PSP0201

Week 2

Writeup

Group Name: DNA

Members

ID	Name	Role
1211102532	DHARVIN SHAH KUMAR BIN MOHAMAD SHAH RAVIN	Leader
1211101179	ALIPH RAIHAN BIN ANUAR	Member
1211102427	NUR NATHIFA BINTI MOHD IZHAR	Member

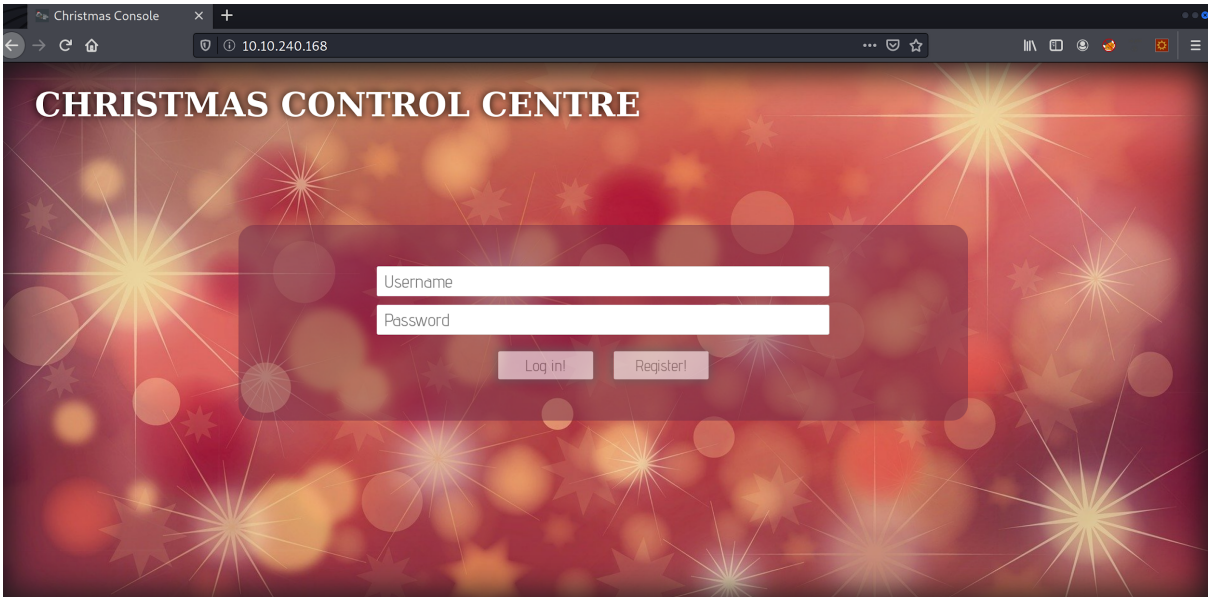
Day 1: Web Exploitation – A Christmas Crisis

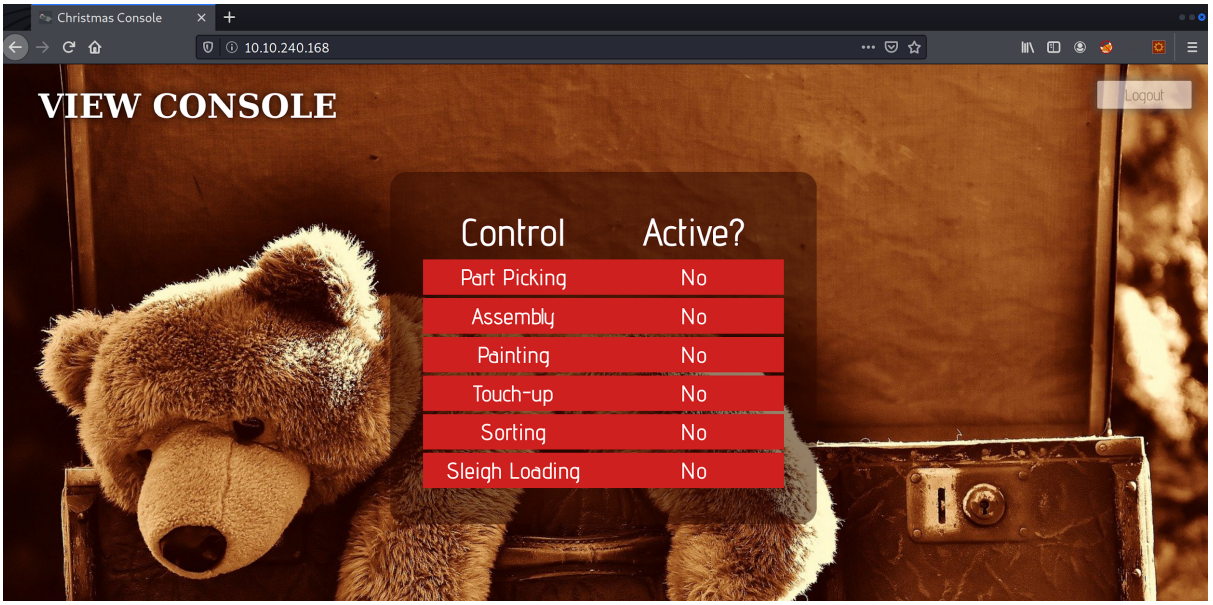
Tools used: Attackbox, Firefox

Solution/walkthrough:

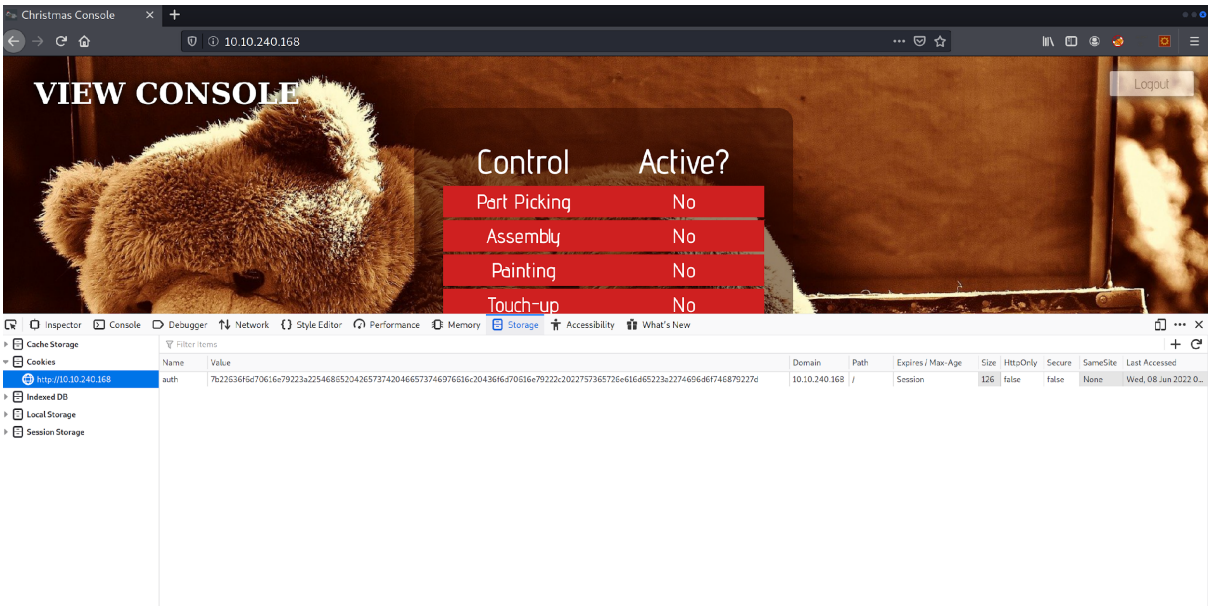
Question 1

Registration and logging in to the Christmas Control Centre. No access to the control console.



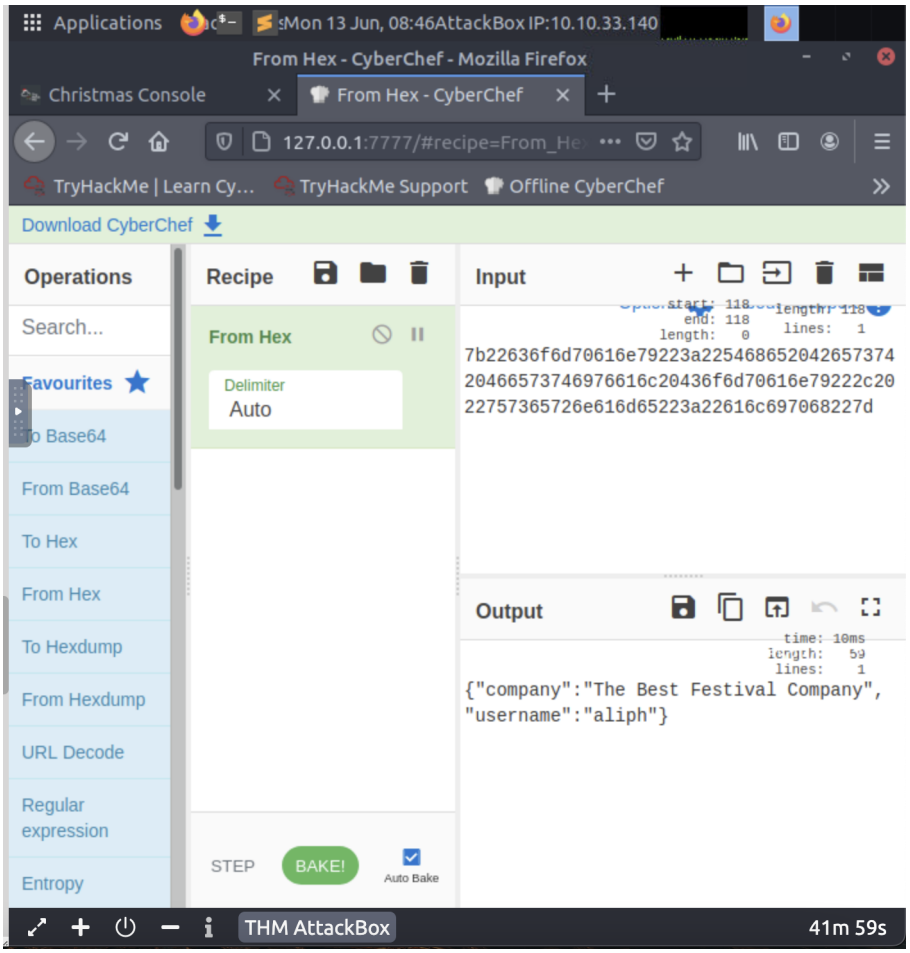


Opening up the browser developer tools to check on the cookie.



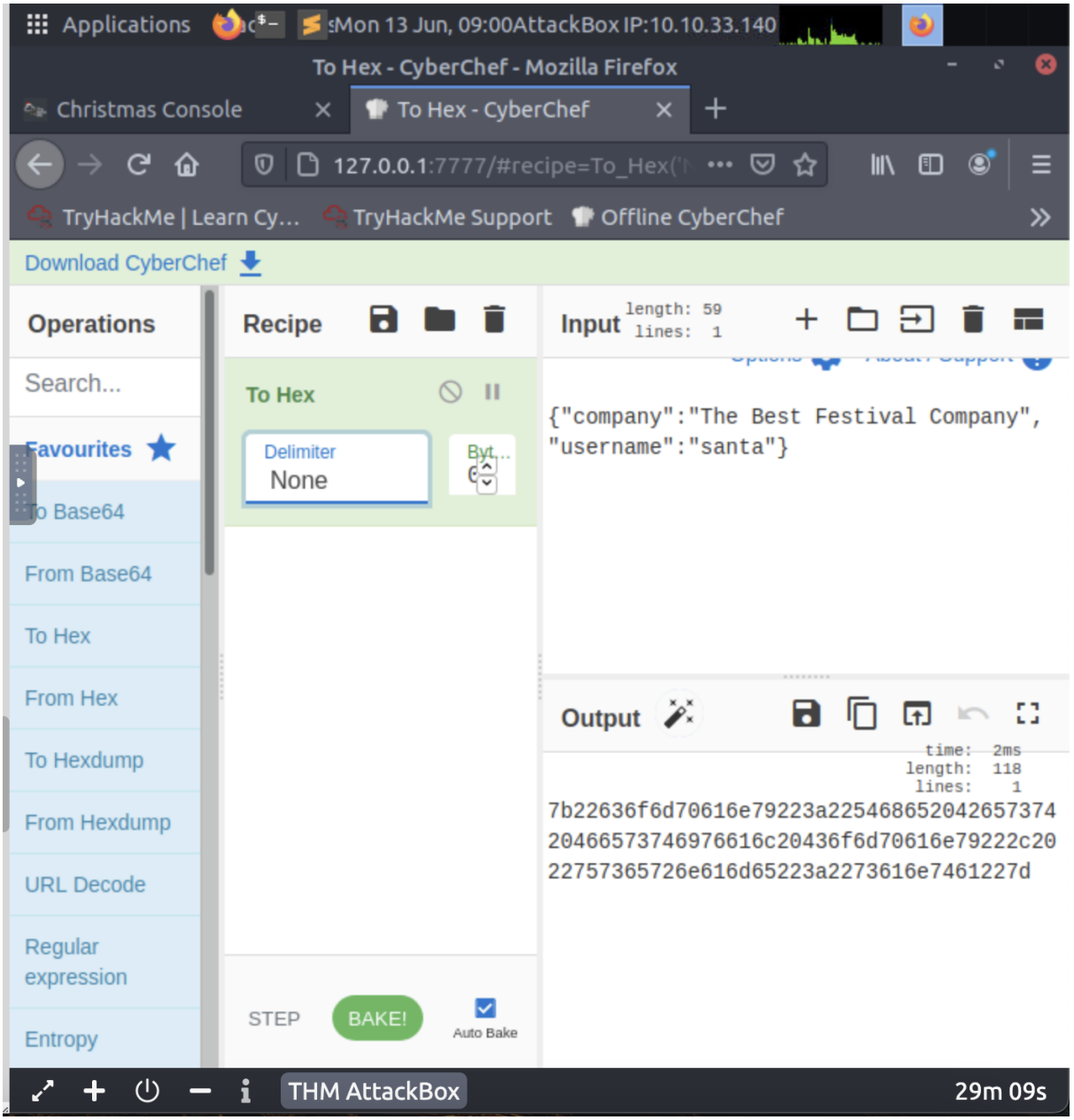
Question 2

Obtain the value of the cookie.



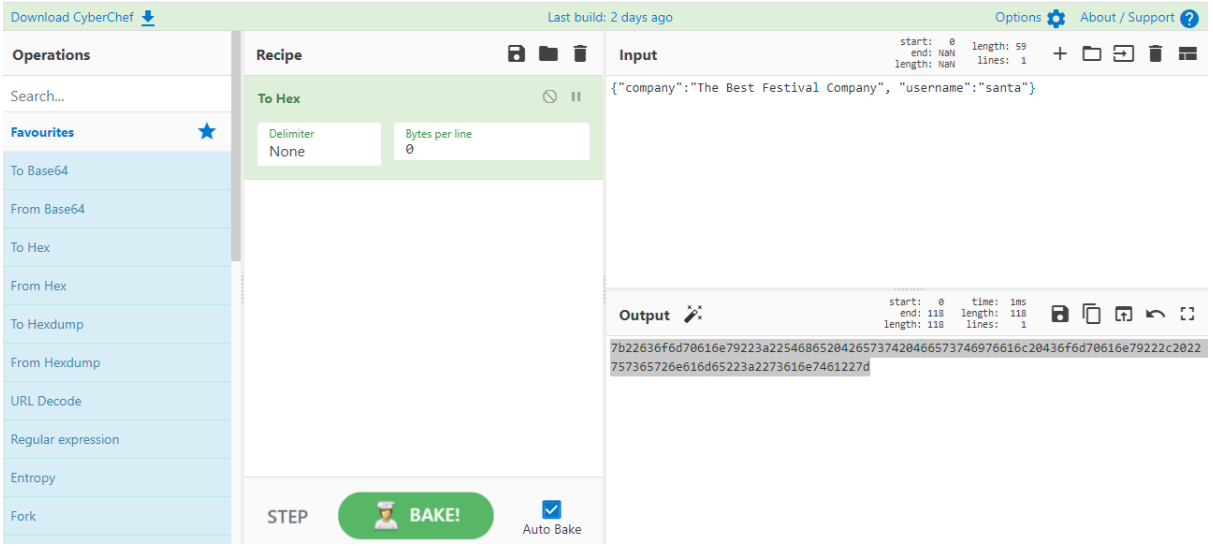
Question 3

Using Cyberchef, convert the cookie value to string.



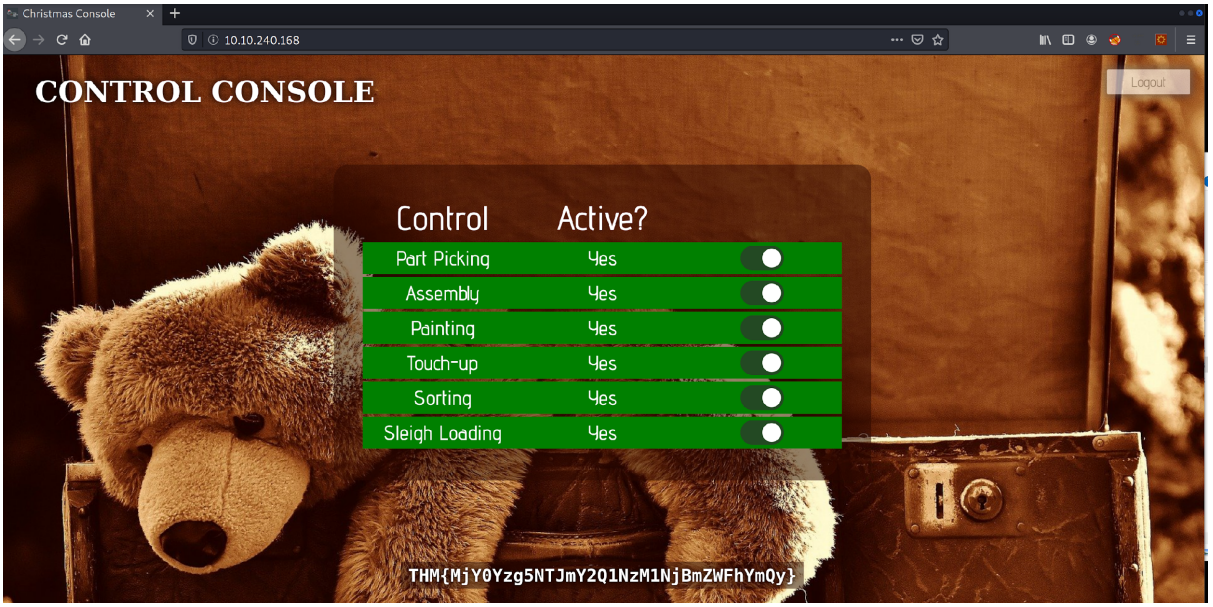
Question 4

Changing the username to ‘santa’, convert the JSON statement to hex.



Question 5

Now having access to the controls, switching on every control shows the flag.



Thought Process/Methodology:

Having accessed the target machine, we were shown a login/registration page. We proceeded to register an account and login. After logging in, we open the browser's developer tool and chose to view the site cookie from the Storage tab. Looking at the cookie value, we deduced it to be a hexadecimal value and proceeded to convert it to text using Cyberchef. We found a JSON statement with the username element. Using Cyberchef, we altered the username to 'santa', the administrator account, and converted it back to hexadecimal using Cyberchef. We replaced the cookie value with converted one and refreshed the page. We are now show an administrator page (Santa's) and proceeded to enable every control, which in turn showed the flag.

Day 2: Web exploitation - The Elf Strikes Back!

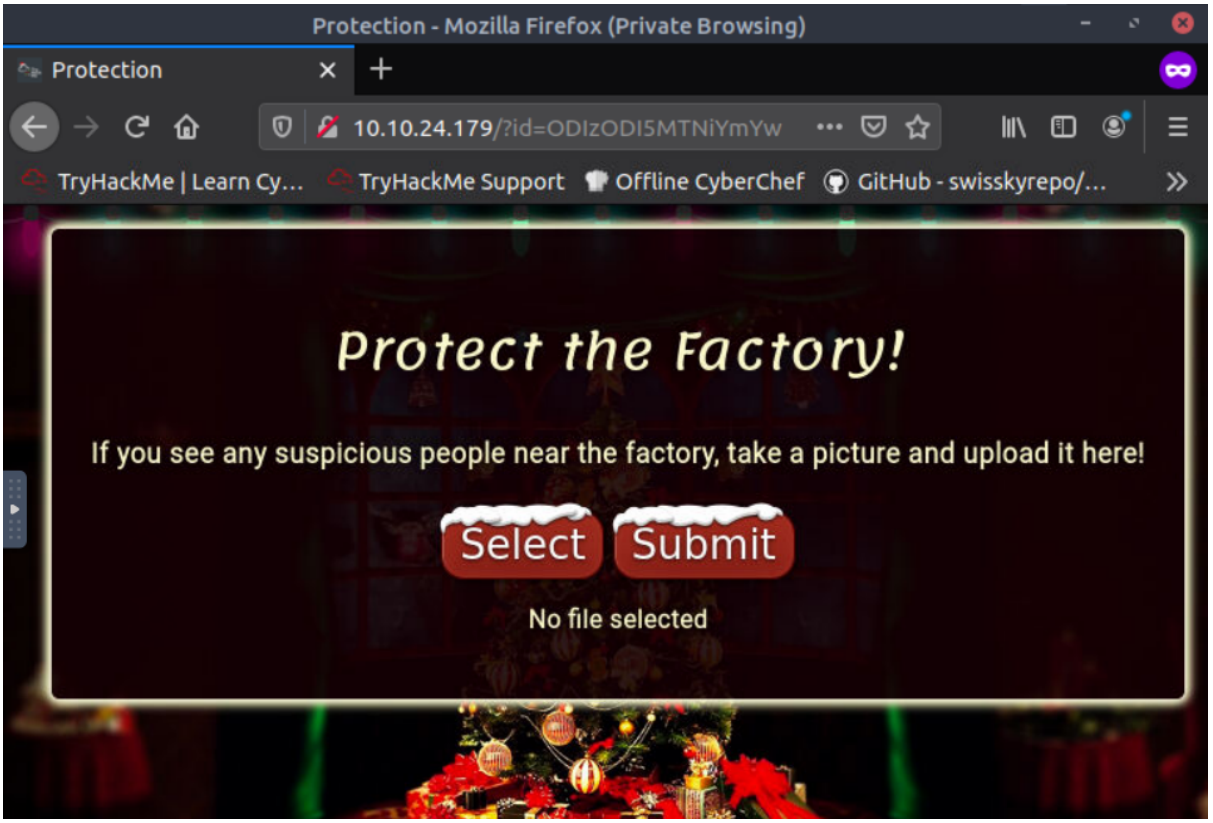
Tools used: mozilla firefox, attackbox

Solution/walkthrough:

Question 1

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

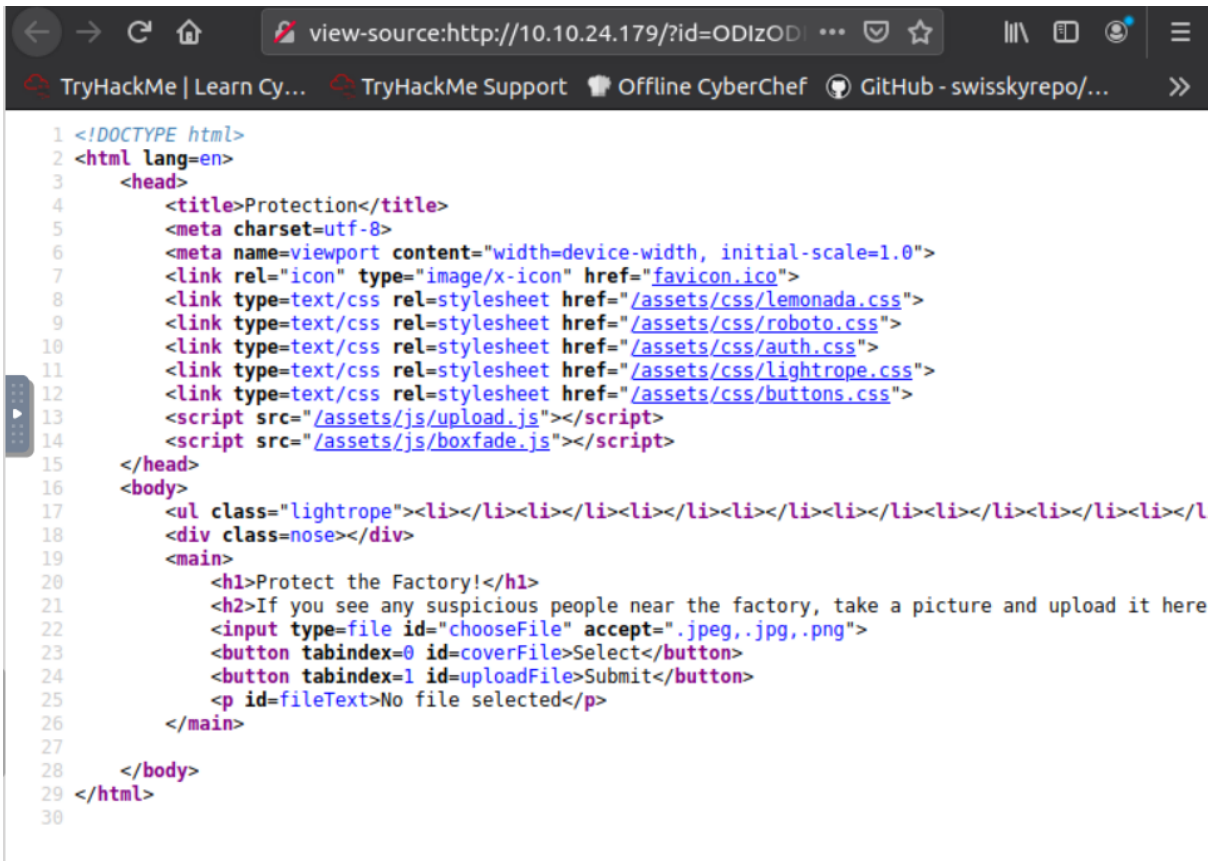
?id=ODIzODI5MTNiYmYw



Question 2

What type of file is accepted by the site?

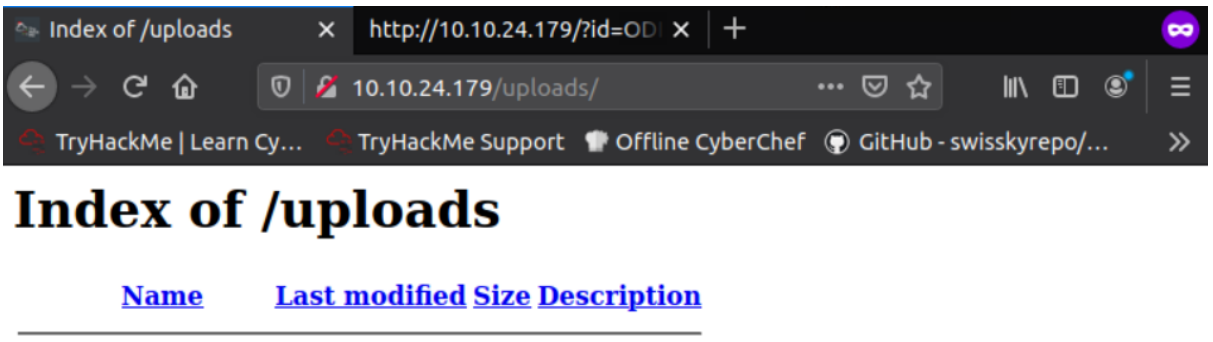
image



Question 3

In which directory are the uploaded files stored?

/uploads/



Question 4

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

Have nc give more verbose output - **v**

Specifies the source port nc should use, subject to privilege restrictions and availability - **p**

Used to specify that nc should listen for an incoming connection rather than initiate a connection to a remote host - **l**

Do not do any DNS or service lookups on any specified addresses, hostnames or ports - **n**

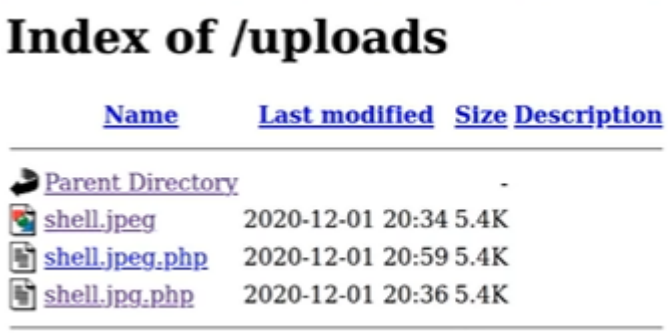
```
-d              detach from console, background mode

-g gateway      source-routing hop point[s], up to 8
-G num          source-routinDesktop\netcat>nc -h ...
-h              this cruft
-i secs         delay interval for lines sent, ports scanned
-l              listen mode, for inbound connects
-L              listen harder, re-listen on socket close
-n              numeric-only IP addresses, no DNS
-o file         hex dump of traffic
-p port         local port number
-r              randomize local and remote ports
-s addr         local source address
-u              UDP mode
-v              verbose [use twice to be more verbose]
-w secs         timeout for connects and final net reads
-z              zero-I/O mode [used for scanning]
```

Question 5

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

THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}




```
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 awesom
e @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}
```

Thought Process/Methodology: we viewed the page source to see the source code. We can see that the site accepted jpeg,jgpg,png which basically means images. We went back to part of the task and we noticed a number of comment directories and /uploads makes the most sense to be the answer. According to the netcat parameter explanation, have nc give more verbose output is v, specifies the source port nc should use, subject to privilege restrictions and availability is p used to specify that nc should listen for an incoming connection rather than initiate a connection to a remote host is l and lastly do not do any DNS or service lookups on any specified addresses, hostnames or ports is n. As we already found the upload form, next we upload shell.jpeg.php to the uploads. We made sure that we had our netcat going on and after a while reverse shell will appear. We ran the command cat /var/www/flag.txt as we will obtain the flag.

Day 3: Web exploitation - Web exploitation - Christmas Chaos

Tools used: Attackbox, Mozilla Firefox, Burpsuite

Solution/walkthrough:

Question 1

What is the flag?

THM{885ffab980e049847516f9d8fe99ad1a}. Once we entered the right credentials which were *admin* for username and *12345* for the password we were able to log in thus showing us the flag.

Question 2

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

Mirai.

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):

- https://hackerone.com/reports/195163 - Starbucks, bug bounty for default credentials.
- https://hackerone.com/reports/804548 - US Dept Of Defense, admin access via default credentials.

In 2017, it was reported that 15% of all IoT devices still use default passwords.

SecLists is a collection of common lists including usernames, passwords, URLs and much more. A password list known as "rockyou.txt" is commonly used in security challenges, and should definitely be a part of your security toolkit.

Question 3

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

$250

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):

- https://hackerone.com/reports/195163 - Starbucks, bug bounty for default credentials.
- https://hackerone.com/reports/804548 - US Dept Of Defense, admin access via default credentials.

In 2017, it was reported that 15% of all IoT devices still use default passwords.

SecLists is a collection of common lists including usernames, passwords, URLs and much more. A password list known as "rockyou.txt" is commonly used in security challenges, and should definitely be a part of your security toolkit.

Question 4

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

ag3nt-j1 was the agent that closed the report

agent-l8 U.S. Dept Of Defense staff changed the status to ● Triaged. Feb 25th (2 years ago)

arm4nd0 posted a comment. May 11th (2 years ago)

agentt2 closed the report and changed the status to ● Resolved. May 22nd (2 years ago)

arm4nd0 posted a comment. Jun 25th (2 years ago)

agent-l8 U.S. Dept Of Defense staff posted a comment. Updated Jun 25th (2 years ago)

arm4nd0 posted a comment. Jun 25th (2 years ago)

arm4nd0 requested to disclose this report. Jun 25th (2 years ago)

ag3nt-j1 U.S. Dept Of Defense staff agreed to disclose this report. Jun 25th (2 years ago)

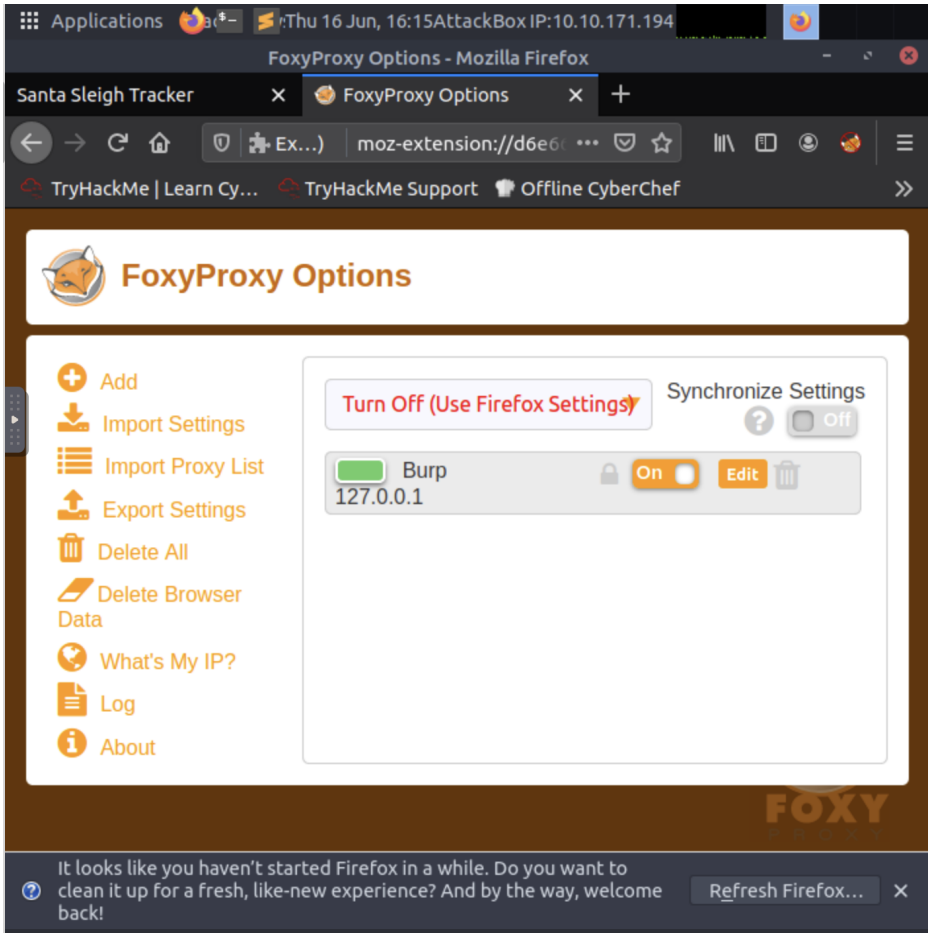
This report has been disclosed. Jun 25th (2 years ago)

U.S. Dept Of Defense has locked this report. Jun 25th (2 years ago)

Question 5

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

Click on foxyproxy on the extension section of firefox then click options. **127.0.0.1** is the port number when looking at the options page.



Question 6

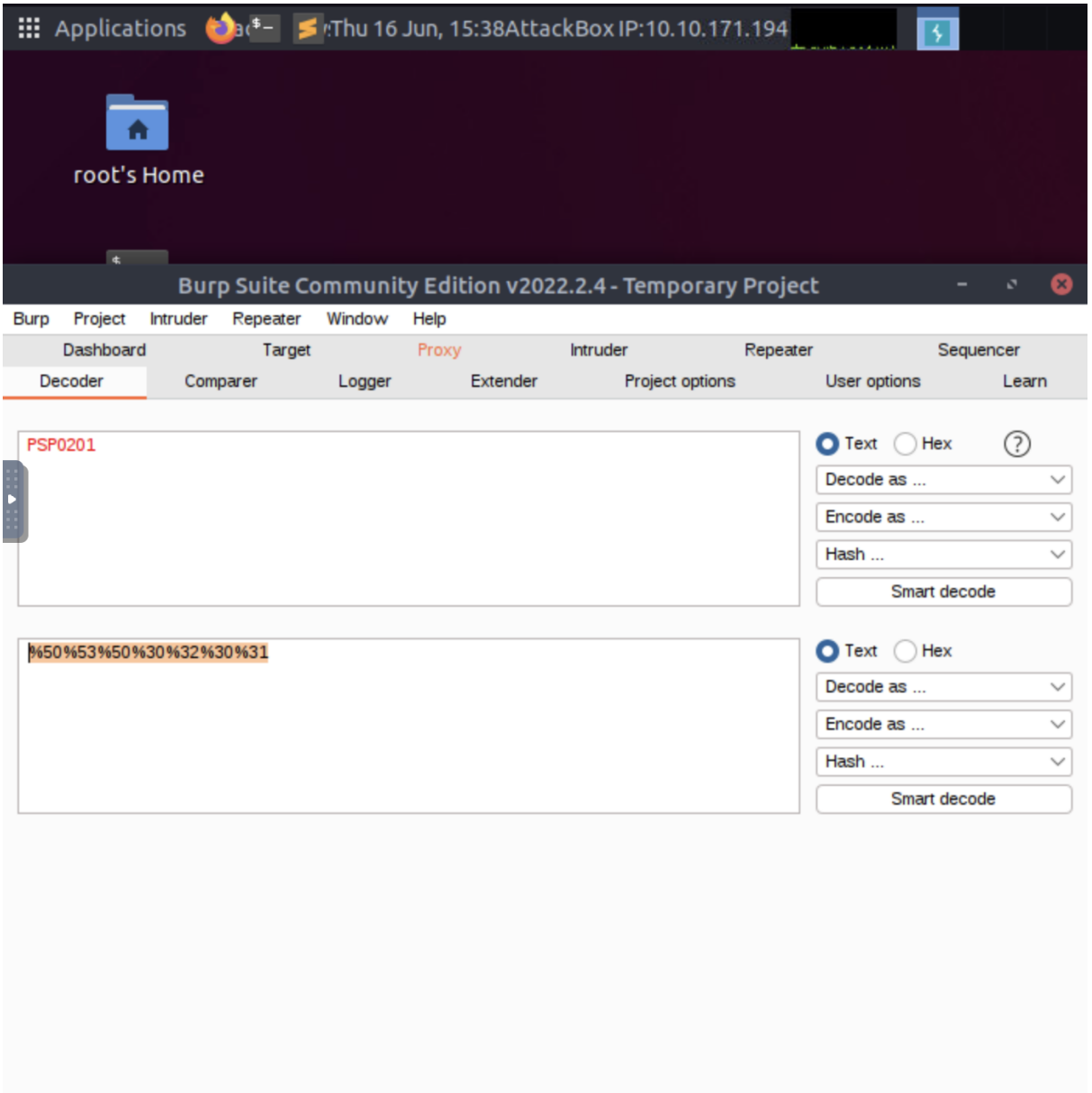
Examine the options on FoxyProxy on Burp. What is the proxy type?

HTTP

Question 7

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

PSP0201 was typed in and the URL was selected as an option to encode the text. It reveals that **%50%53%50%30%32%30%31** was the encoding.



Question 8

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.

Cluster bomb

Thought Process/Methodology:

After accessing the target machine we were shown the Santa sleigh tracker login page. We started up burpsuite to start “intercepting” our traffic. On firefox we used the extension named Foxy Proxy to change our proxy from firefox settings to burp. When we tried to login to santa sleigh tracker with a credential the page does not forward nor proceed. The site continues to hang. When looking at burpsuite on the proxy tab it shows that the site has been intercepted and the credentials that were entered earlier appeared on the request. We sent the request to a burpsuite tool called intruder so that we can manipulate and modify the request. The request appeared on the intruder tab. In the positions tab of the intruder tab the attack type called cluster bomb is used. For payloads, we use a selected list of usernames and passwords for payload 1 and payload 2 respectively. We manually added the entries based on our list. Once we entered the necessary information we started the attack and on the results page we observed a list of the combination of payload 1 (username) and payload 2 (password) created. For one of the combinations which was ‘admin ’as username and ‘12345’ as password, it was abnormal in the discrepancy of length compared to the rest of the combinations. We assumed that this request might have been a successful one. We entered this credential back on the Santa sleigh tracker site and we were able to log in successfully which in turn showed the flag.

Day 4: Web exploitation - Santa’s Watching

Tools used: Attackbox, Gobuster, Mozilla Firefox

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)

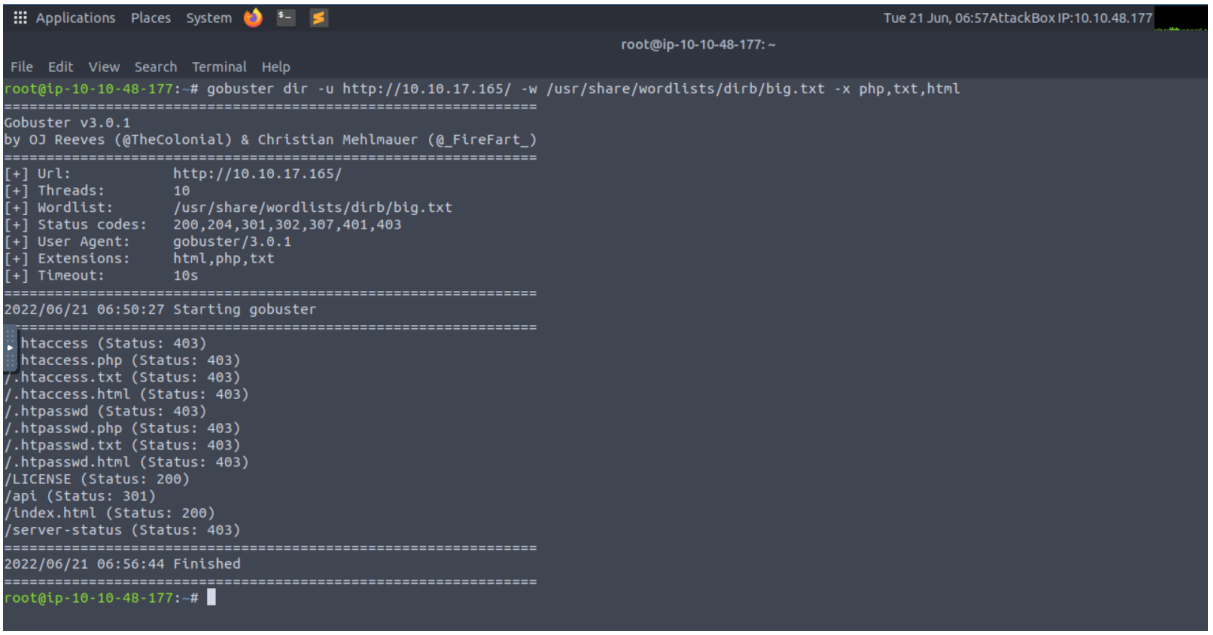
wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ

Question 2

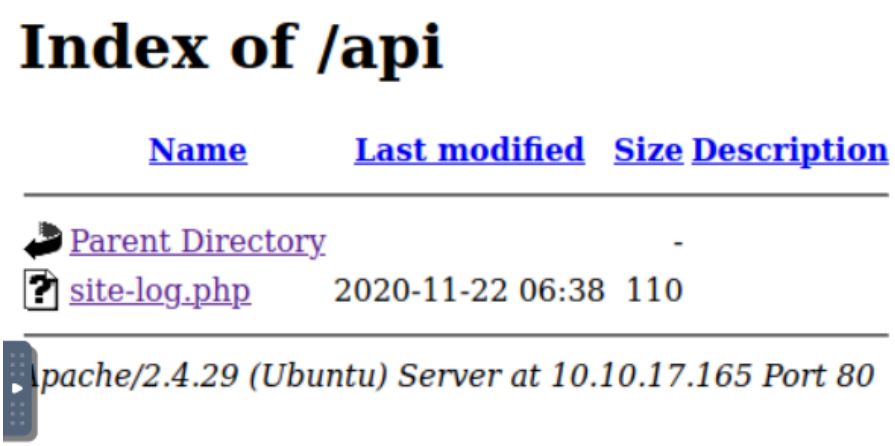
Use GoBuster (against the target you deployed -- not the shibes.xyz domain) to find the API directory. What file is there?

site-log.php

ran GoBuster on the main page



go to **/api** where we found the file we wanted



Question 3

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

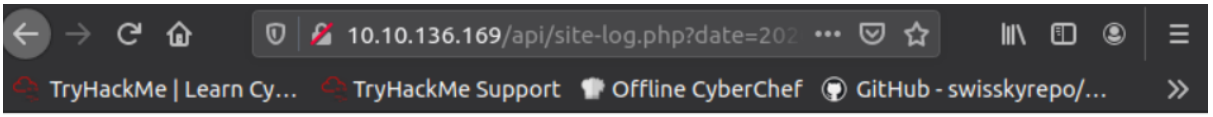
THM{D4t3_AP1}

as we ran the wfuzz command, we something that looked different from the rest

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

000019:  C=200      0 L       0 W          0 Ch        "20201118"
000001:  C=200      0 L       0 W          0 Ch        "20201100"
000002:  C=200      0 L       0 W          0 Ch        "20201101"
000011:  C=200      0 L       0 W          0 Ch        "20201110"
000003:  C=200      0 L       0 W          0 Ch        "20201102"
000021:  C=200      0 L       0 W          0 Ch        "20201120"
000004:  C=200      0 L       0 W          0 Ch        "20201103"
000005:  C=200      0 L       0 W          0 Ch        "20201104"
000012:  C=200      0 L       0 W          0 Ch        "20201111"
000006:  C=200      0 L       0 W          0 Ch        "20201105"
000007:  C=200      0 L       0 W          0 Ch        "20201106"
000008:  C=200      0 L       0 W          0 Ch        "20201107"
000009:  C=200      0 L       0 W          0 Ch        "20201108"
000010:  C=200      0 L       0 W          0 Ch        "20201109"
000013:  C=200      0 L       0 W          0 Ch        "20201112"
000020:  C=200      0 L       0 W          0 Ch        "20201119"
000022:  C=200      0 L       0 W          0 Ch        "20201121"
000023:  C=200      0 L       0 W          0 Ch        "20201122"
000024:  C=200      0 L       0 W          0 Ch        "20201123"
000026:  C=200      0 L       1 W         13 Ch        "20201125"
000025:  C=200      0 L       0 W          0 Ch        "20201124"
000027:  C=200      0 L       0 W          0 Ch        "20201126"
```

navigate there and the flag will be visible

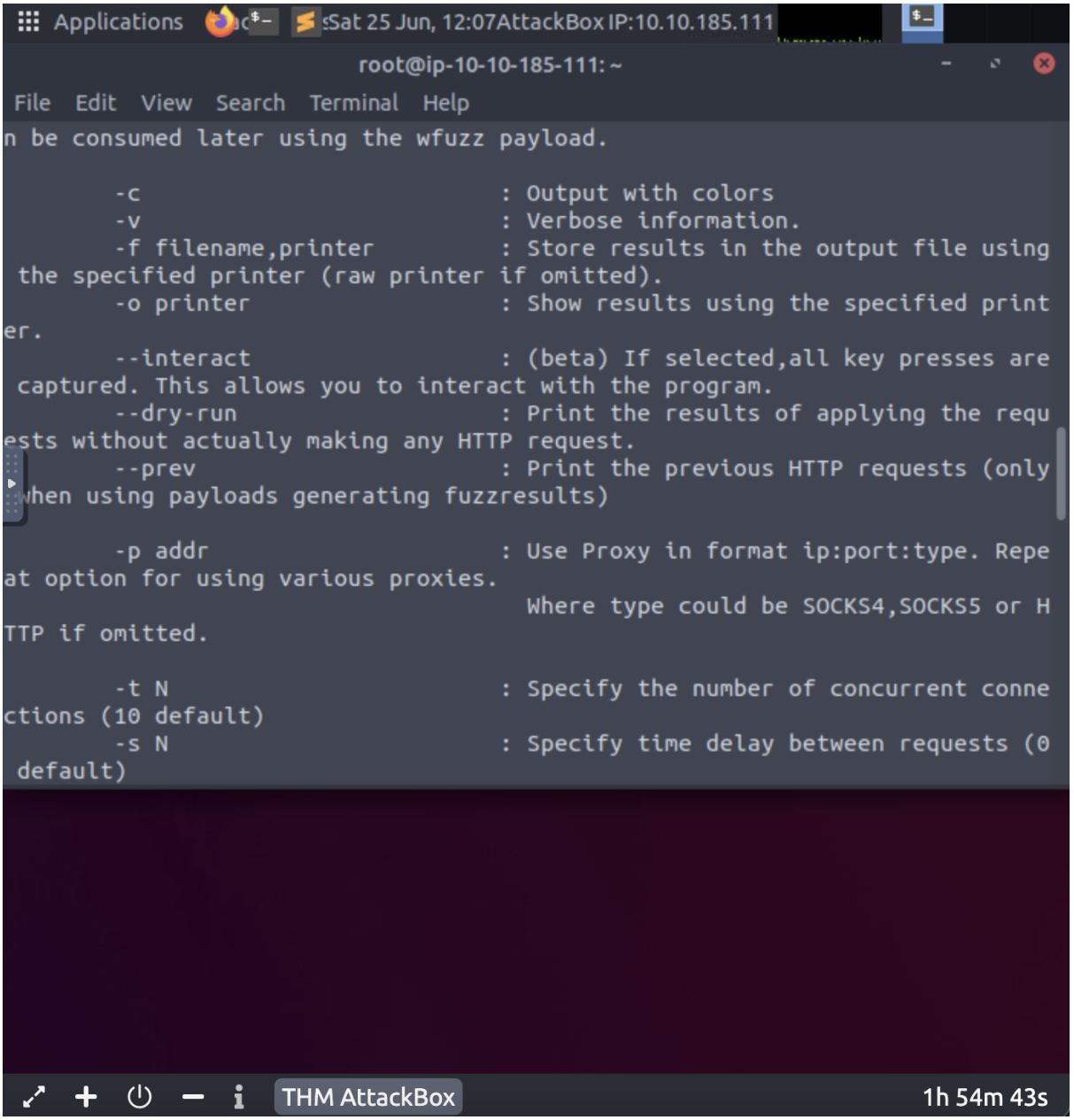


THM{D4t3_AP1}

Question 4

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

printer



Thought Process/Methodology: while we can't actually fuzz the website, we had to imagine how the command would look like. Then we ran gobuster on main page go to **/api** where we found the file we wanted which is the site-log.php. Lastly we ran the wfuzz command and notice that one looked different than the other. as the others show 0 character, this certain one shows 13 characters. We navigate the odd one in the web browser and the flag is visible.

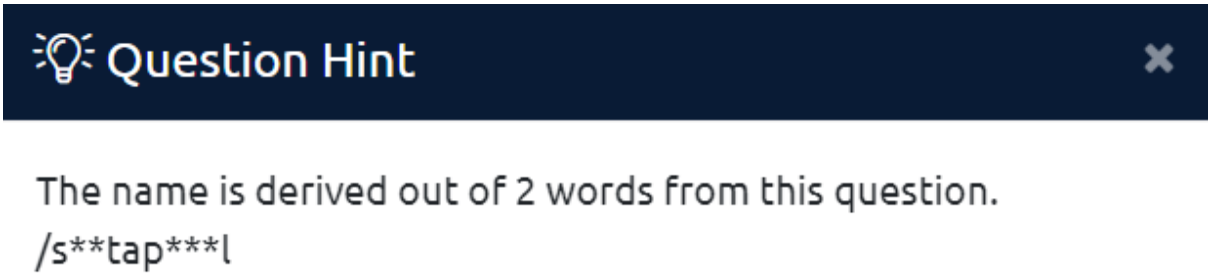
Day 5: Web exploitation - Someone stole Santa's gift list

Tools used: Attackbox, Mozilla Firefox, Burp Suite and SqlMap

Solution/walkthrough:

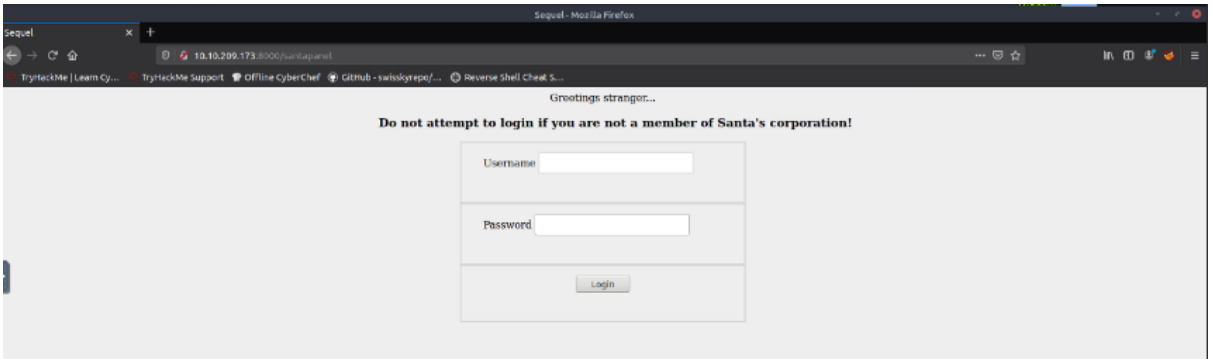
Question 1

We simply made a guess based on the hint. GoBuster, for example, might have been used to accomplish this, but it is specifically forbidden.

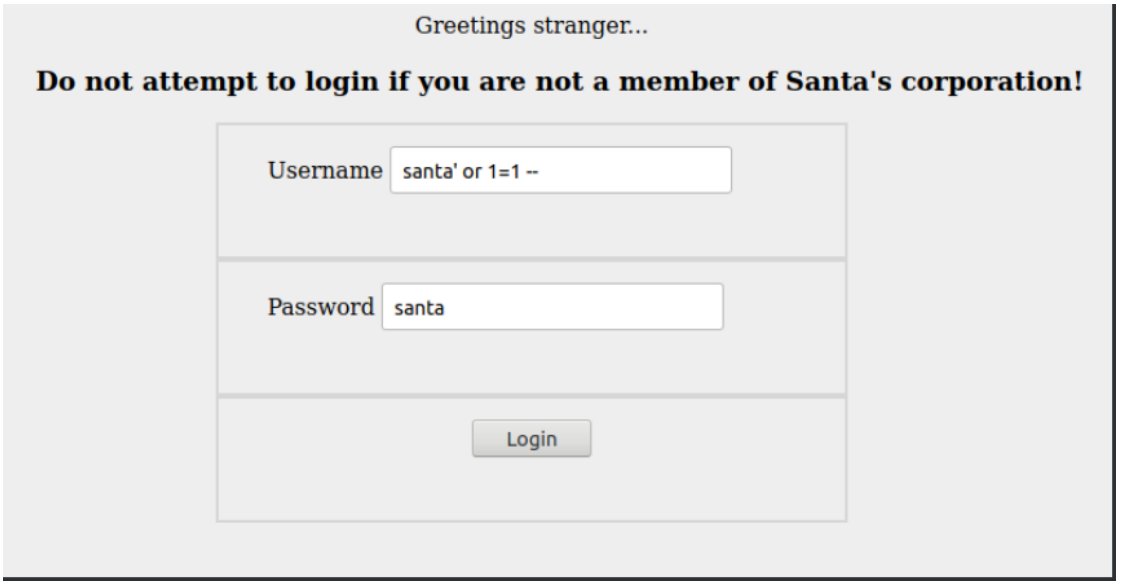


Question 2

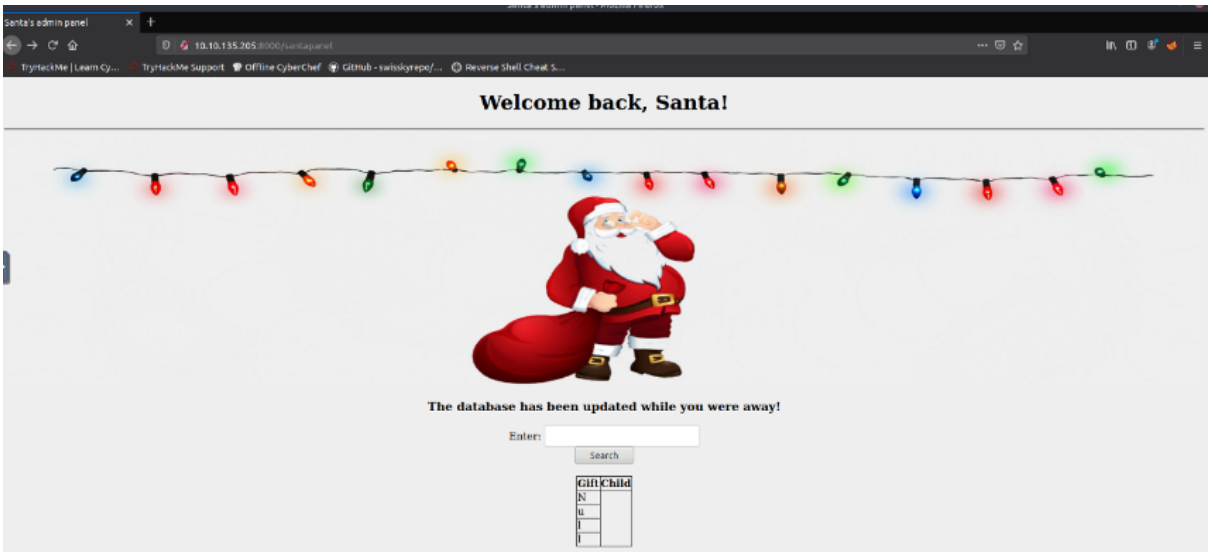
Santa's Secret Login Panel.



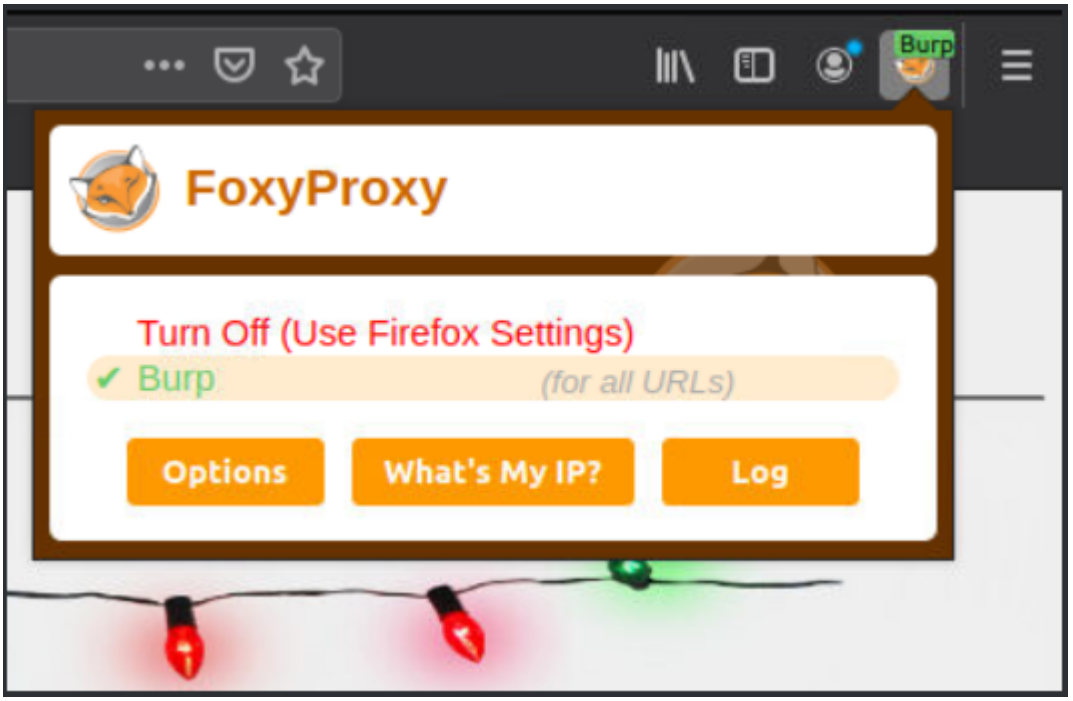
Using the extensive guide provided with today's challenge, we eventually discovered how to get past this login page.



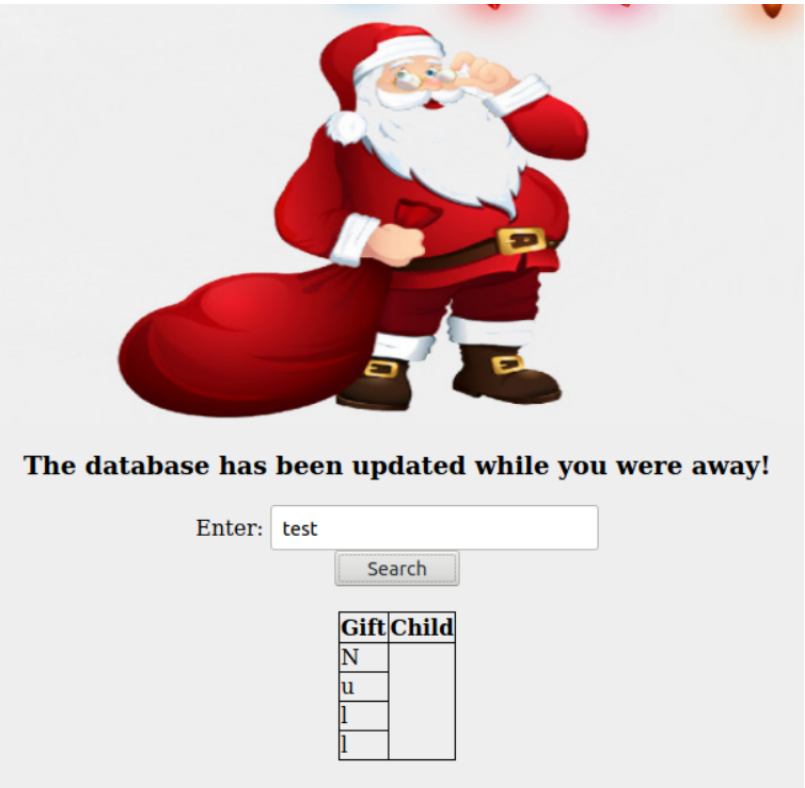
Then it took us to a new page where I am able to traverse the database.



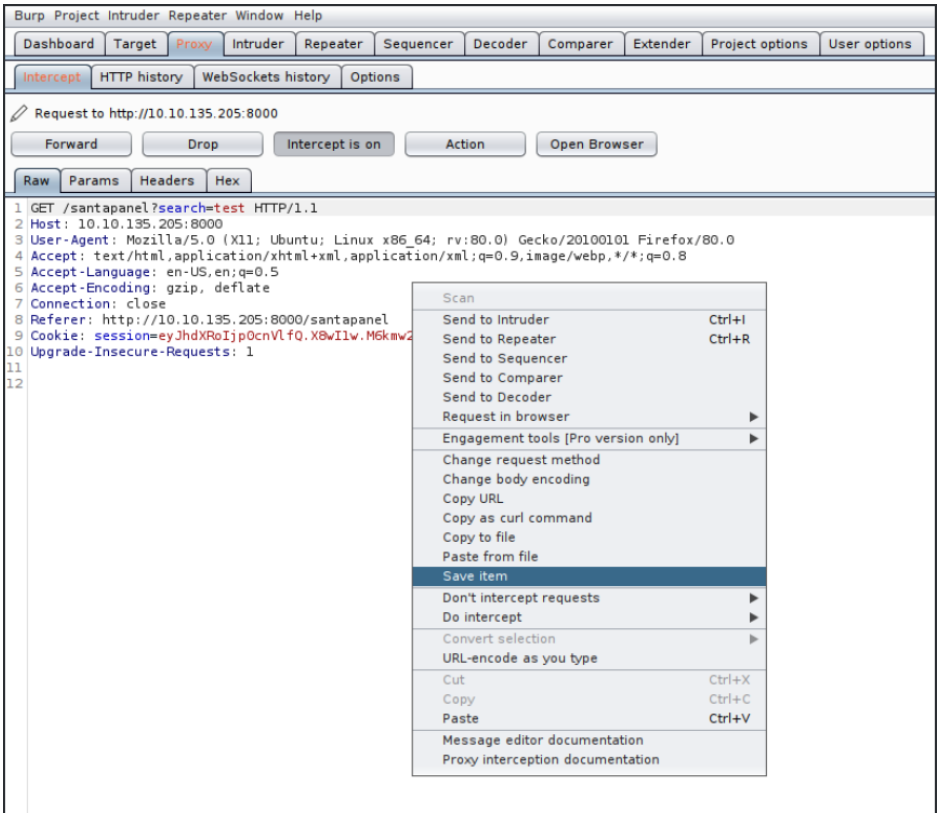
Burp Suite and SqlMap will be used by us to automate this process. We opened Burp Suite and activate Foxy Proxy to begin intercepting afterward.



We went back to the webpage to do a test request.



We checked Burp again after pressing search to view the request. So that SqlMap may use it. At this time, we can disable Foxy Proxy and intercept.



We can see there are 22 entries in the gift database.

```
Database: SQLite_masterdb
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                       |
```

Question 4

We can see Paul requested github ownership using the same table.

Question 5

The flag is in the "hidden table," but since I exported the whole database, it also included that.

```
Database: SQLite_masterdb
Table: hidden_table
[1 entry]
+---------------------------------------+
| flag                                  |
+---------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+---------------------------------------+
```

Question 6

```
Database: SQLite_masterdb
Table: users
[1 entry]
+----------+------------------+
| username | password         |
+----------+------------------+
| admin    | EhCNSWzzFP6sc7gB |
+----------+------------------+
```

Thought Process/Methodology: We used Burp Suit and Sqlmate to retrieve Santa's Stolen gift list.