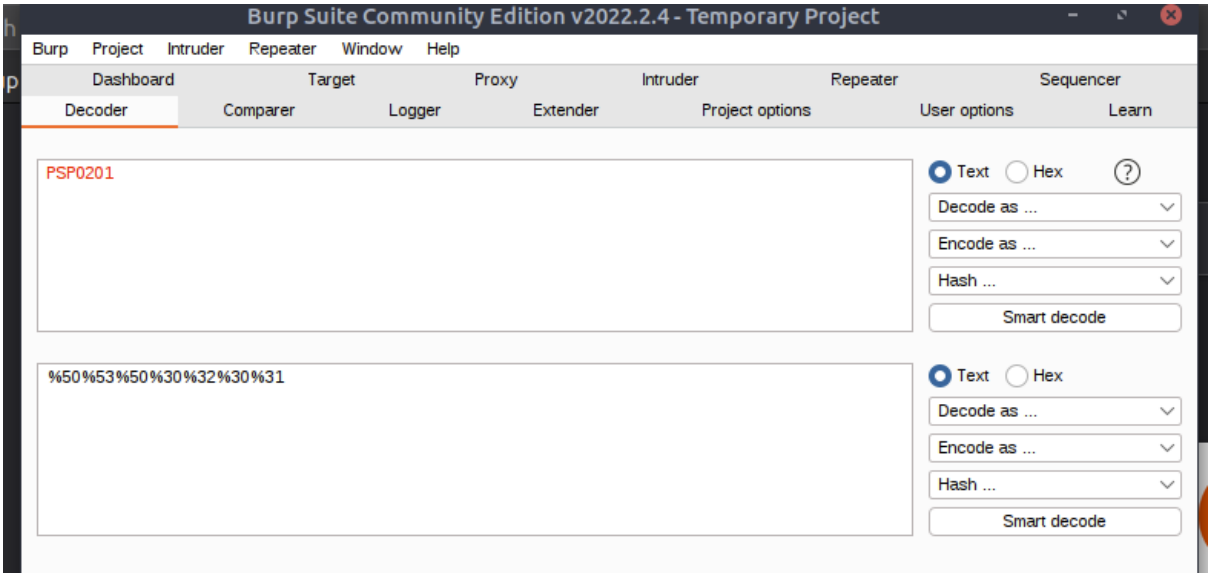
Examine the options on FoxyProxy on Burp. What is the proxy type?



Press Edit Proxy Burp in FoxyProxy. The proxy type of FoxyProxy on Burp is HTTP.

Question 6

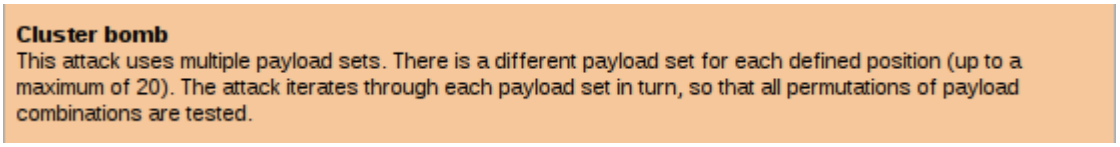
Experiment with decoder on Burp. What is the URL encoding for "PSP0201"?



In BurpSuite, select “Decoder” and key in “PSP0201”, under “Encode as”, select URL to get the encoded text.

Question 7

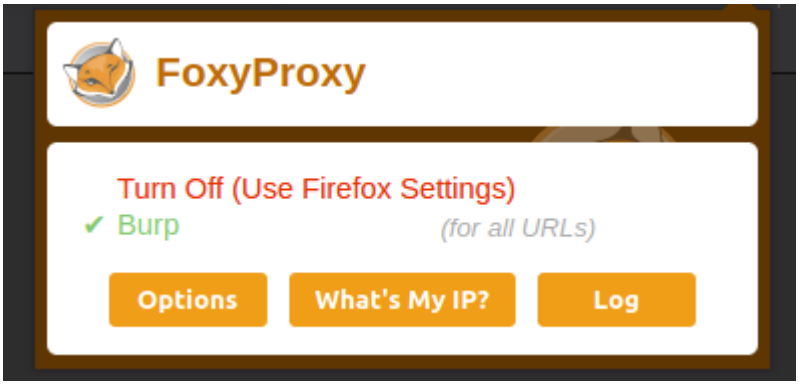
Look at the list of attack type options on intruder. Which of the following options matches the one in the description?

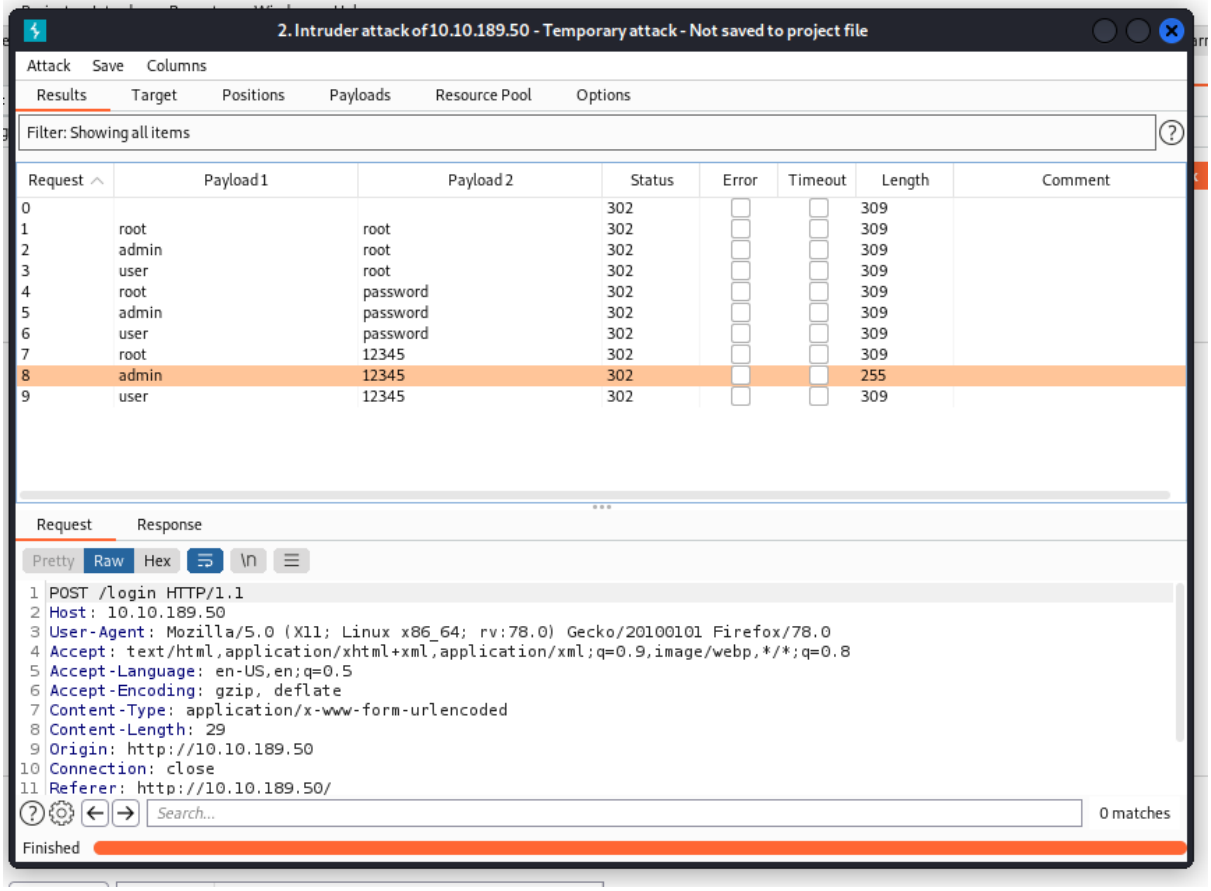


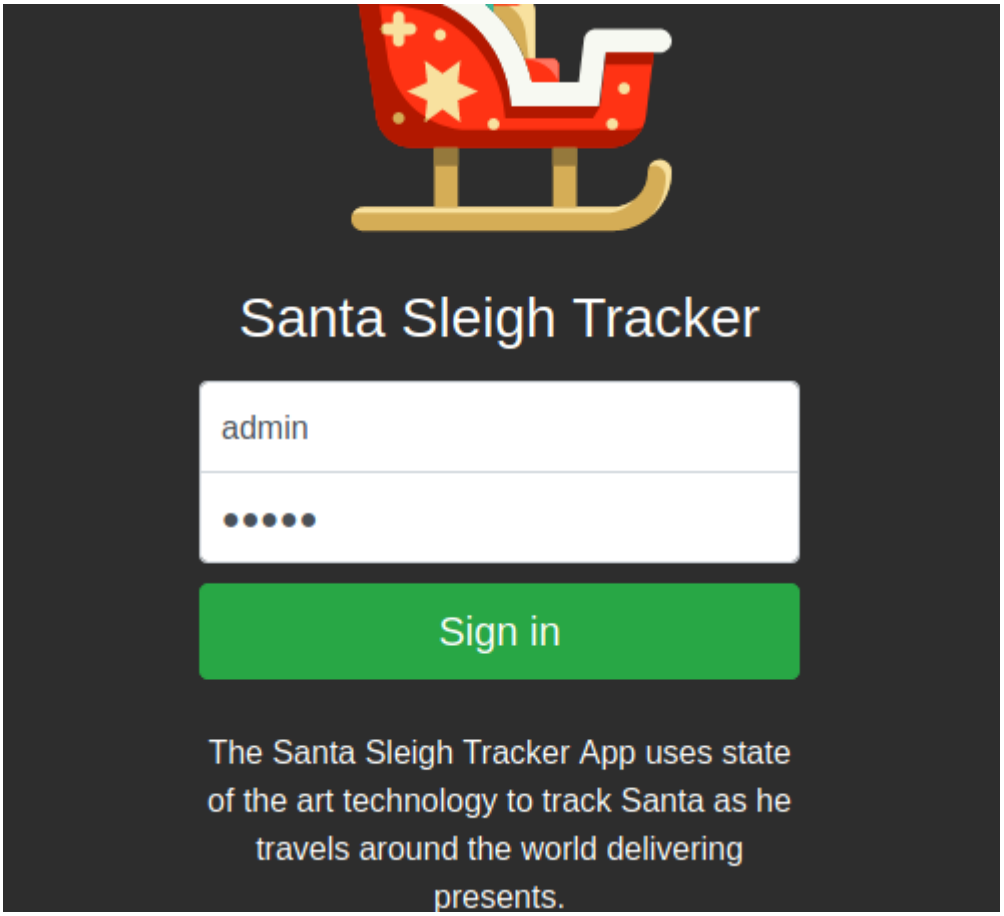
Click on the drop down list of attack types. The cluster bomb attack type matches the one in the description.

Question 8

What is the flag?




2. Intruder attack of 10.10.189.50 - Temporary attack - Not saved to project file
Attack
Save
Columns
Results
Target
Positions
Payloads
Resource Pool
Options
Filter: Showing all items
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
Request
Response
Pretty
Raw
Hex
\n
1 POST /login HTTP/1.1
2 Host: 10.10.189.50
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://10.10.189.50
10 Connection: close
11 Referer: http://10.10.189.50/
Search...
0 matches
Finished


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

We opened up the website given to us by THM and were prompted with a login page. We then opened BurpSuite. We burped the website using the FoxyProxy browser extension. In the Proxy tab in BurpSuite, and clicked on the "Intercept is on" button. After that, we forwarded the proxy to let the webpage load. We then filled in a random username and password and tried to login. Now, the proxy in BurpSuite shows the username and password we typed. We then send the proxy to the Intruder tab. In the positions tab in the Intruder section, we added the selected positions for the attack and chose the Cluster bomb attack type. At the payloads tab, we selected our payload sets. In set 1 which is the username set, we added the list of common usernames and in set 2 which is the password set, we added the list of common passwords. Then we proceeded to start the attack. BurpSuite tried every combination between the 2 sets and only one combination gave a different output. The different output produced used the correct username and password and we were able to login to the website. Then, the flag was shown after logging in, which was

THM{885ffab980e049847516f9d8fe99ad1a}

Thought Process/Methodology:

We used the FoxyProxy browser extension to relay the webpage proxy to BurpSuite. We tested the login by putting a random username and password in the webpage which changed the proxy in BurpSuite. We then sent the proxy to the Intruder tab. Using the cluster bomb attack type, we added

a set of different usernames and a set of different passwords so that BurpSuite can try every combination. We then proceeded to attack and the results show one different outcome which showed the correct login credentials. We logged into the website and obtained the flag.

Day 4: Web Exploitation – Santa's watching

Tools used: Kali Linux, Firefox, Terminal, wfuzz, gobuster

Solution/walkthrough:

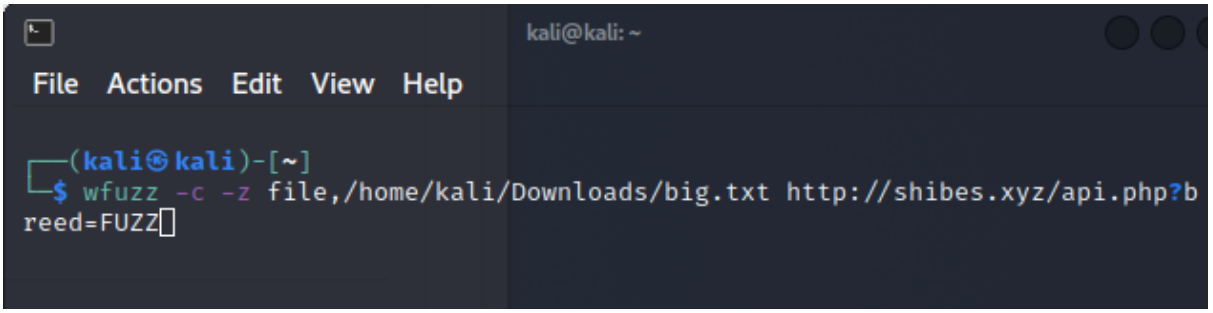
Question 1

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)

Q1: 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) * 5 points

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

	[a]	[b]	[c]	[d]	[e]
breed	○	○	○	○	◉
shibes	○	○	◉	○	○
big.txt	○	◉	○	○	○
wfuzz	◉	○	○	○	○
php	○	○	○	◉	○



The entire wfuzz command would be

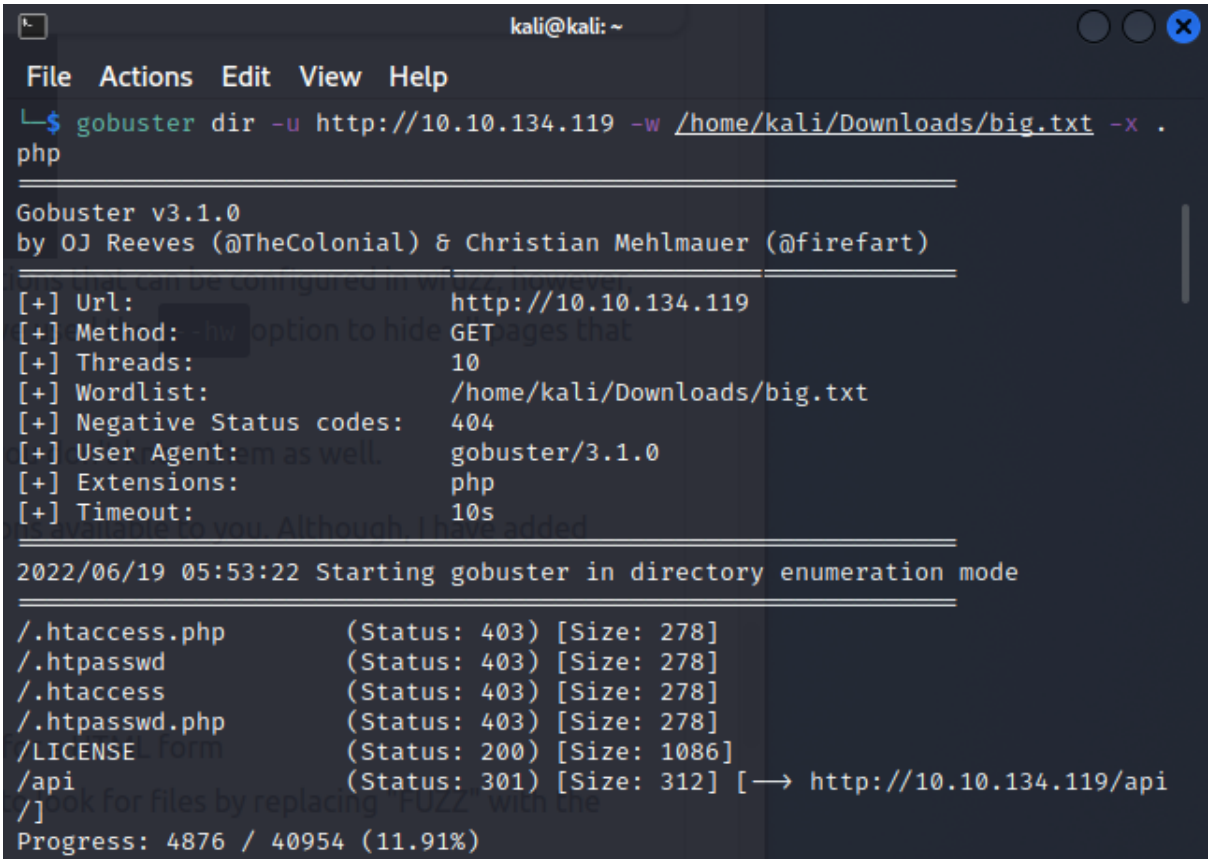
wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ

The -c parameter shows the output in colour, the -z parameter tells wfuzz to replace the word “FUZZ” with the words located in the file right after it (in this case it is the big.txt wordlist). Then follows the

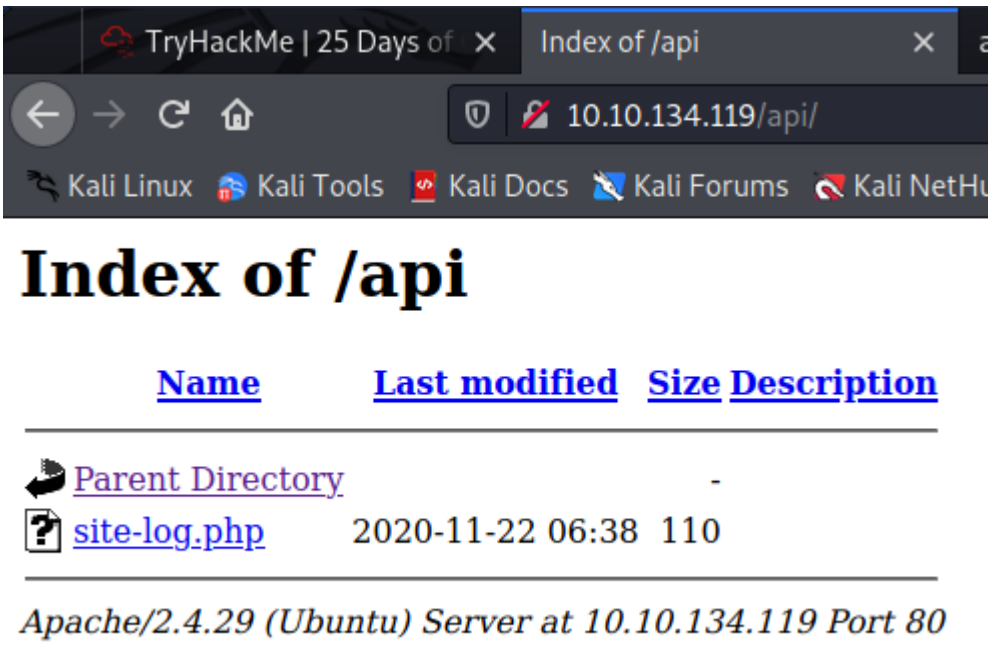
URL of the website with a breed query. (?breed=FUZZ)

Question 2

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



Run GoBuster command in the terminal with big.txt as the wordlist, after a few minutes of progress, it returns “/api” which turns out to be the API directory address.

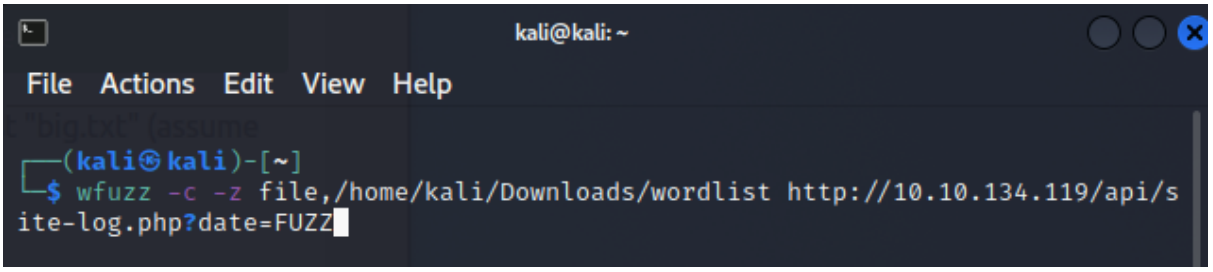


Navigated to the API Directory from the GoBuster results to find the answer.

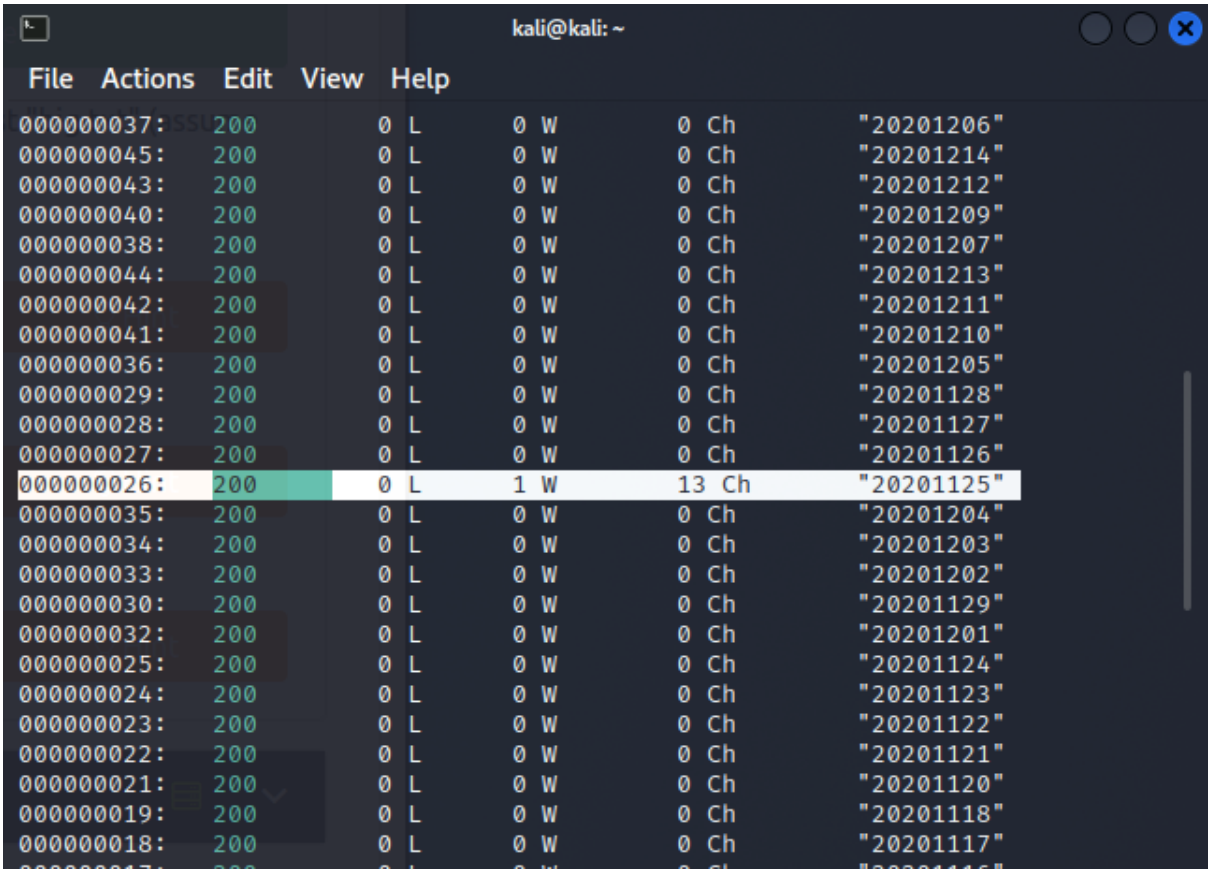
The file stored in the API directory is site-log.php

Question 3

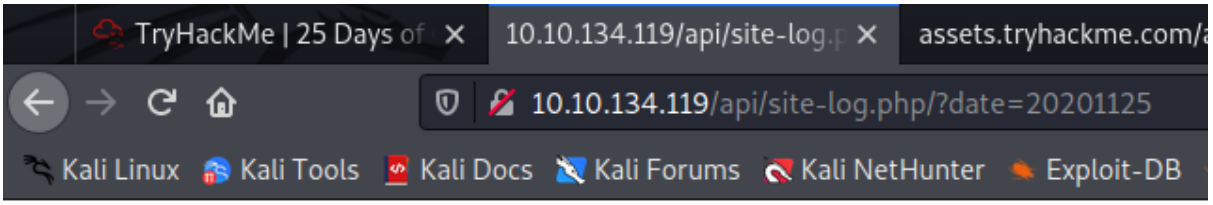
Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?



Run the wfuzz command with another wordlist (provided by THM or included with attackbox) containing a list of dates together with the address of the API Directory to look for the correct date.



Many entries are shown and they all share the same outputs except for one of them. The one with the different output is expected to be the correct date.

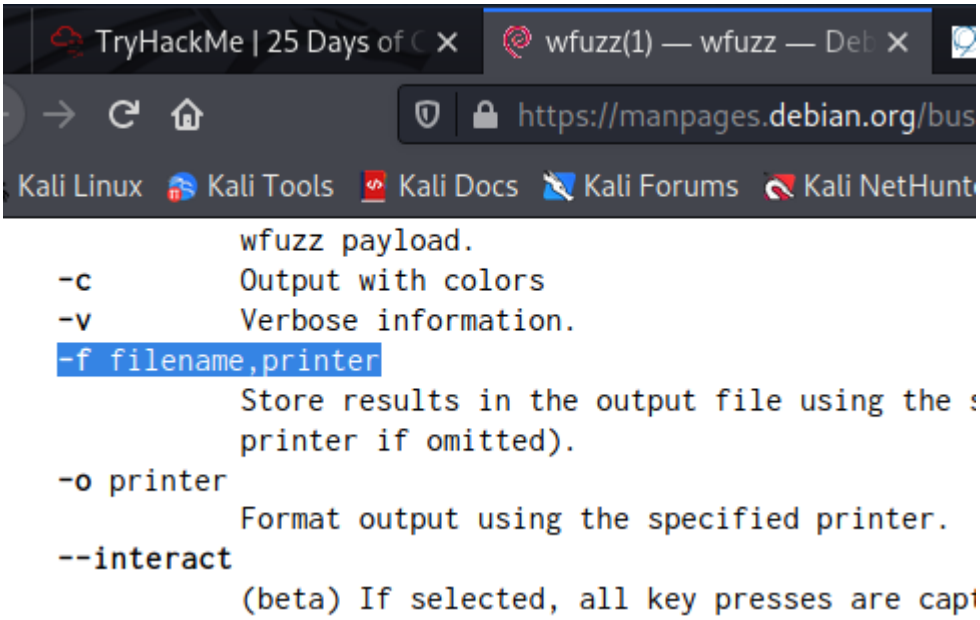


THM{D4t3_AP1}

The date value is then entered into the URL as a GET Parameter for the date query and the flag is shown. The flag is THM{D4t3_AP1}.

Question 4

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



In the manpage, it is stated that the wfuzz -f parameter stores the results in the file named after it.

Thought Process/Methodology:

Firstly, we used the gobuster dir command line to find the API directory using big.txt wordlist and the results show that one of the directories are /api. We navigated to the directory by adding /api in the URL to find a file in it (site-log.php). After that, we used a wfuzz command line with the wordlist given by THM on the site-log.php file to find the date. We eliminated the entries that showed similar output by the wfuzz command and found only one different output. We used the value of the different output as a GET parameter with the date query and added it to the URL. The flag is then shown.

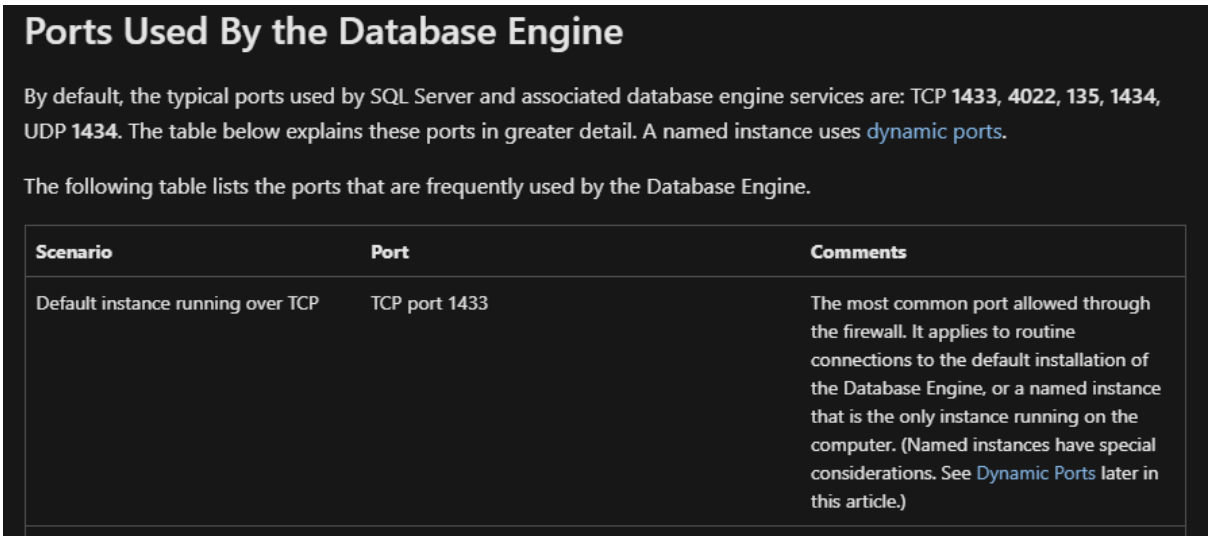
Day 5: Web Exploitation – Someone stole Santa's gift list!

Tools used: Kali Linux, Firefox, FoxyProxy, Burpsuite, sqlmap

Solution/walkthrough:

Question 1

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



Ports Used By the Database Engine

By default, the typical ports used by SQL Server and associated database engine services are: TCP **1433**, **4022**, **135**, **1434**, UDP **1434**. The table below explains these ports in greater detail. A named instance uses dynamic ports.

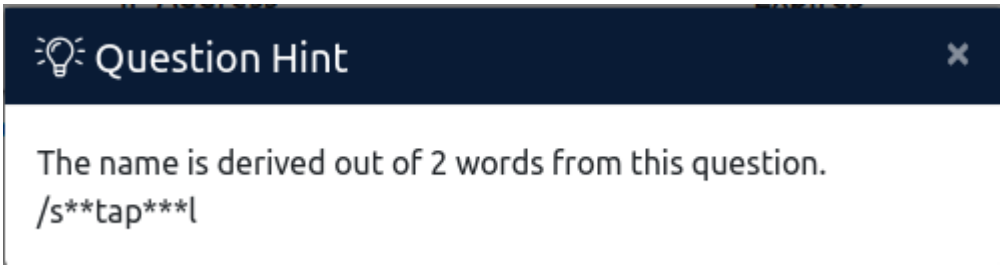
The following table lists the ports that are frequently used by the Database Engine.

Scenario	Port	Comments
Default instance running over TCP	TCP port 1433	The most common port allowed through the firewall. It applies to routine connections to the default installation of the Database Engine, or a named instance that is the only instance running on the computer. (Named instances have special considerations. See Dynamic Ports later in this article.)

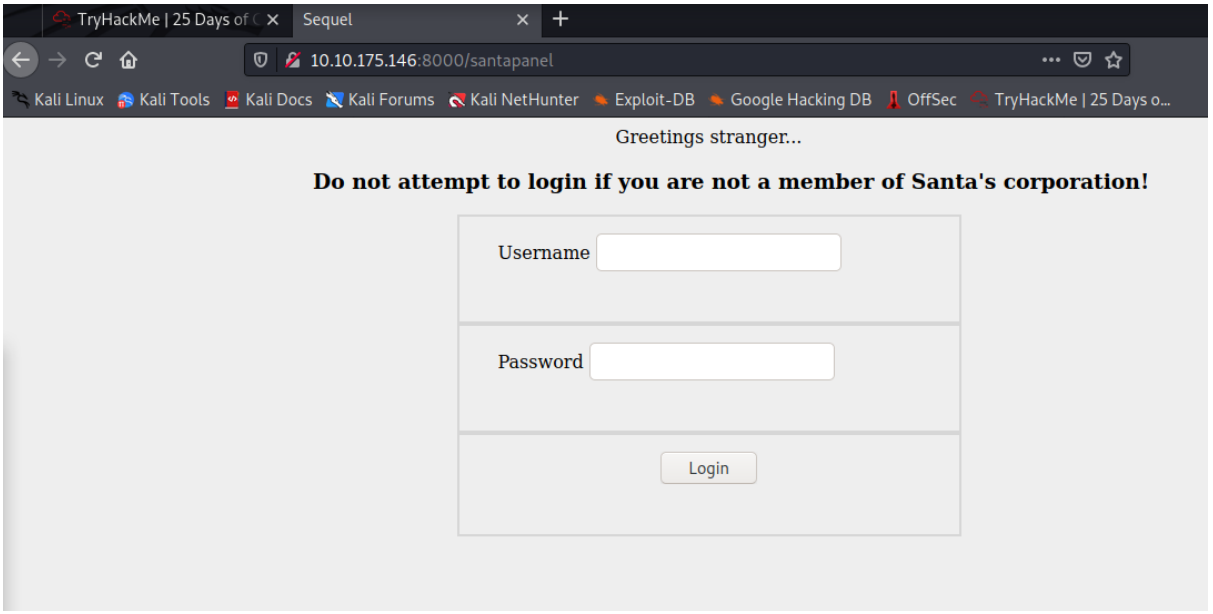
The default port used by SQL server running on TCP is 1433 as stated by Microsoft's documentation.

Question 2

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



what's Santa's secret login panel?



By looking at the hint for the question, we conclude that the directory for Santa's secret login panel is /santapanel.

Question 3

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

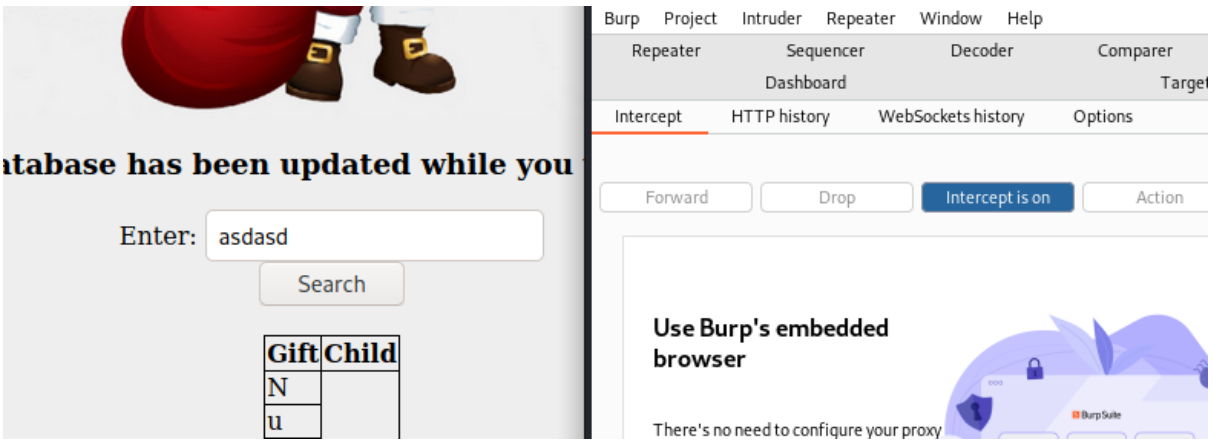
Santa reads some documentation that he wrote when setting up the application, it reads:

Santa's TODO: Look at alternative database systems that are better than sqlite. Also, don't forget that you installed a Web Application Firewall (WAF) after last year's attack. In case you've forgotten the command, you can tell SQLMap to try and bypass the WAF by using `--tamper=space2comment`

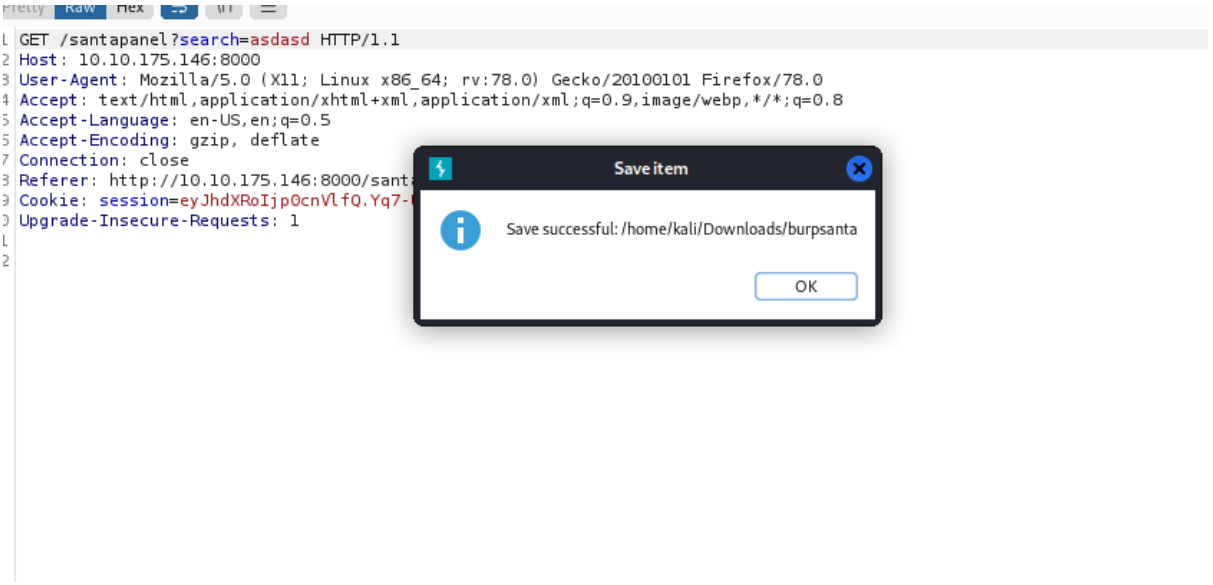
Question 4

How many entries are there in the gift database?

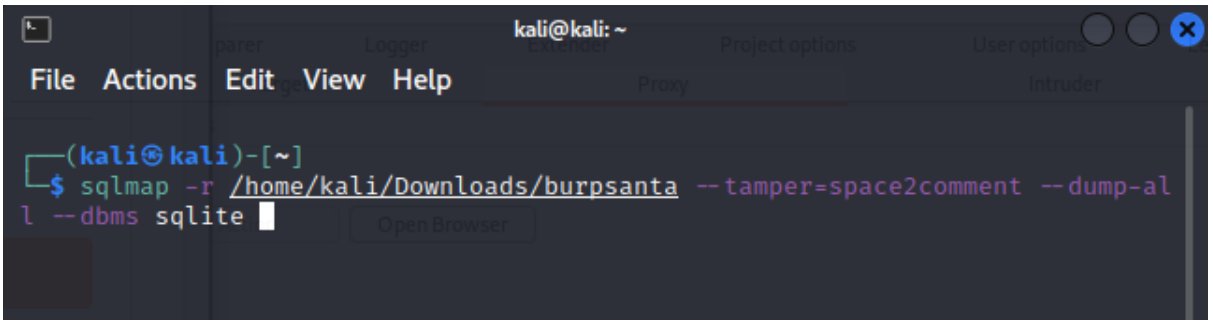
Login bypass with SQL injection



Use FoxyProxy and Burp to intercept the http connection



Save the proxy after intercept



Enter the command to request SQLMap “sqlmap -r filename” together with “--tamper=space2comment” to bypass the installed WAF, “--dump-all” to dump the entire database, and “--dbms” to tell sqlmap the type of database that is running. The result shows us all the information needed.

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

In the results, it shows a table, ”sequels” with 22 entries, which is the answer to this question.

Question 5

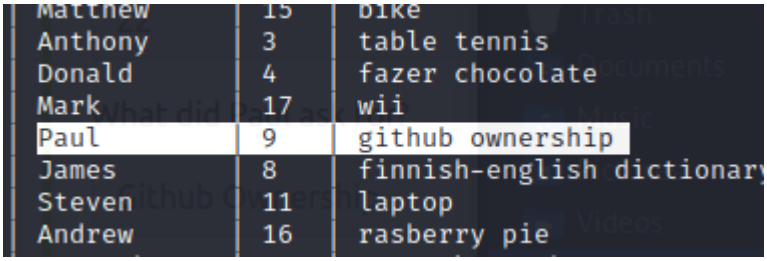
What is James' age?

```
| 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                 |
```

James’ age can be found in the table

Question 6

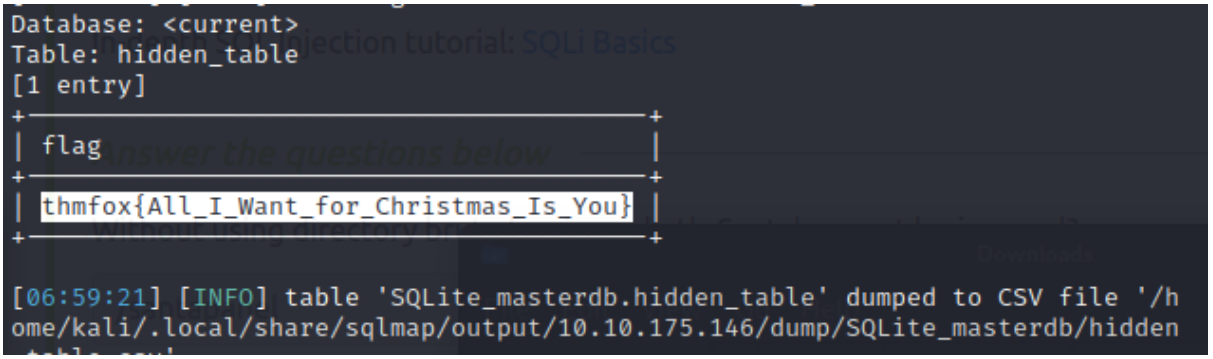
What did Paul ask for?



The answer is found in the table.

Question 7

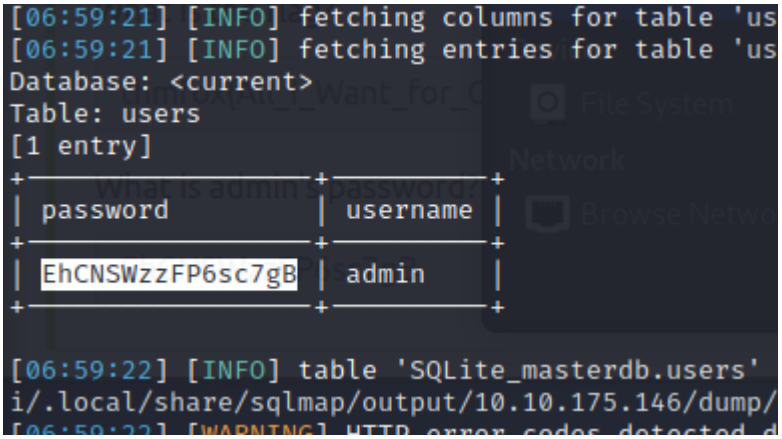
What is the flag?



Another table, named “hidden_table” has the flag.

Question 8

What is the admin's password?



“users” contains the username and password of admin.

Thought Process/Methodology:

After correctly guessing the directory for Santa's secret login panel, we were greeted with a login page. We followed the instructions in THM and used SQL Injection to log into santa's site. We then used Burp with Foxyproxy to save the intercept into our attackbox/kali linux. We ran the sqlmap command in the terminal with "--tamper=space2comment" to bypass the installed WAF, "--dump-all" to dump the entire database, and "--dbms" to tell sqlmap the type of database that is running. The result shows us all the information needed. All we had to do then was look for the answers based on the questions given.