PSP0201
WEEK 2
WRITEUP

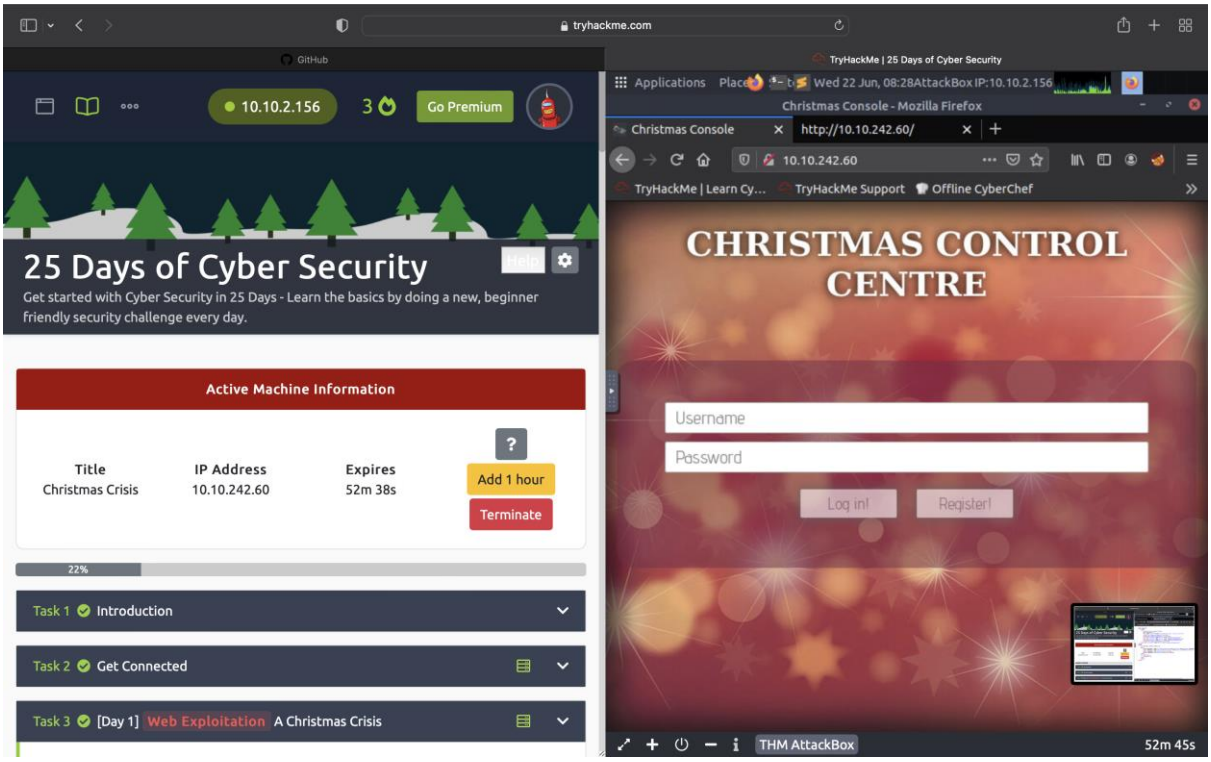
Group Members	ID
1) Nevendra Eravanan	1211101778
2) Avinnaesh A/L G Baramesvaran	1211101658
3) Arvind A/L Krishna Kumar	1211101977

Day 1: Web exploitation – A Christmas Crisis

Walkthrough/solution

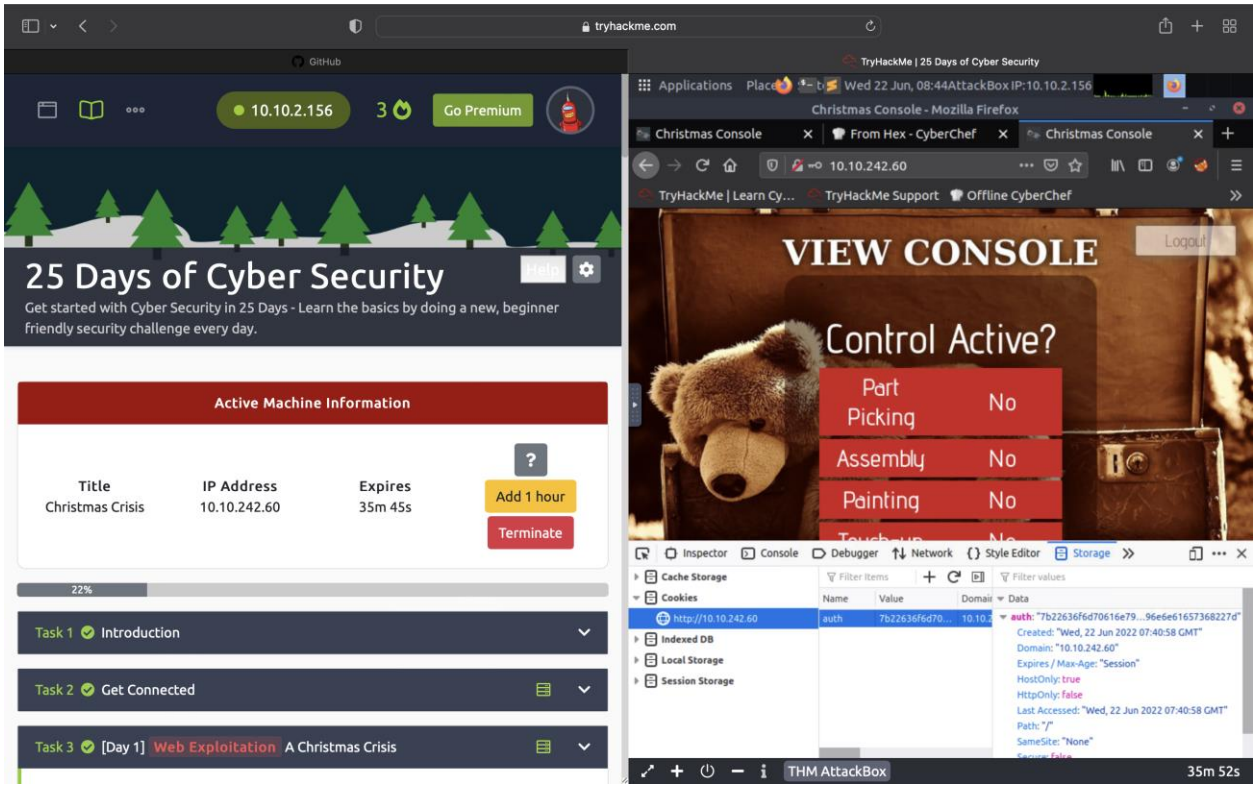
Question 1 : Inspect the website. What is the title of the website?

- Registration and login page of Christmas Console. Register an account in the website to login.



Question 2: What is the name of the cookie used for authentication?

- Once logged in the website, inspect the elements in the website to bring up the console. Navigate to the storage tab to obtain the auth cookie.



Question 3 : In what format is the value of this cookie encoded?

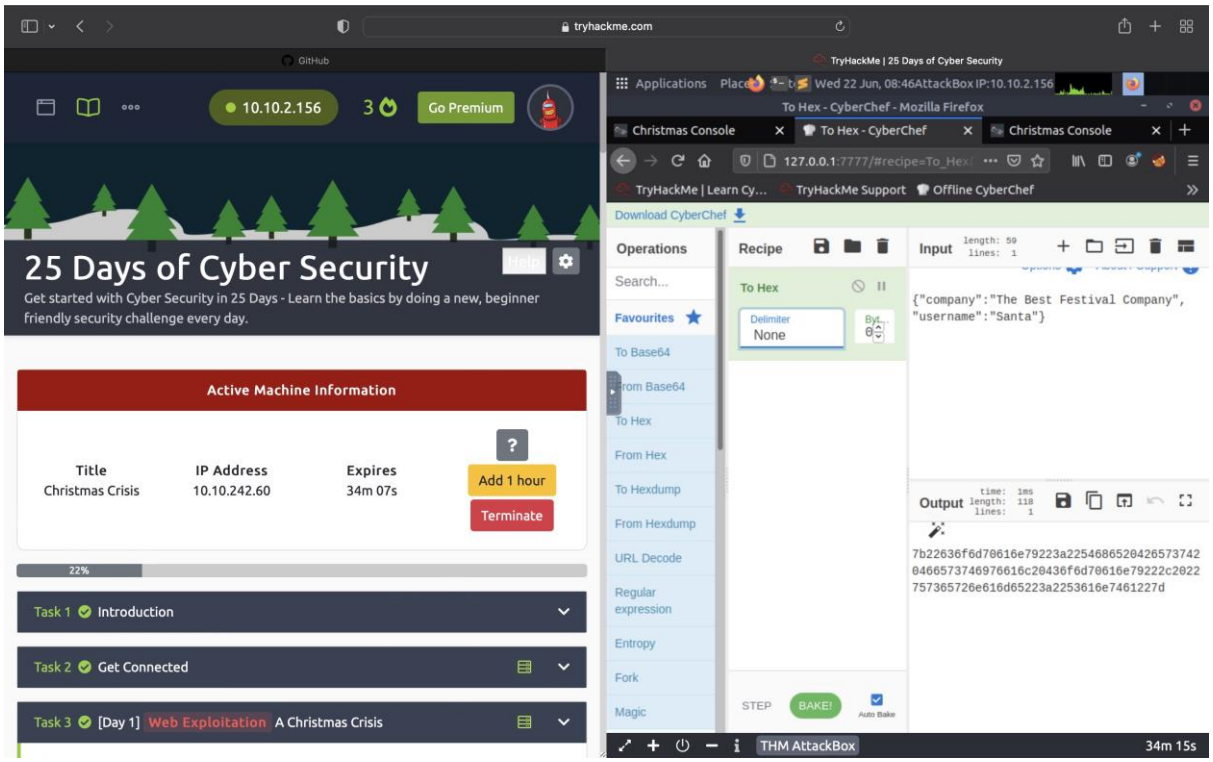
- Using Cyberchef, convert the cookie value to a string.

Question 4 : Having decoded the cookie, what format is the data stored in?

- Copy the and paste the cookie value in JSON format and change the username to santa to convert it to hex value and obtain santa's cookie.

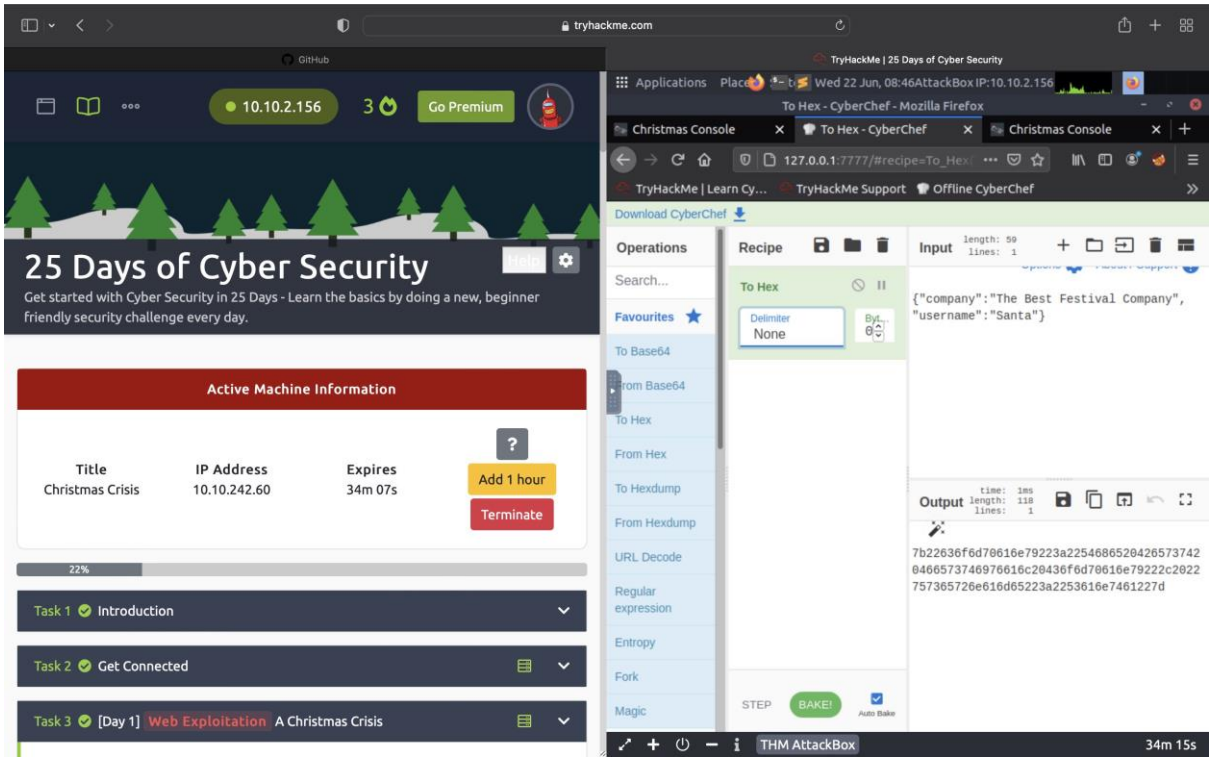
Question 5 : What is the value for the company field in the cookie?

- Decode the cookie value and it will reveal the value of the company field.



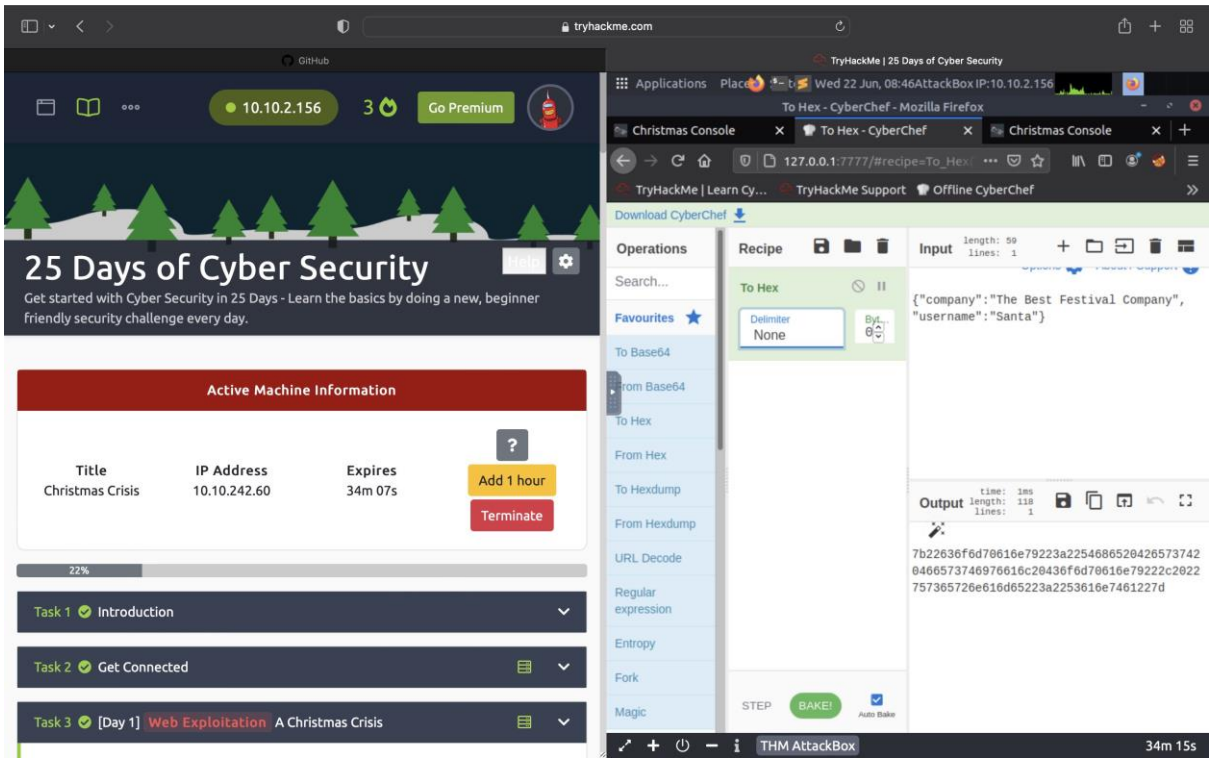
Question 6 : What is the other field found in the cookie?

- Decode the cookie value and it will reveal two fields.



Question 7 : What is the value of Santa's cookie?

- Copy the and paste the cookie value in JSON format and change the username to santa to convert it to hex value and obtain santa’s cookie.



Question 8 : What is the flag you're given when the line is fully active?

- Activate all the controls to reveal the flag.

Day 2 – [Web exploitation] The elf strikes back!

Question 1: What string of text needs adding to the URL to get access to the upload page

- Use “?” to indicate that a GET parameter forthcoming. Enter “id=” with the value of the assigned id number.

At the bottom of the dossier is a sticky note containing the following message:

For Elf McEager:
You have been assigned an ID number for your audit of the system: `ODIzODI5MTNiYmYw` . Use this to gain access to the upload section of the site.
Good luck!

You note down the ID number and navigate to the displayed IP address (MACHINE_IP) in your browser.

Question 2 - What type of file is accepted by the site

- In the page source code, there is three file type accepted by the upload form.
- The site accepts image file type

```
    <body>
        <ul class="lightrope"><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></l
        <div class=nose></div>
        <main>
            <h1>Protect the Factory!</h1>
            <h2>If you see any suspicious people near the factory, take a picture and upload it here!</h2>
            <input type=file id="chooseFile" accept=".jpeg,.jpg,.png">
            <button tabindex=0 id=coverFile>Select</button>
            <button tabindex=1 id=uploadFile>Submit</button>
            <p id=fileText>No file selected</p>
        </main>

    </body>
</html>
```

Question 3 - In which directory are the uploaded files stored

- The uploaded files are stored in the “/uploads/” directory.

Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
home.jpg	2020-12-06 02:07	20K	

Question 4: What is the flag in /var/www/flag.txt

- Open the flag.txt file from the terminal using the command “cat flag.txt”.
- THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}

Day 3 [web exploitation] Christmas Chaos

Question 1 - What is the name of the botnet mentioned in the text that was reported in 2018?

- Mirai

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.

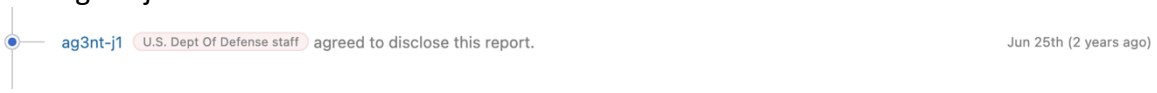
Question 2 - How much did Starbucks pay in USD for reporting default credentials according to the text

- Starbuck paid 250 USD

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 - who was the agent assigned from the Dept of Defense that disclosed the report on Jun 25th?

- ag3nt-j1



Question 4 - Examine the options on FoxyProxy on Burp. What is the port number for Burp?

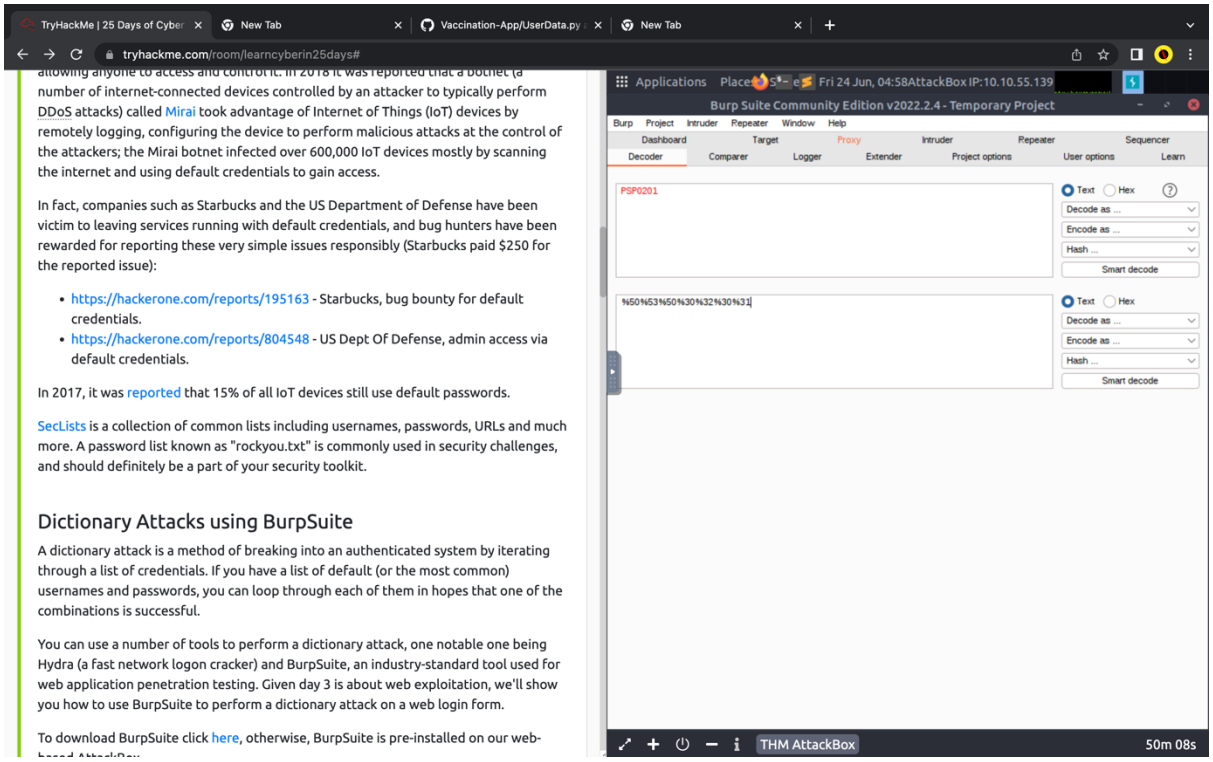
- The port number for Burp in the options is “8080”

Question 5- Examine the options on FoxyProxy on Burp. What is the proxy type?

- The proxy type for Burp is SOCKS5

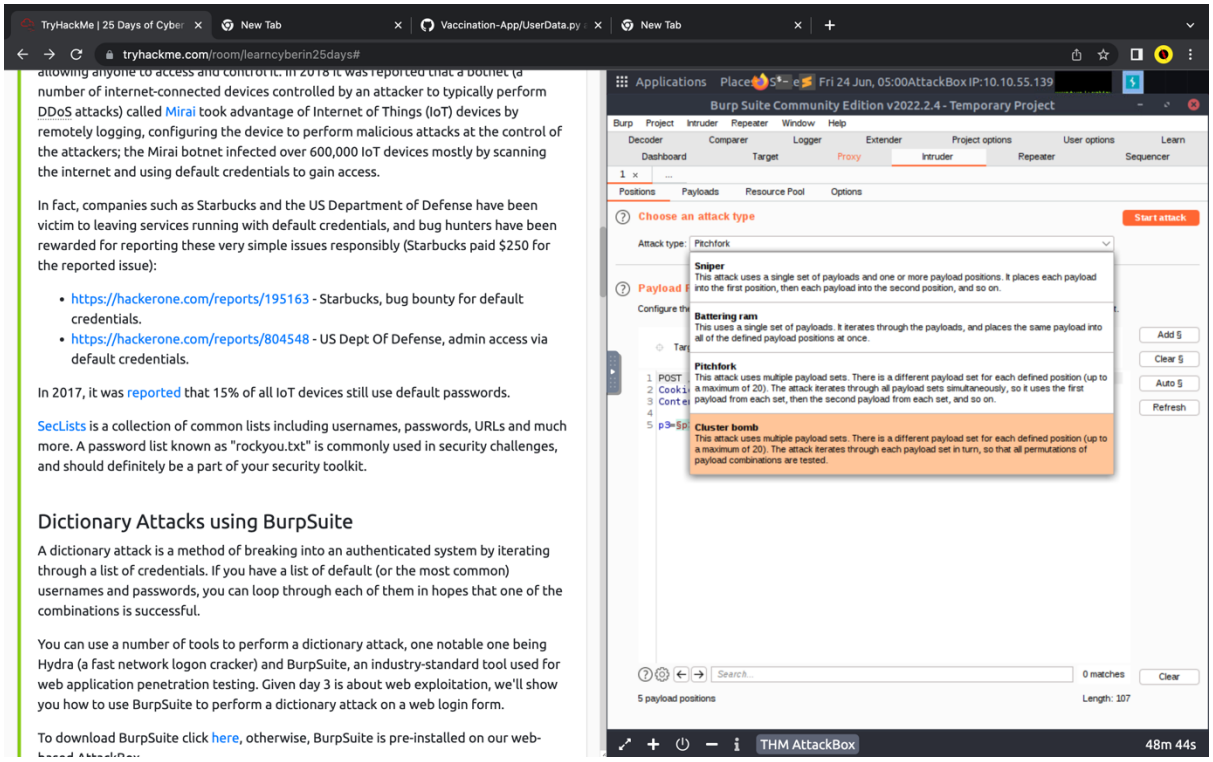
Question 6 - Experiment with decoder on Burp. What is the URL encoding for "PSP0201"?

- Navigate to the decoder tab and type out “PSP0201” and decode the value in URL format.



Question 7 - Look at the list of attack type options on intruder. Which of the following options matches the one in the description?

- Cluster bomb



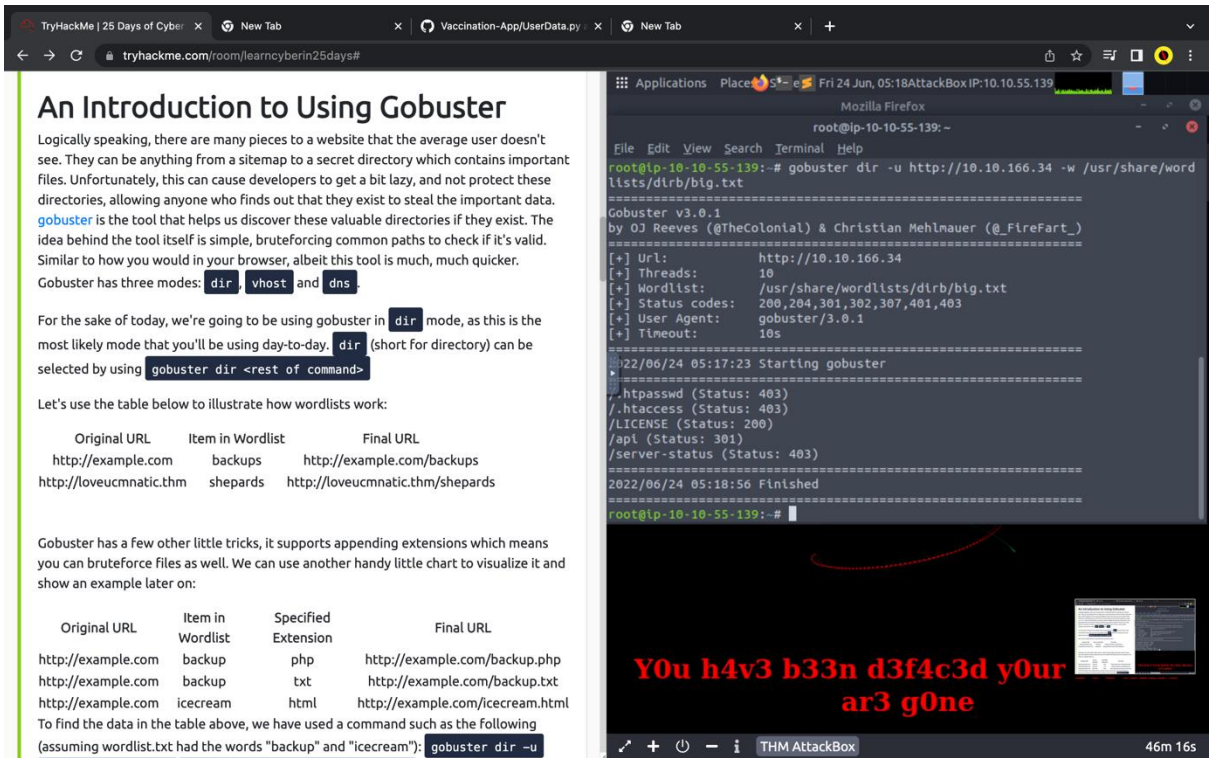
Question 8- What is the flag?

- The flag obtained is THM{885ffab980e049847516f9d8fe99ad1a}

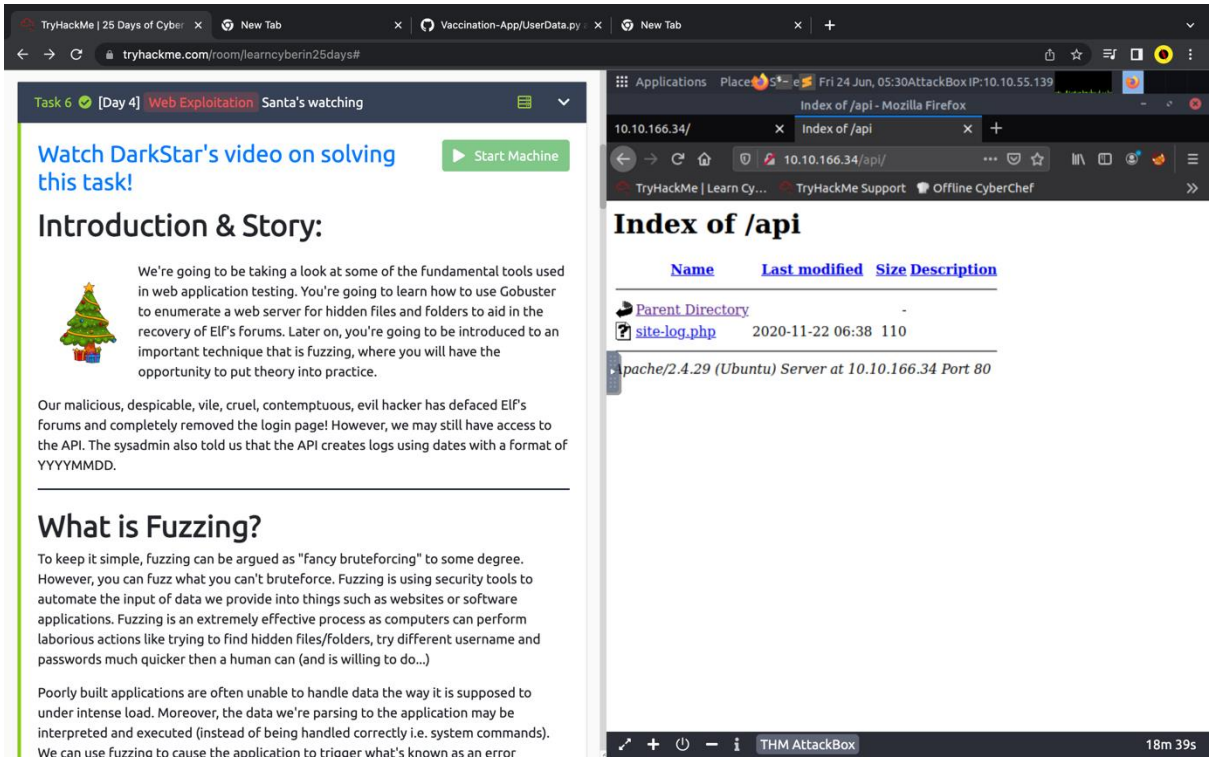
Day 4 – [Web Exploitation] Santa's Watching

Question 1: Use GoBuster (against the target you deployed -- not the shibes.xyz domain) to find the API directory. What file is there?

- Open the terminal and type out the command "gobuster dir -u http://your_ip_adress -w /usr/share/wordlists/big.txt"

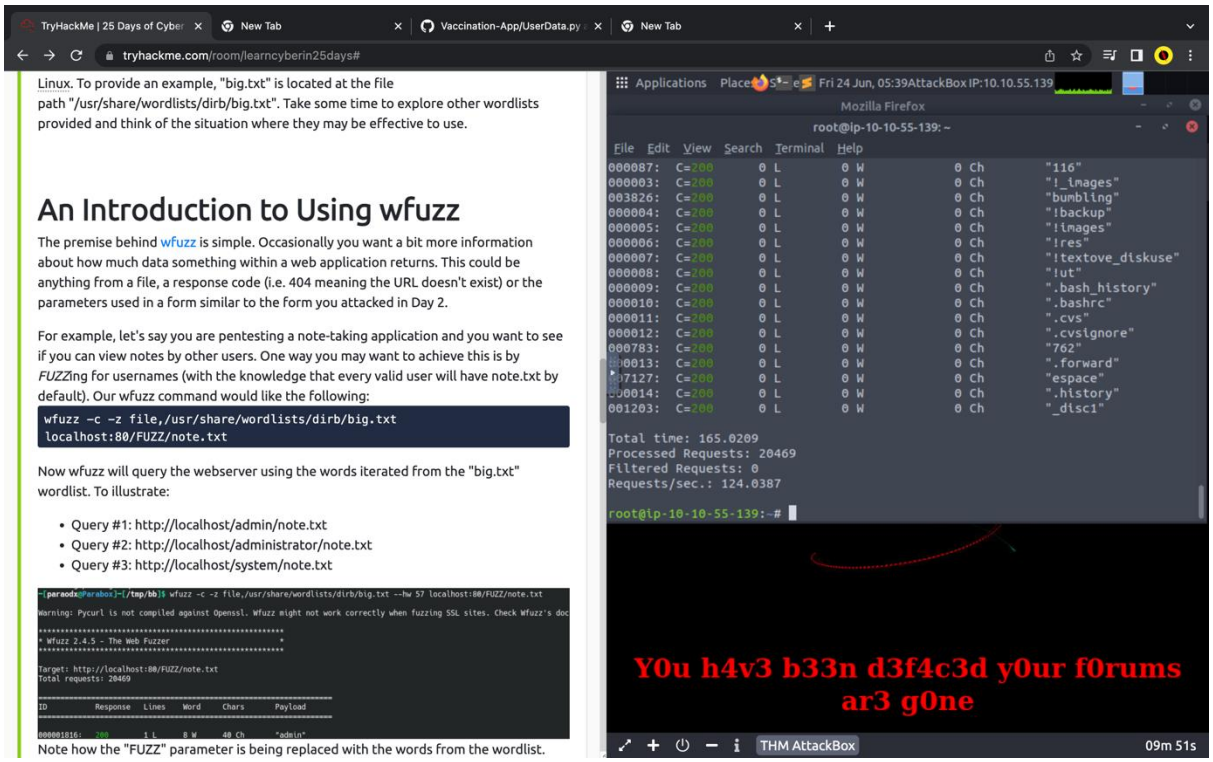


- Open the browser and navigate to the website "your_ip_address/api"

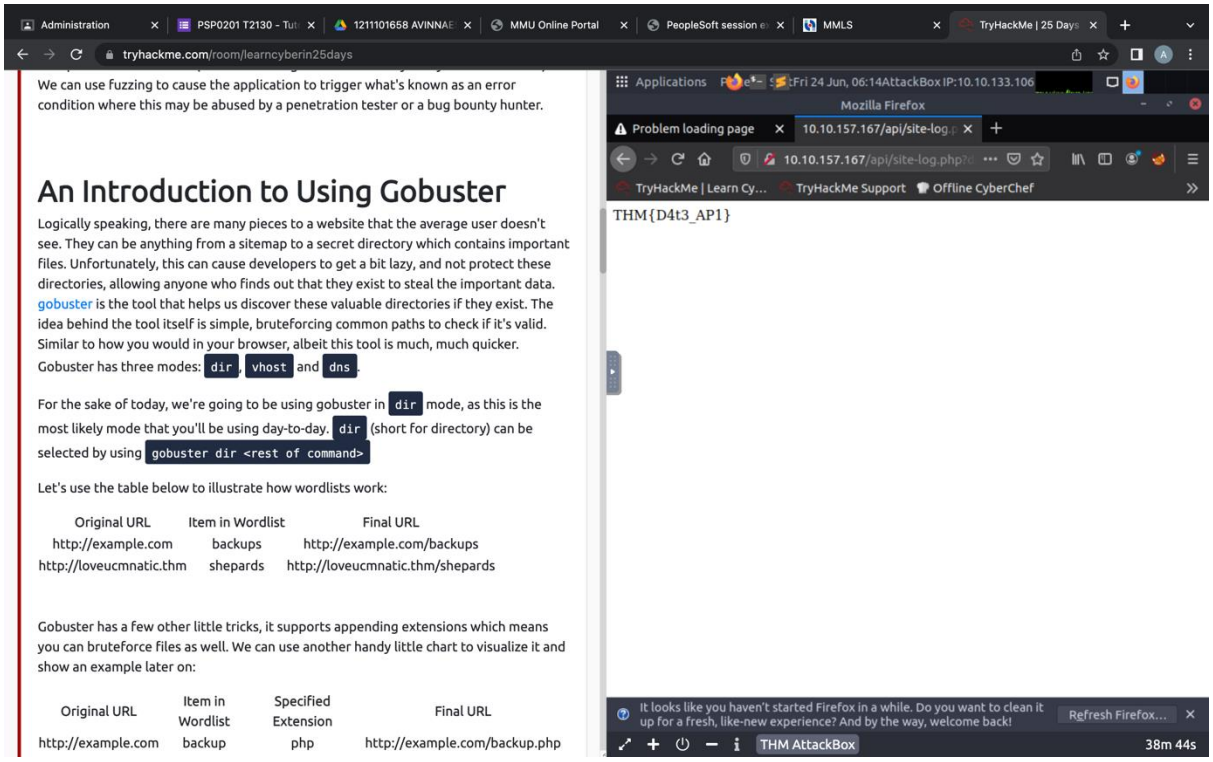


Question 2: Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?

- Use the command “wfuzz -c -z file,/usr/share/wordlists/dirb/big.txt localhost:80/FUZZ/note.txt” to obtain the website directory.



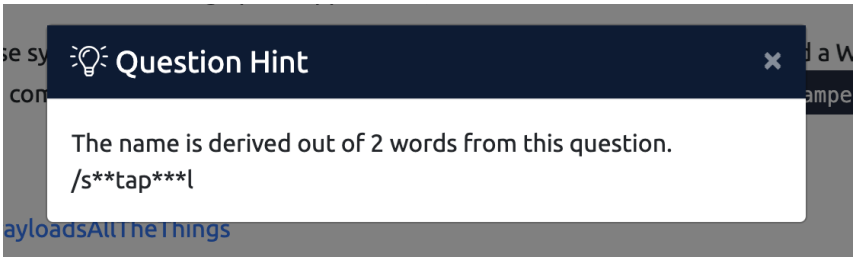
- Enter the date obtained in the url “your_ip_address/api/site-log?date=xxxxxx” to reveal the flag.

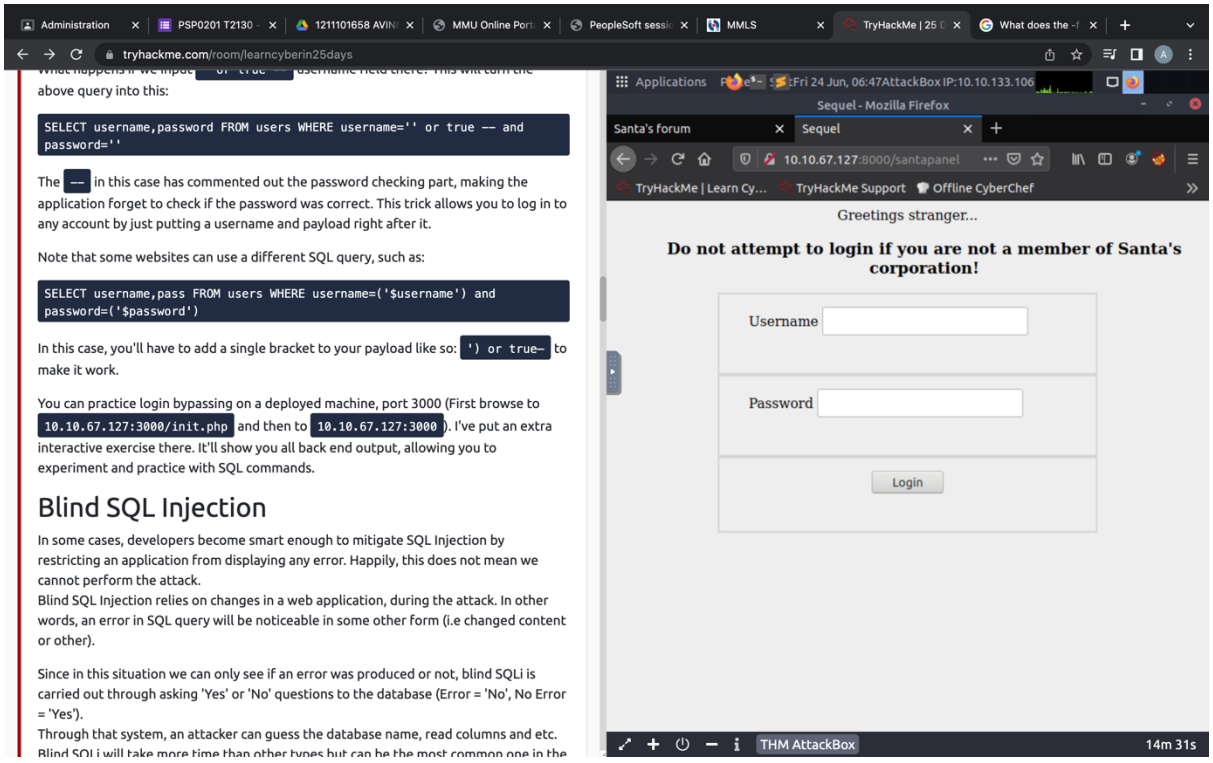


Day 5 – [Web Exploitation] Someone stole Santa's gift list

Question 1: Without using directory brute forcing, what's Santa's secret login panel?

- The secret Santa's login panel was accessed through trial and error.





- We do not have access to the website.

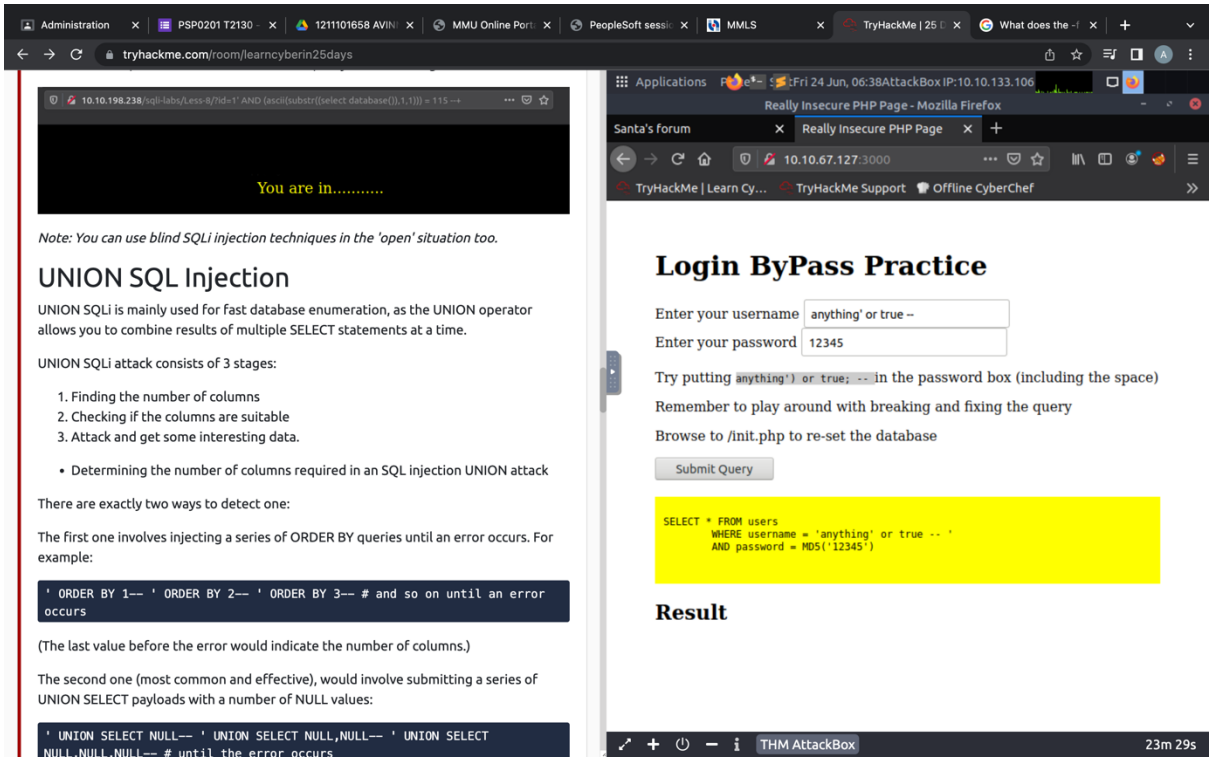
Question 2: What is the database used from the hint in Santa's TODO list?

- Sqlite

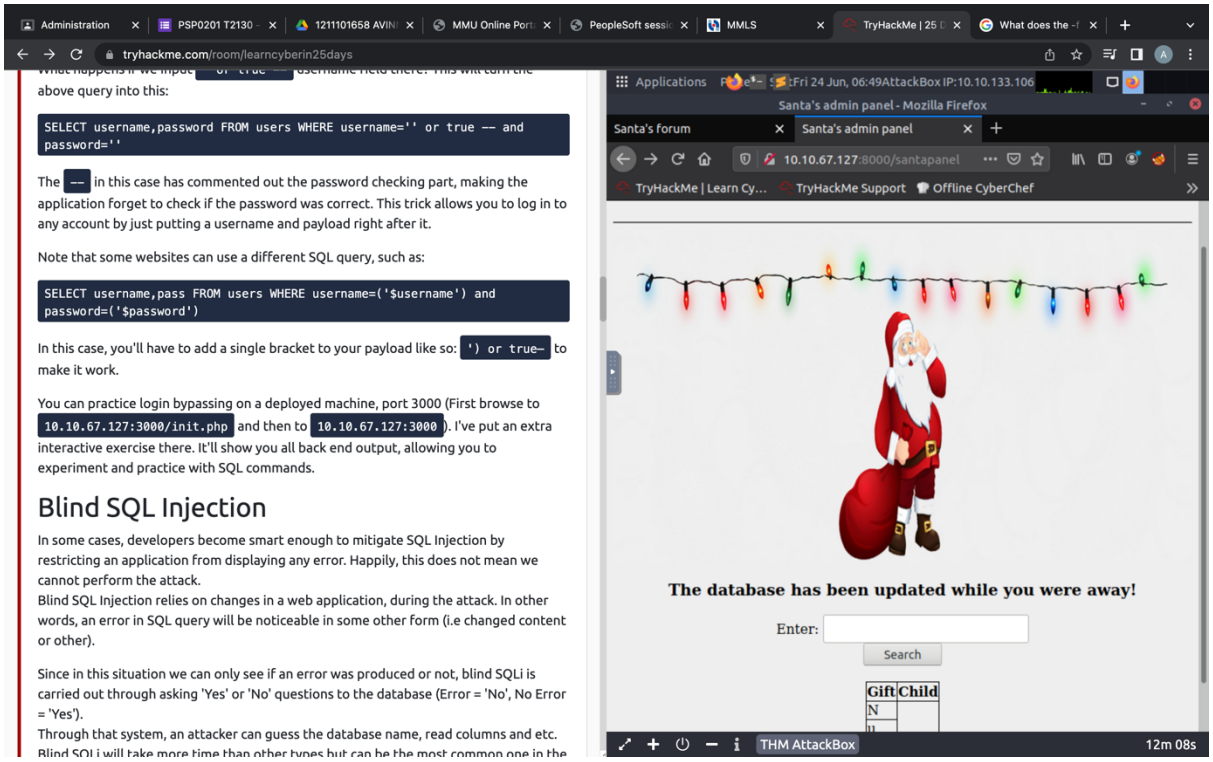
Santa's TODO: Look at alternative database systems that are better than sqlite. Also, don't forget that you installed a Web Application Firewall (WAF) after last year's attack. In case you've forgotten the command, you can tell SQLMap to try and bypass the WAF by using `--tamper=space2comment`

Question 3: How many entries are there in the gift database?

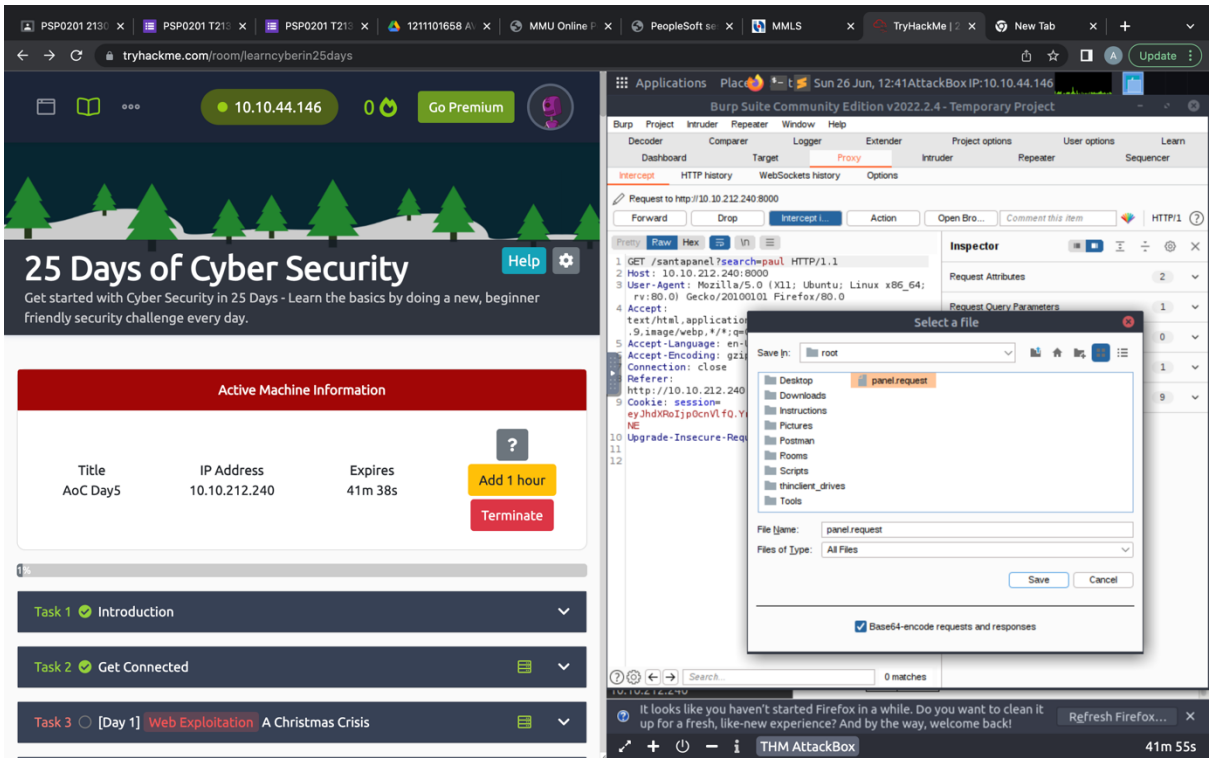
- Open the browser and type out the url “your_ip_address:3000 to get into the login bypass page.
- Enter the username as “anything’ or true --“ and the password as “12345”.



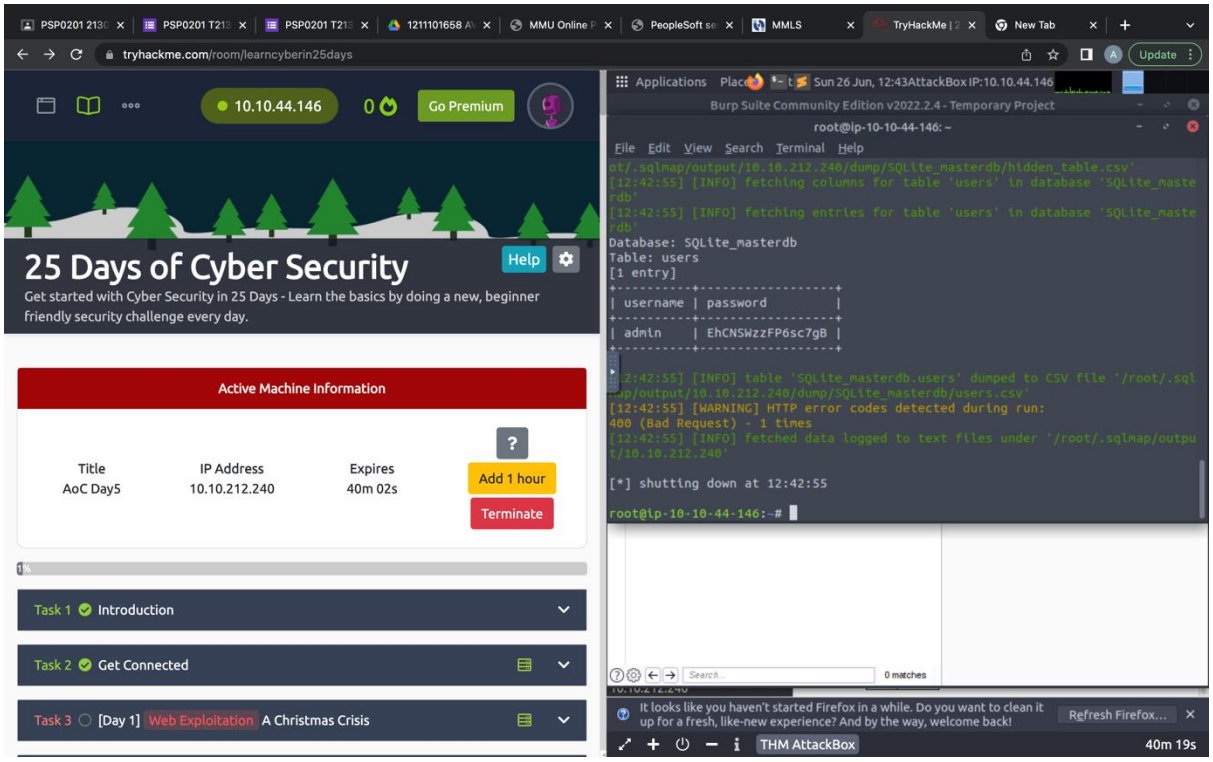
- Then go to the website “your_ip_address:8000/santapanel”, enter the username and password to login.



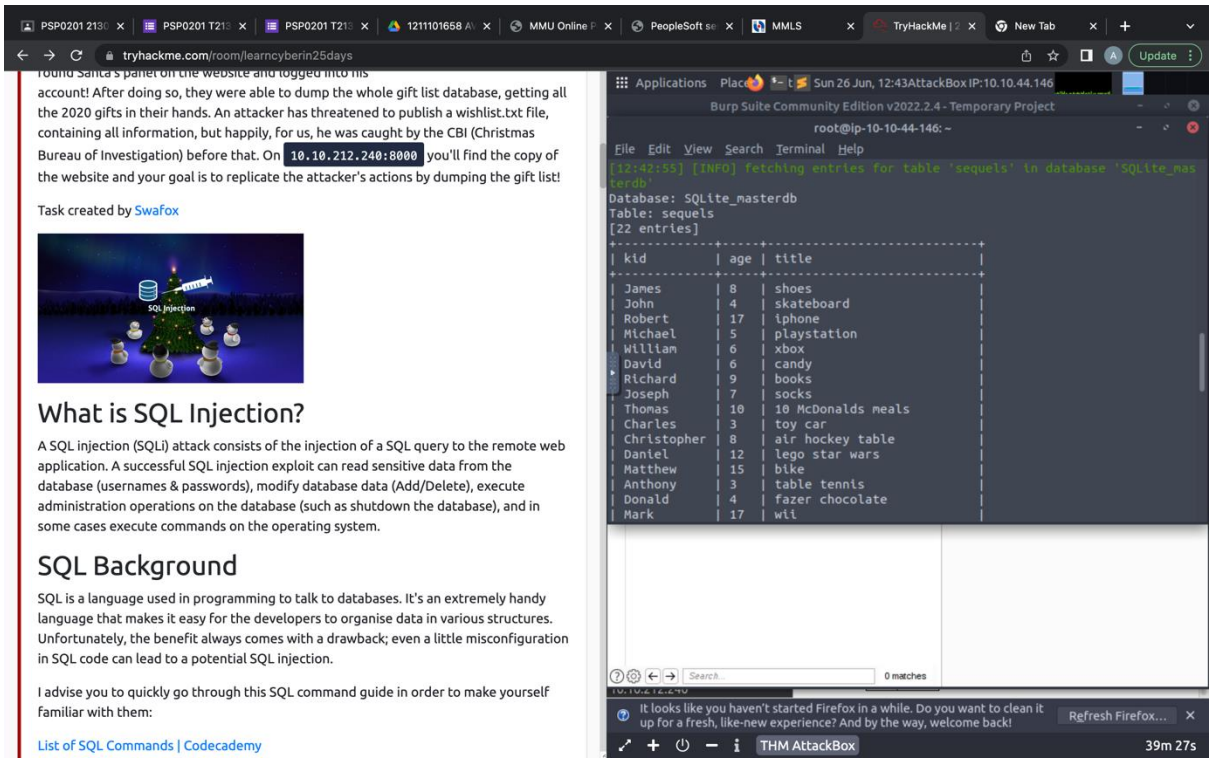
- Turn on the Burp proxy on the website and open the burp app.
- Do a search through the database.
- Turn on the intercept on Burp and save the item under panel.request.



- Open the terminal and run the command “sqlmap -r panel.request –tamper=space2comment –dump-all –dbms sqlite.

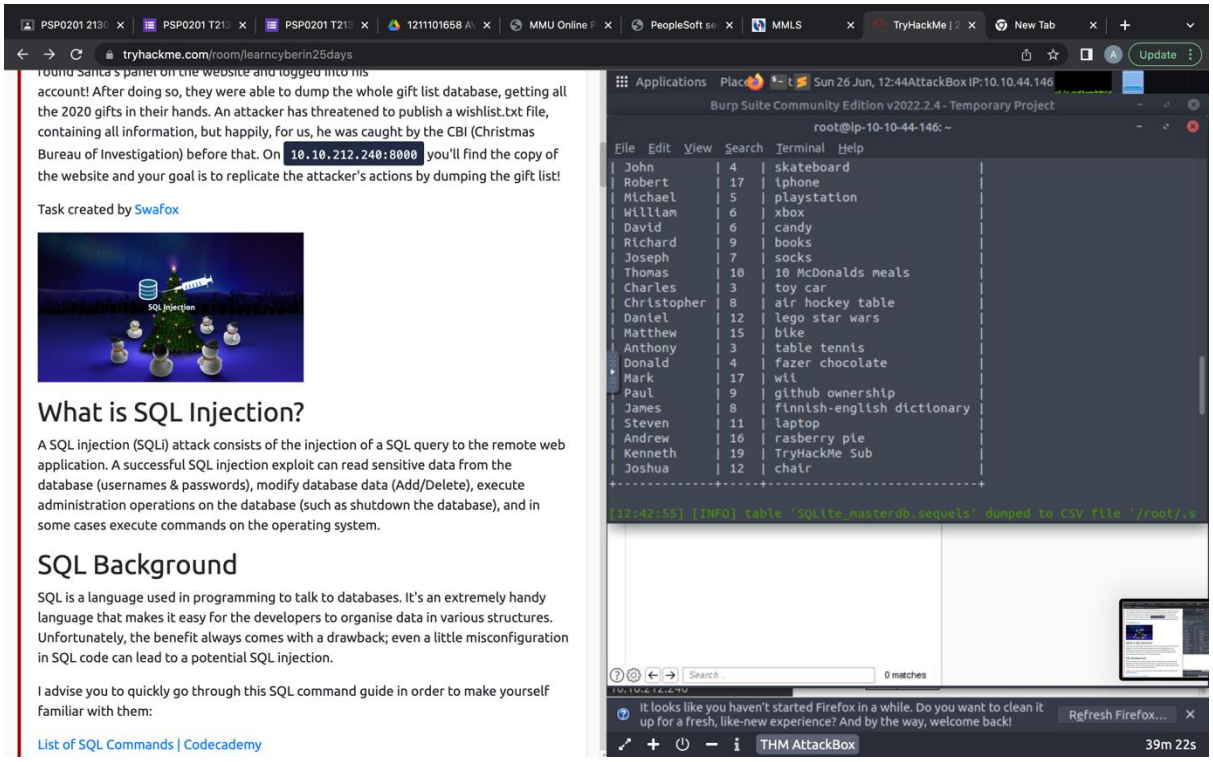


- There will be 22 entries in the database.



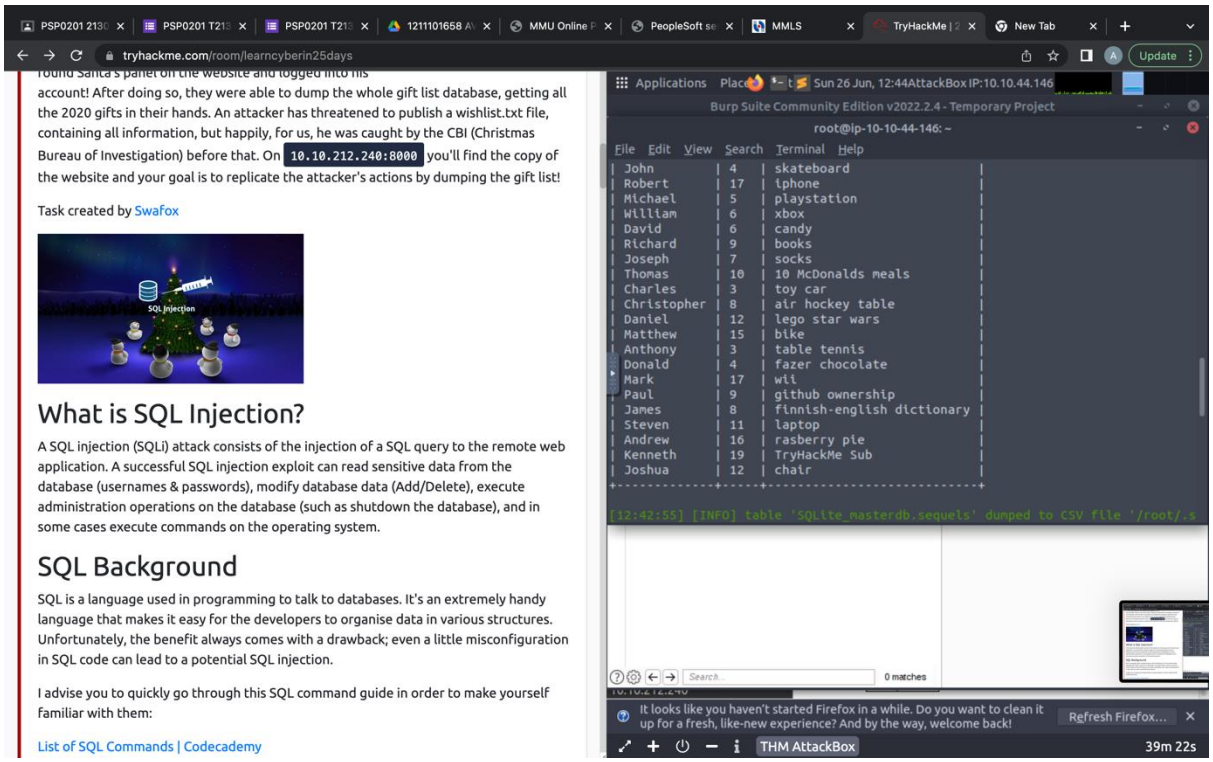
Question 4: What is James' age?

- James’ age can be found in the table.



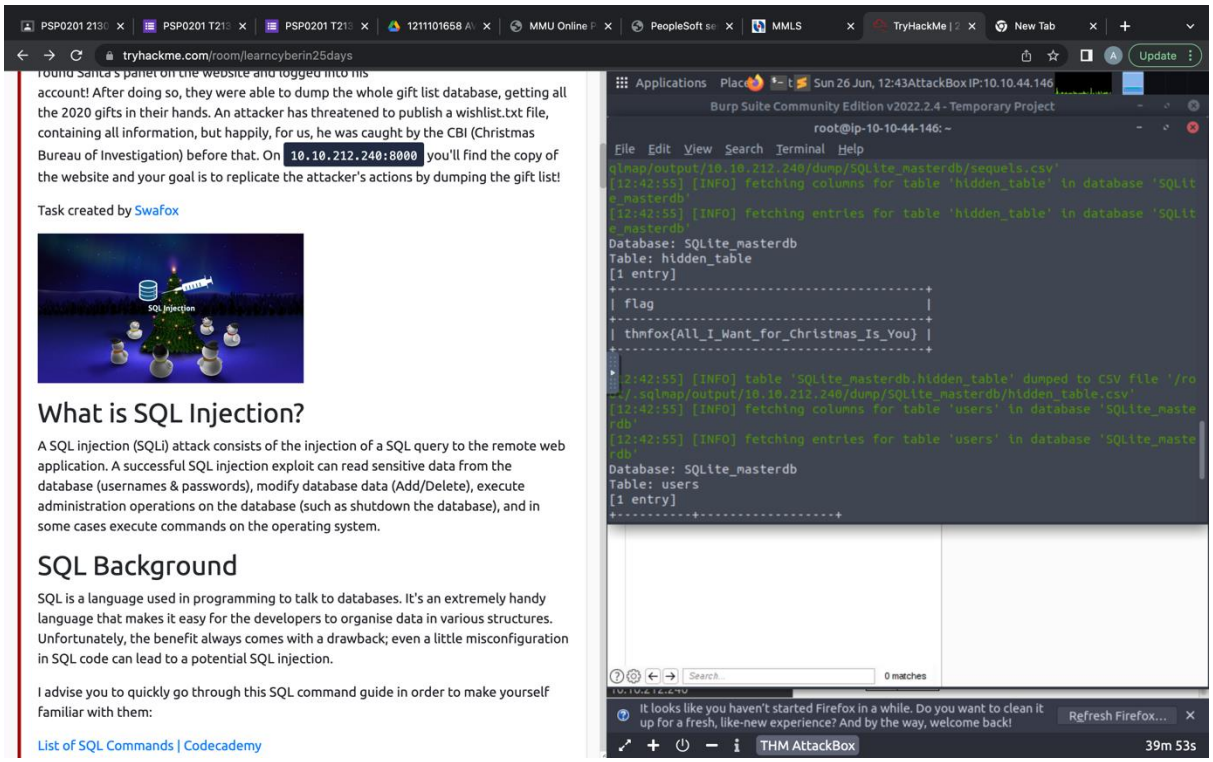
Question 5: What did Paul ask for?

- Paul asked for github ownership based on the same table



Question 6: What is the flag?

- The flag can be obtained in the hidden table



Question 7: What is admin's password?

- The admins password can be found in the users table