PSP0201 WEEK 2 WRITE-UP

Group: 1K HONDA

Members

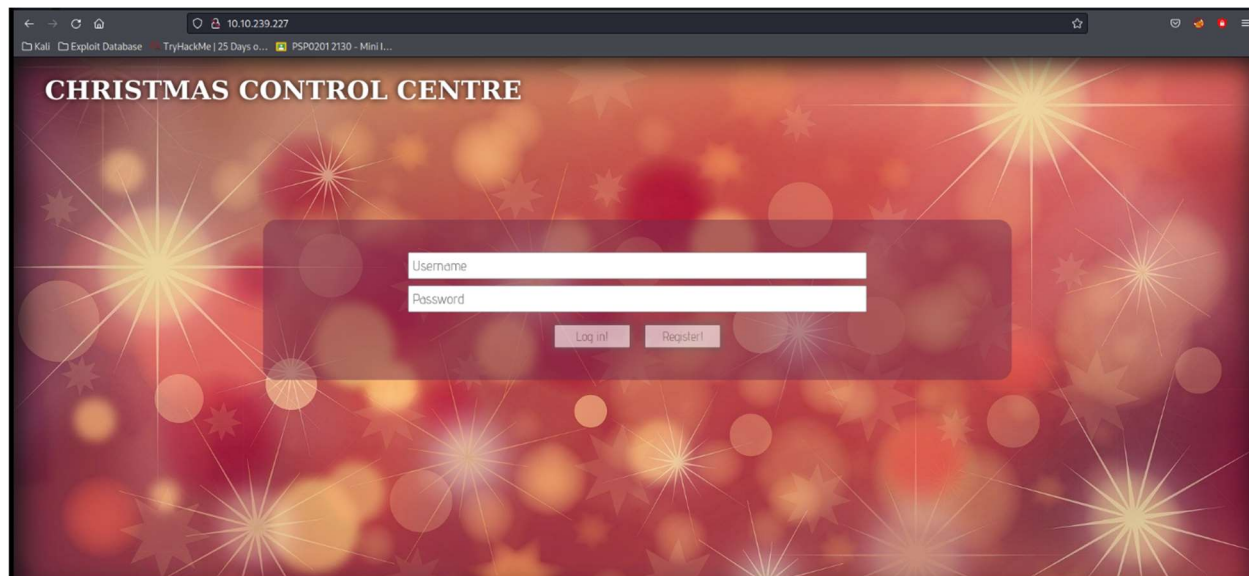| ID	Name	Role
1211100415	Muhammad Ummar Hisham bin Ahmad Madzlan	Leader
1211103066	Balqis Afiqah binti Ahmad Fahmi	Member
1211101925	Nur Alya Nabilah binti Md. Naser	Member

Day 1: Web Exploitation – A Christmas Crisis

Tools: Kali Linux, Firefox
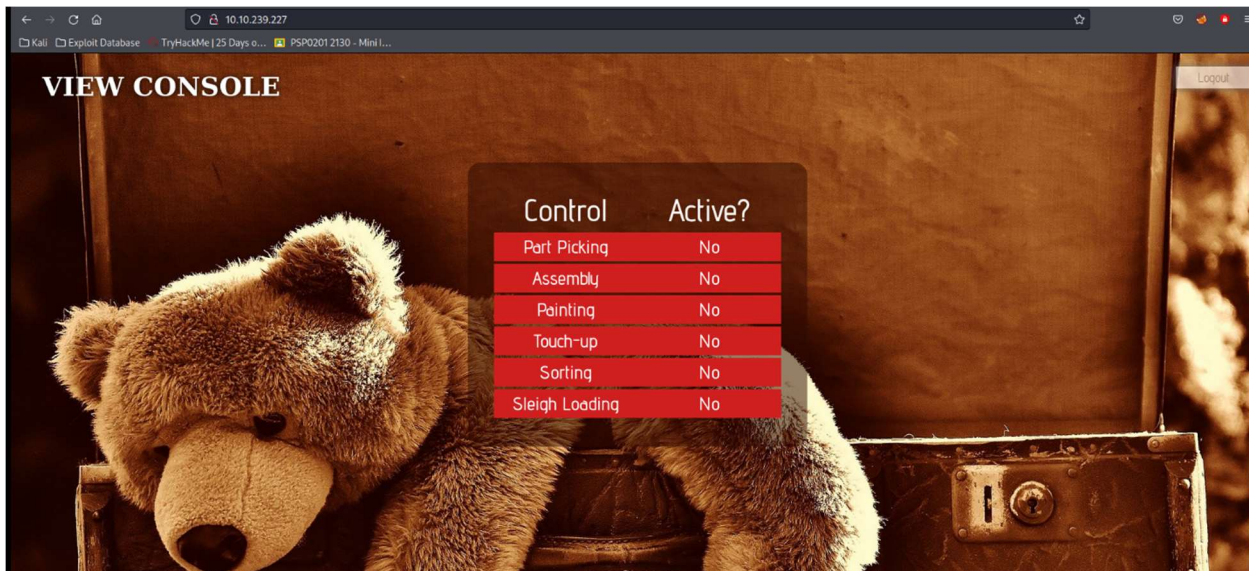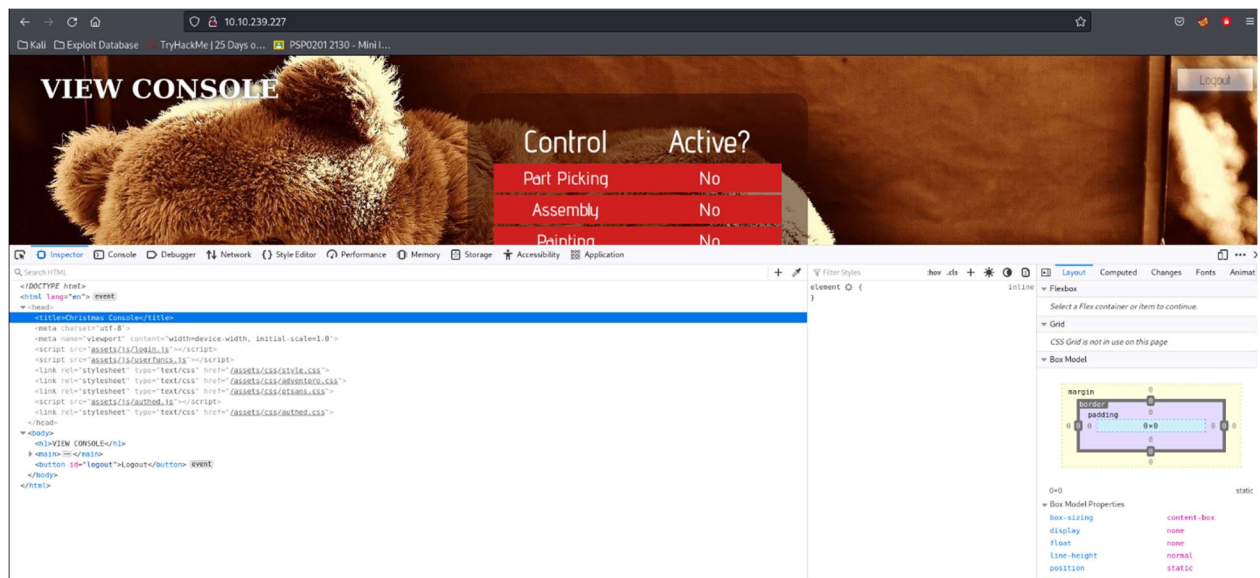
Solution:

Question 1

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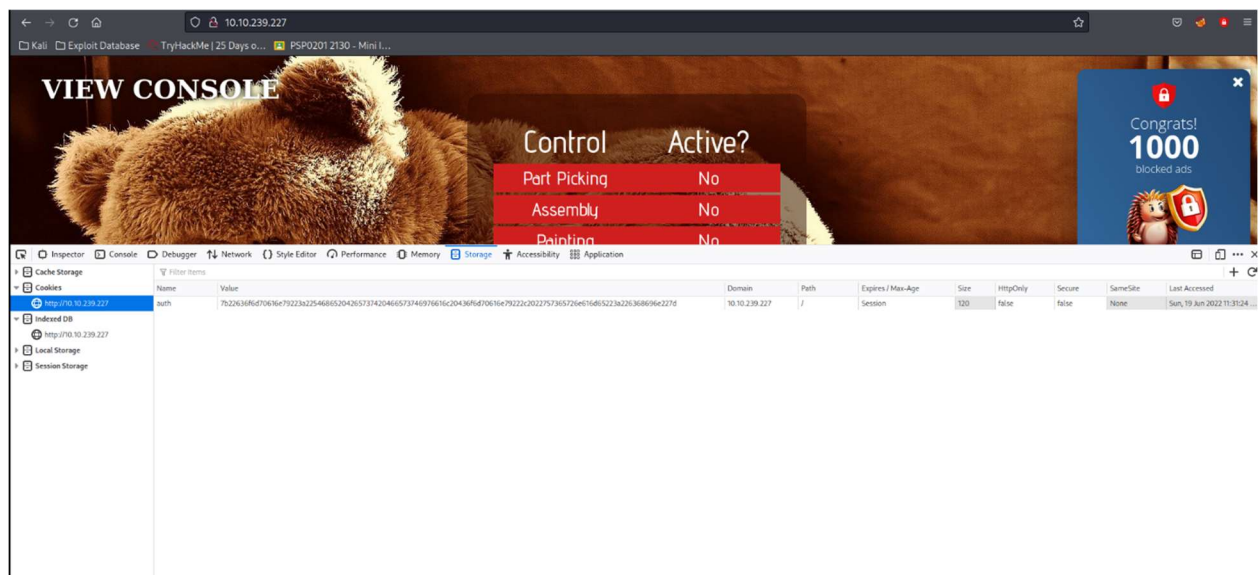

However, there is no access to the control panel.

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:
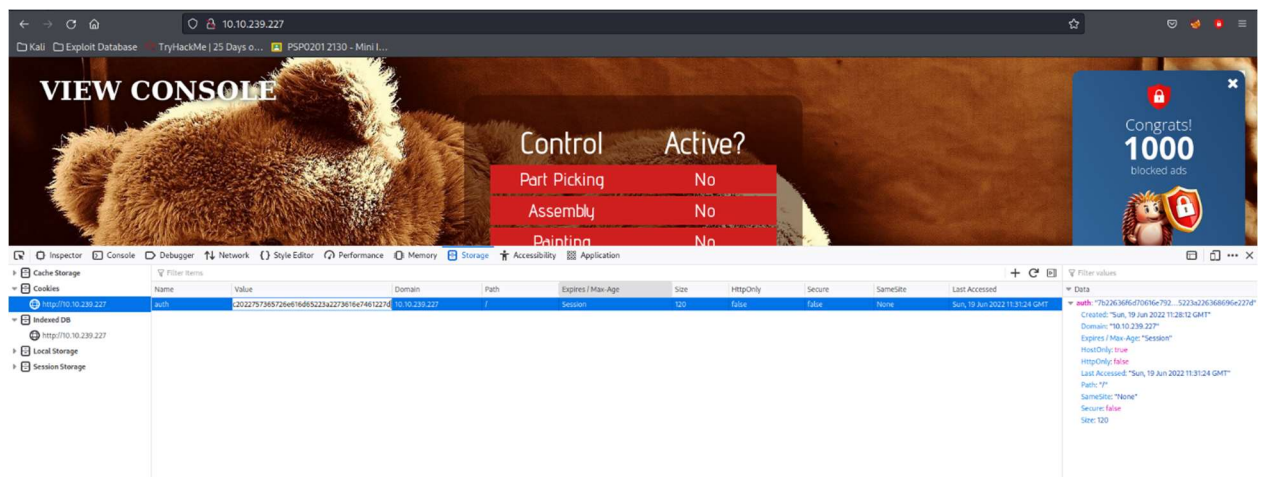
Decode the value of the cookie using CyberChef.

Question 7:

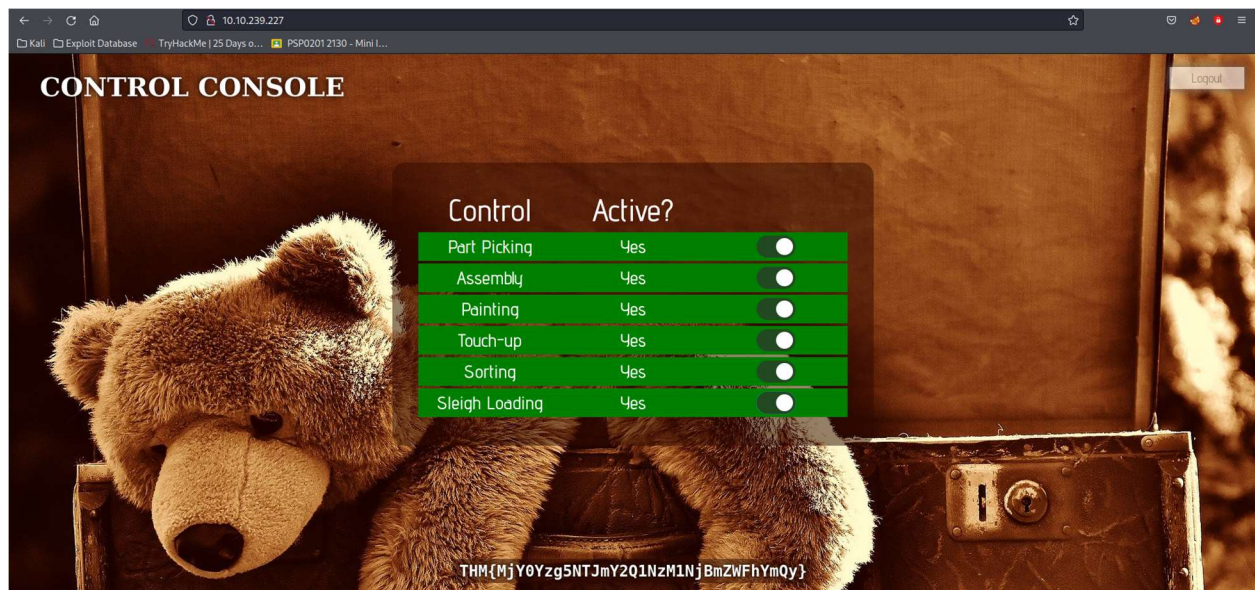Copy & paste the JSON statement. Then, change username field to "santa".
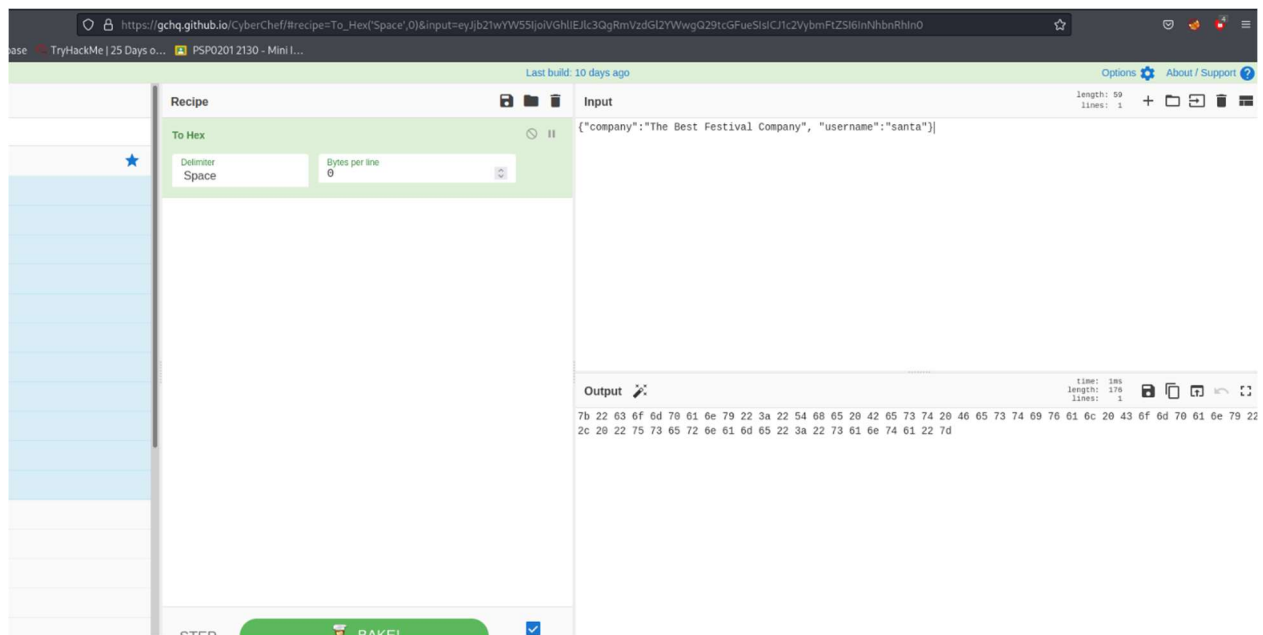
Question 8:

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 are brought to a login/registration screen. Then, we create an account and log in using that account. Once we are inside the control panel, we will open the developers' tool and inspect the storage tab to view the name and value of the cookie. After that, we open CyberChef to decode the value of the cookie and we can see the JSON statement. Copy the JSON statement and paste it into CyberChef. Change the value of username to "santa" and encode it to hexadecimal. Copy and paste the hexadecimal value into the developers' tool and we will be brought to the admin's control panel. Refresh the page and turn all the controls on.

Day 2: Web Application – The Elf Strikes Back

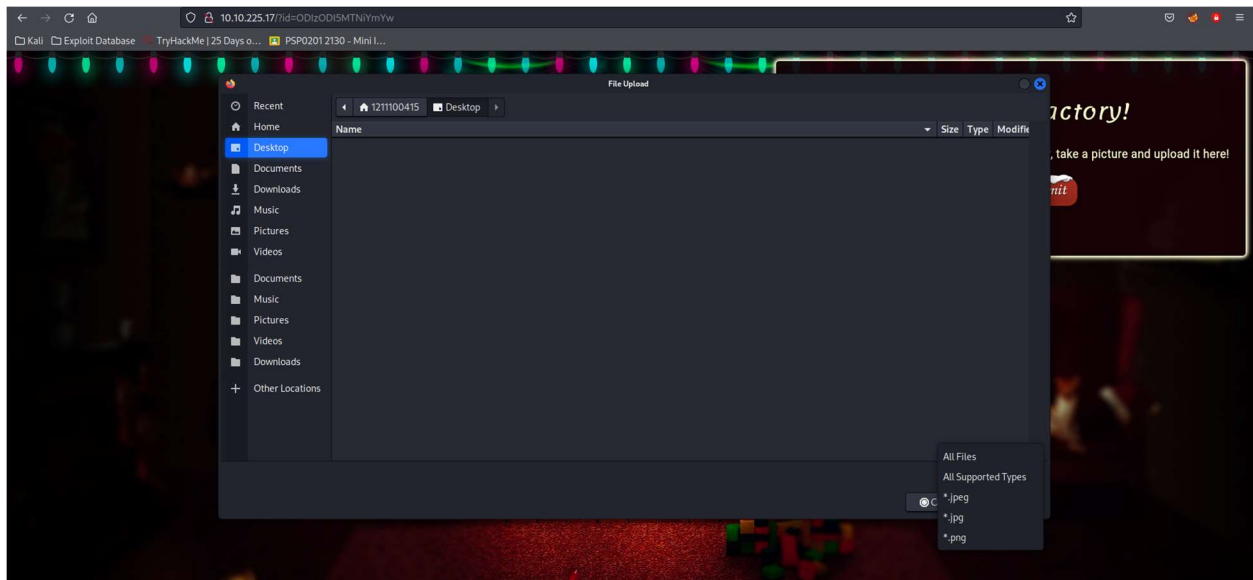**Tools:** Kali Linux, Mousepad, Firefox

Question 1:

Using the GET parameter, input the ID given in the sticky note into the URL.
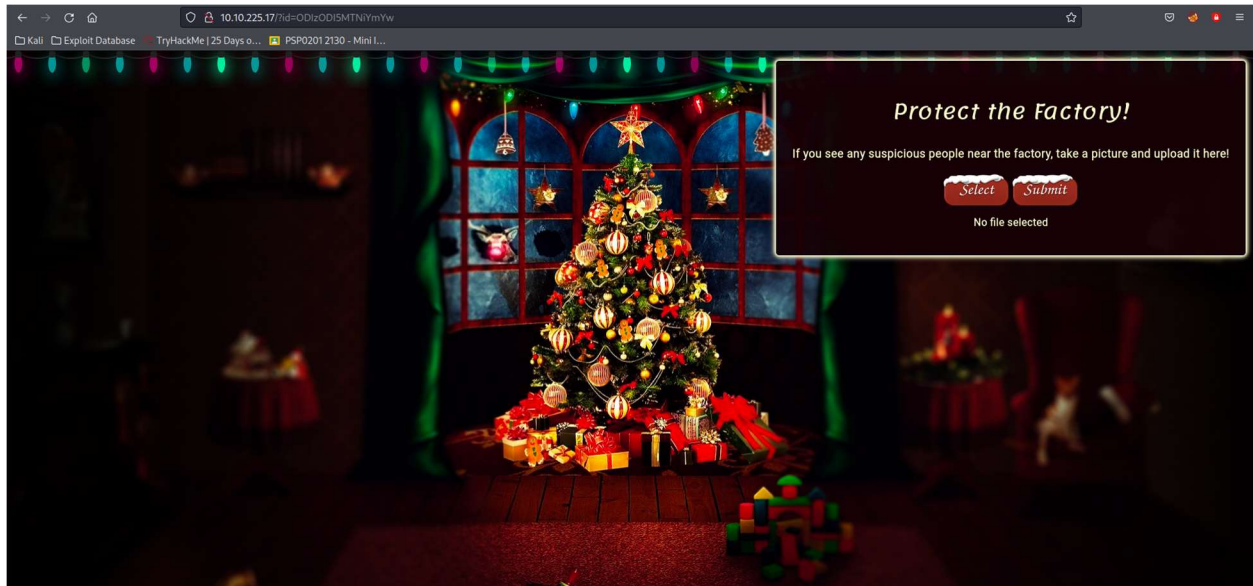
Question 2:

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, use the GET parameter and the username given in the dossier to log into the page. After that, investigate what type of files that is are supported by the page. Copy the reverse shell script and paste into a notepad. Save the notepad as shell.jpg.php and upload into the page. Go to the page where the uploaded file is stored. Activate the netcall listener and reverse shell.

Day 3: Web Exploitation – Christmas Chaos

Tools: Kali Linux, Firefox, Burpsuite, Foxyproxy

Solution:

Question 1 & 2:

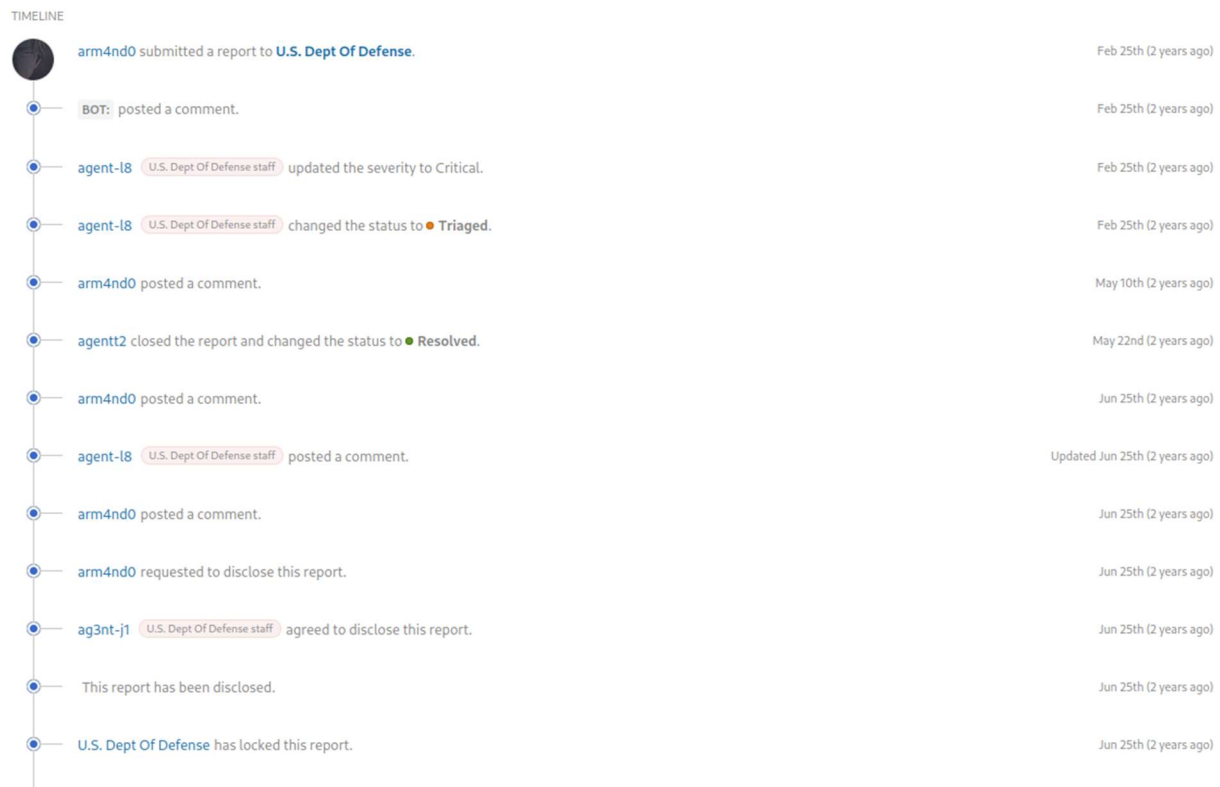Read the passage in TryHackMe.

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):
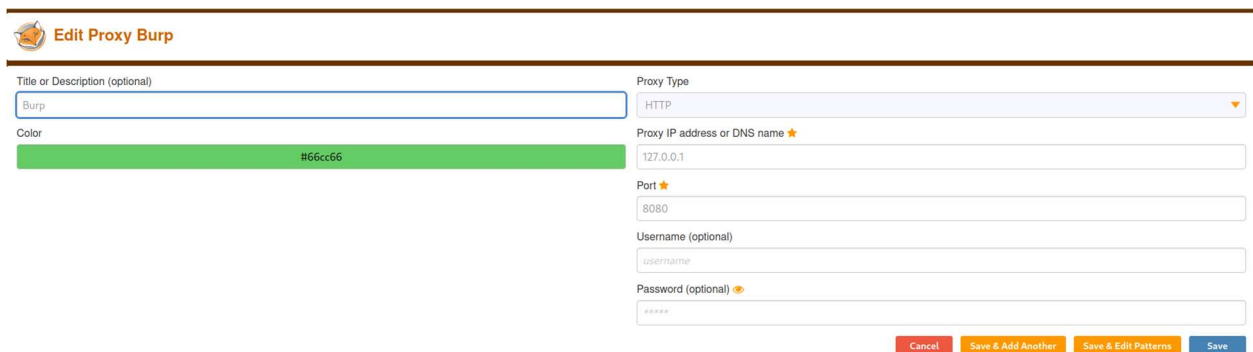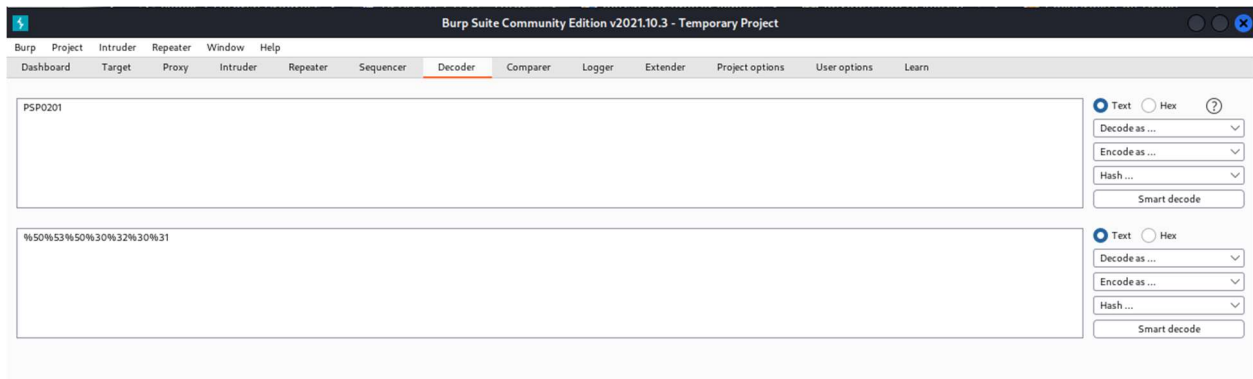
Question 3:

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.
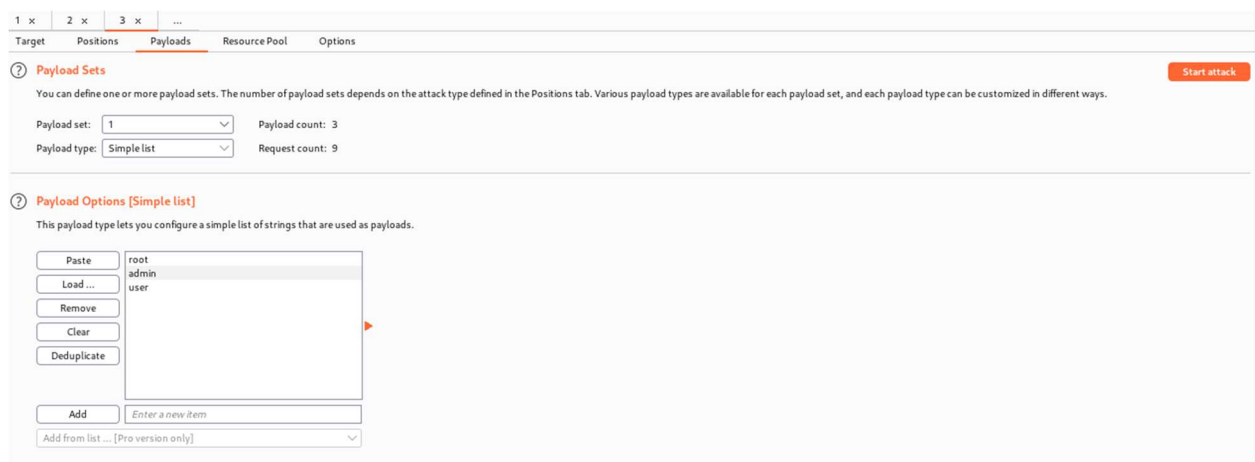

Open the intruder tab and navigate to positions.
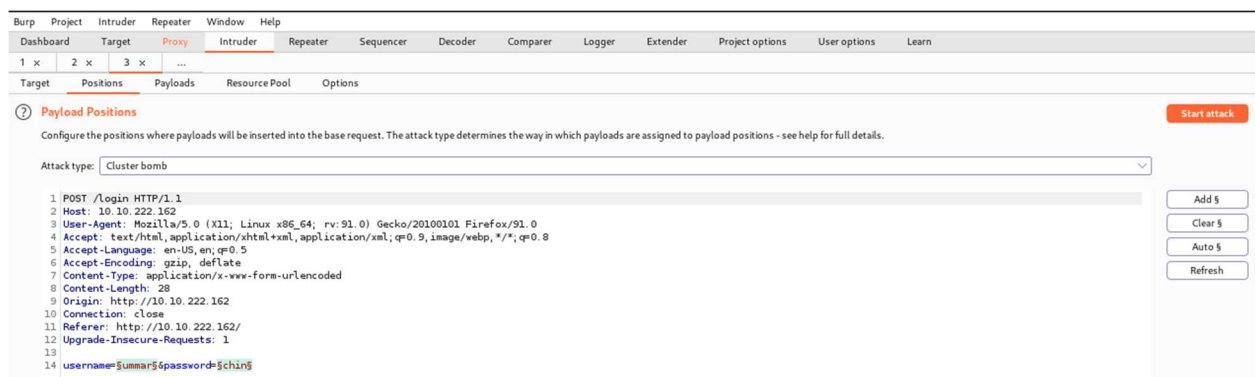
Question 8:

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

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.

Paste	root
Load ...	password
Remove	12345
Clear	
Deduplicate	

Add

Add from list ... [Pro version only]

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

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	

Request   Response

Pretty   Raw   Hex

```
1 POST /login HTTP/1.1
2 Host: 10.10.222.162
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://10.10.222.162
10 Connection: close
11 Referer: http://10.10.222.162/
12 Upgrade-Insecure-Requests: 1
```
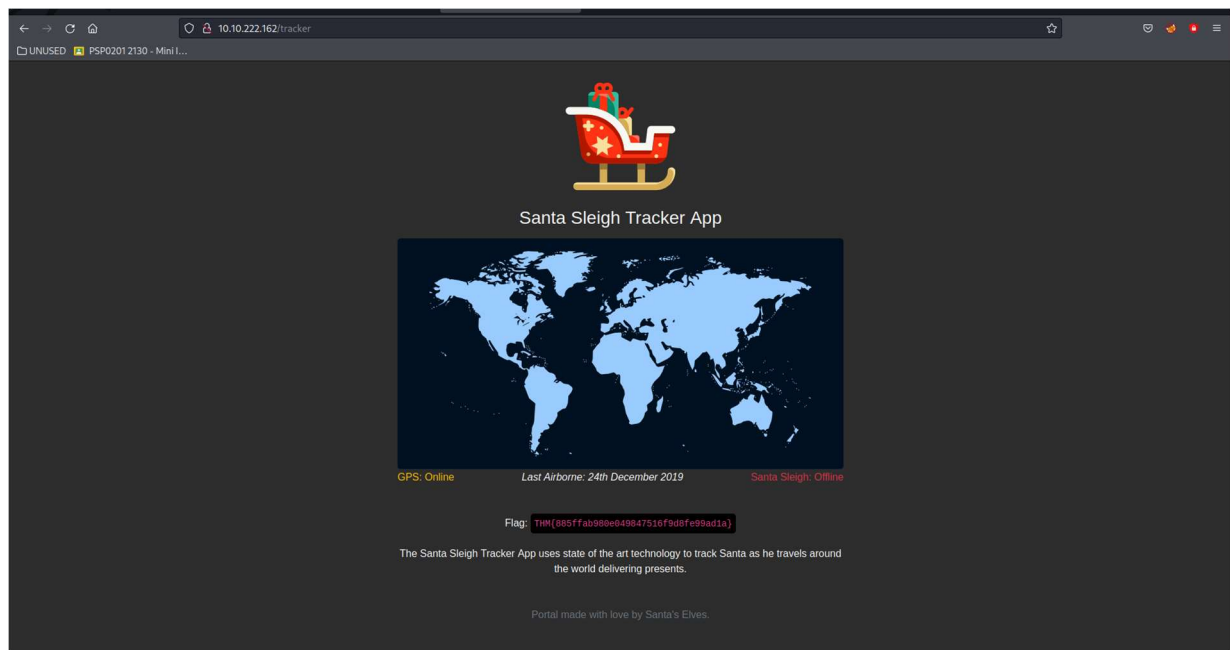
? ⚙ ← → Search...   0 matches

Finished

Enter the correct credentials.

Thought Process/Methodology

After accessing the IP address of the target's machine, fill the sign in form. Open FoxyProxy and Burpsuite and click on register. A request will be sent to Burpsuite and send the request to intruder. Go to intruder tab on Burpsuite and set the position as cluster bombs. Go to payload and fill in the default credentials given in TryHackMe. Start the attack and wait for it to ends. Inspect the length of the request and choose the one with the different length of request. Use the correct credentials to fill in the registration form.

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.

THM{D4t3_AP1}

Question 4

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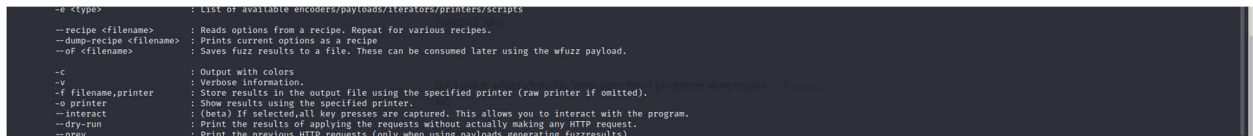
Thought Process/Methodology

After accessing the IP address of the target's machine, use GoBuster to search for the directory on where the file is stored. Once we have found the file inside the directory fuzz the date parameter of the file in the directory to find the correct post. Then head to the post.
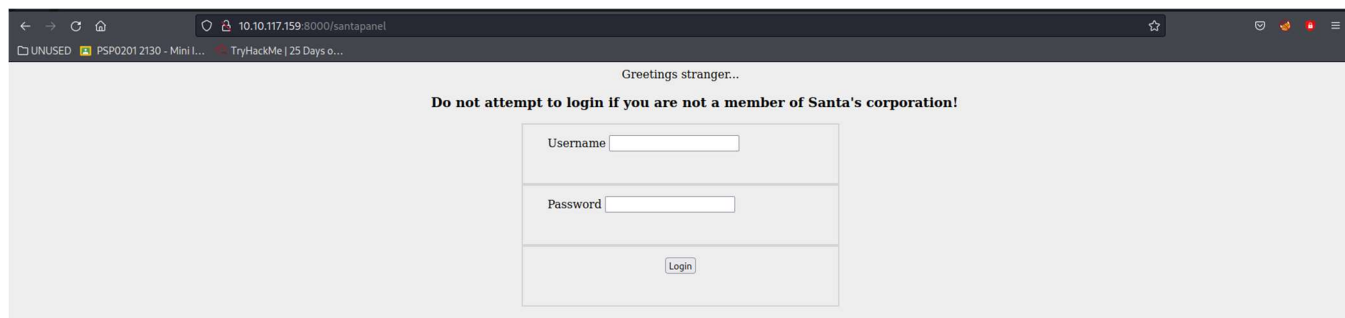
Day 5: Web Exploitation - Someone stole Santa's gift list!

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`
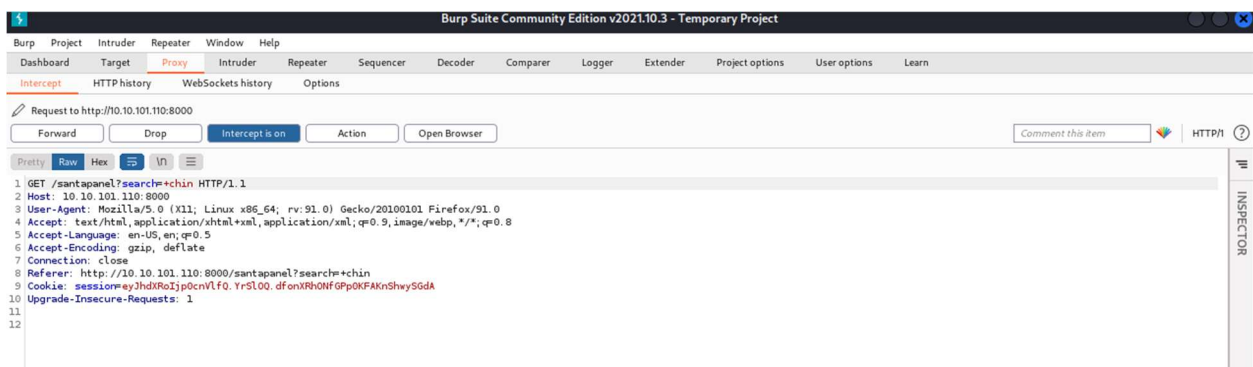
Question 4:

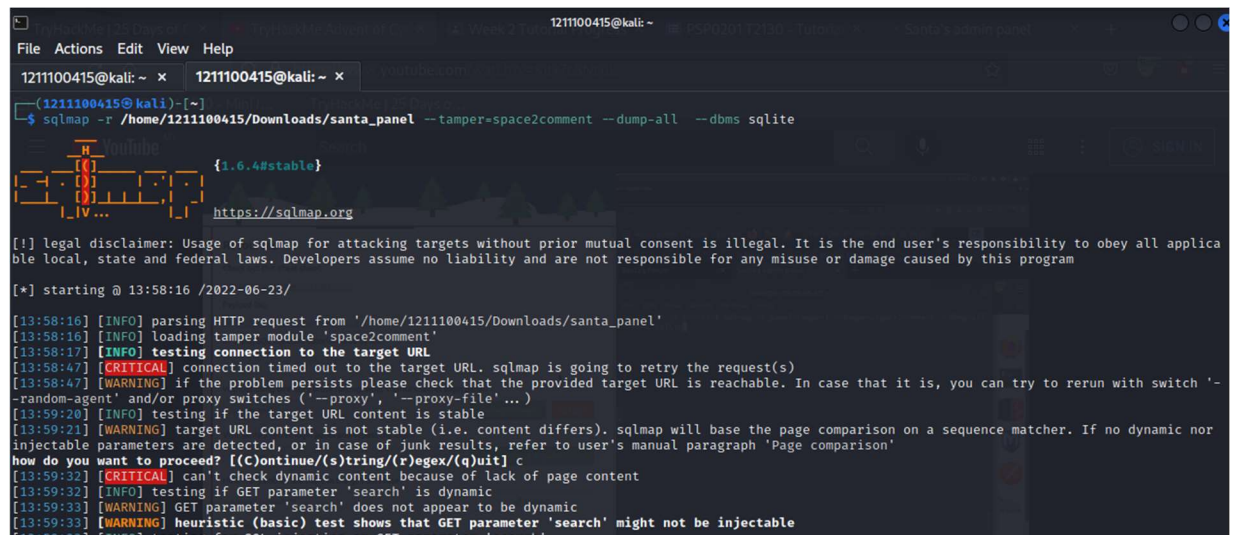Input 'or 1=1 as the username to bypass the password authentication.
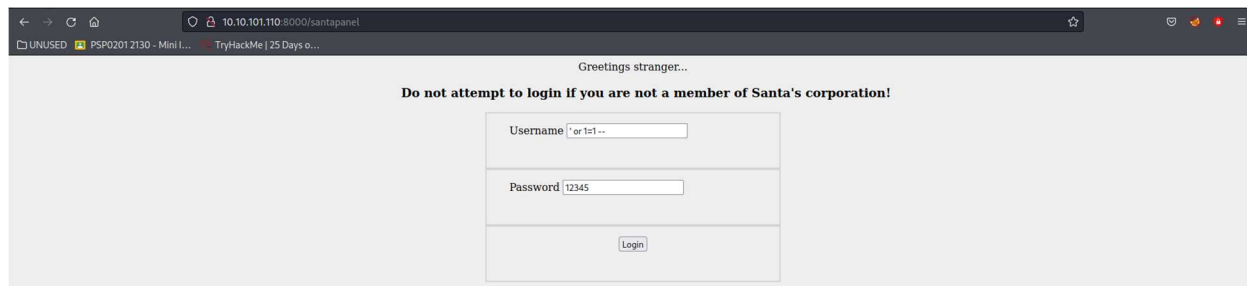
Now we are logged into Santa's forum.
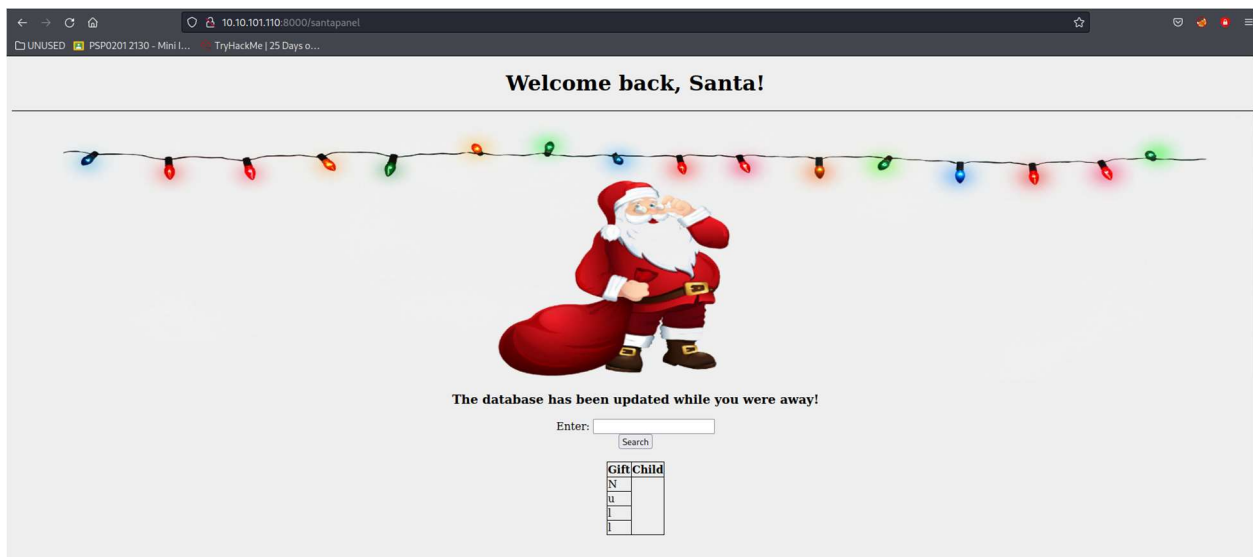
Open proxy and use the searchbox. Use Burpsuite to intercept the request and send to repeater. Save the request as file.

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, go to the hidden page. We will be brought to a login page and fill in the username with ' or 1=1 to bypass the authentication. Once we are inside Santa's forum, open Burpsuite and Foxyproxy and use 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.