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

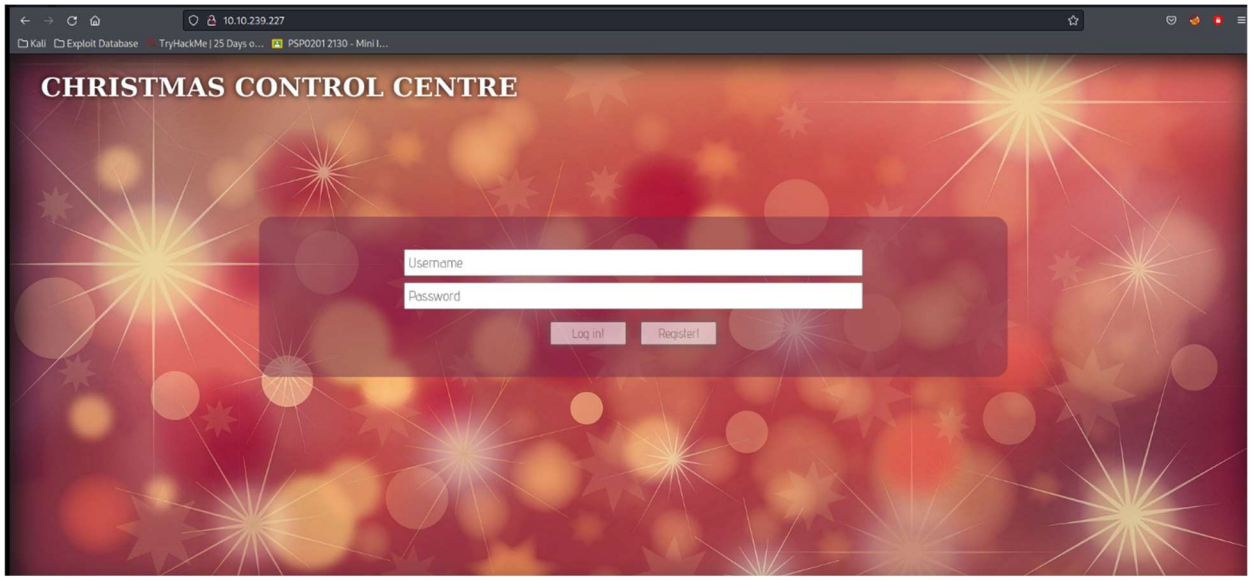
Day 1: Web Exploitation – A Christmas Crisis

Tools: Kali Linux, Firefox

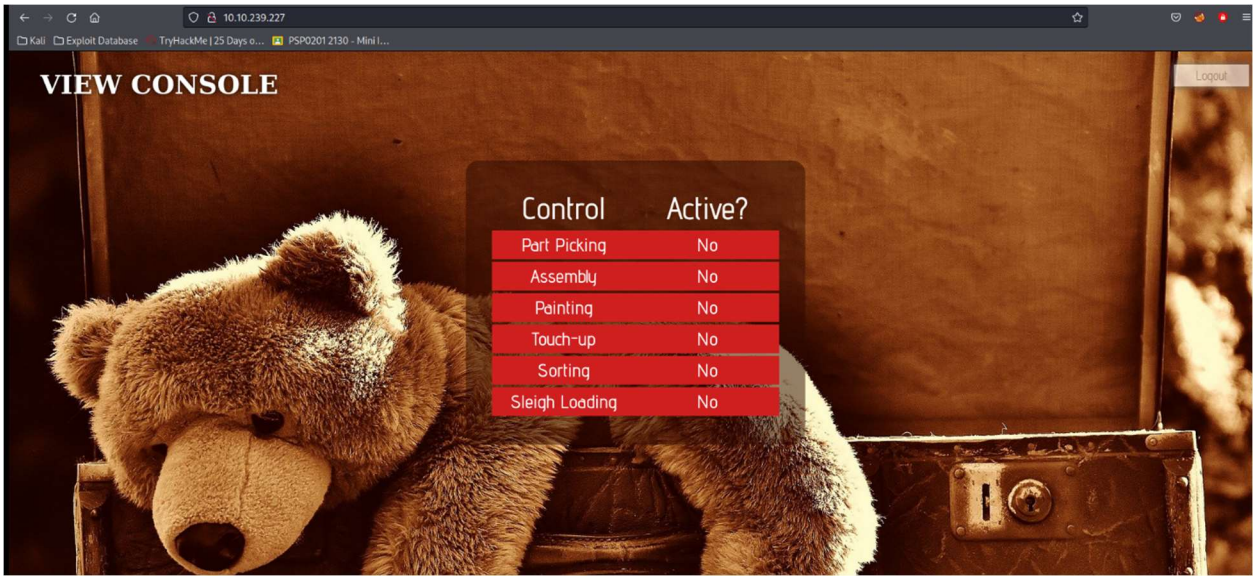
Solution:

Question 1

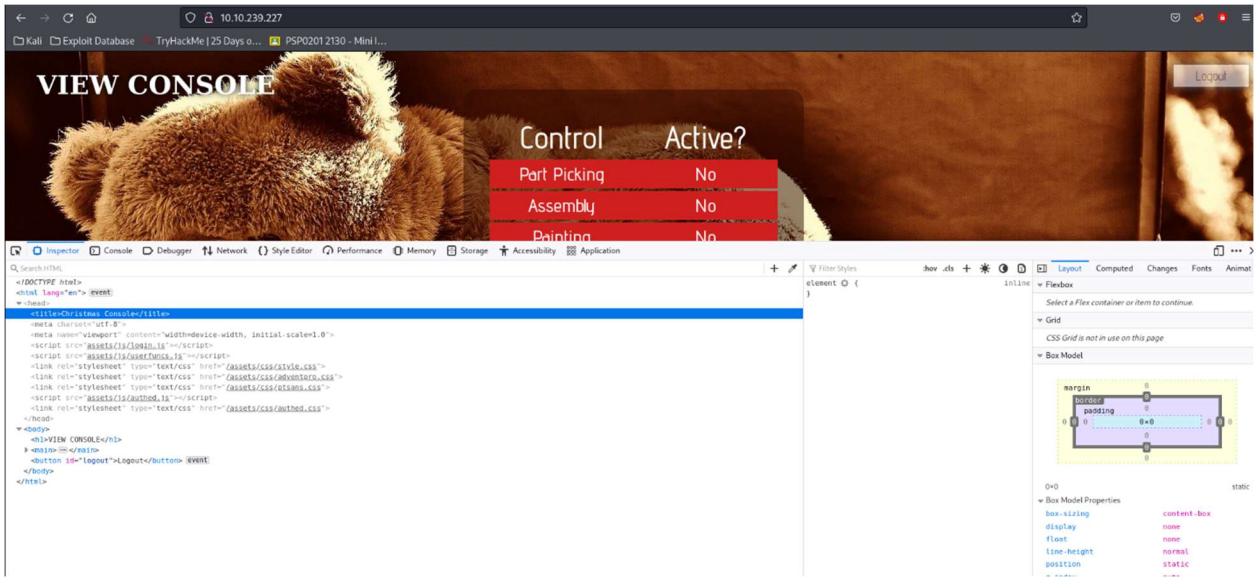
New username and password registration and log in to the Christmas Control Centre.



However, there is no access to the control panel.

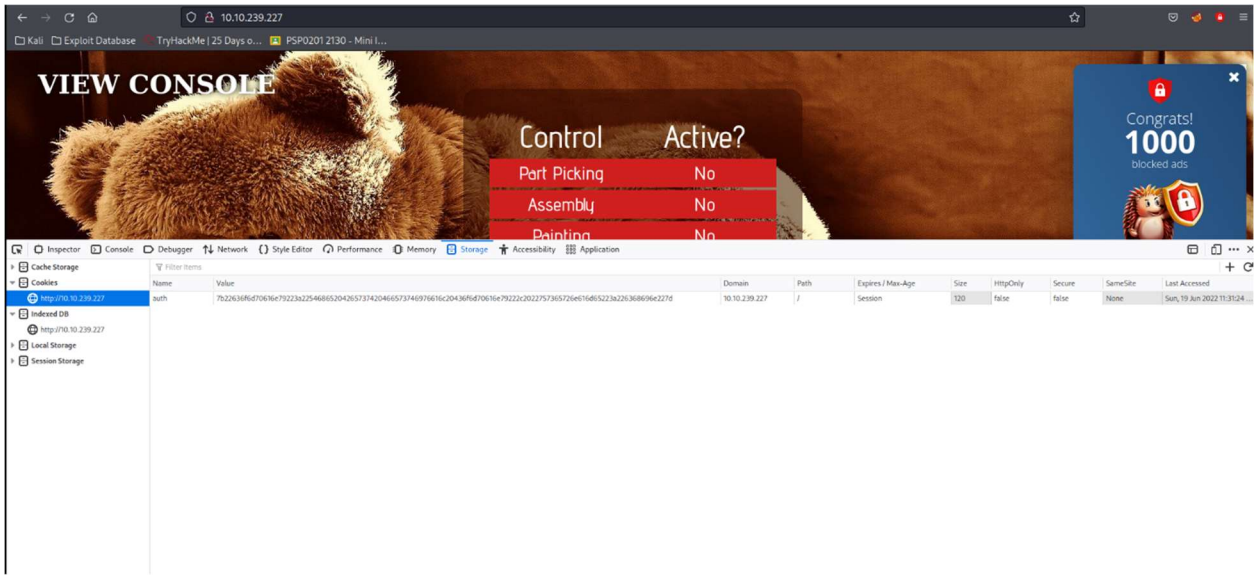


Open the browser developer tools to inspect the title of the website.



Question 2:

Navigate to the storage inspector to inspect the cookie.

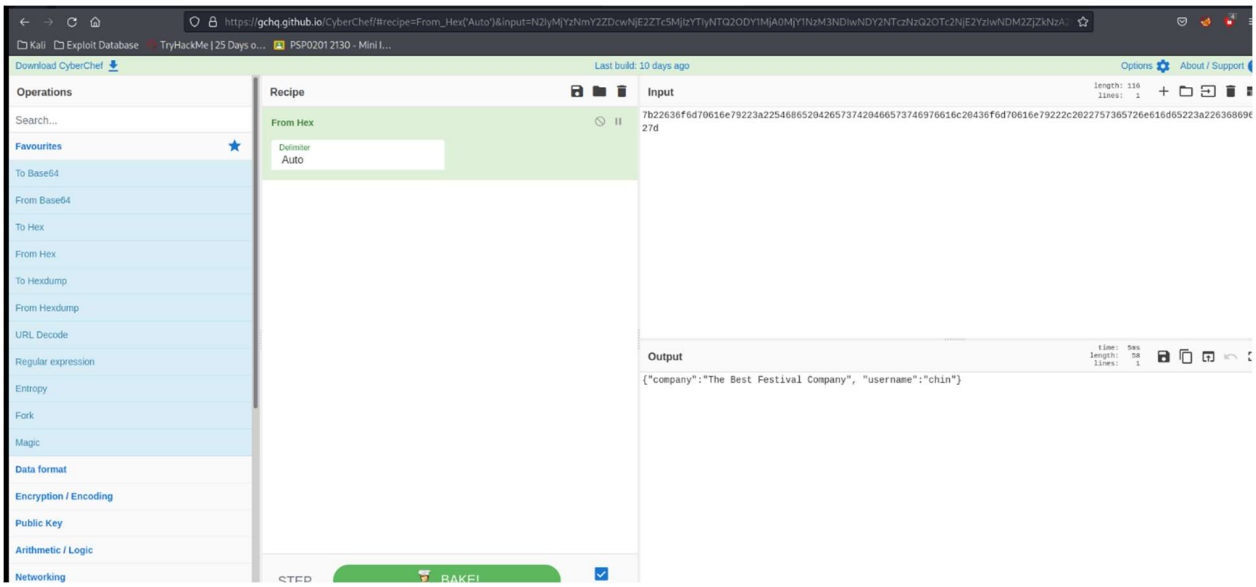


Question 3:

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

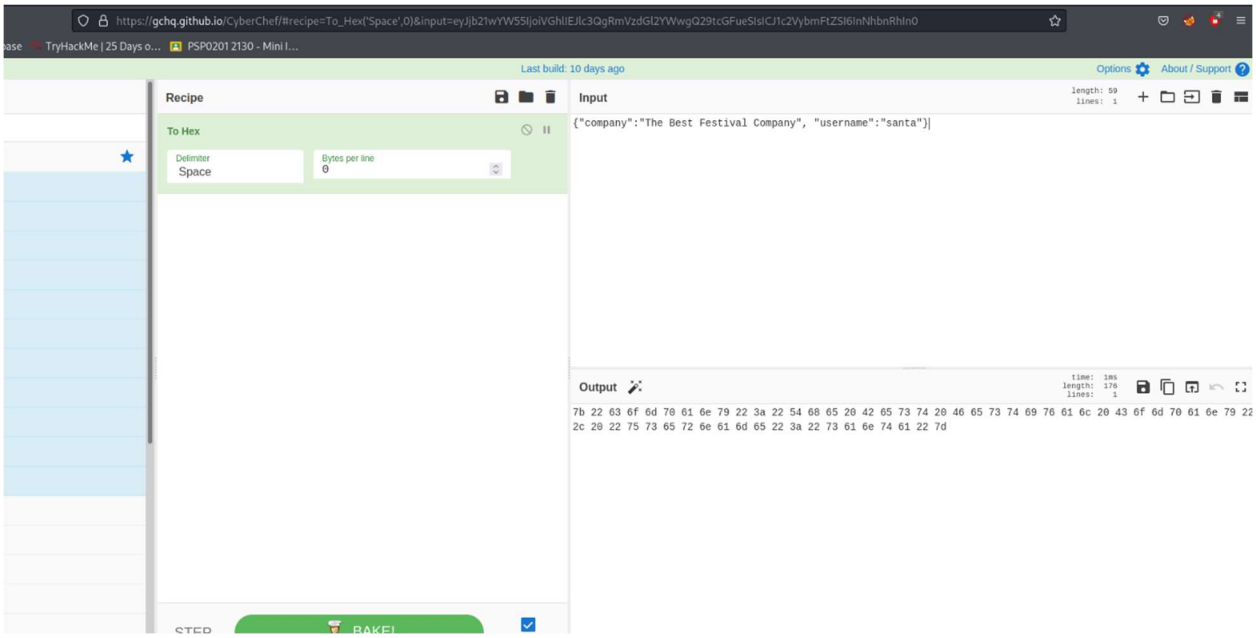
Question 4, 5 & 6:

Decode the value of the cookie using CyberChef.



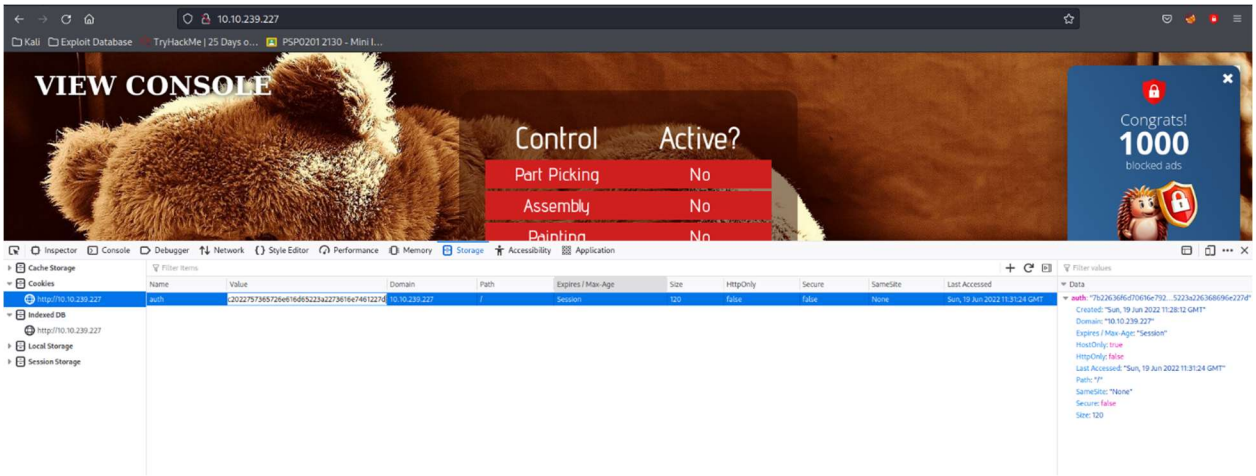
Question 7:

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

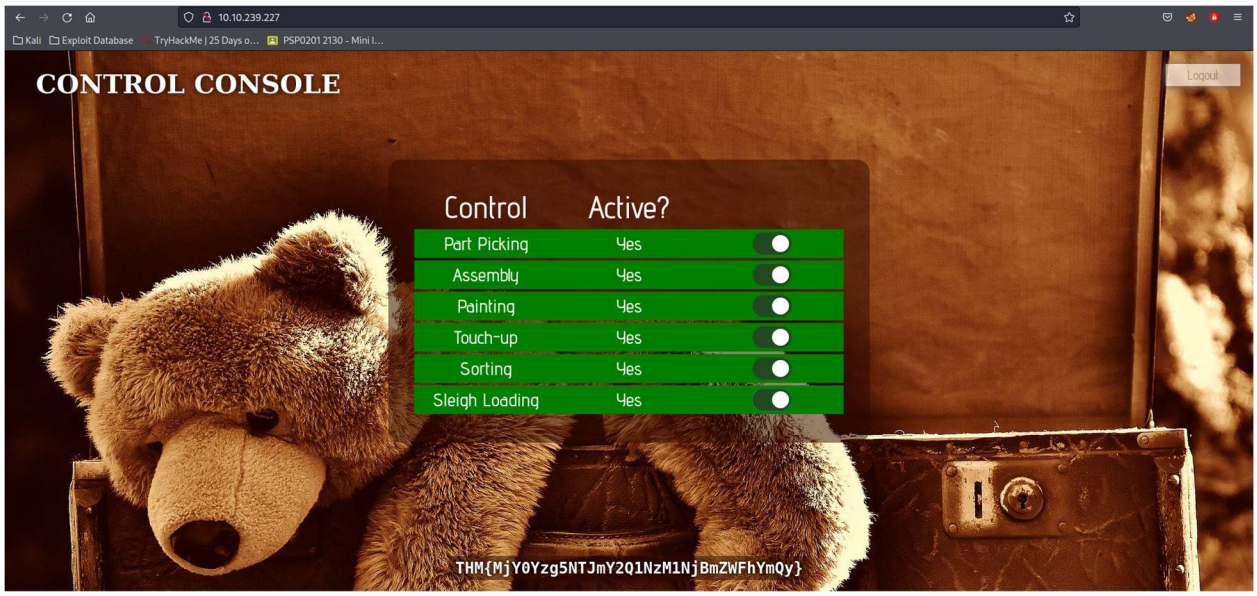


Question 8:

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.



Thought process/Methodology:

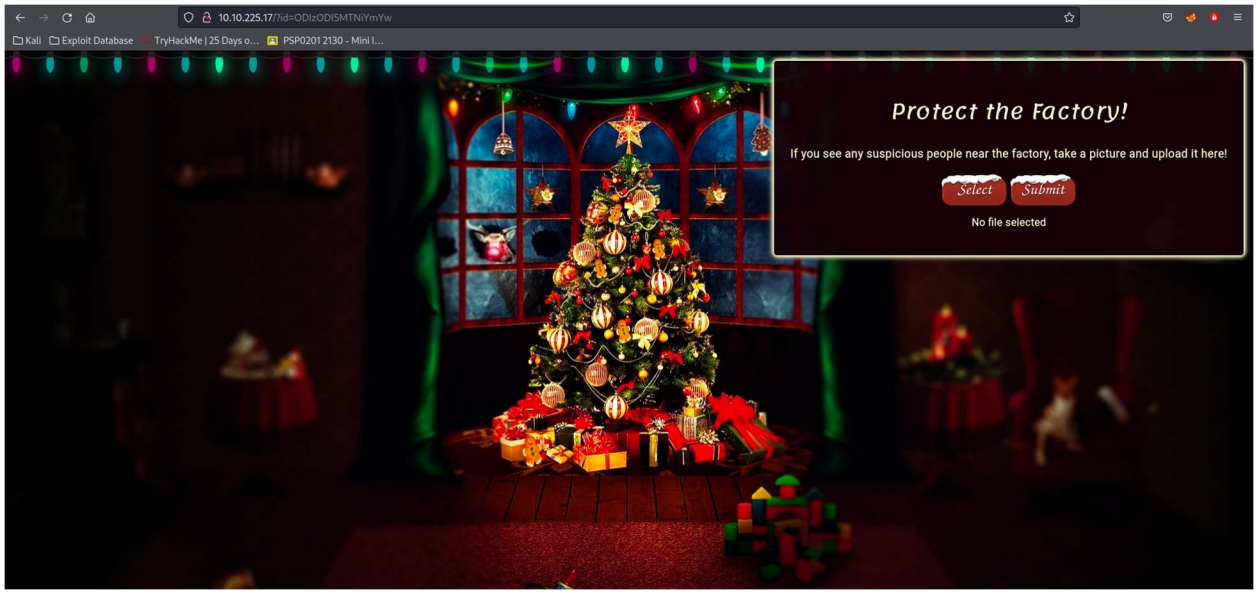
After accessing the IP address of the target's machine, we were brought to a login/registration screen. Then, we created an account and log in. Once we were inside the control panel, we opened the developers' tool and inspected the Element; checked the HTML title tag and we knew the title of the website was Christmas Console. Afterwards, we inspect the Storage to check for the name and the value of the cookie. We deduced from the value that it was encoded in hexadecimal. We copied and pasted the value of the cookie into CyberChef to convert it to text. Once the value had been decoded, we knew that the data is stored as JSON statement with the company and username element. Using CyberChef, we changed the value of the username element to "santa". Then, we converted the JSON statement to hexadecimal using CyberChef. We replaced the value of the cookie with the one that we had converted and refreshed the page to gain access to the admin page. We proceeded to switch on all the controls to reveal the flag.

Day 2: Web Application – The Elf Strikes Back

Tools: Kali Linux, Mousepad, Firefox

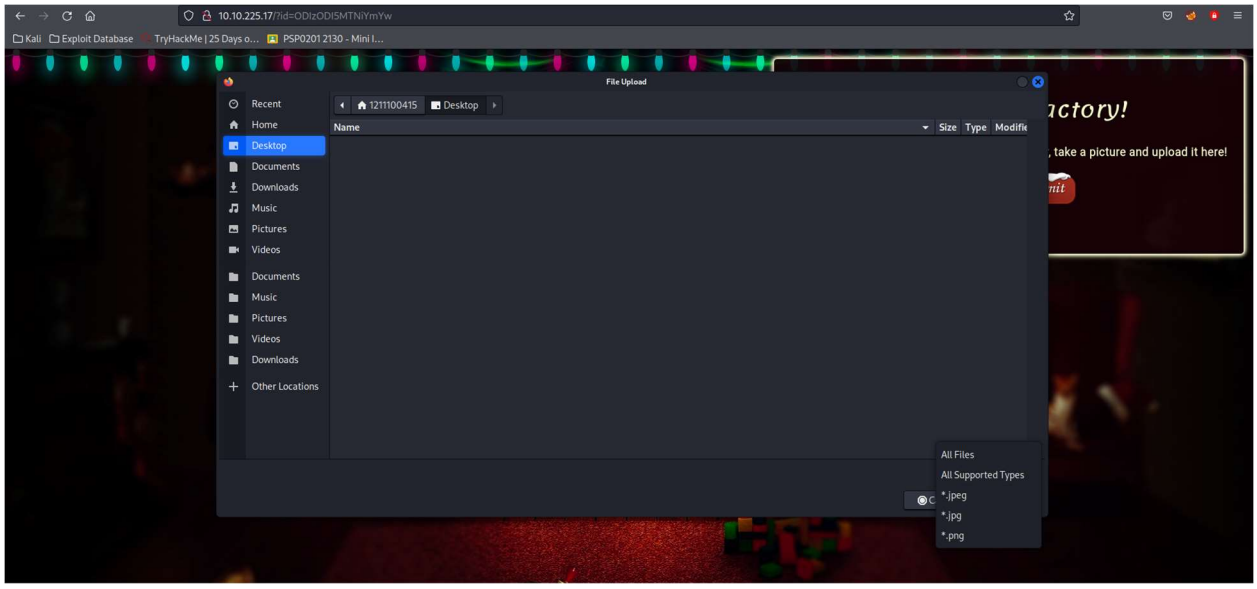
Question 1:

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



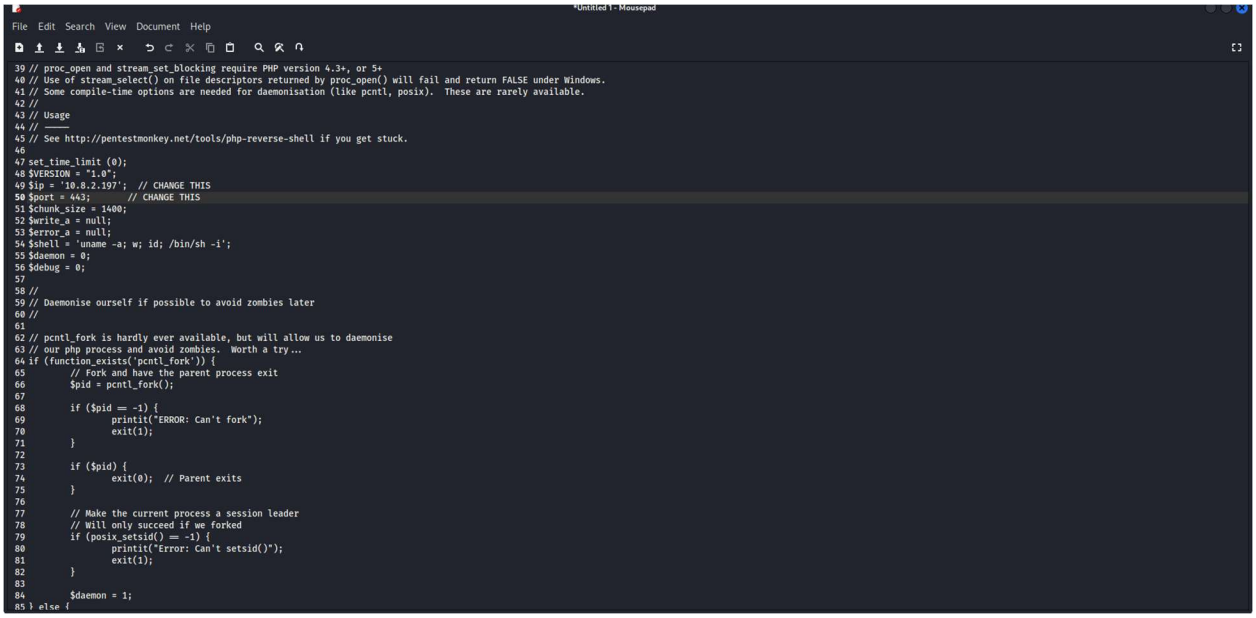
Question 2:

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



Question 3:

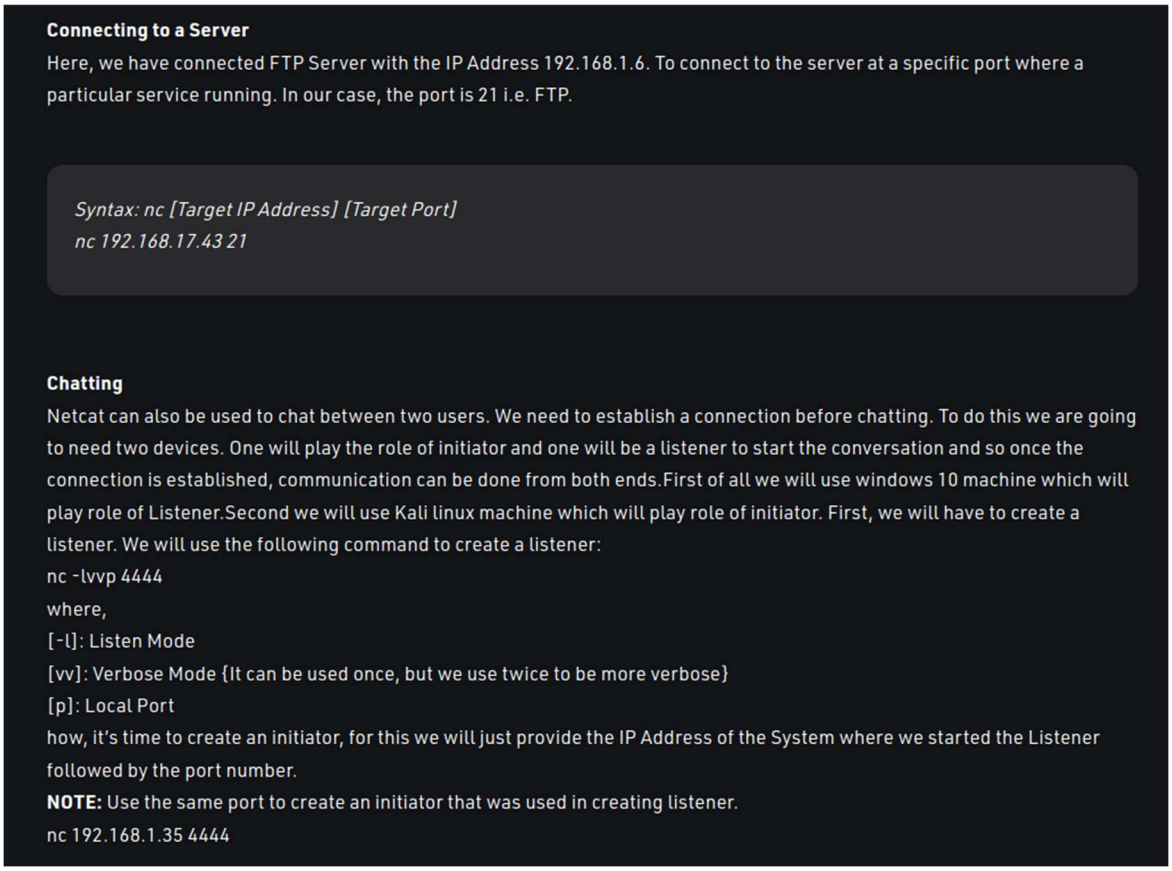
Copy the reverse shell script and paste into Mousepad. Change the IP address to your current IP address and the port to 443. Save the file as shell.jpg.php. Upload the file into the site.



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

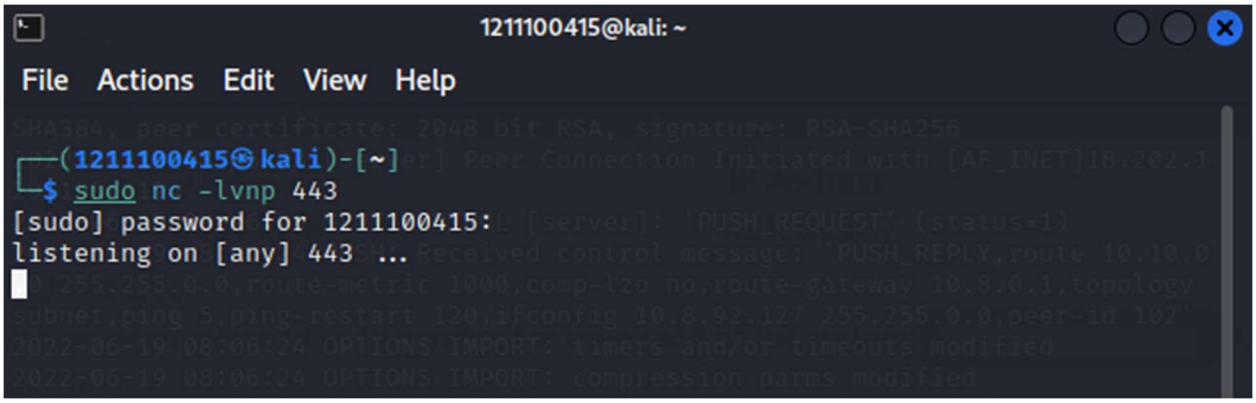
how, it's time to create an initiator, for this we will just provide the IP Address of the System where we started the Listener followed by the port number.

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

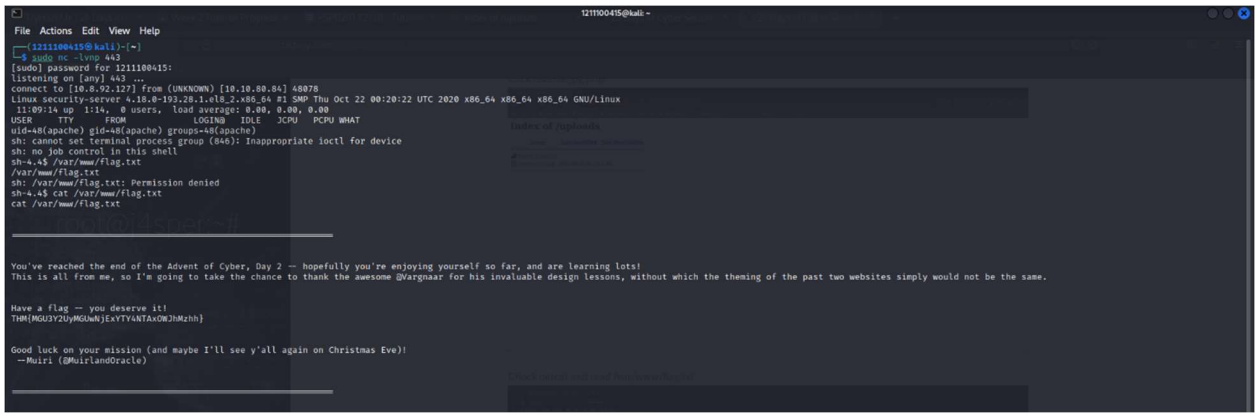
nc 192.168.1.35 4444

Question 5:

Activate the netcat listener on your terminal.



Activate the reverse shell.



Thought process/Methodology:

After accessing the IP address of the target's machine, by using the GET parameter and the username given in the dossier we can gain access to the page. After that, we investigated what type of files that would be supported by the webpage by clicking on the select file button, where we knew that the webpage only accepted images. We copied the reverse shell script and pasted it into a notepad. We changed the IP address to our current one and the port to 443. Afterwards, we saved the notepad as shell.jpg.php and uploaded the PHP file into the page. Once the file had been uploaded, we navigated to the page where the uploaded file is stored. Then, we activated both the netcall listener and reverse shell. Once the reverse shell had been connected, we navigated to /var/www//flag.txt to receive the flag.

Day 3: Web Exploitation – Christmas Chaos

Tools: Kali Linux, Firefox, Burpsuite, Foxyproxy

Solution:

Question 1 & 2:

Read the passage in TryHackMe.

Default Credentials

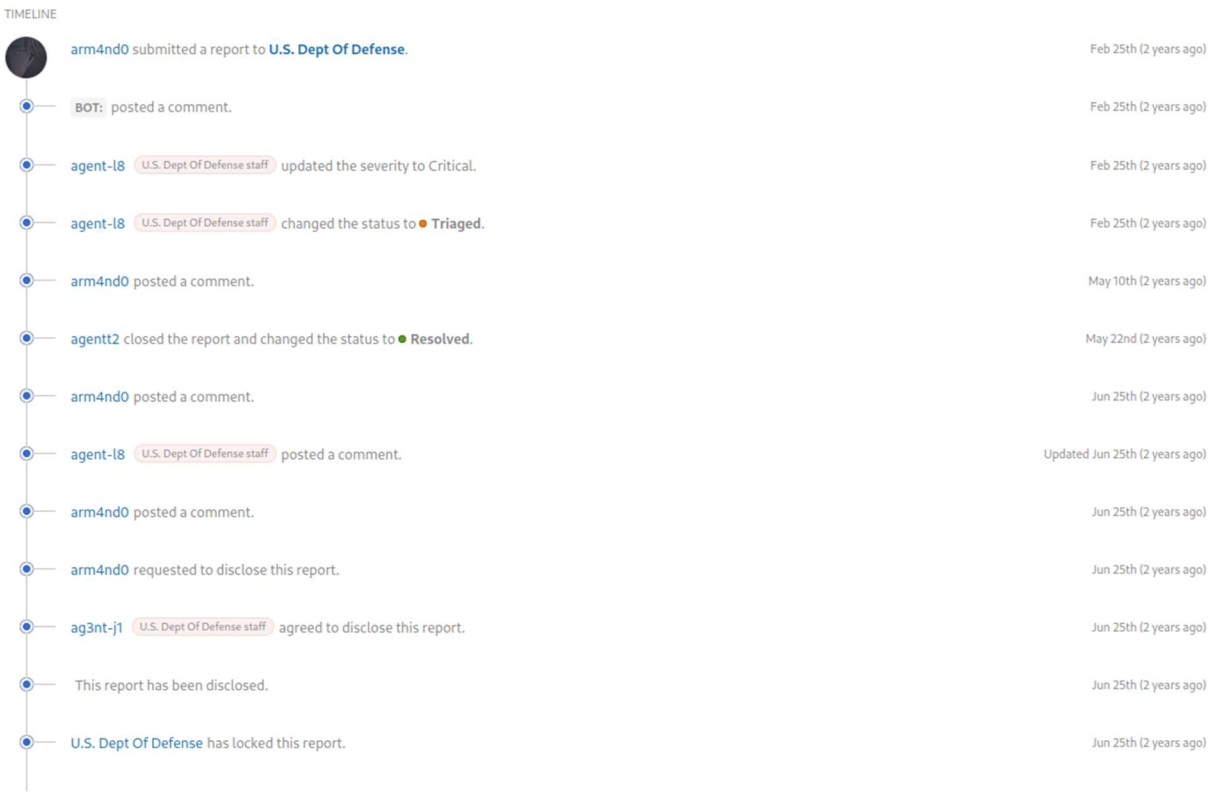
You've probably purchased (or downloaded a service/program) that provides you with a set of credentials at the start and requires you to change the password after it's set up (usually these credentials that are provided at the start are the same for every device/every copy of the software). The trouble 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):

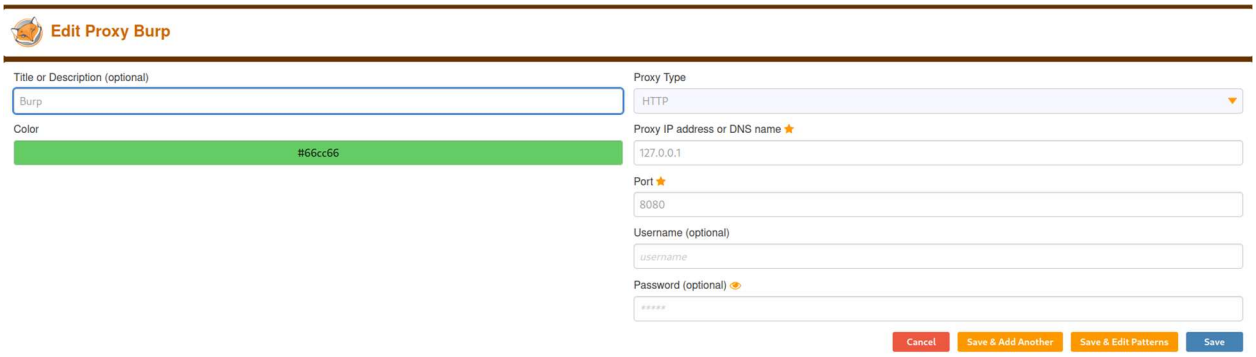
Question 3:

Read the report from Hackerone ID:804548.



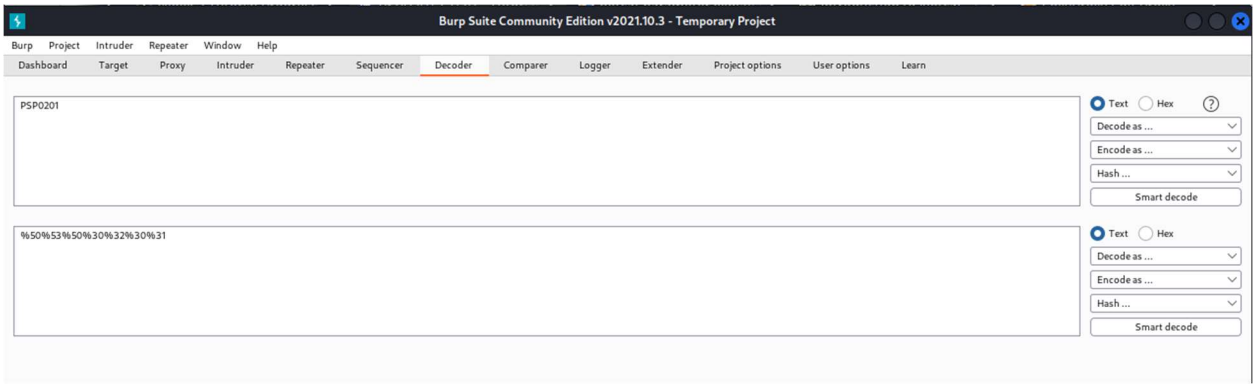
Question 4 & 5:

Open the options on Foxyproxy.



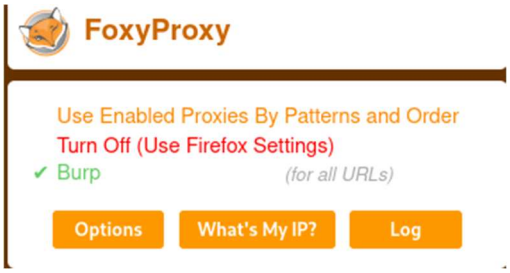
Question 6:

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

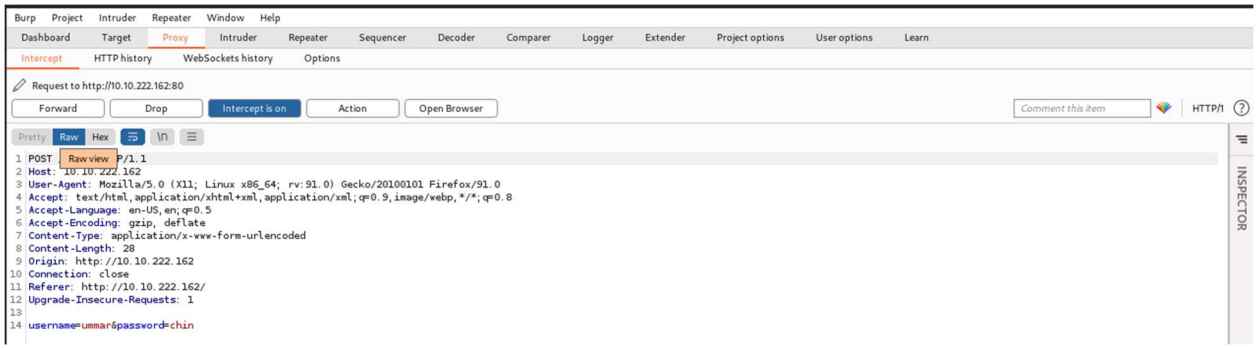


Question 7:

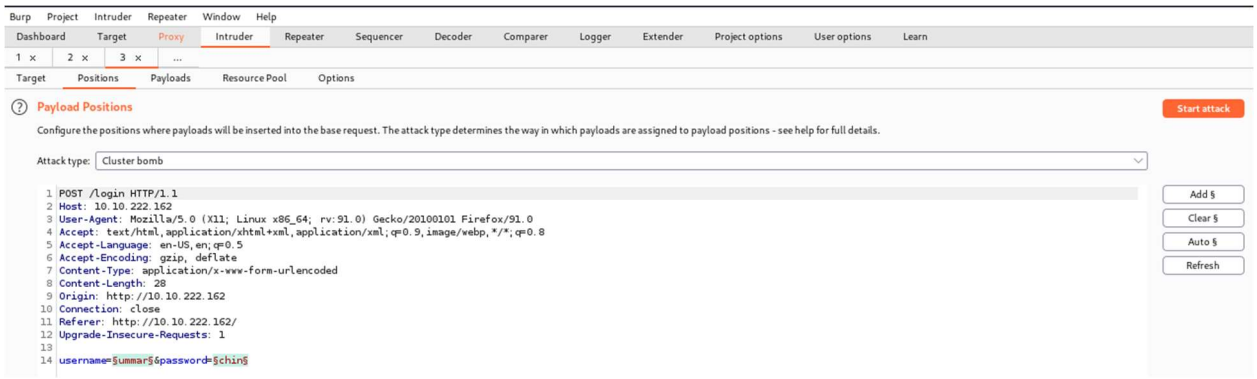
Turn on Foxyproxy and Burpsuite.



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

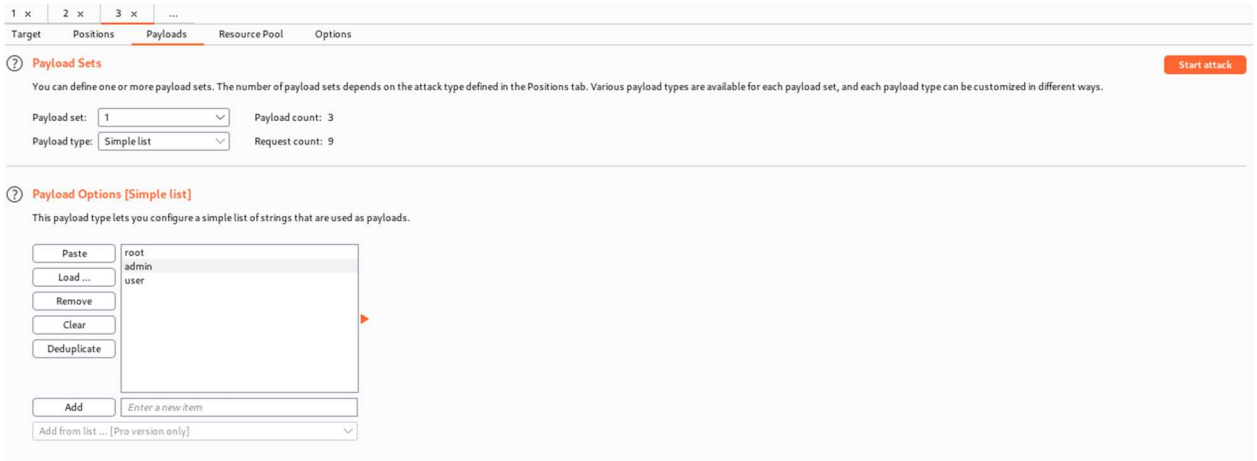


Open the intruder tab and navigate to positions.

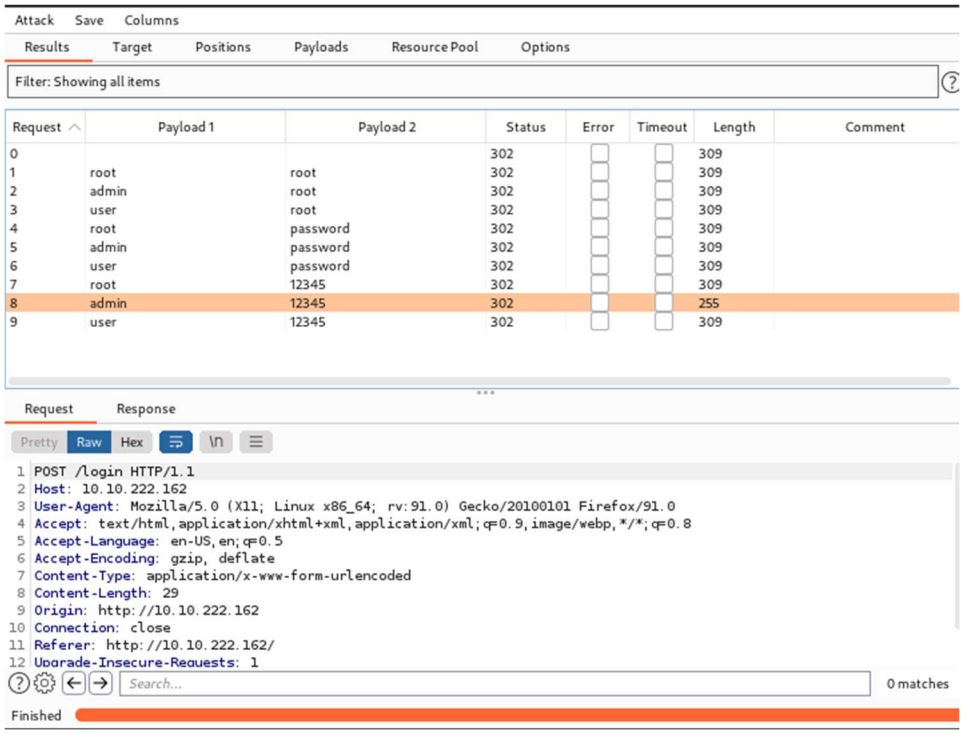


Question 8:

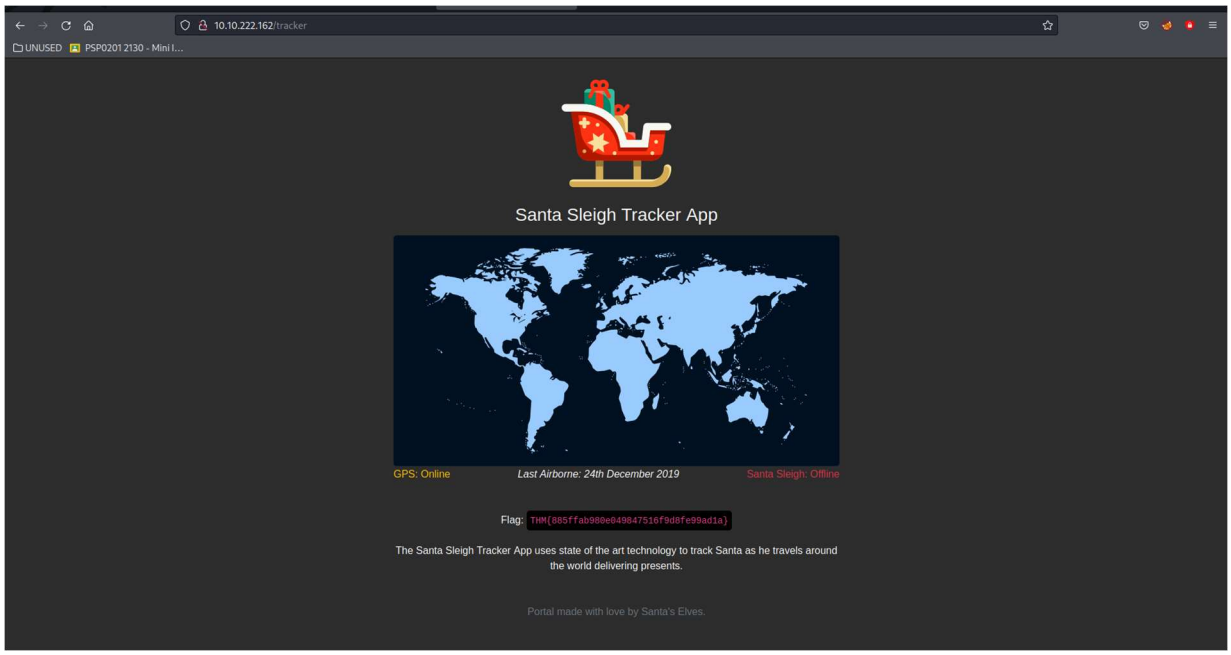
Navigate to payloads and set the default credentials. Launch the attack.



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



Enter the correct credentials.



Thought Process/Methodology

After accessing the IP address of the target's machine, we filled in the sign in form. Then, we opened FoxyProxy and Burpsuite and clicked on register. A request was sent to Burpsuite and we sent the request to intruder. We went to intruder tab on Burpsuite and set the position as cluster bombs. Afterwards, we went to payload and filled in the default credentials given in TryHackMe. We started the attack and waited for it to end. We inspected the length of the request and chose the one with the different length of request. Afterwards, we used the correct credentials to fill in the registration form. Once we were inside the Santa Sleigh Tracker App, we found the flag.

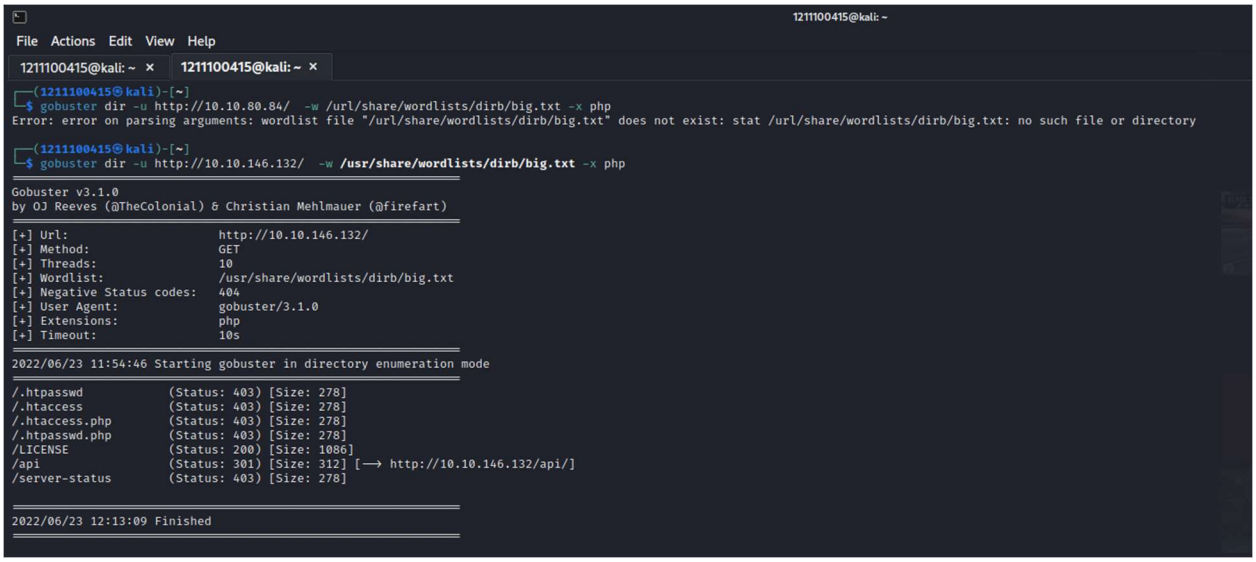
Day 4: Web Exploitation – Santa's watching

Tools: Kali Linux, Firefox, GoBuster, wfuzz

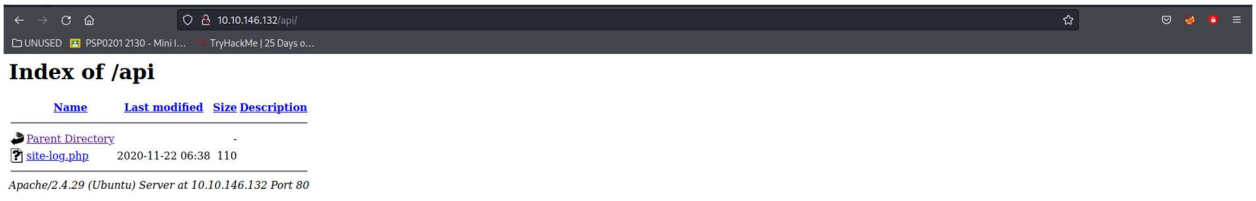
Solution:

Question 2

Use GoBuster to find the API directory.

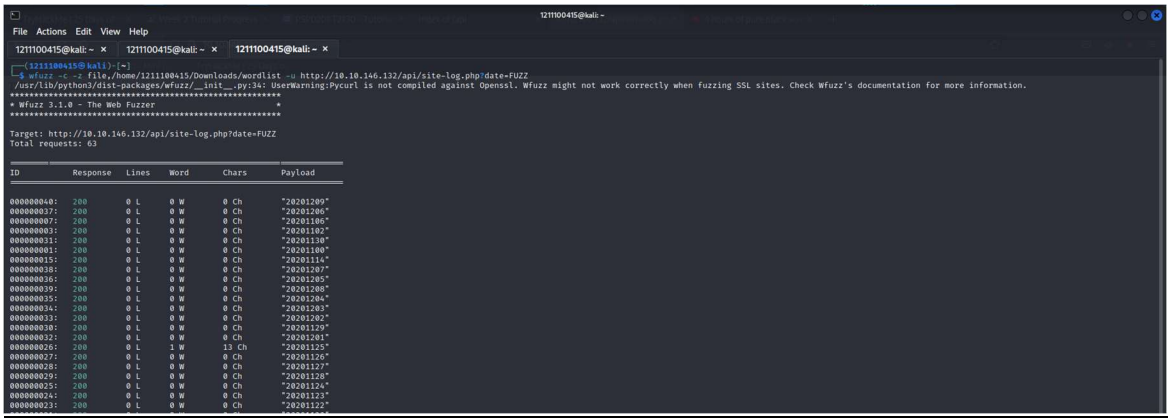


Head to the API directory.



Question 3

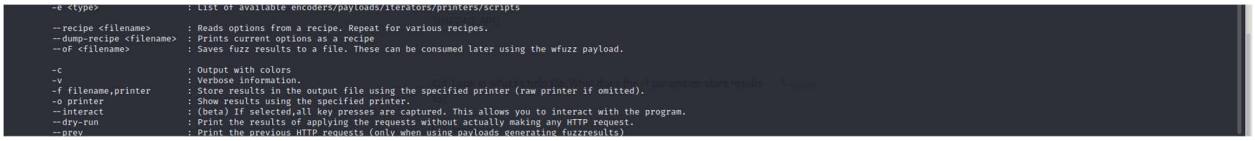
Fuzz the date parameter on the site.log.php in the API directory.



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.



Thought Process/Methodology

After accessing the IP address of the target's machine, we found out that the login page had been removed. Seeing this, we decided to use GoBuster to search for the API directory on where the file was stored. Once we had found the file inside the directory fuzz the date parameter of the file in the directory to find the response that contained the file that we needed. Then, we headed to the correct post to find the flag.

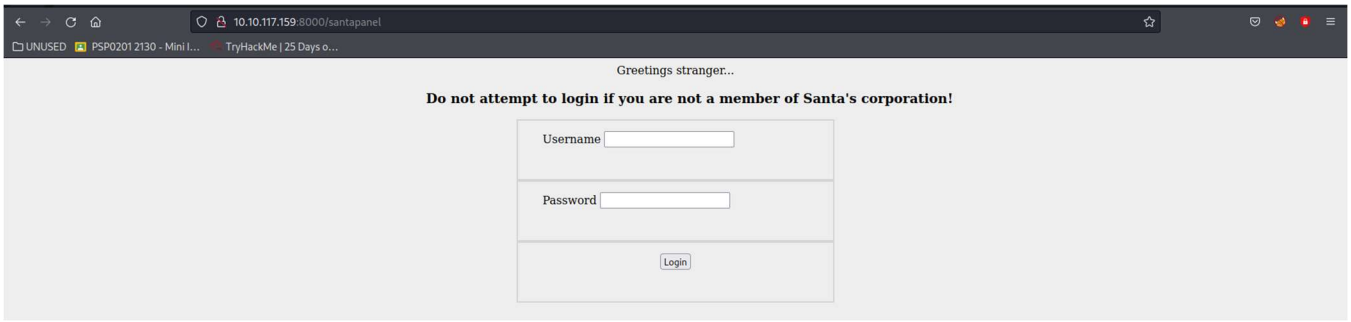
Day 5: Web Exploitation - Someone stole Santa's gift list!

Tools: Kali Linux, Firefox, SQLMap

Solutions:

Question 2:

Navigate to Santa's secret control panel.



Question 3:

Read the documentation.

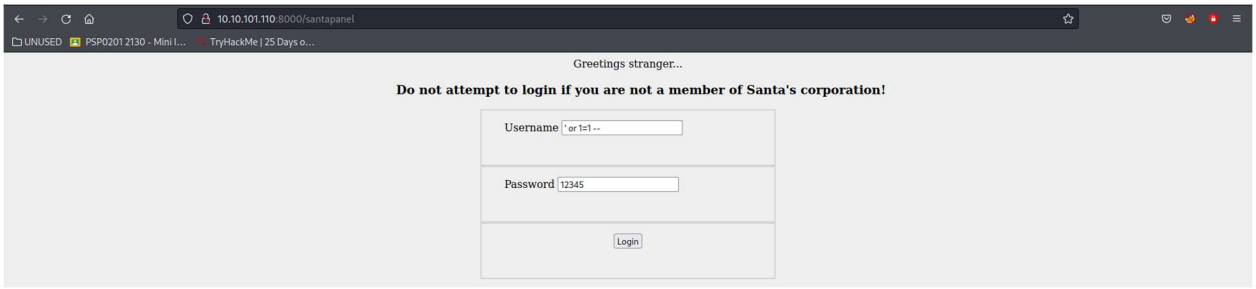
Visit the vulnerable application in Firefox, find Santa's secret login panel and bypass the login. Use some of the commands and tools covered throughout today's task to answer Questions #3 to #6.

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

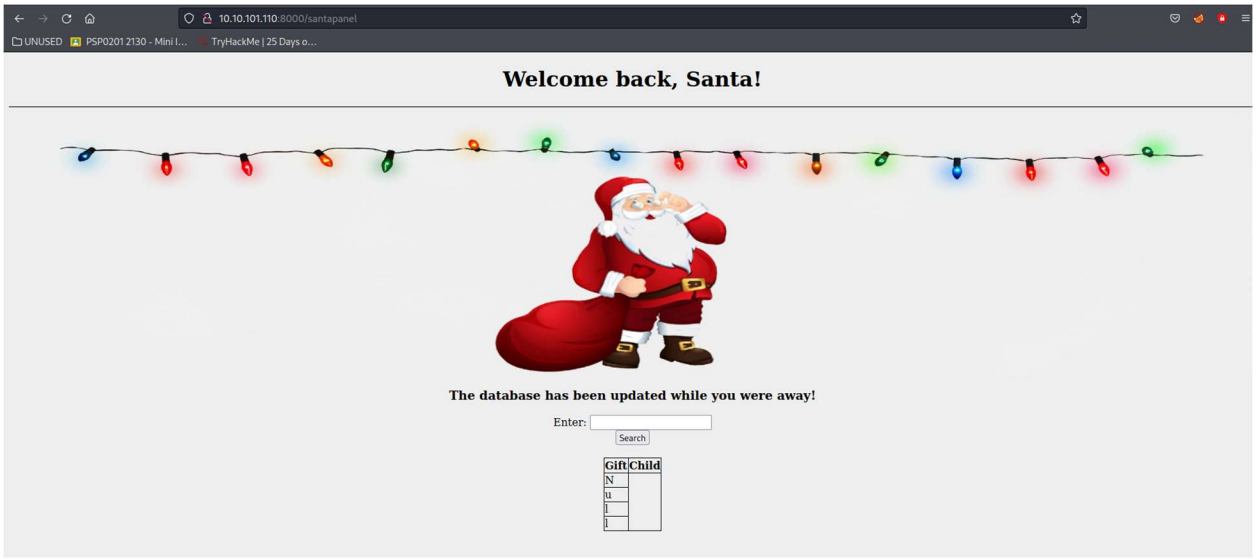
Santa's TODO: Look at alternative database systems that are better than sqlite. Also, don't forget that you installed a Web Application Firewall (WAF) after last year's attack. In case you've forgotten the command, you can tell SQLMap to try and bypass the WAF by using `--tamper=space2comment`

Question 4:

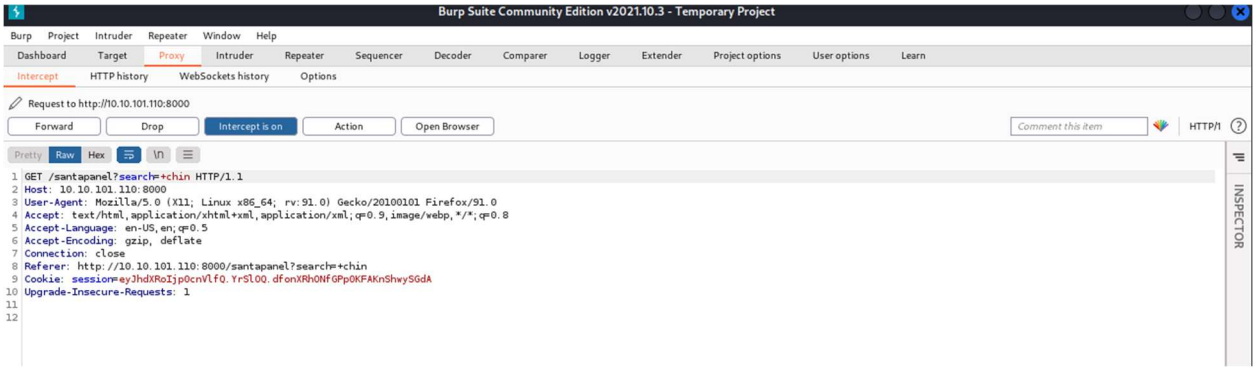
Input 'or 1=1 as the username to bypass the password authentication.



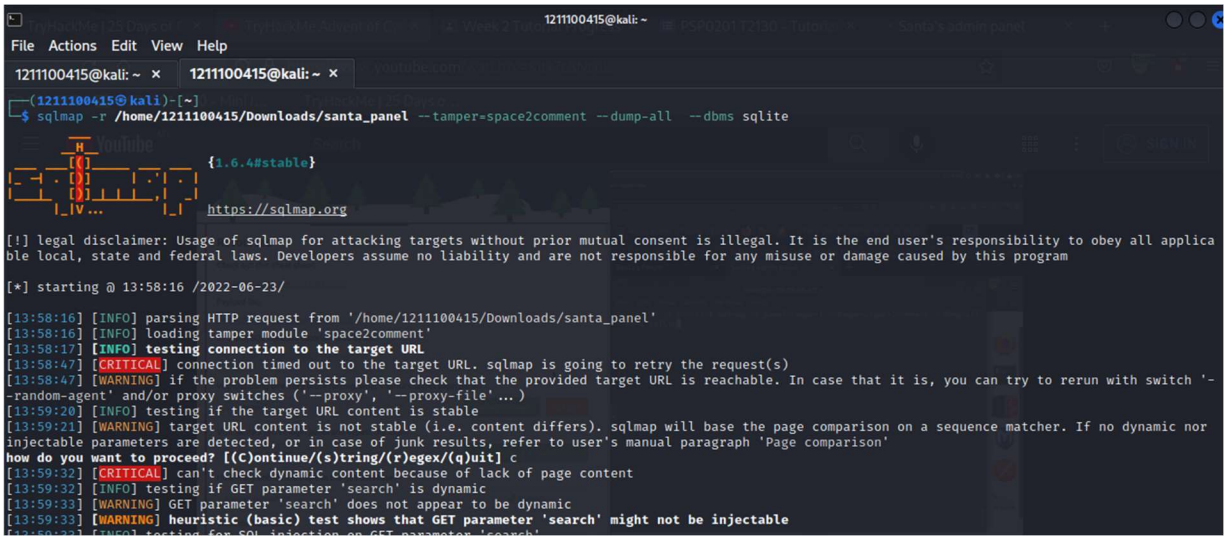
Now we are logged into Santa's forum.



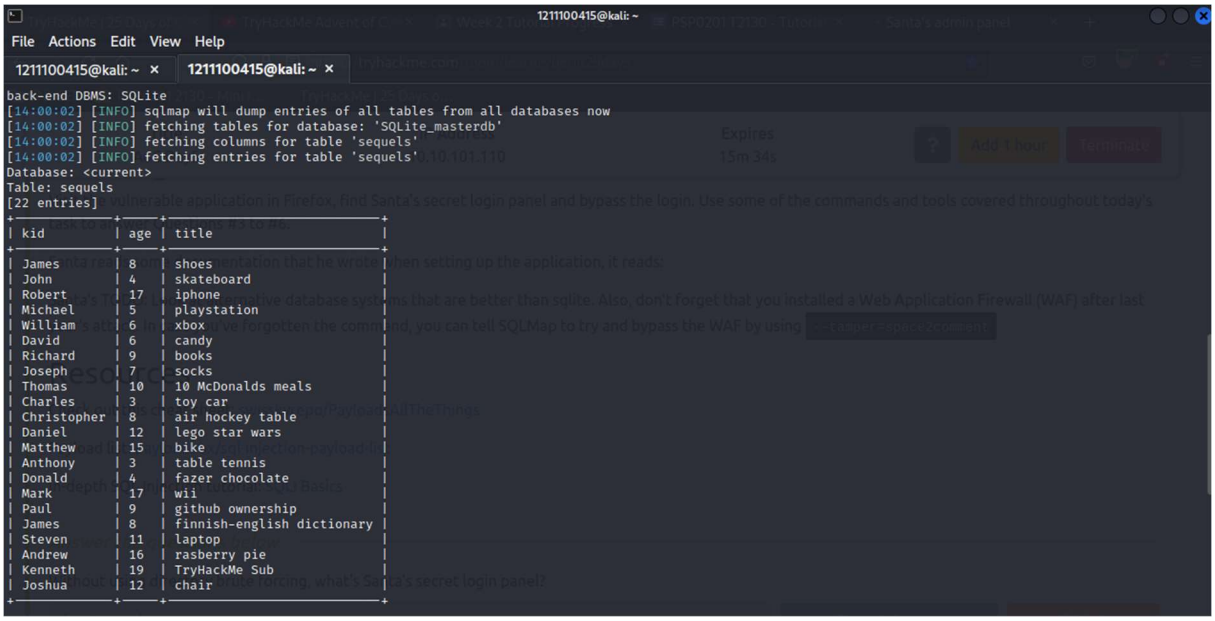
Open proxy and use the searchbox. Use Burpsuite to intercept the request and send to repeater. Save the request as file.



Use SQLMap to translate the request.

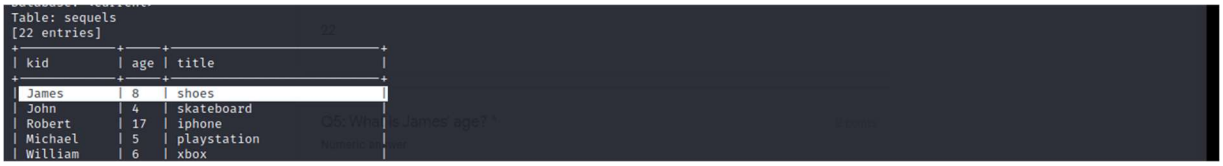


Look for the number of entries.



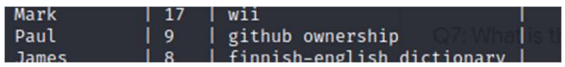
Question 5

Look for James' age.



Question 6

Look for what Paul wishes for Christmas.

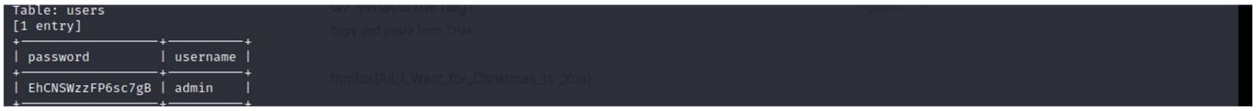


Question 7

Go to hidden_table.

Question 8

Go to users' table.



Thought Process/Methodology:

After accessing the IP address of the target's machine, we went to the hidden page. On Santa's secret login panel, we filled in the username with " ' or 1=1" to bypass the password authentication. Once we were inside Santa's forum, we opened Burpsuite and Foxyproxy and used the search box on the page. We will be given a request inside the Burpsuite; send the request to repeater and save the item as santa_panel. Use SQLMap to translate request. Once the request had been translated, we could see three tables which were "sequel", "hidden_table" and "users". We found the flag inside the "user" table.