PSP0201

Week 2

Write-up

Group Name: **PennCake**

ID	Name	Role
1211103144	Vaarindran Nyenasegran	Leader
1211103222	Asyrani Syazwan Yuhanis	Member
1211104230	Nur Aisyah Nabila Nahar	Member
1211101169	Tengku Alyssa Sabrina Tengku Erwin Martino	Member

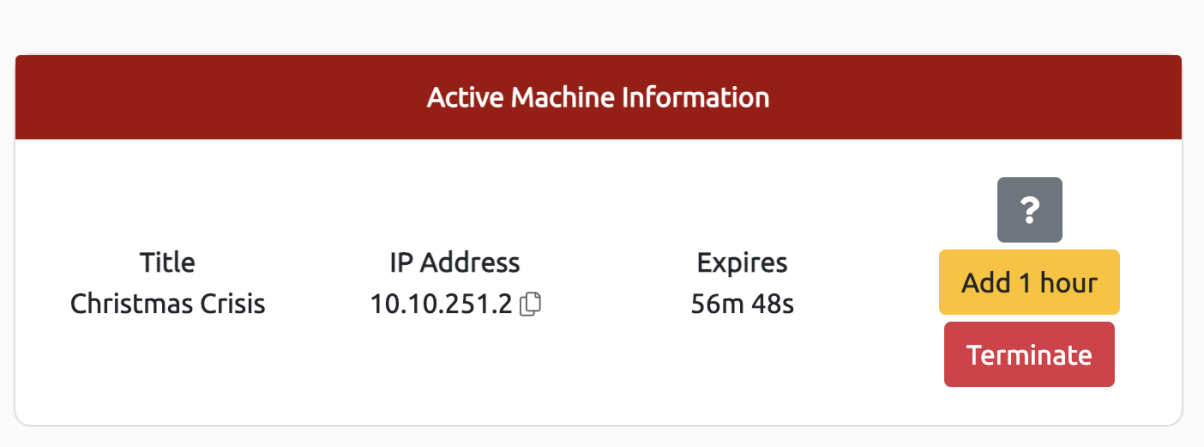
Day 1: Web Exploitation – A Christmas Crisis

Tools used: Attack Box, Google Chrome

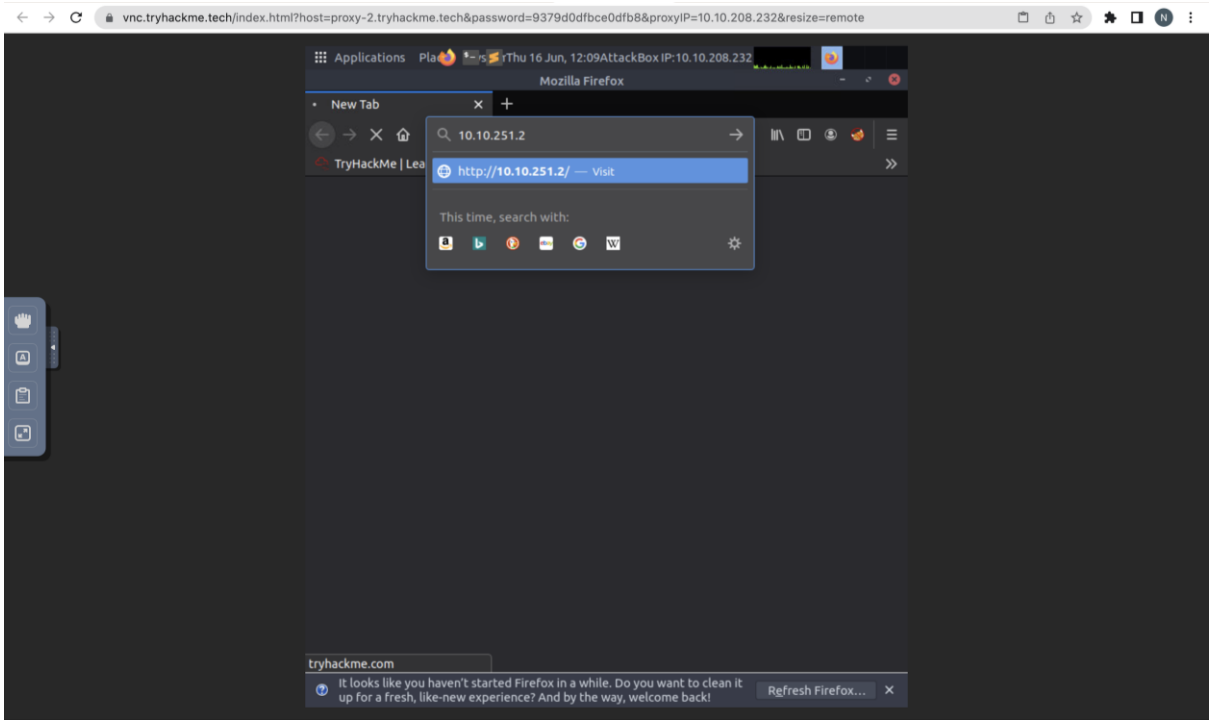
Solution/walkthrough:

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

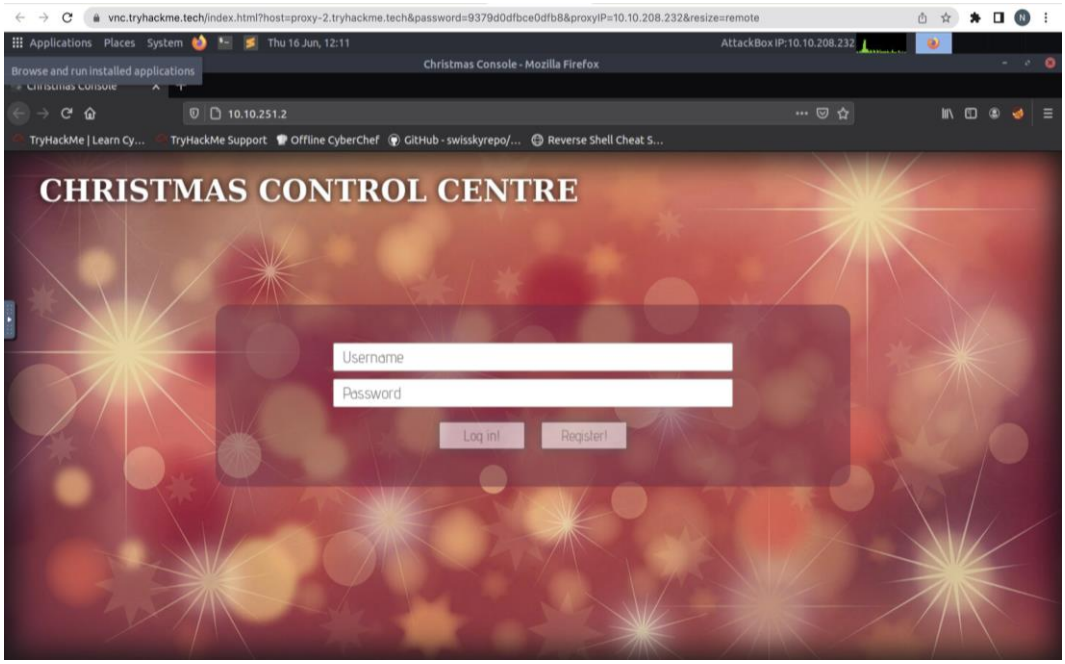
Activate the machine and attackbox in tryhackme website. Access the victim's IP Address.



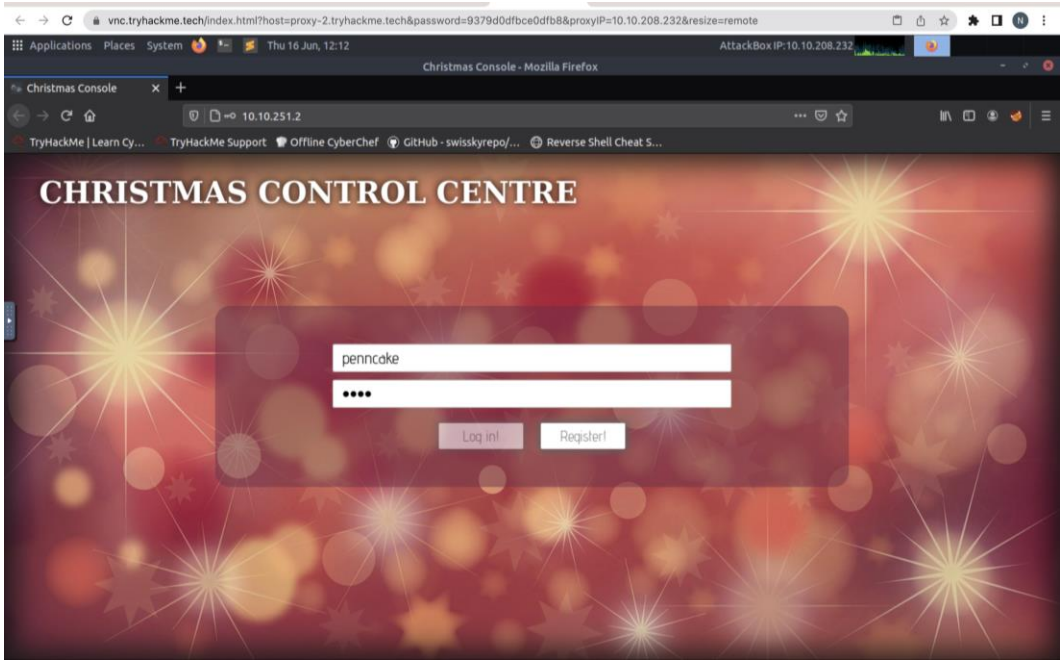
Paste the victim's IP Address in the searchbar.



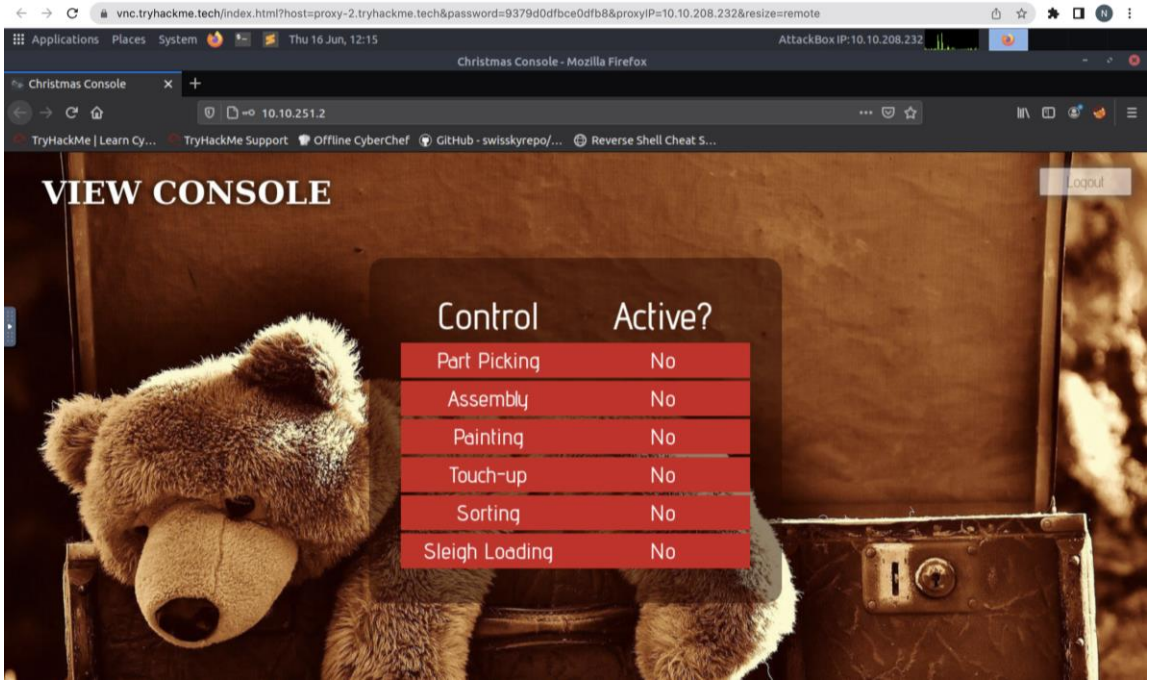
After entering the IP Address, the registration/login page will be shown.



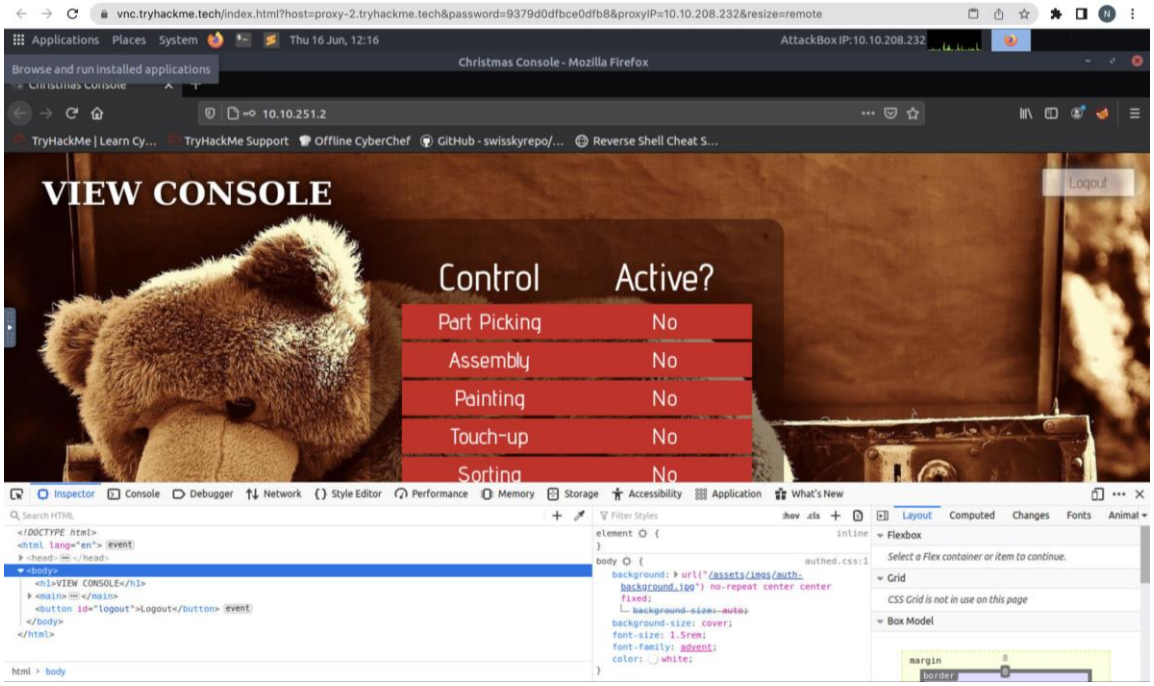
Register for a new account and log in into the account.

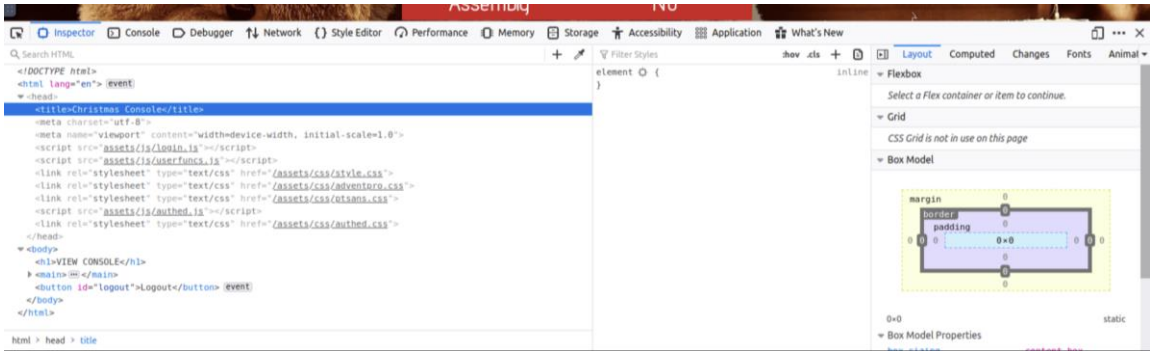


After successfully registering and logging in, the view console will be displayed. We have no access to all the controls.



Inspect the website using browser developer tools to find the title of the webpage and to check on the cookies. Click on the **three dots between the header html tag <head></head>**.



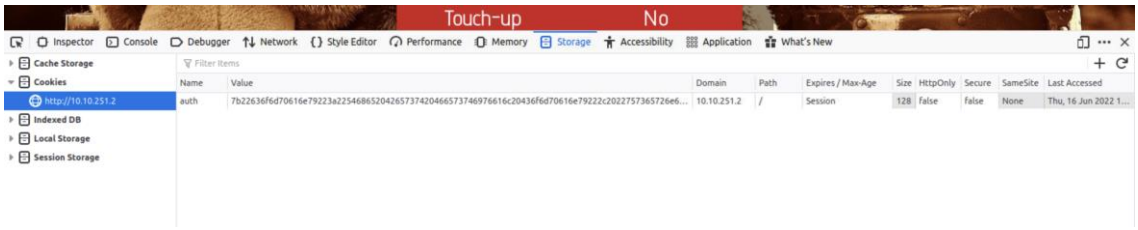


The title of the webpage, ‘Christmas Console’ is shown between the title html tags.

Answer: **Christmas Console**

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

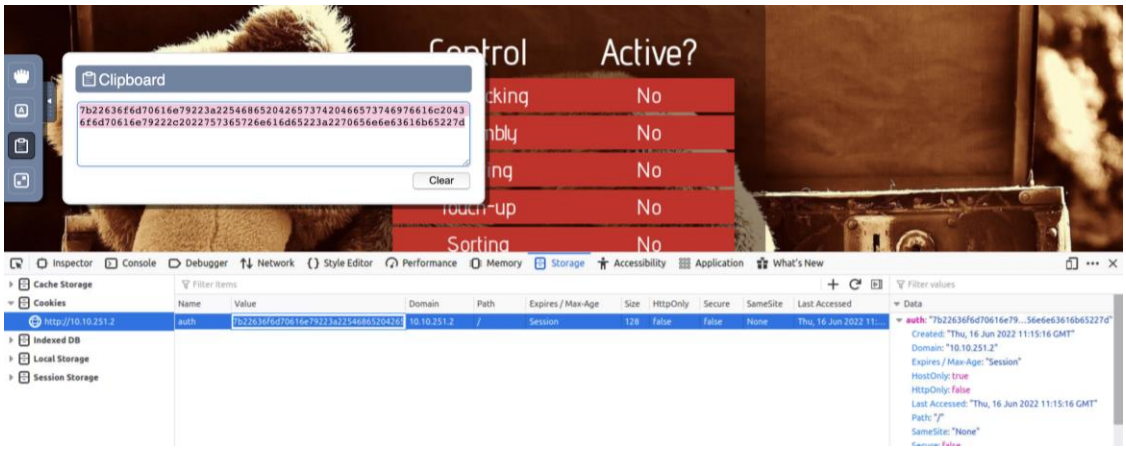
Click on the storage tab. Then, click on Cookies to check the name of the cookie used.



Answer: **auth**

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

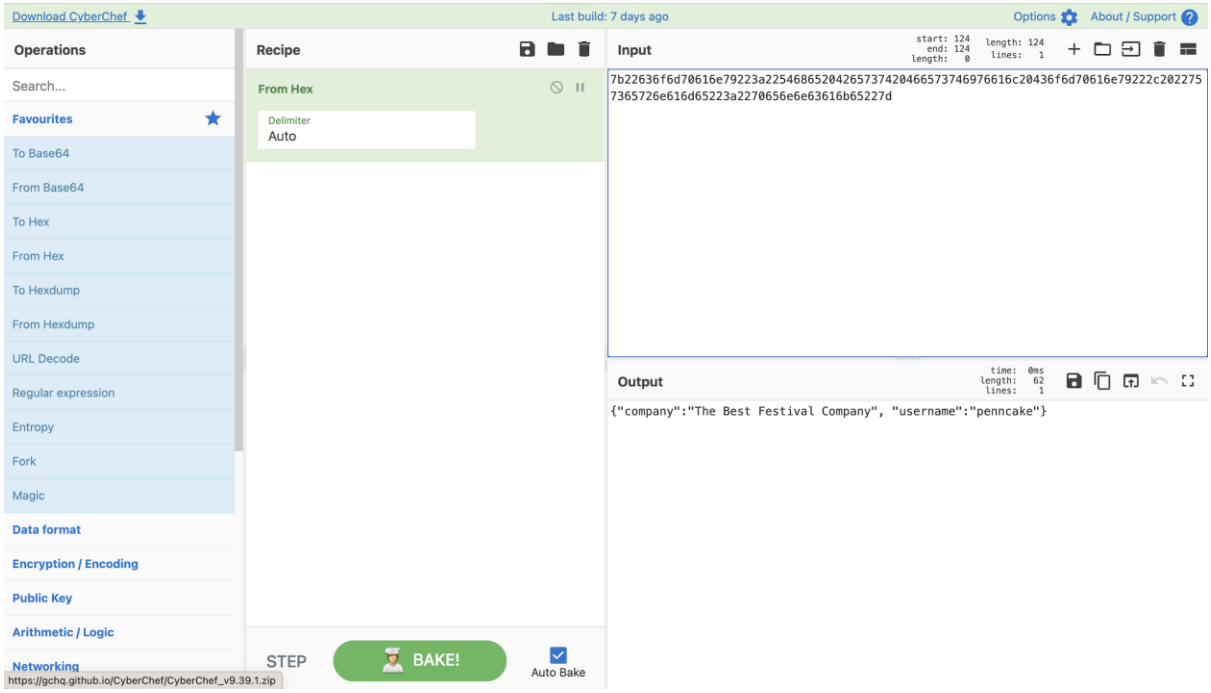
Obtain the value of the cookie and copy using clipboard.



Answer : **Hexadecimal**

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

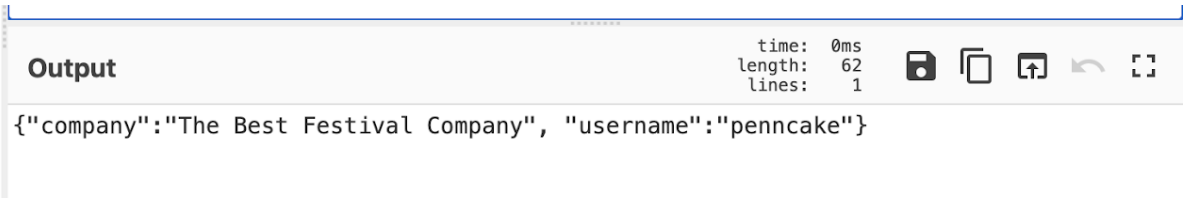
Using Cyberchef, paste and convert the cookie value from hex to string.



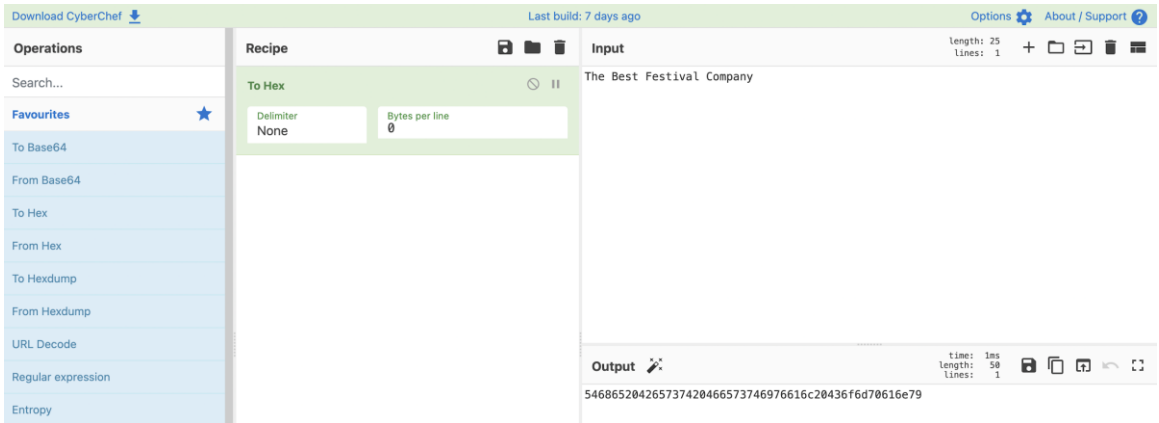
Answer: **JSON**

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

Using the information from the cookie that was decoded, we now know that the name of the company in the company field is The Best Festival Company.

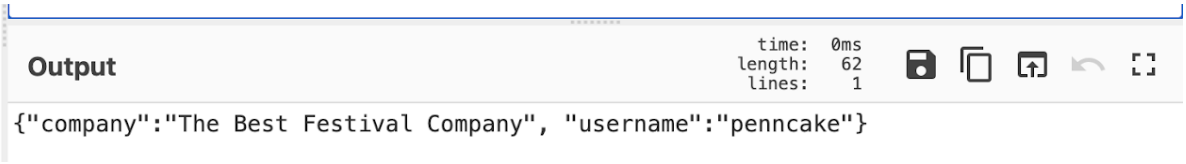


Copy the company name and convert it back to its hexadecimal value.



Answer: **5468652042657374204665737469766 16c20436f6d70616e79**

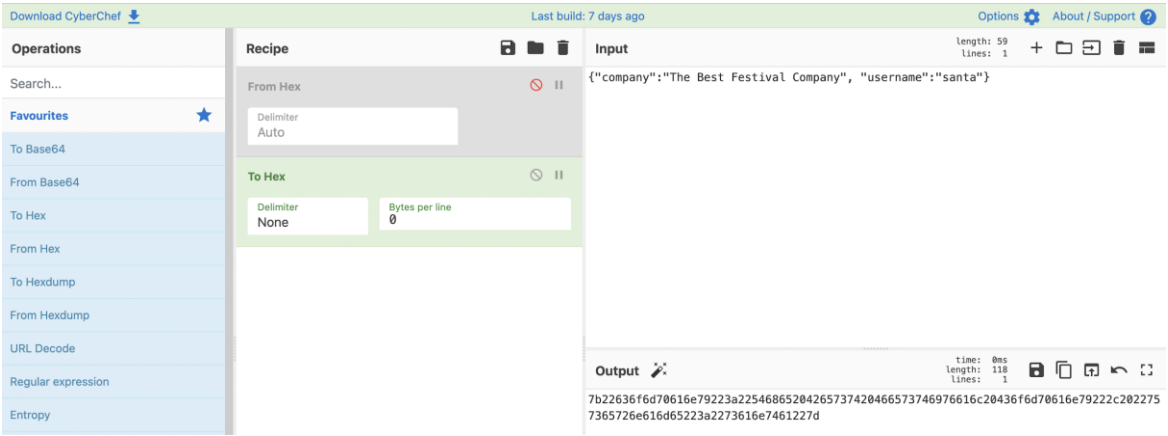
Question 6: What is the other field found in the cookie?



Answer: **username**

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

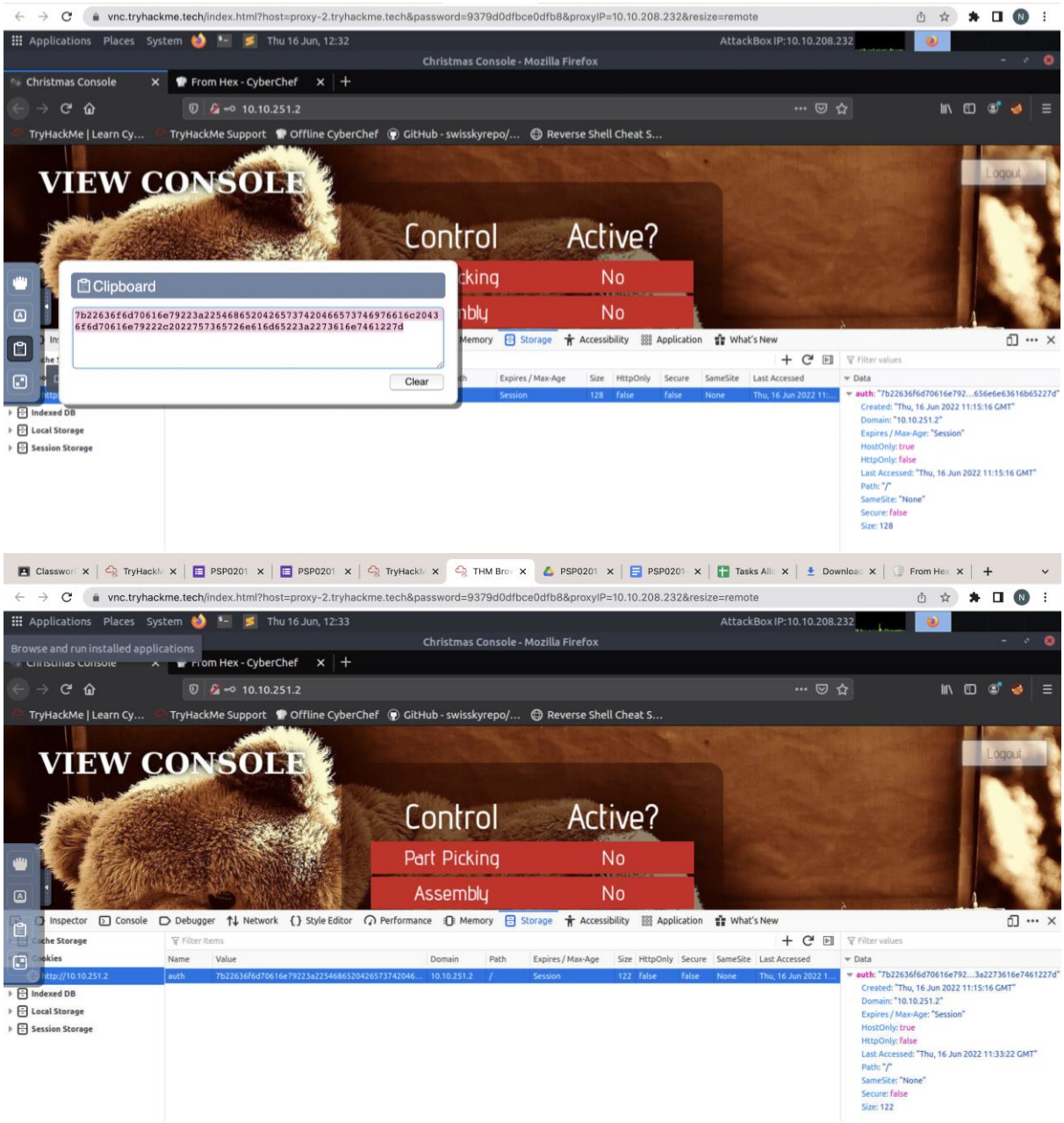
Change the username to santa. Then, convert the string input back to its new hexadecimal value.



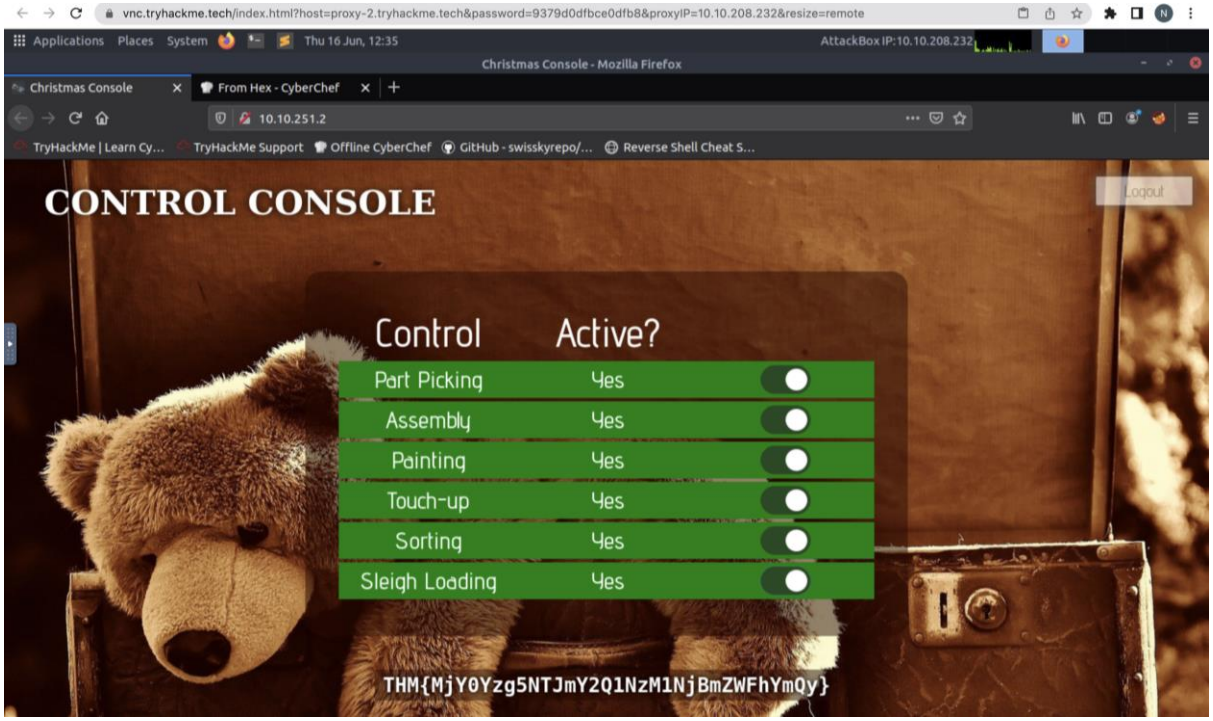
Answer:
7b22636f6d70616e79223a2254686520426573742046657374697661c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d

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

Copy santa's cookie value from cyberchef. Replace the old cookie with santa's cookie.



Refresh the page. We will be automatically logged in into santa's account. All controls can be accessed. Turn all the controls on. Then, the flag is shown on the bottom of the page.



Thought Process/Methodology:

Having accessed the target machine, we copied the victim's IP address. After entering the IP address, we were shown a login/registration page. We proceeded to register a new account and logged in. After logging in, we opened the **browser's developer tool** to **inspect the website**. We found the title of the webpage by **inspecting the html title tag of the webpage**. Then, we **viewed the site cookie** by clicking on the **Storage tab**. Looking at the cookie value, we deduced it to be a **hexadecimal value since it uses base 16.** We used **Cyberchef** to convert it to text. After we converted the string, we found a **JSON statement** with the **company field and username element**. Using Cyberchef, we altered the username to **'santa'**, the administrator account. To access all the controls in the control console, we **converted it back to hexadecimal using Cyberchef** and **replaced the old cookie value with the converted one.** Then, we refreshed the page and were shown the administrator page. Thus, we proceeded to enable every control, which in turn showed the flag.

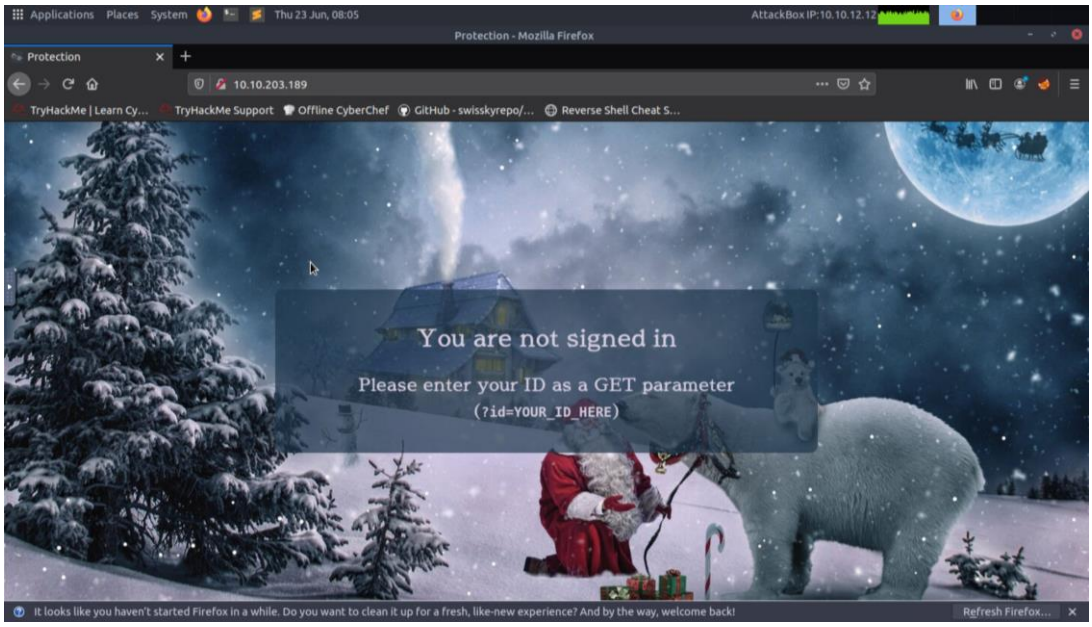
Day 2: Web Exploitation - The Elf Strikes Back

Tools used: Attack Box, OpenVPN, Firefox, WSL (subsystem for linux)

Solution/walkthrough:

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

By entering the IP address of the machine, you will be greeted with a homepage which states that you aren't signed in. In which, you are supposed to enter your ID as a **GET** parameter **(http://your_ip_address/?id=your_id_here)**:



Based on the text, we have the user 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 (10.10.203.189) in your browser.

Answer the questions below

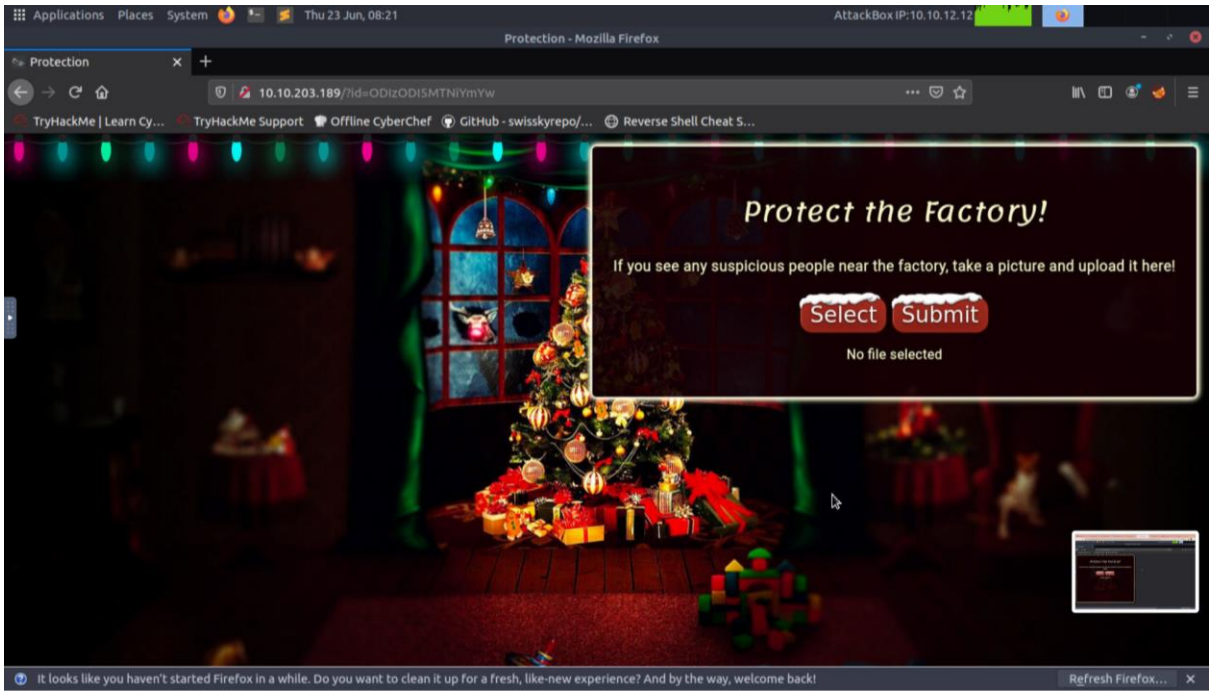
What string of text needs adding to the URL to get access to the upload page?

?id=ODIzODI5MTNiYmYw

Correct Answer

Hint

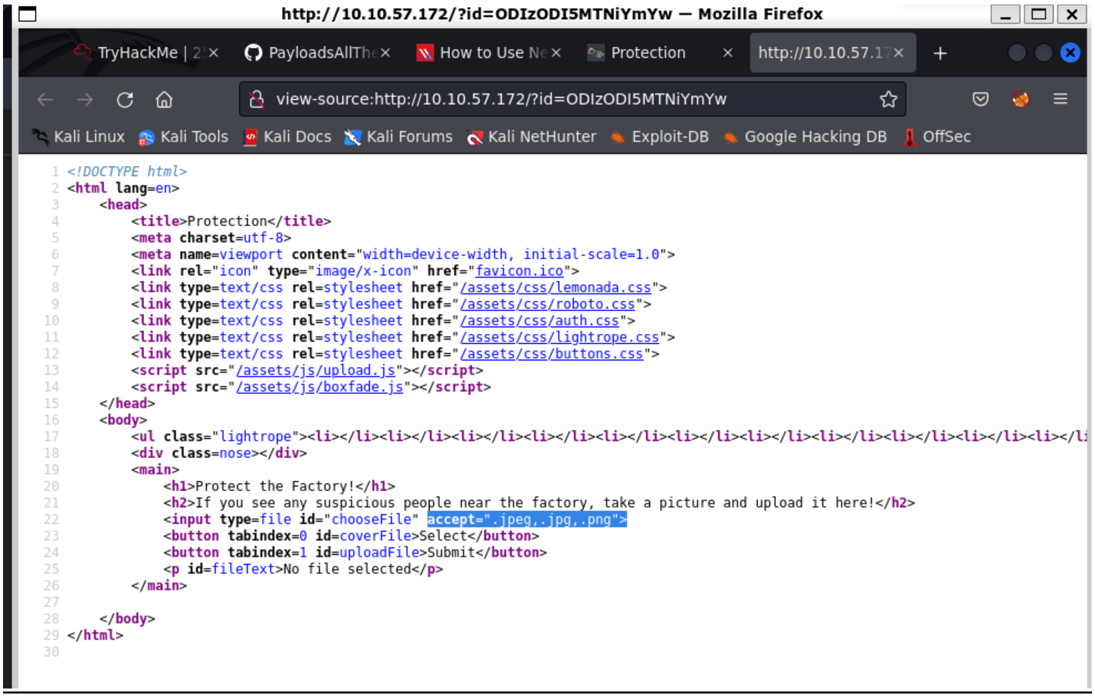
Therefore, by entering the user ID given as a get parameter, we have successfully entered the webpage.



Answer: **?id=ODIzODI5MTNiYmYw**

Question 2: What type of file is accepted by this site?

By viewing the page source, we can determine what type of files accepted by the site.



Answer: **image (jpeg, jpg, png)**

Question 3: In which directory are the uploaded files stored?

From the passage above, we can determine some of the common directories used by most websites.

File Uploads

There are countless uses for file uploads in the modern internet -- profile pictures, school/university submissions, diagrams, pictures of your dog, you name it! Whilst file uploads are very common, they're also very easy to implement in an insecure fashion. For this reason, it's important that we understand the gravity of the attack vector.

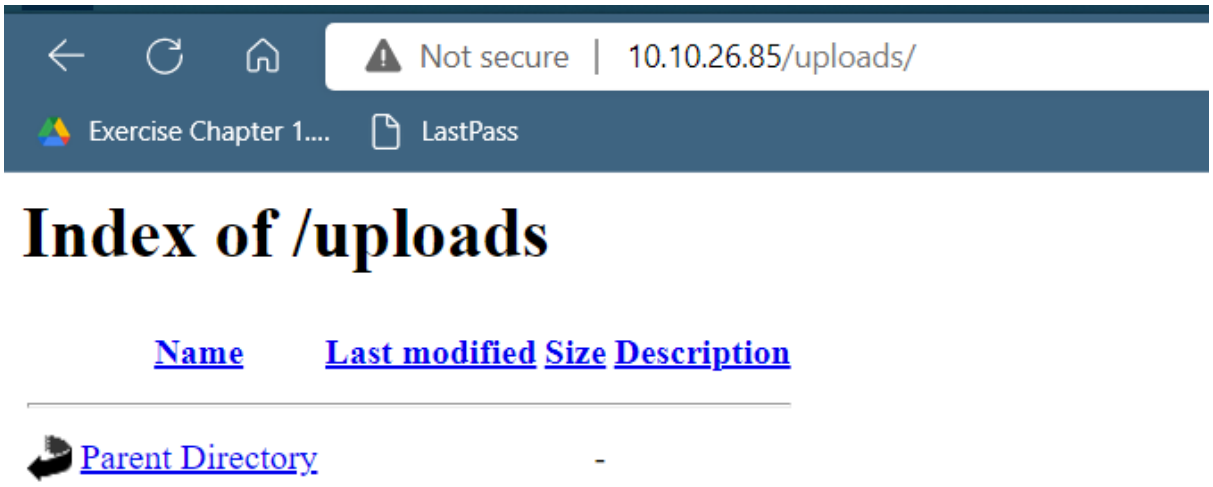
When you have the ability to upload files to a server, you have a path straight to RCE (Remote Command Execution). An upload form with no restrictions would mean that you could upload a script that, when executed, connects back to your attacking machine and gives you the ability to run any command you want. It would be very unusual to find a file upload with *no* filtering; but it's much less uncommon to find a file upload that employs flawed filtering techniques which can be circumvented to upload a malicious script. The script has to be written in a language which the server can execute. PHP is usually a good choice for this, as most websites are still written with a PHP back end.

There isn't time to go over every kind of filter bypass in this task (there is literally an entire room on this topic, which is recommended for further practice). Instead, we'll just cover one of the most common types of filter and its bypass:

- *File Extension Filtering:* As the name suggests extension filtering checks the file extension of uploaded files. This is often done by specifying a list of allowed extensions, then checking the uploaded file against the list. If the extension is not in the allowlist, the upload is rejected.
- So, what's the bypass? Well, the answer is that it depends entirely on how the filter is implemented. Many extension filters split a filename at the dot (`.`) and check what comes after it against the list. This makes it very easy to bypass by uploading a double-barrelled extension (e.g. `.jpg.php`). The filter splits at the dot(s), then checks what it thinks is the extension against the list. If jpg is an allowed extension then the upload will succeed and our malicious PHP script will be uploaded to the server.

When implementing an upload system, it's good practice to upload the files to a directory that can't be accessed remotely. Unfortunately, this is often not the case, and scripts are uploaded to a subdirectory on the webserver (often something like `/uploads`, `/images`, `/media`, or `/resources`). For example, we might be able to find the uploaded script at `https://www.thebestfestivalcompany.xyz/images/shell.jpg.php`.

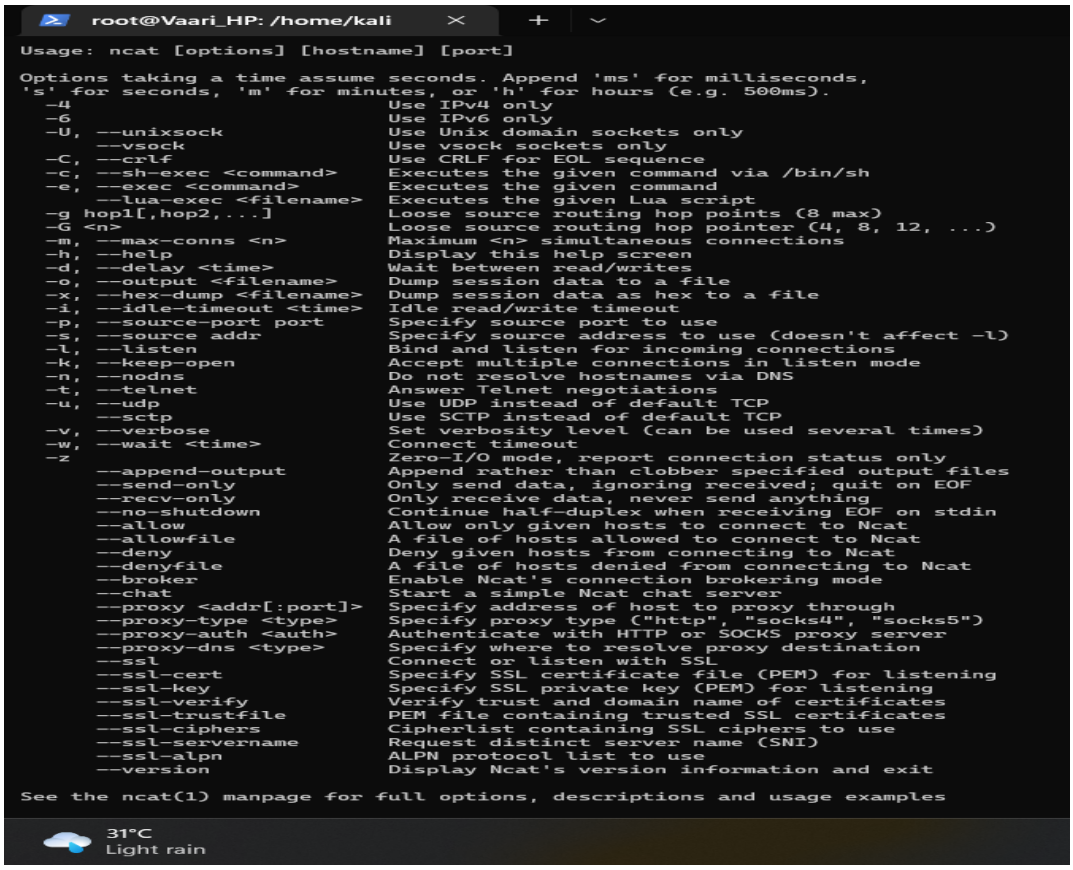
Therefore, with some trial and error we have managed to find the subdirectory of the uploaded files.



Answer: **/uploads/**

Question 4: Read up on netcat's parameter explanations. Match the parameter with the explanation below.

To obtain the netcat's parameter explanation, you can simply go to terminal and type nc -h



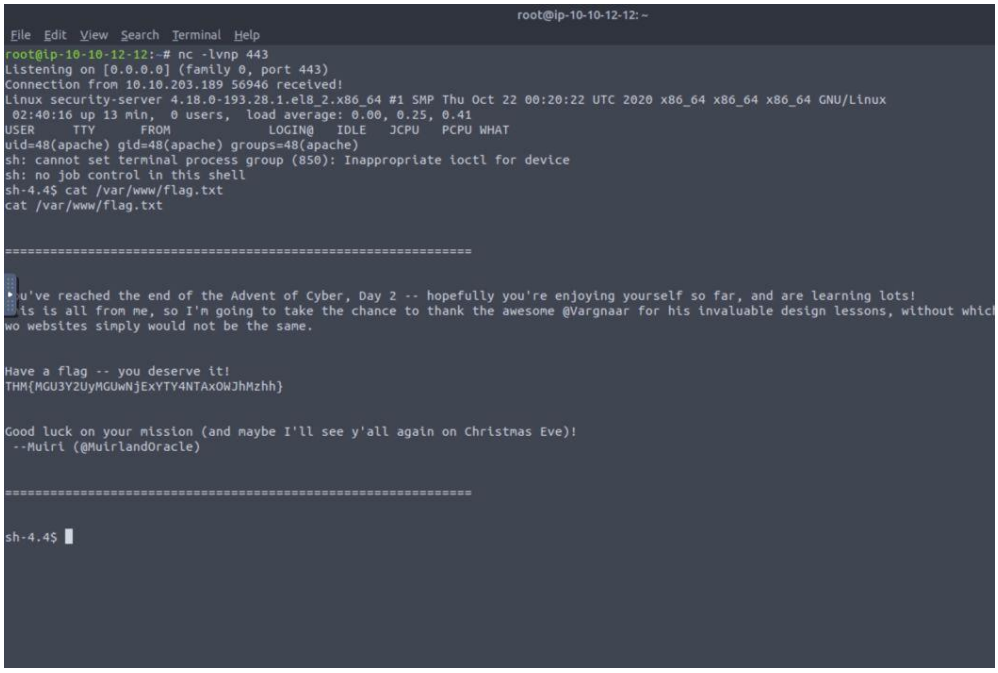
Answer:

Do not do any DNS or service lookups on any specified addresses, hostnames or ports	**-n** *(--nodus)*
Have nc give more verbose output.	**-v** *(--verbose)*
Specifies the source port nc should use, subject to privilege restrictions and availability.	**-p** *(--source-port)*
Used to specify that nc should listen for an incoming connection rather than initiate a connection to a remote host.	**-l** *(--listen)*

Question 5: What is the flag in /var/www/flag.txt?

We can determine the flag after successfully receiving the shell by netcat.

Once you have successfully a connection, just input **'cat /var/www/flag.txt'** into the terminal, and you will receive the output.



Answer: **THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}**

Thought Process/Methodology:

After successfully deploying the machine, we were greeted with a homepage where we are supposed to login using a **GET parameter**. From the passage above, we are assigned with an **ID number (ODIzODI5MTNiYmYw)**. Therefore, by inputting the ID number using the GET parameter, we have successfully login to the site where we can select files and upload them. To view the file type the site can receive, we decided to **view the page source**, and we found out that the supported file type were **JPEG, JPG, and PNG**. After figuring out that the site accepts images only, we have created a **reverse shell php script** by copying the source code to a notepad, then **altering the IP address to our openVPN and port to 443.** After **altering the PHP scrip**t, we save and rename the file as **shell.jpg.php** and upload them to the site. After uploading, we started a **netcat listene**r by inputting **nc -lvnp 443** to the terminal as a root user. After confirming that we have your port listener setup, we then used a technique called **'trial and error'** to figure out the subdirectory where we can view the directory. After figuring out the directory which was **/uploads/** we then proceeded to click on our PHP file, and we have successfully received the connection. Then, we proceeded to find the THM flag by inputting **cat/var/www/flag.txt** into the terminal, and we are done.

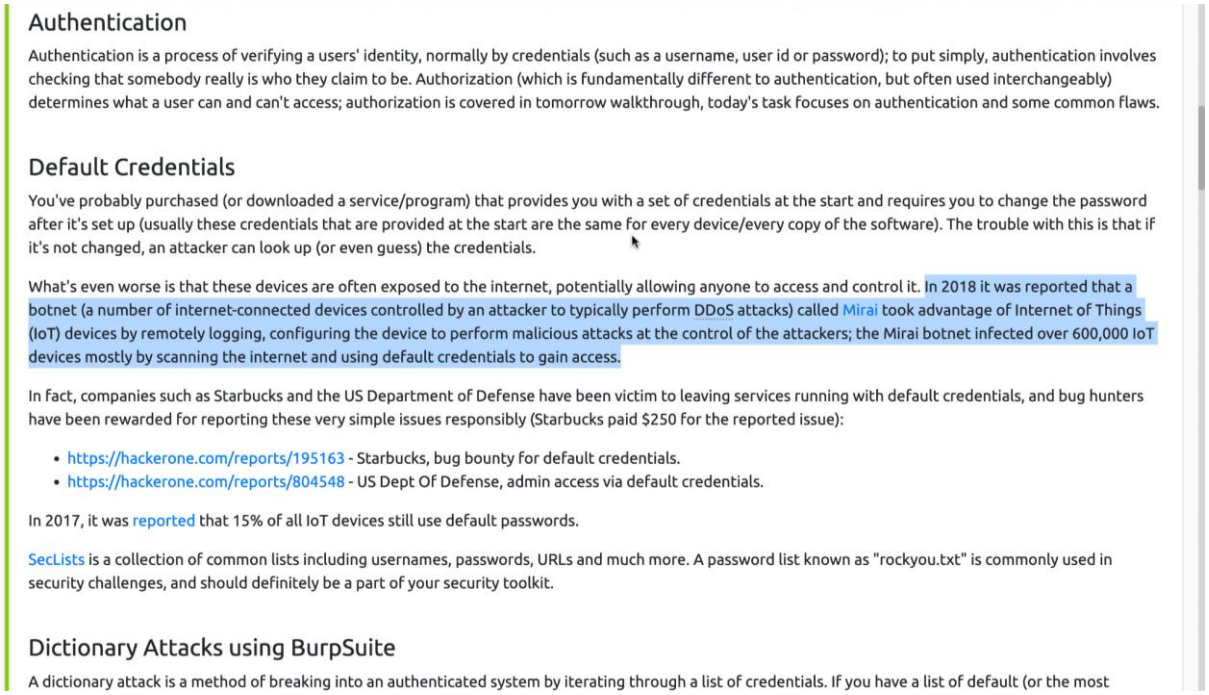
Day 3: Web Exploitation - Christmas Chaos

Tools used: Attack Box, OpenVPN, Firefox

Solution/walkthrough:

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

Based on the text, the name of the botnet that was reported in 2018 is mentioned.



Authentication

Authentication is a process of verifying a users' identity, normally by credentials (such as a username, user id or password); to put simply, authentication involves checking that somebody really is who they claim to be. Authorization (which is fundamentally different to authentication, but often used interchangeably) determines what a user can and can't access; authorization is covered in tomorrow walkthrough, today's task focuses on authentication and some common flaws.

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):

- https://hackerone.com/reports/195163 - Starbucks, bug bounty for default credentials.
- https://hackerone.com/reports/804548 - US Dept Of Defense, admin access via default credentials.

In 2017, it was reported that 15% of all IoT devices still use default passwords.

SecLists is a collection of common lists including usernames, passwords, URLs and much more. A password list known as "rockyou.txt" is commonly used in security challenges, and should definitely be a part of your security toolkit.

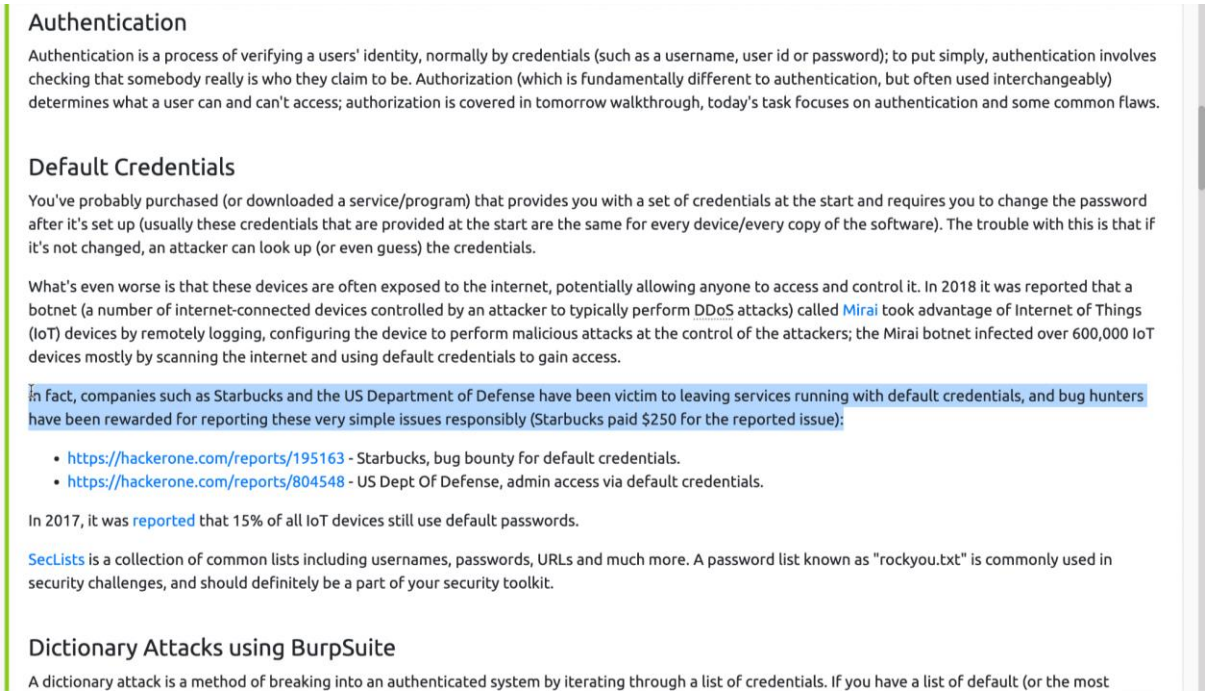
Dictionary Attacks using BurpSuite

A dictionary attack is a method of breaking into an authenticated system by iterating through a list of credentials. If you have a list of default (or the most

Answer: **Mirai**

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

The information can be found in the text given.



Authentication

Authentication is a process of verifying a users' identity, normally by credentials (such as a username, user id or password); to put simply, authentication involves checking that somebody really is who they claim to be. Authorization (which is fundamentally different to authentication, but often used interchangeably) determines what a user can and can't access; authorization is covered in tomorrow walkthrough, today's task focuses on authentication and some common flaws.

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):

- https://hackerone.com/reports/195163 - Starbucks, bug bounty for default credentials.
- https://hackerone.com/reports/804548 - US Dept Of Defense, admin access via default credentials.

In 2017, it was reported that 15% of all IoT devices still use default passwords.

SecLists is a collection of common lists including usernames, passwords, URLs and much more. A password list known as "rockyou.txt" is commonly used in security challenges, and should definitely be a part of your security toolkit.

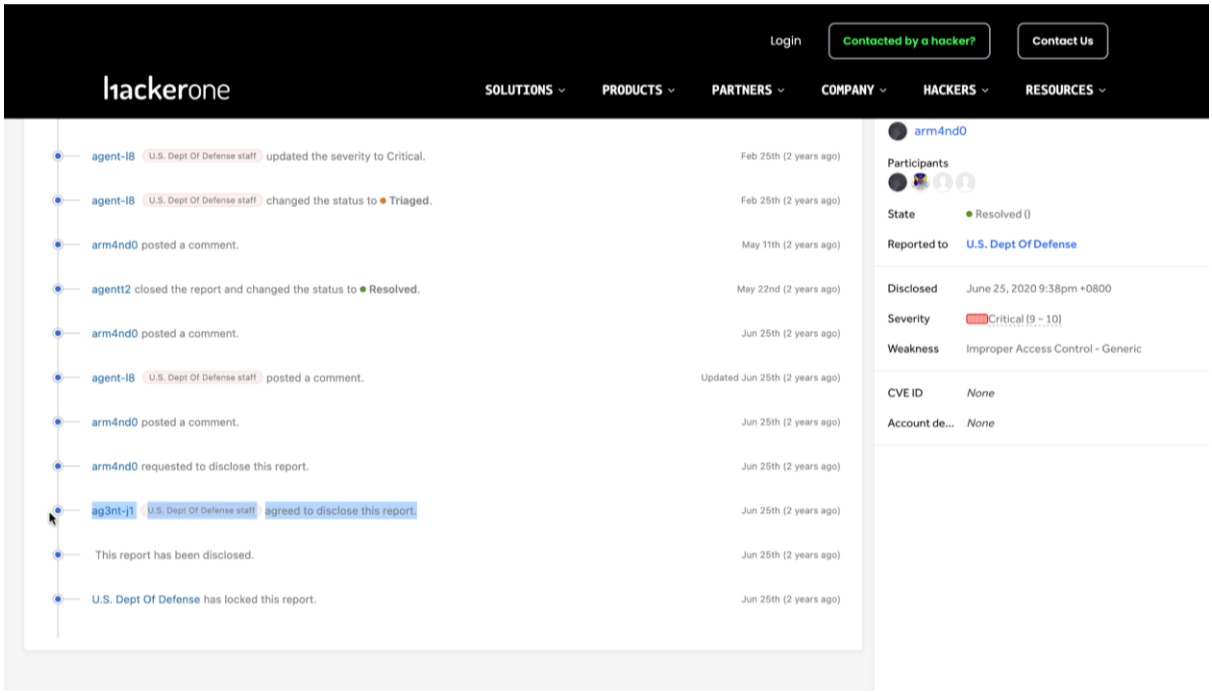
Dictionary Attacks using BurpSuite

A dictionary attack is a method of breaking into an authenticated system by iterating through a list of credentials. If you have a list of default (or the most

Answer: **250**

Question 3: Read the report from Hackerone ID:804548 - who was the agent assigned from the Dept of Defense that disclosed the report on June 25th?

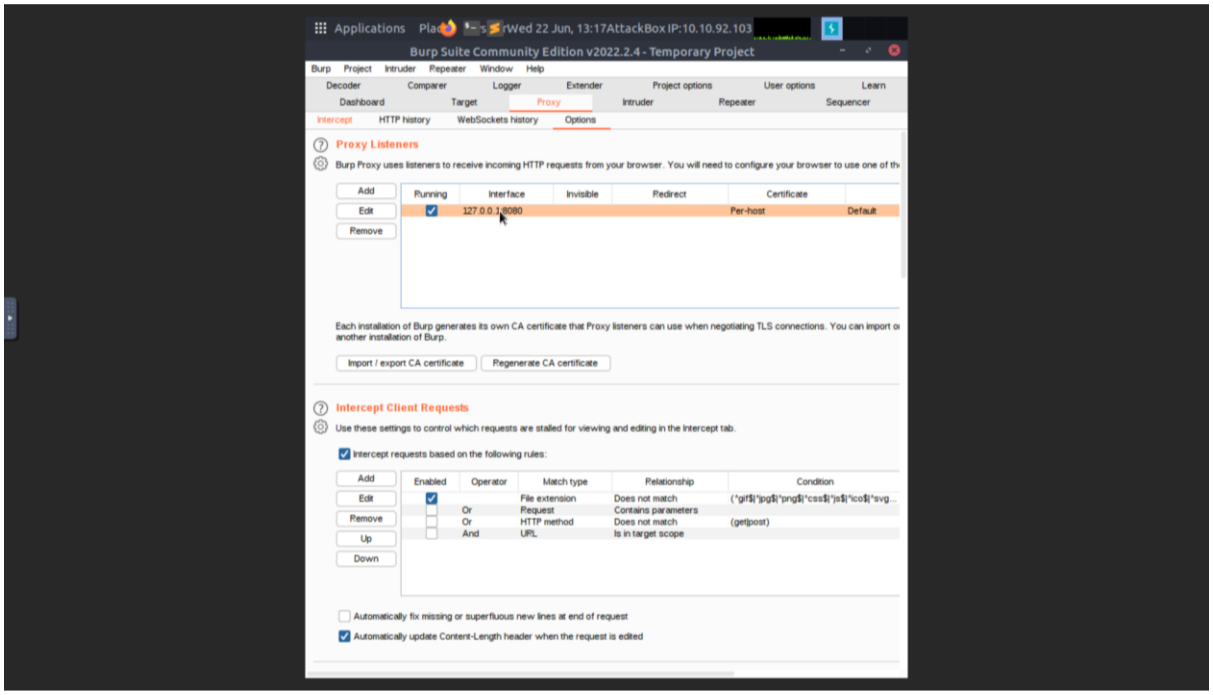
The name of the agent can be obtained from the report given (Hackerone ID:804548).



Answer: **ag3nt-j1**

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

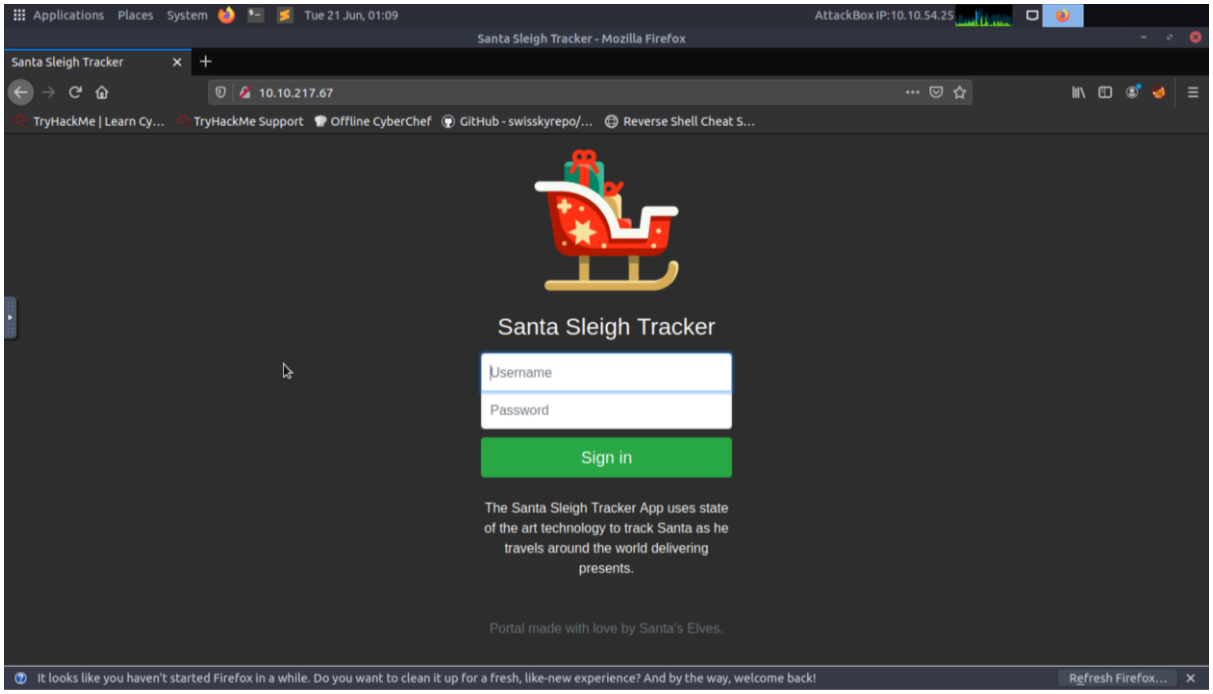
Port number can be obtained from the Option tab in the Proxy tab.



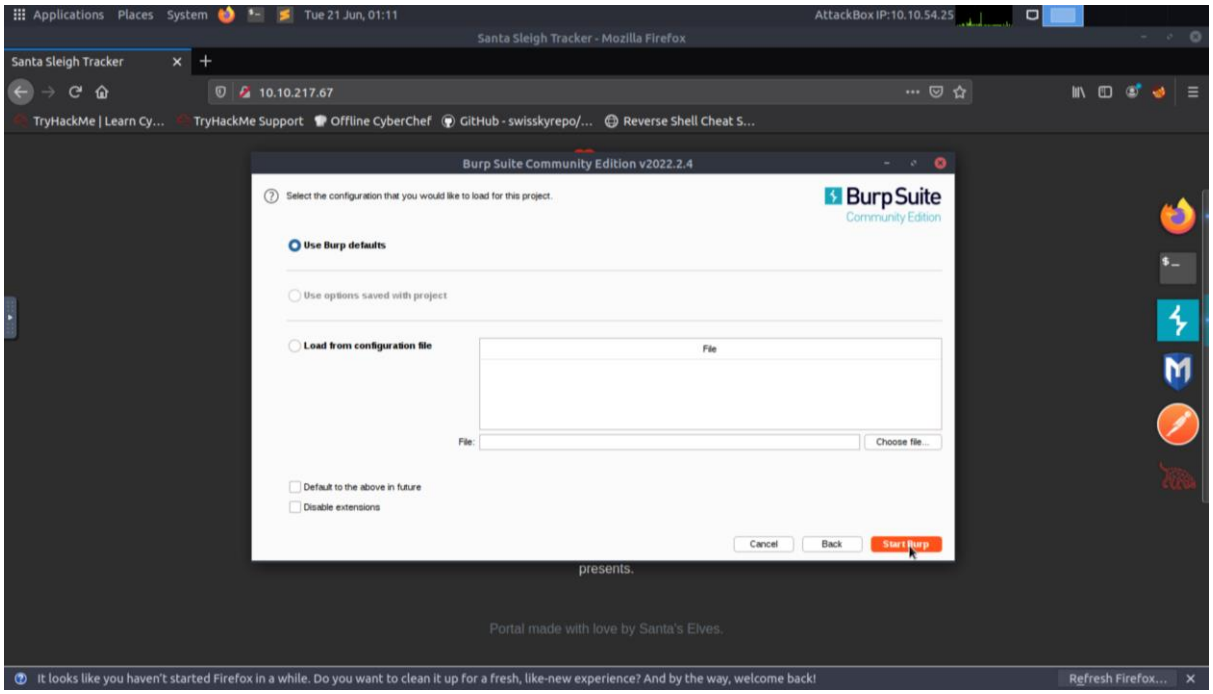
Answer: **8080**

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

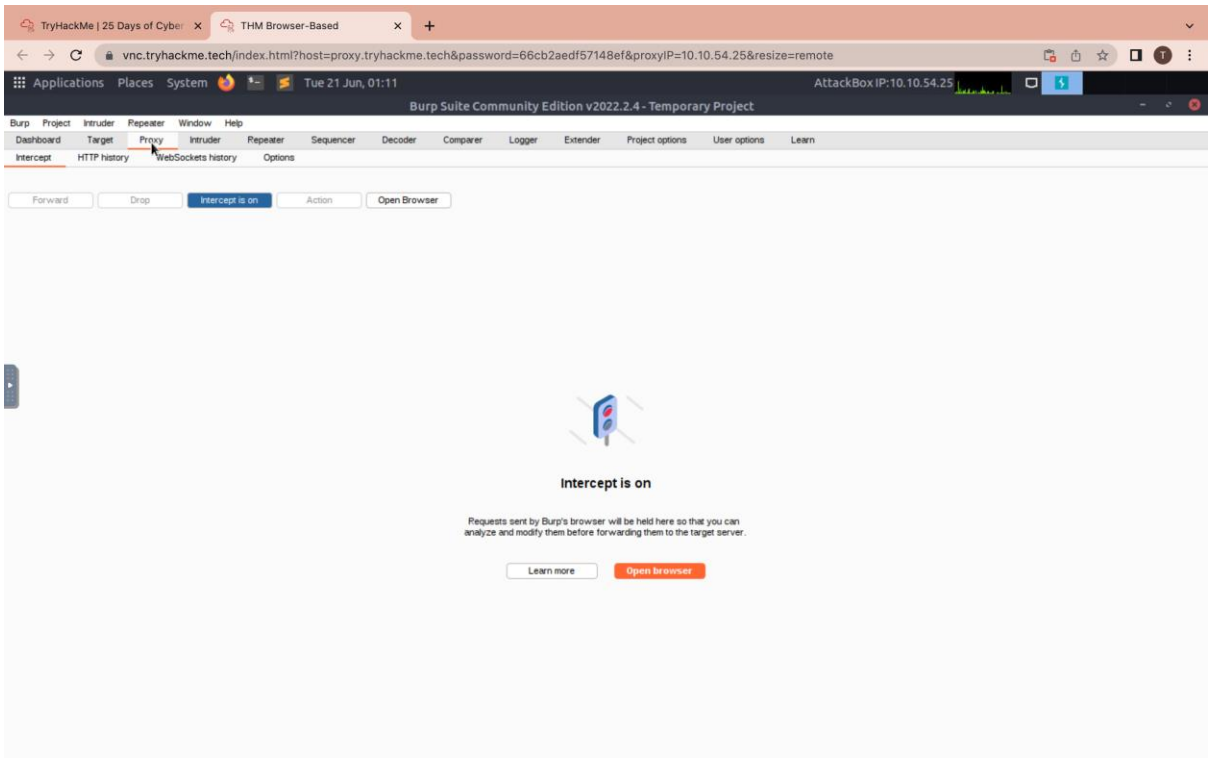
Copy and paste IP address given on the browser search bar to see the Santa Sleigh Tracker app page.



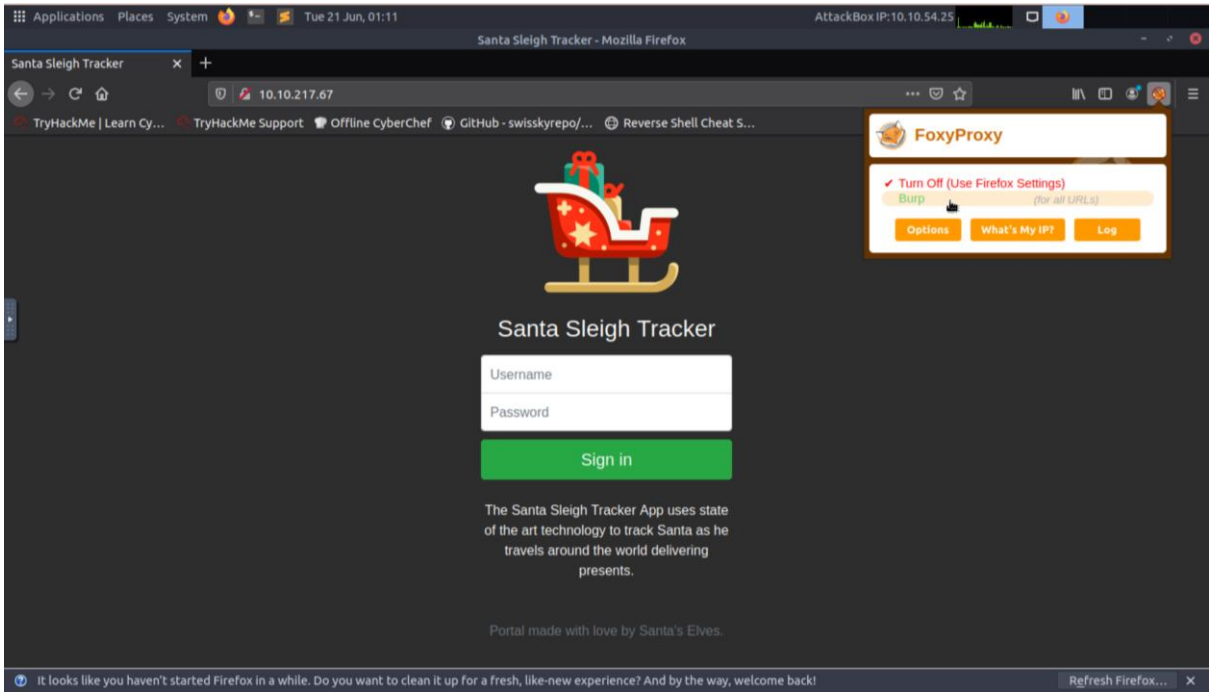
Start BurpSuite.



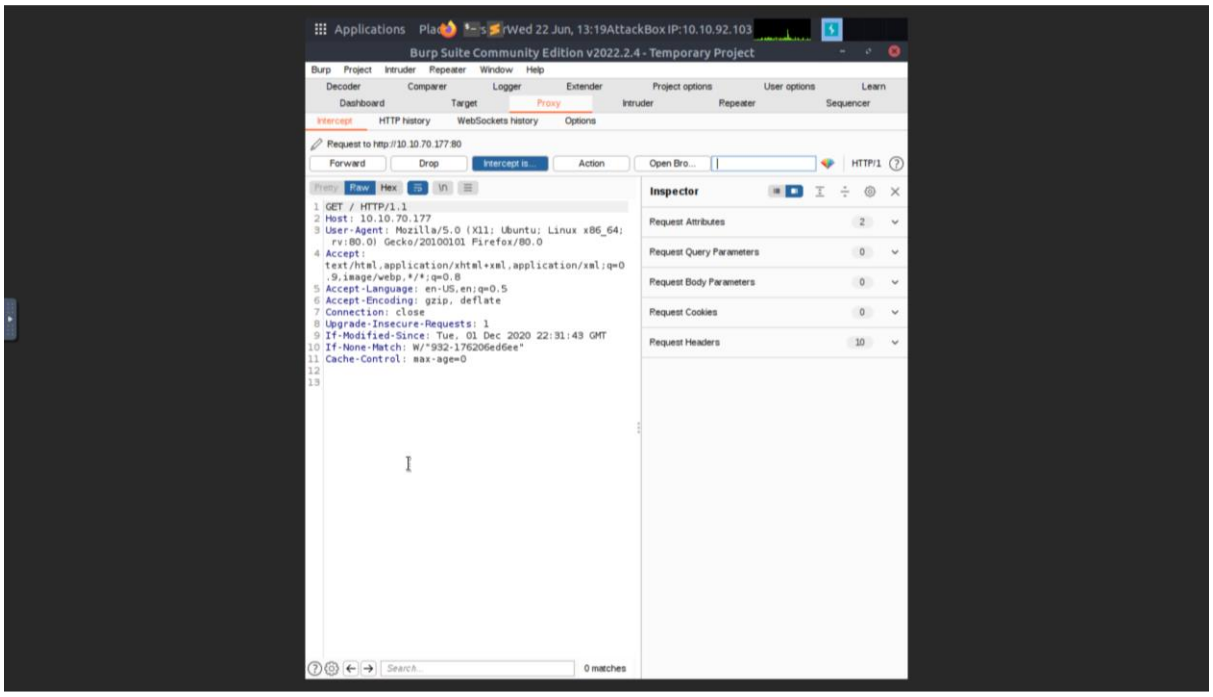
Click the ‘Intercept is On’ button to intercept traffic.



Turn on FoxyProxy to obtain a request.



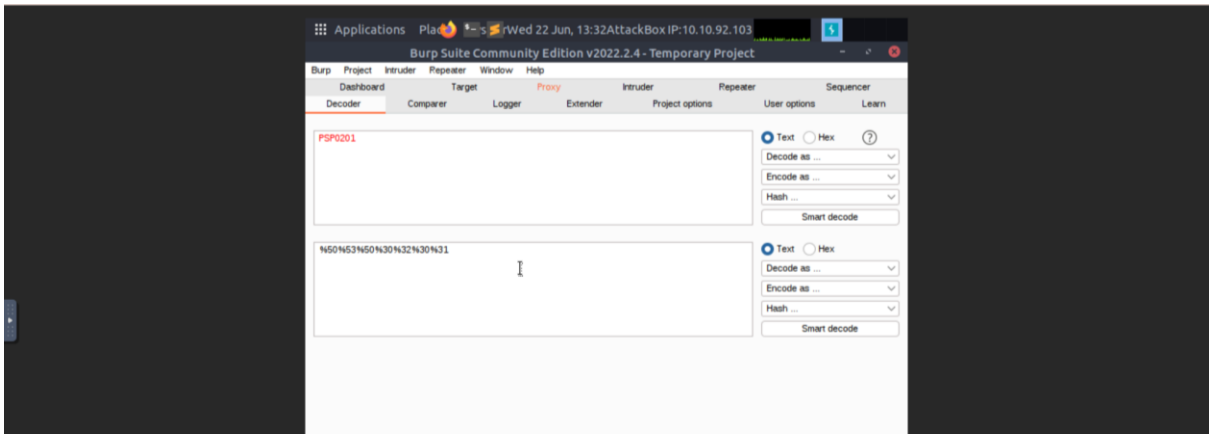
Open BurpSuite and click the Proxy tab to see the proxy type.



Answer: **HTTP**

Question 6: Experiment with decoder on Burp. What is the URL encoding for “PSP0201”?

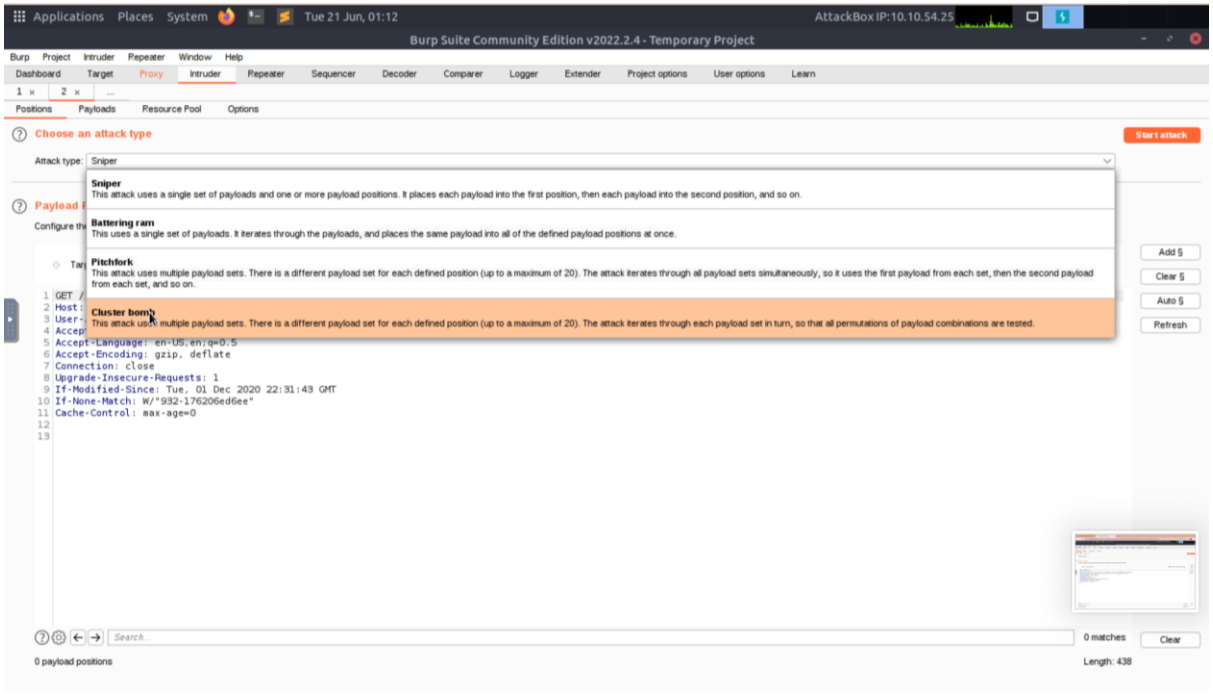
Go to the Decoder tab on BurpSuite and type “PSP0201” and encode as URL.



Answer: **%50%53%50%30%32%30%31**

Question 7: Look at the list of attack type options on intruder. Which of the following options matches the one in the description? Uses multiple payload sets. Different payload for each defined position up to maximum 20. Iterates through each payload set in turn, so all permutations of payload combinations are tested.

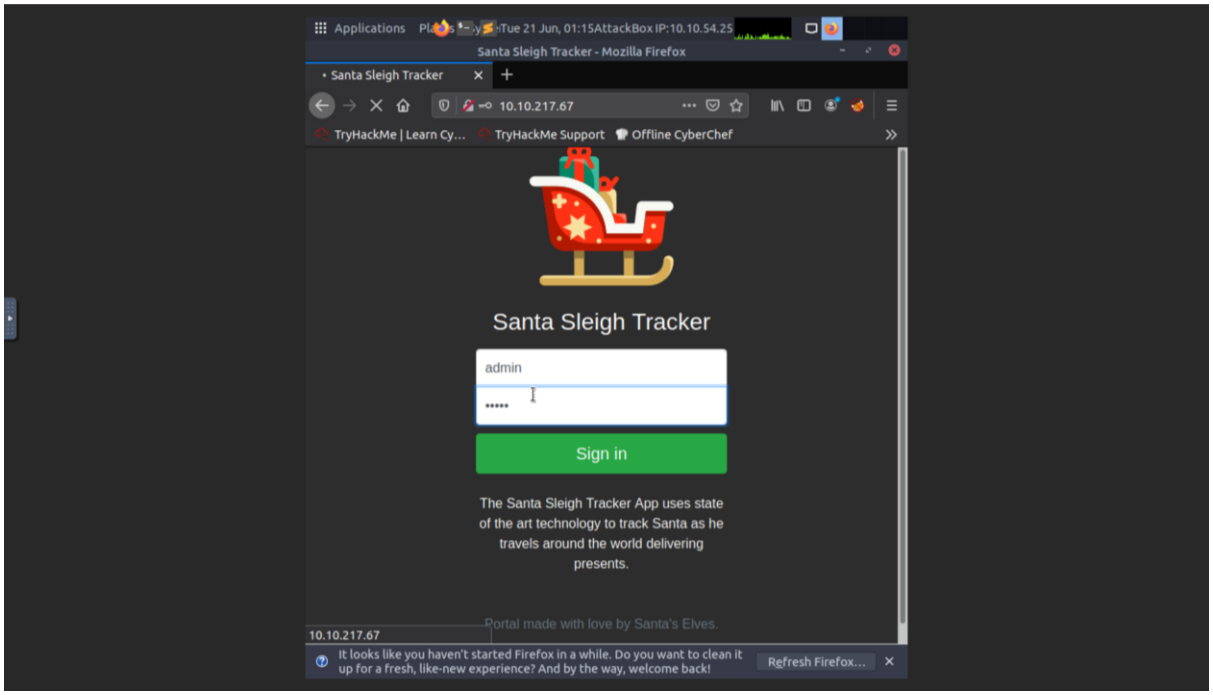
Open BurpSuite. Go to the Intruder tab to see the list of attack type options.



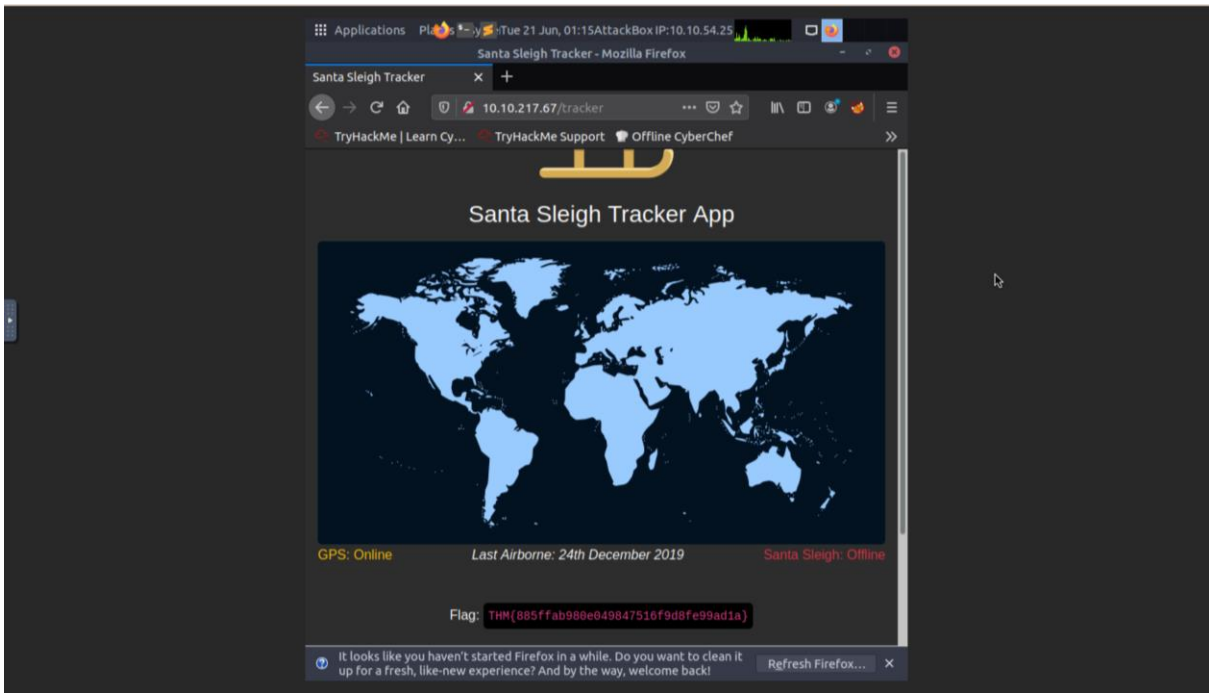
Answer: **Cluster bomb**

Question 8: What is the flag?

After BurpSuite has finished attacking, use the correct credentials to log in to the Santa Sleigh Tracker app. (Username: admin and Password: 12345)



Click sign in to obtain the flag.



Answer: **THM{885ffab980e049847516f9d8fe99ad1a}**

Thought Process/Methodology:

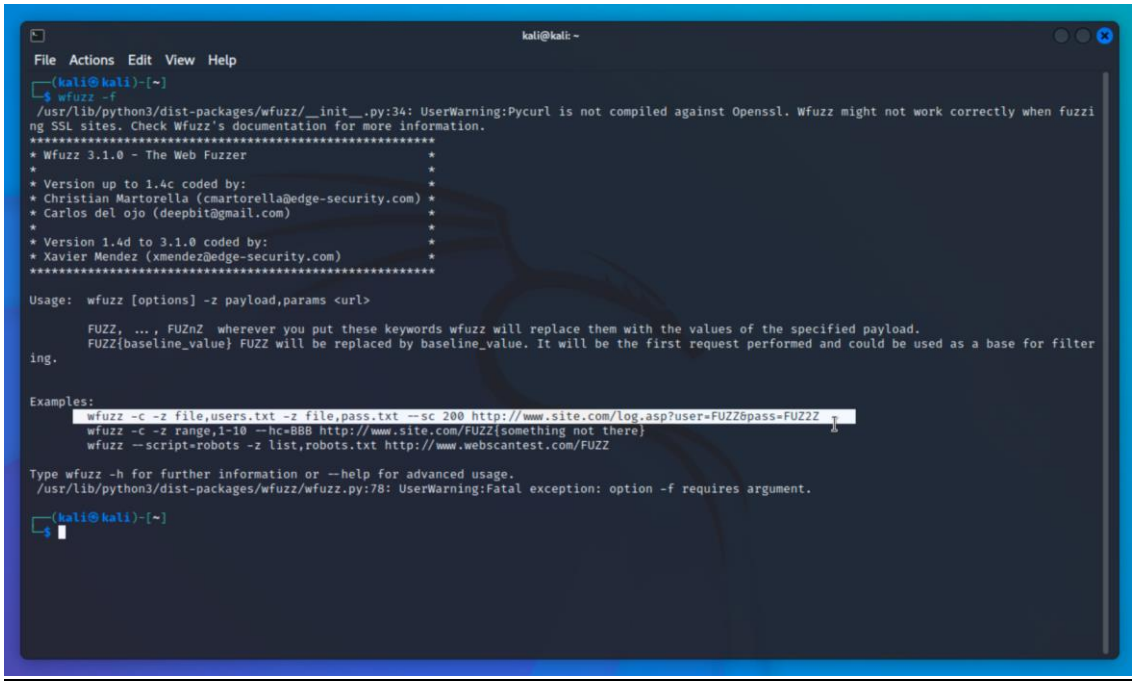
Start AttackBox and click Start Machine on the task. Copy and paste the IP address given into the browser search bar. Start BurpSuite and click “Intercept is On” and turn on FoxyProxy on the browser to intercept traffic. Open BurpSuite application to obtain the request. Right click on the request on the Proxy tab and send to intruder. After sending to the intruder, go to the Intruder tab and click the Position tab. Add usernames and passwords values as positions in the request **(username=test&password=test&Login=Login).** Click the Payload tab to add a few common default usernames and passwords in the Payload Option [Simple Lists]. Click the “Start Attack” button. Once BurpSuite has finished attacking, turn off FoxyProxy and choose correct credentials to log in to the Santa Sleigh Tracker app. After the correct credentials have been logged in, the flag can be obtained on the page.

Day 4: Web Exploitation - Santa's Watching

Tools used: GoBuster, wfuzz, Kali, OpenVPN, Firefox

Solution/walkthrough:

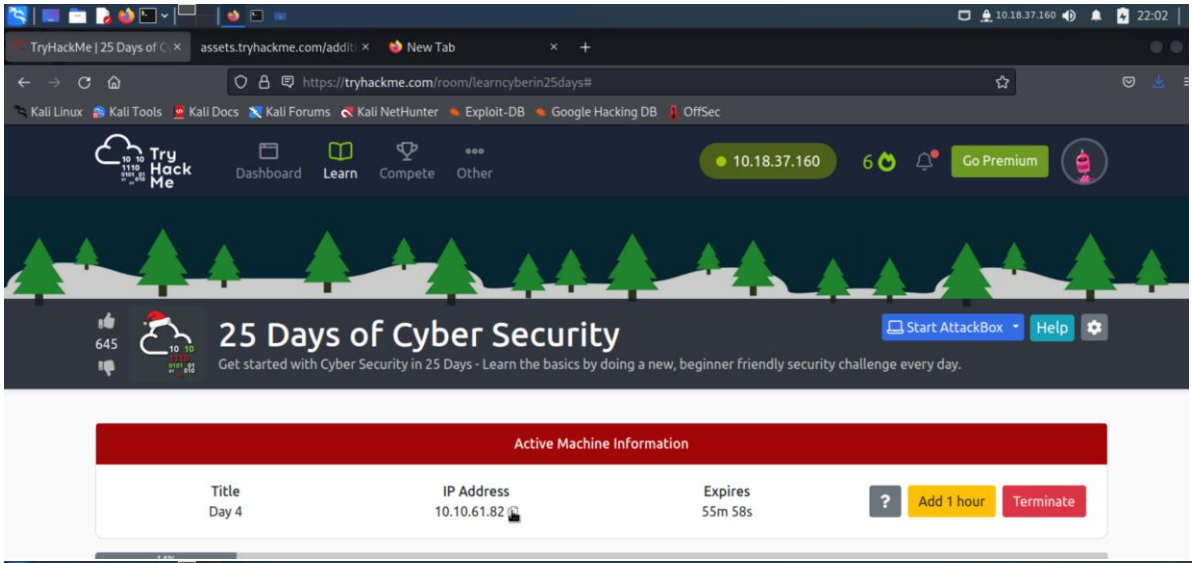
Question 1: Given the URL "http://shibes.xyz/api.php", what would the entire wfuzz command look like to query the "breed" parameter using the wordlist "big.txt" (assume that "big.txt" is in your current directory)

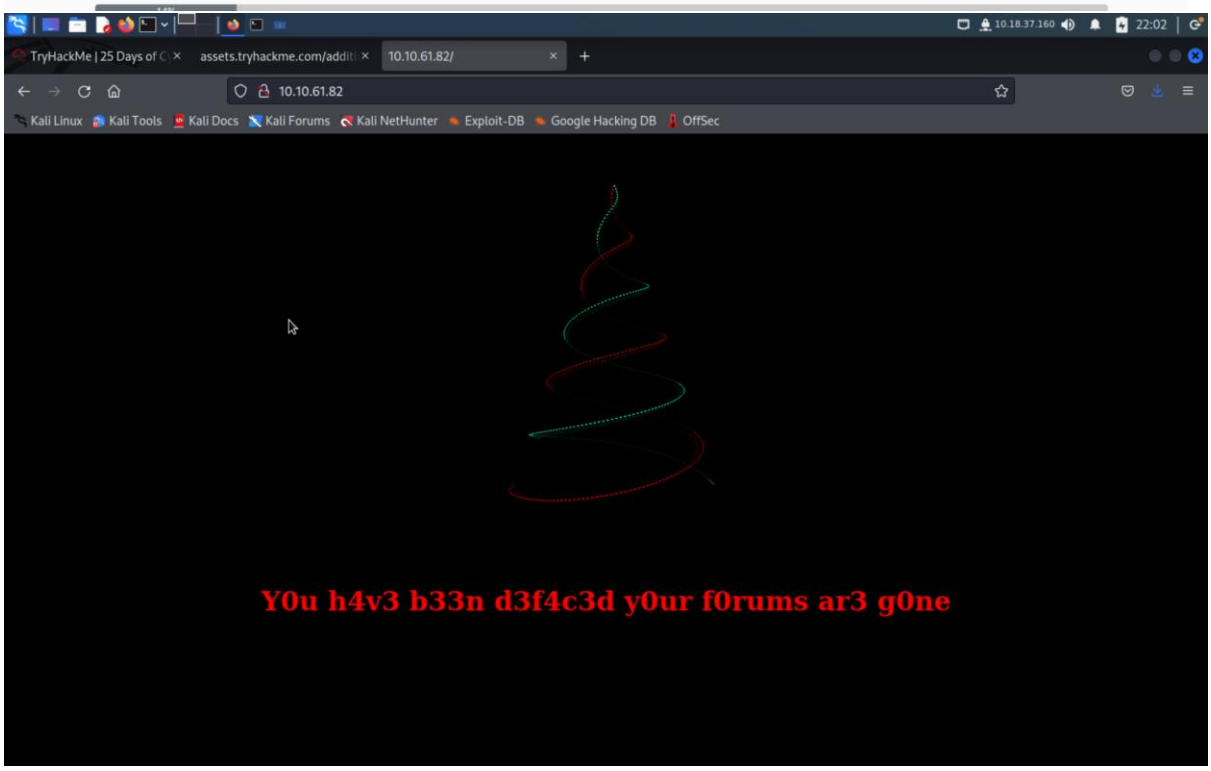


Answer**: wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ**

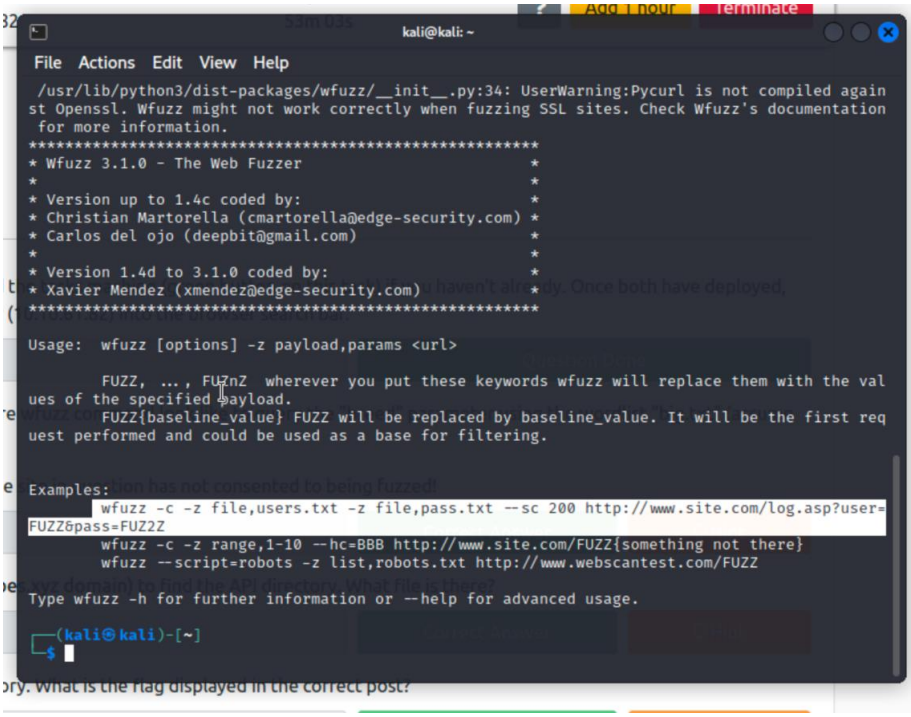
Question 2: Use GoBuster (against the target you deployed -- not the shibes.xyz domain) to find the API directory. What file is there?

Copy the IP address from tryhackme.com and paste into searchbar.

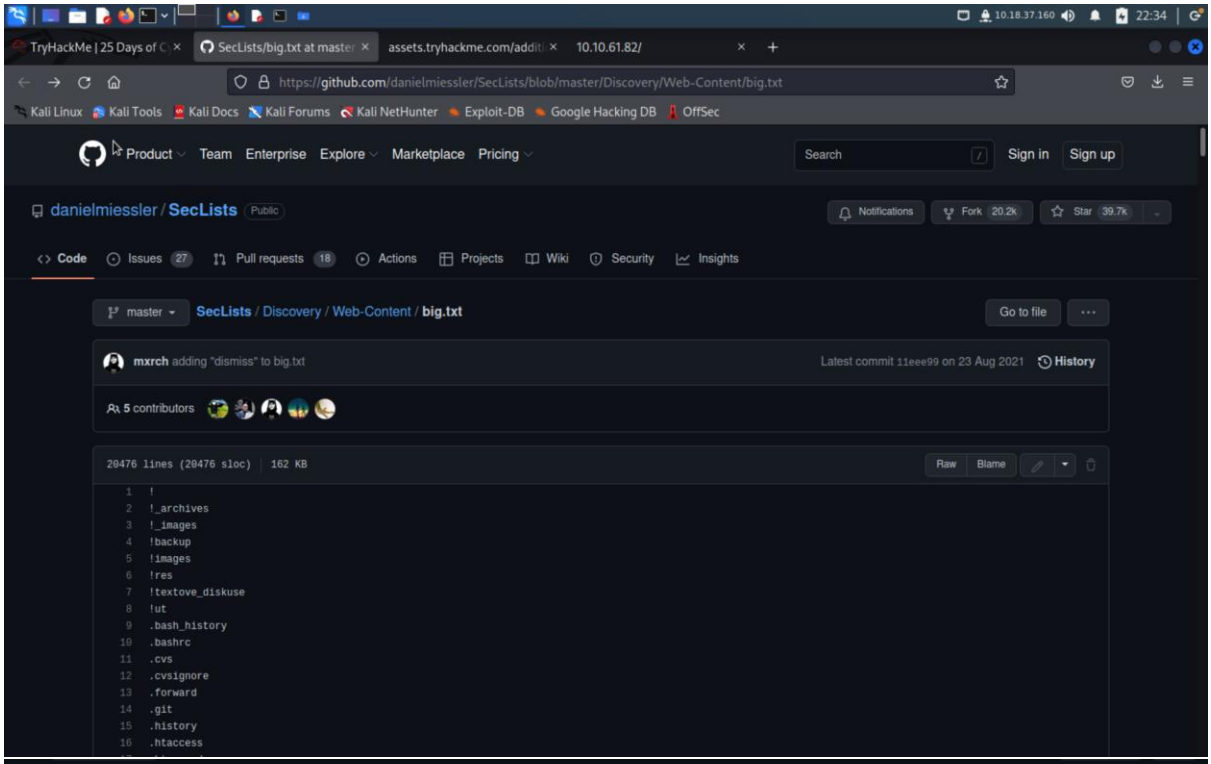


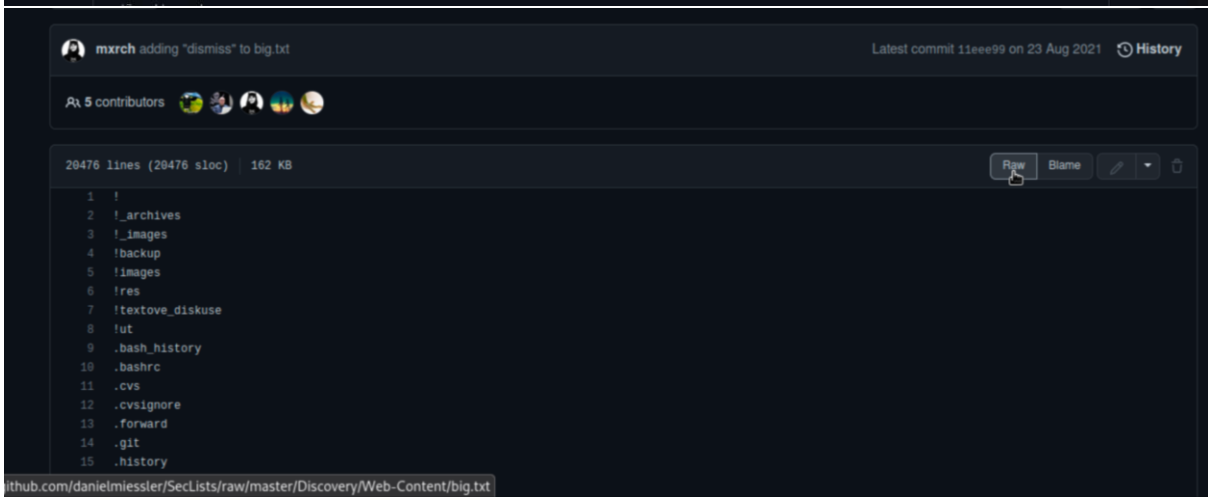


Install wfuzz in Kali by executing **sudo apt install wfuzz** in command prompt. Insert password for Kali to install wfuzz.

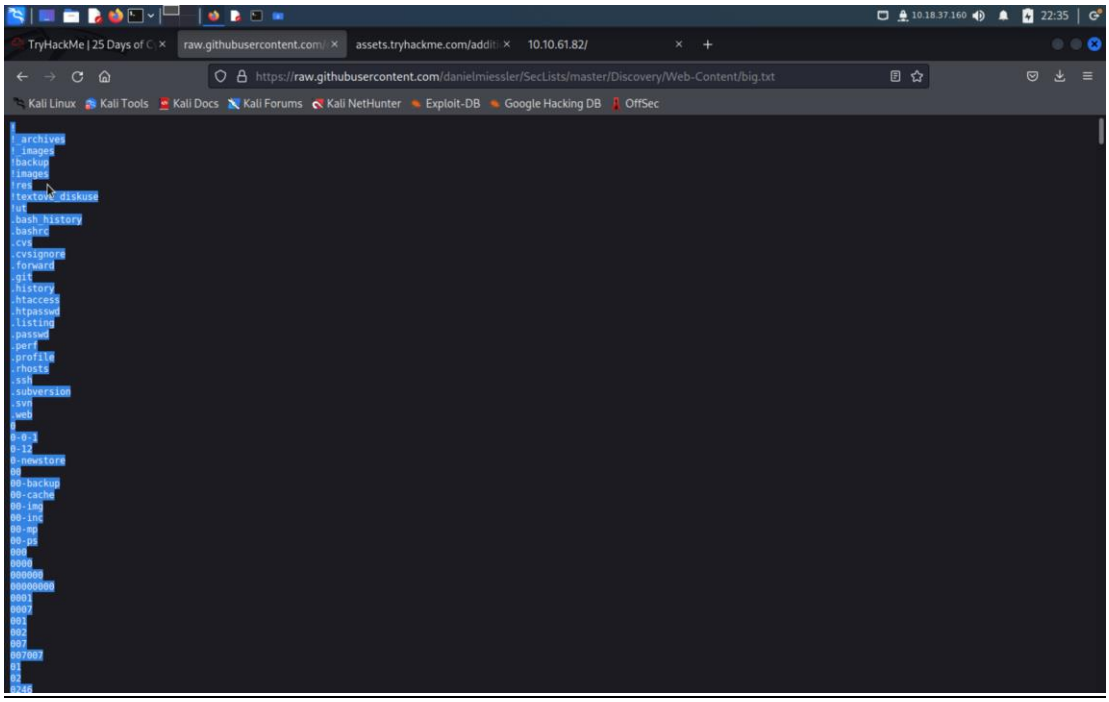


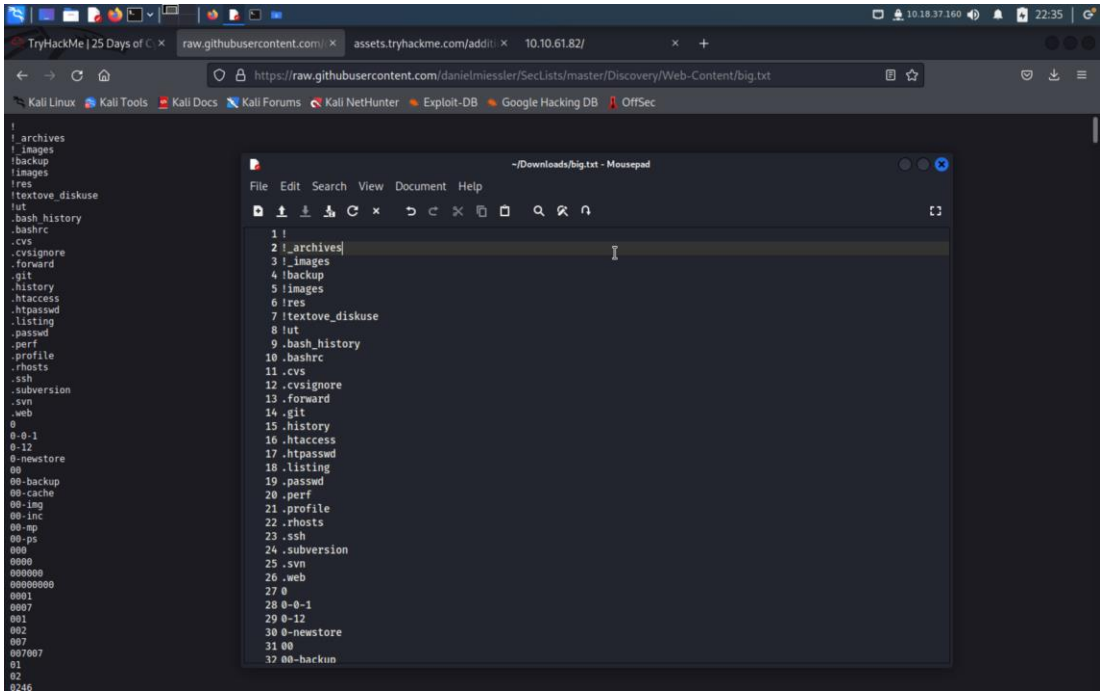
Download the big.txt file from the link given in tryhackme or **https://github.com/danielmiessler/SecLists/blob/master/Discovery/Web-Content/big.txt**. The file can be downloaded by clicking on the raw button to get the text.



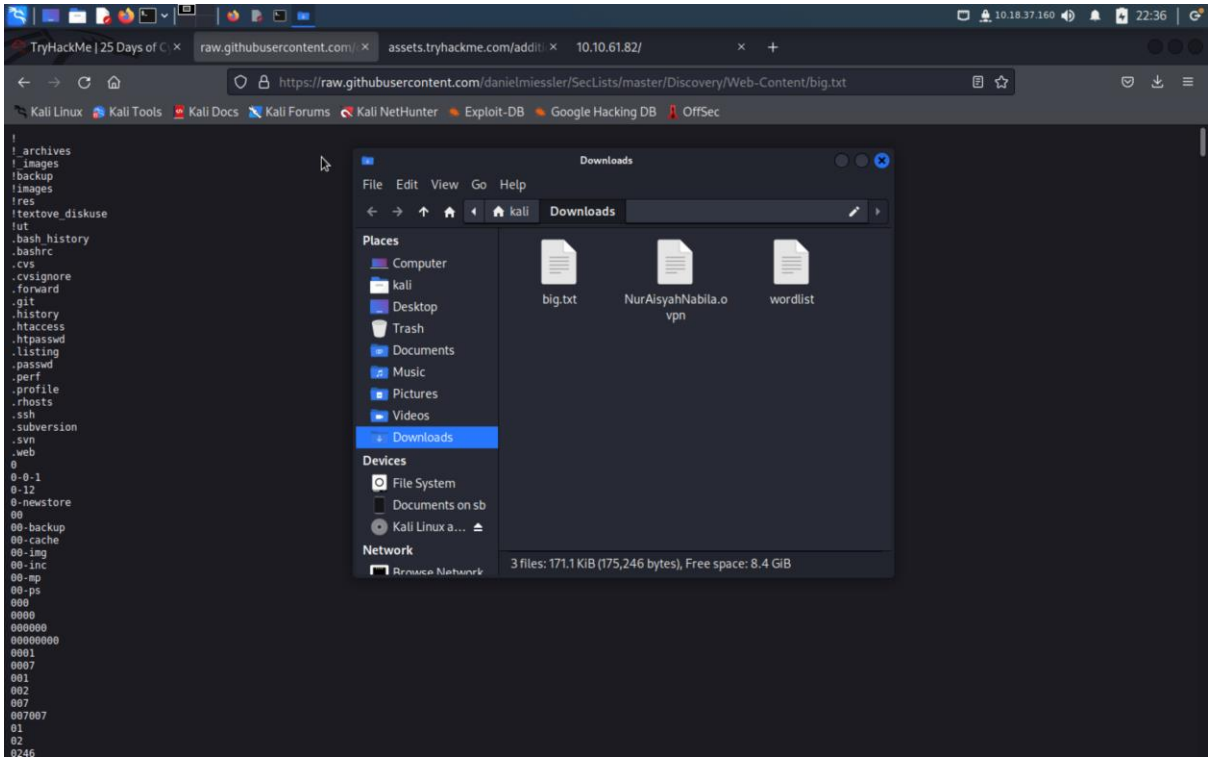


Then, copy and paste the text into your notebook.



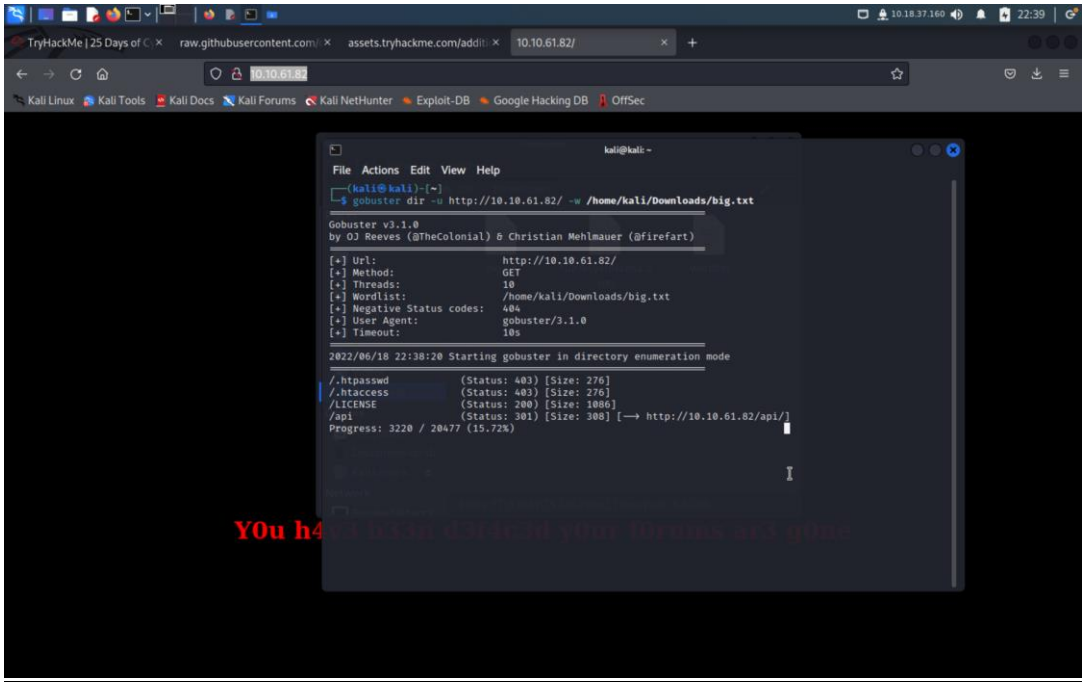


Save the file as **big.txt** into your downloads folder.

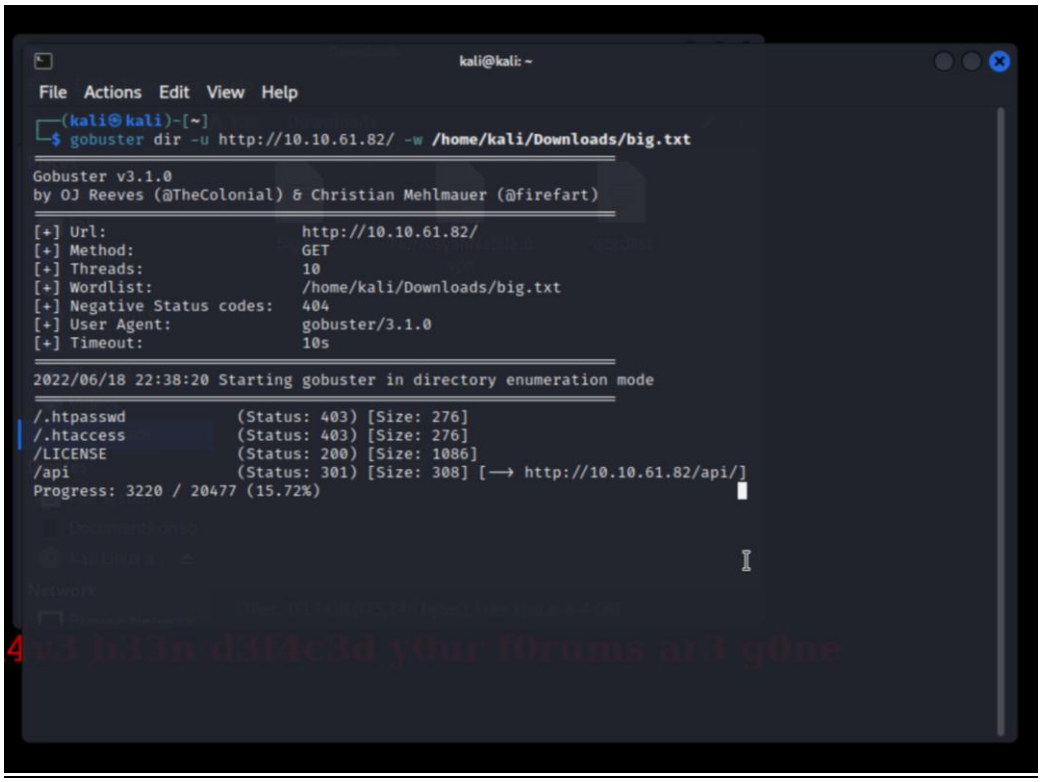


To find the data in the big.txt file, in the command prompt, execute **gobuster dir -u http://10.10.61.02 -w /home/kali/Downloads/big.txt**

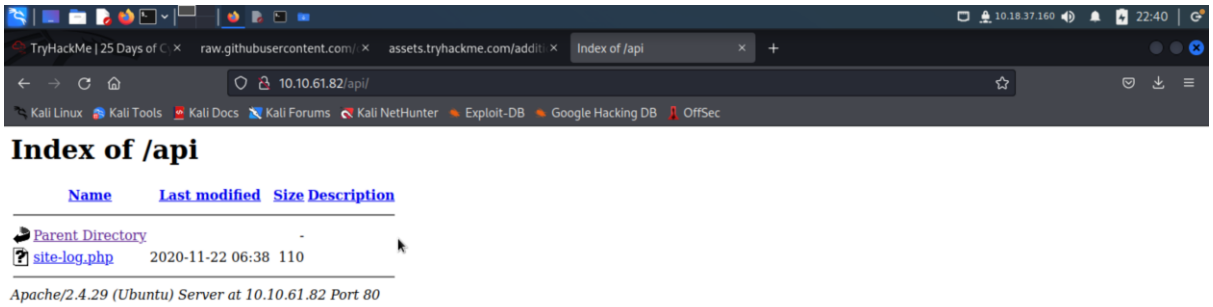
The **dir** command is used for directory, while the **w** command is the path for the wordstring. Since the big.txt file is saved into the Downloads folder, the pathway will be written as **-w /home/kali/Downloads/big.txt** .



In the command prompt, there is **/api** and [→ http://10.10.61.02/api/]. Type this url into the searchbar to open the API directory.



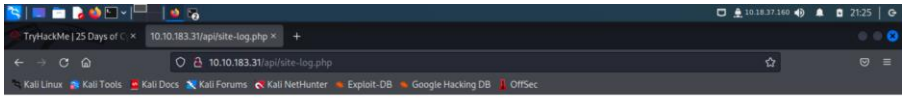
Now, we can see there is the file site-log.php in the API directory.



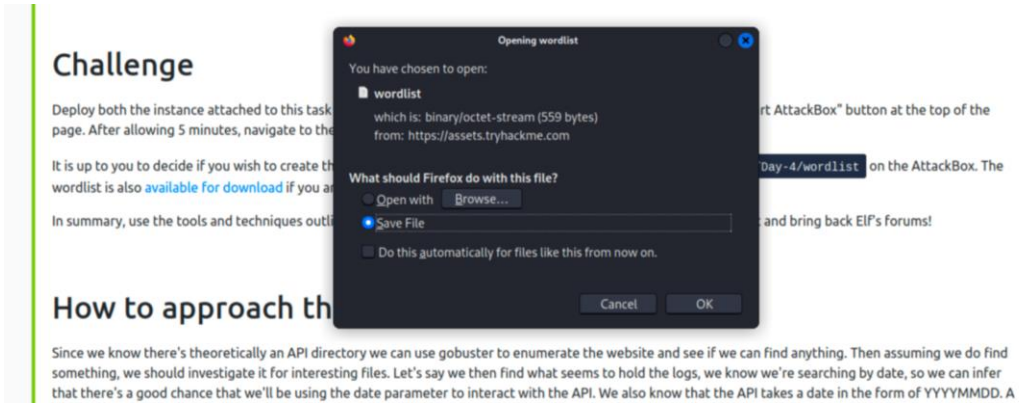
Answer: **site-log.php**

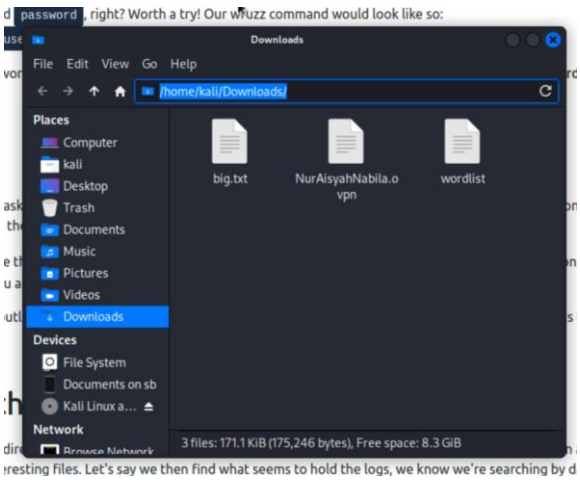
Question 3: Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?

Click on the site-log.php. Nothing is seen on the page.



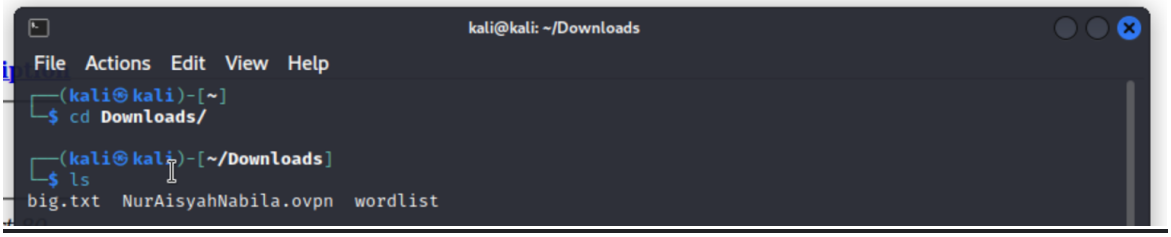
Download the wordlist file into the Downloads folder from tryhackme.



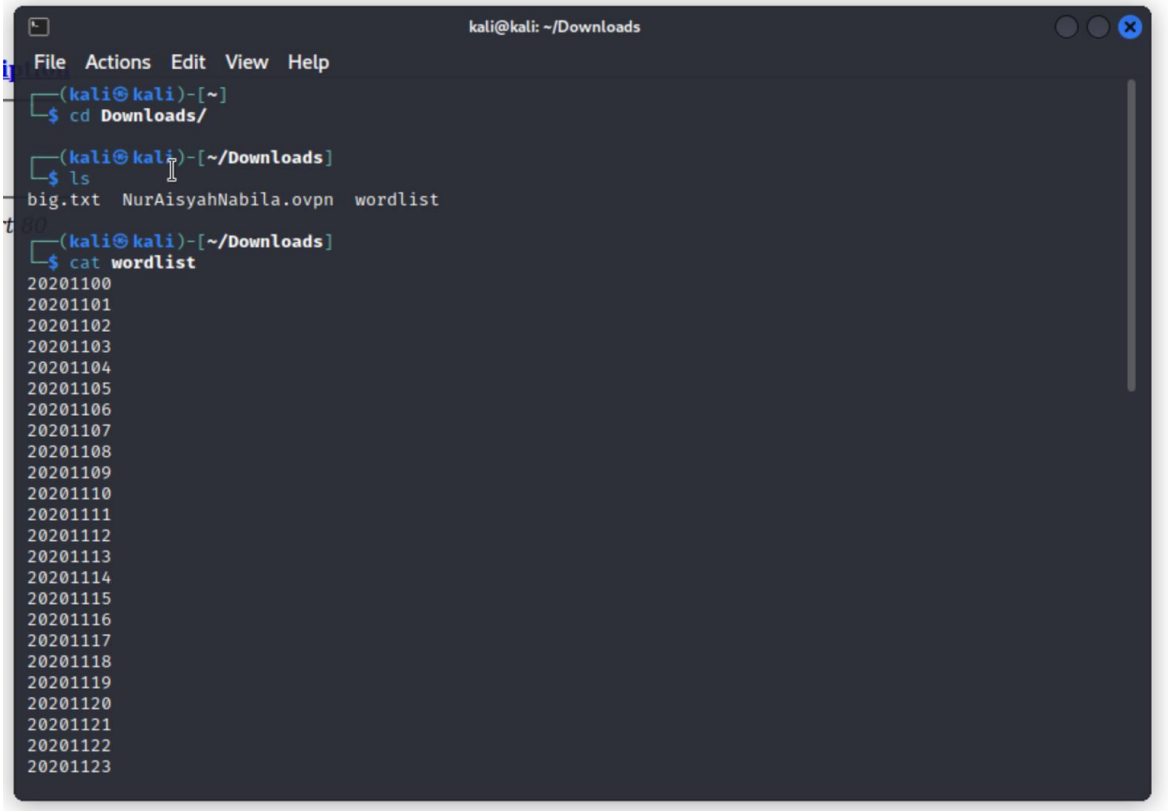


Change directory to the Downloads folder by executing the command-line shell command **cd Downloads/** .

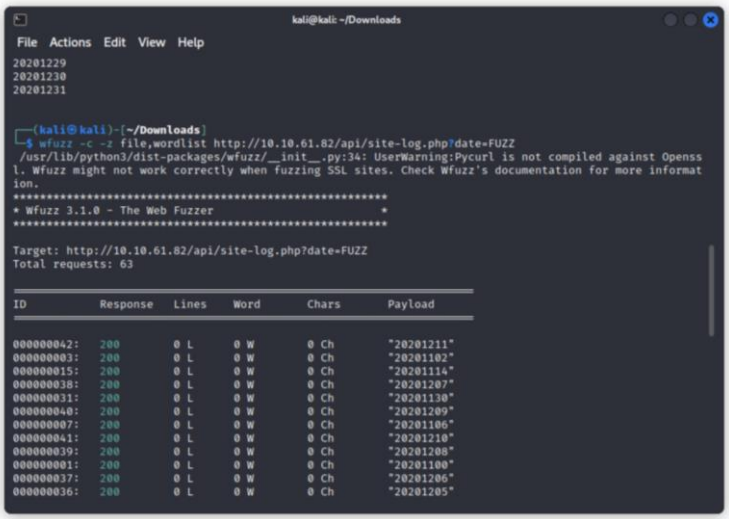
To see if the wordlist file exists in the Downloads directory, use the **ls** command to list files.



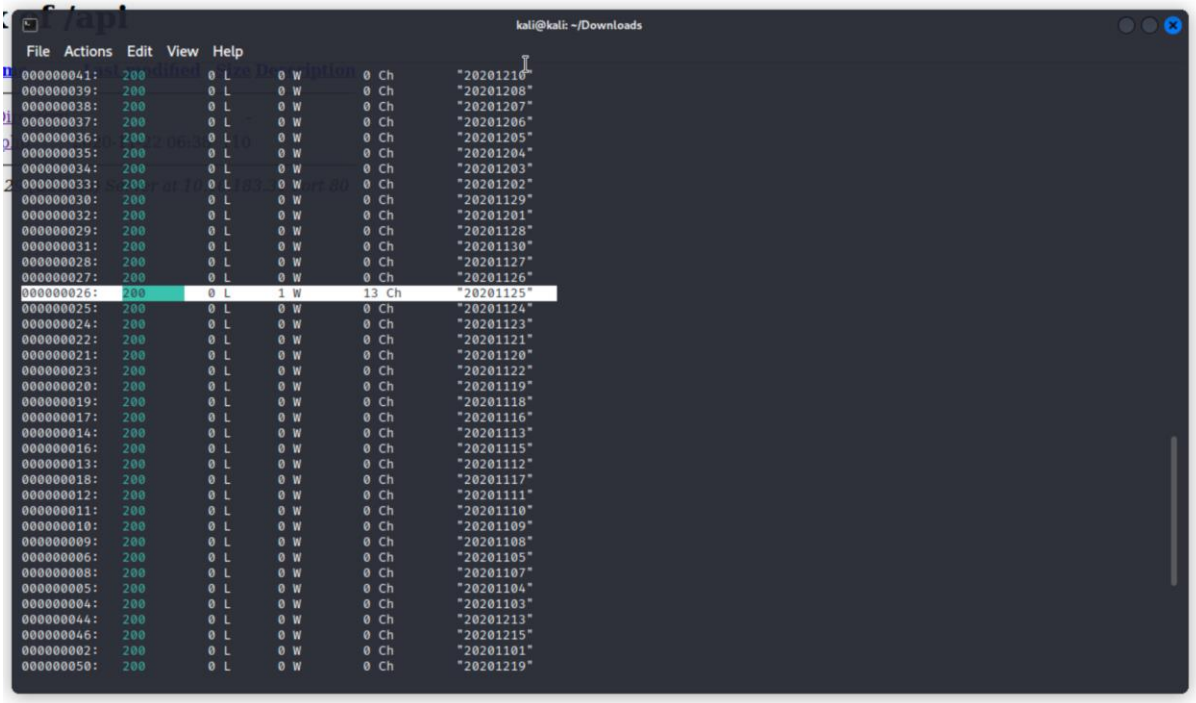
To view the contents of the wordlist file, use the **cat wordlist** command.



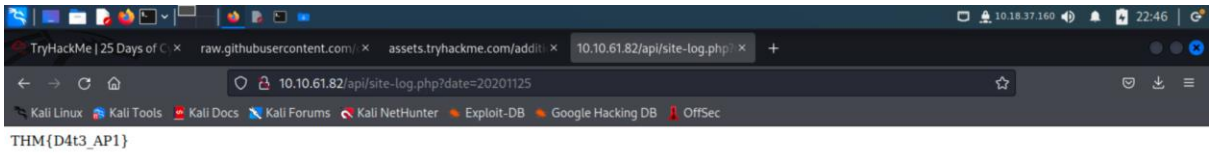
To filter out parameters that do not return anything from the wordlist, wfuzz will be used. To fuzz the date parameter found in site-log.php, execute **wfuzz -c -z file,wordlist http://10.10.61.82/api/site-log.php?date=FUZZ** .



We can see there is one date variable with 13 Ch at chars, which is **20201125**. Copy this date, and replace FUZZ in the url with the copied date.



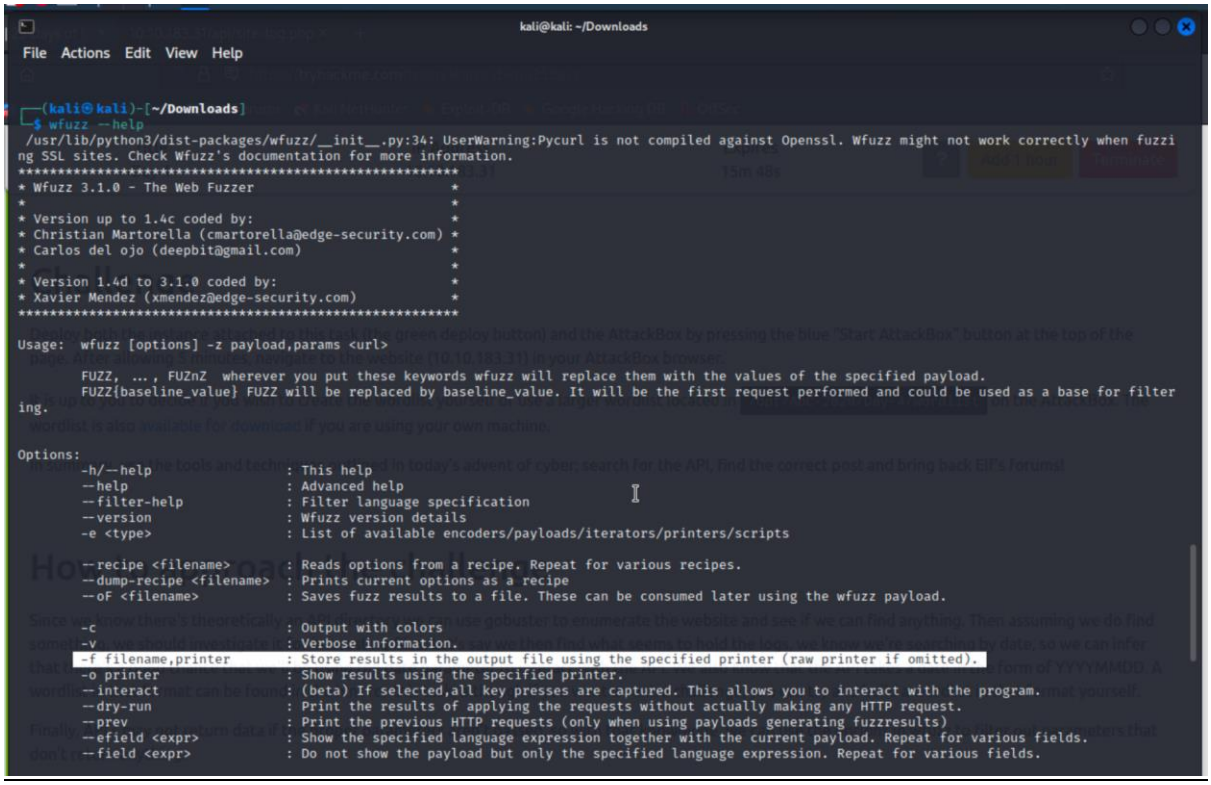
The url should look like **http://10.10.61.82/api/site-log.php?date=20201125** .Type the url into the searchbar and the flag will be seen on the webpage.



Answer**: THM{D4t3_API}**

Question 4: Look at wfuzz's help file. What does the -f parameter store results to?

Execute **wfuzz --help in** command prompt to open wfuzz's advanced help file.



Answer: **filename, printer**

Thought Process/Methodology:

We accessed the target machine and we were shown the IP Address target's website. After we managed to access the website, we were shown a webpage containing a picture of a christmas tree and text which was "Y0u h4v3 b33n d3f4c3d y0ur f0rums ar3 g0ne". The login page has been completely removed. However, we managed to find the API directory and enumerate the website using GoBuster. Firstly, we downloaded the big.txt file from tryhackme that contains the wordlist. To find the API directory, we used the command **gobuster dir -u http://10.10.61.02 -w /home/kali/Downloads/big.txt.** After the GoBuster runs, it eventually finds the API directory which is **http://10.10.61.02/api/.** On the webpage, we can see there is a php file named **site-log.php**. Secondly, we used wfuzz to fuzz the date parameters in the site-log.php file. In this file, we noticed that the API takes the date parameter in the form of **YYYYMMDD**. Therefore, we downloaded a wordlist with the same format of the date parameter from the tryhackme website into the Downloads folder. Next, we used wfuzz to filter out parameters that do not return any data from the wordlist using the command **wfuzz -c -z file,wordlist http://10.10.61.82/api/site-log.php?date=FUZZ.** After wfuzz successfully runs, we get a response with 13 characters, which is different from all the other logs. We copied the date 20201125 and pasted it into our url, **http://10.10.61.82/api/site-log.php?date=20201125.** After entering it into the searchbar, we managed to receive the flag.

To see the advanced help directory for wfuzz, we executed the command **wfuzz --help** in the command prompt. In the command prompt, we found that -f parameter stores results to filename and printer.

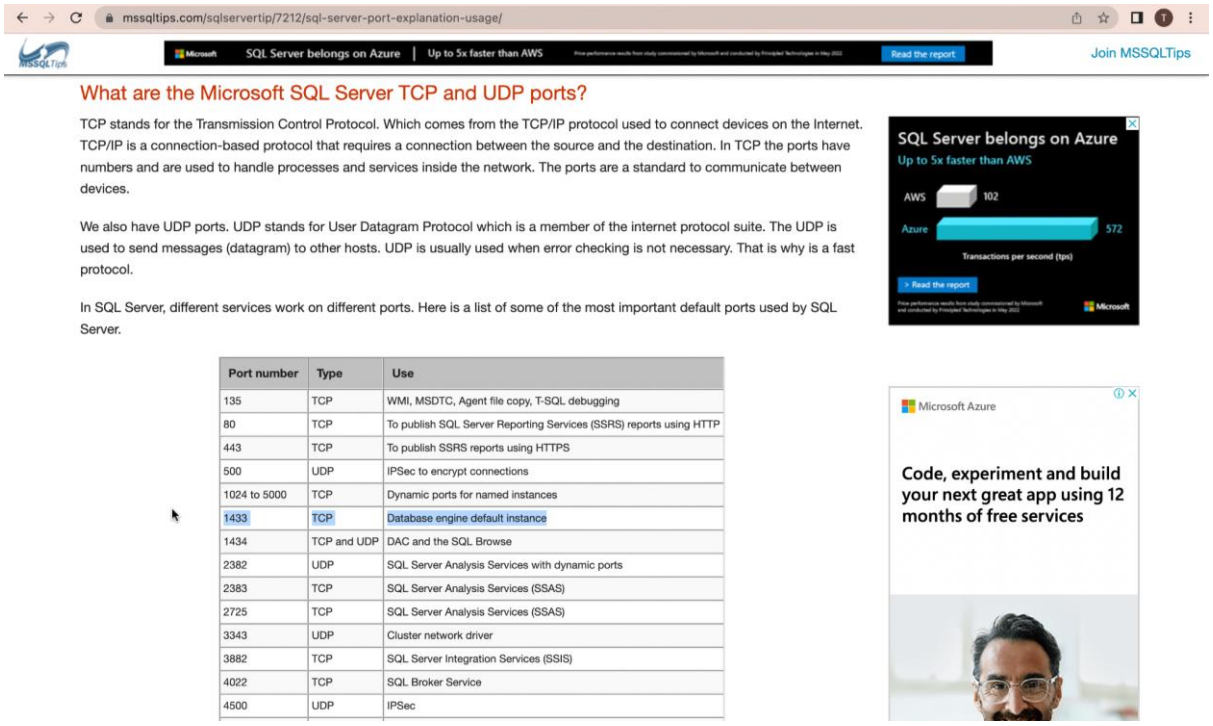
Day 5: Web Exploitation - Someone stole Santa's gift list

Tools used: Attack Box, OpenVPN, Firefox, OWASP ZAP

Solution/walkthrough:

Question 1: What is the default port number for SQL Server running on TCP?

Default port number for SQL Server running on TCP can be found in the Microsoft Documentation.

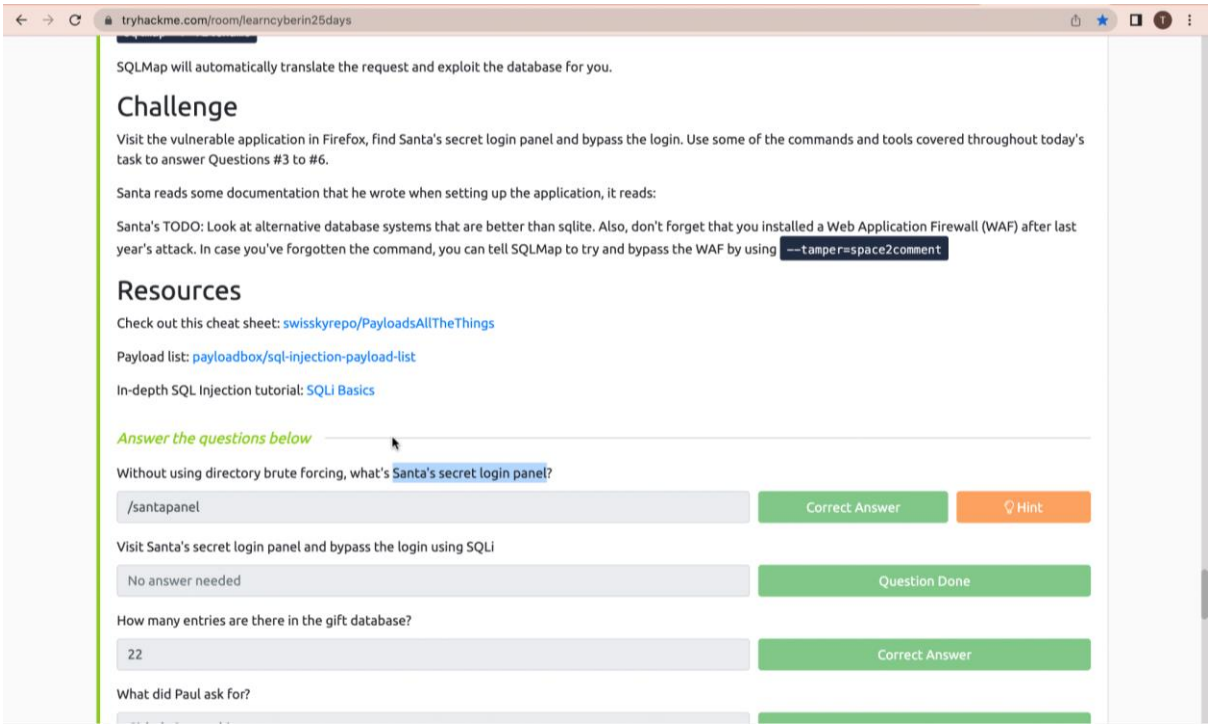


Port number	Type	Use
135	TCP	WMI, MSDTC, Agent file copy, T-SQL debugging
80	TCP	To publish SQL Server Reporting Services (SSRS) reports using HTTP
443	TCP	To publish SSRS reports using HTTPS
500	UDP	IPSec to encrypt connections
1024 to 5000	TCP	Dynamic ports for named instances
1433	TCP	Database engine default instance
1434	TCP and UDP	DAC and the SQL Browse
2382	UDP	SQL Server Analysis Services with dynamic ports
2383	TCP	SQL Server Analysis Services (SSAS)
2725	TCP	SQL Server Analysis Services (SSAS)
3343	UDP	Cluster network driver
3882	TCP	SQL Server Integration Services (SSIS)
4022	TCP	SQL Broker Service
4500	UDP	IPSec

Answer: **1433**

Question 2: Without using directory brute forcing, what's Santa's secret login panel?

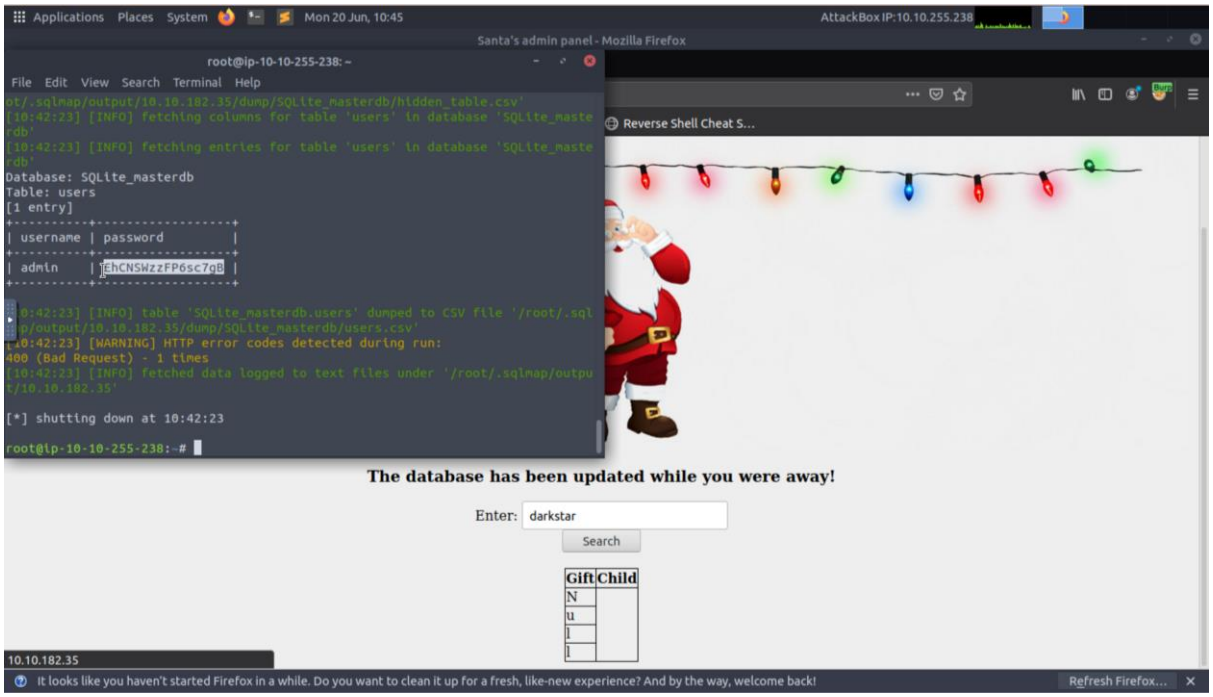
By deriving out of the words from the question, we can get the subdirectory by the method called try and error.



Answer: **/santapanel**

Question 3: What is the database used from the hint in Santa's TODO list?

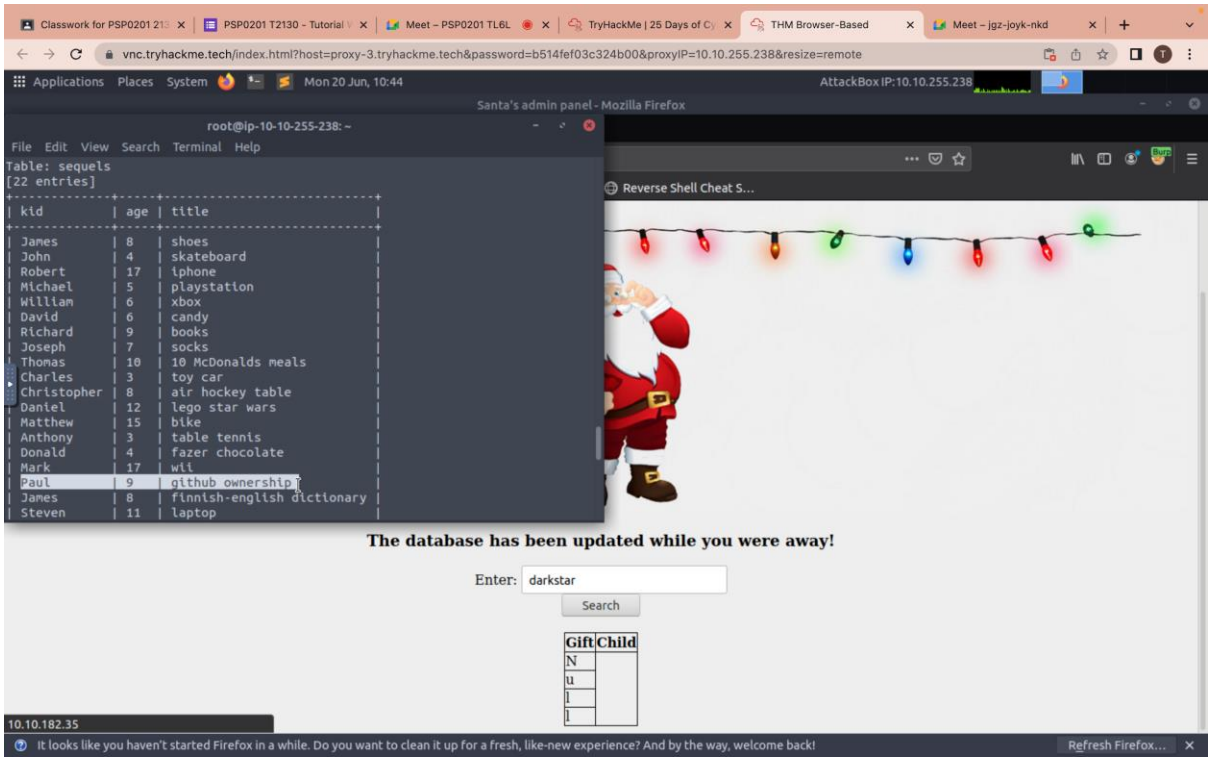
By using ***sqlmap -r <filename> –tamper=space2comment –dump-all –dbms sqlite***, the database used is shown.



Answer: **sqlite**

Question 4: How many entries are there in the gift database?

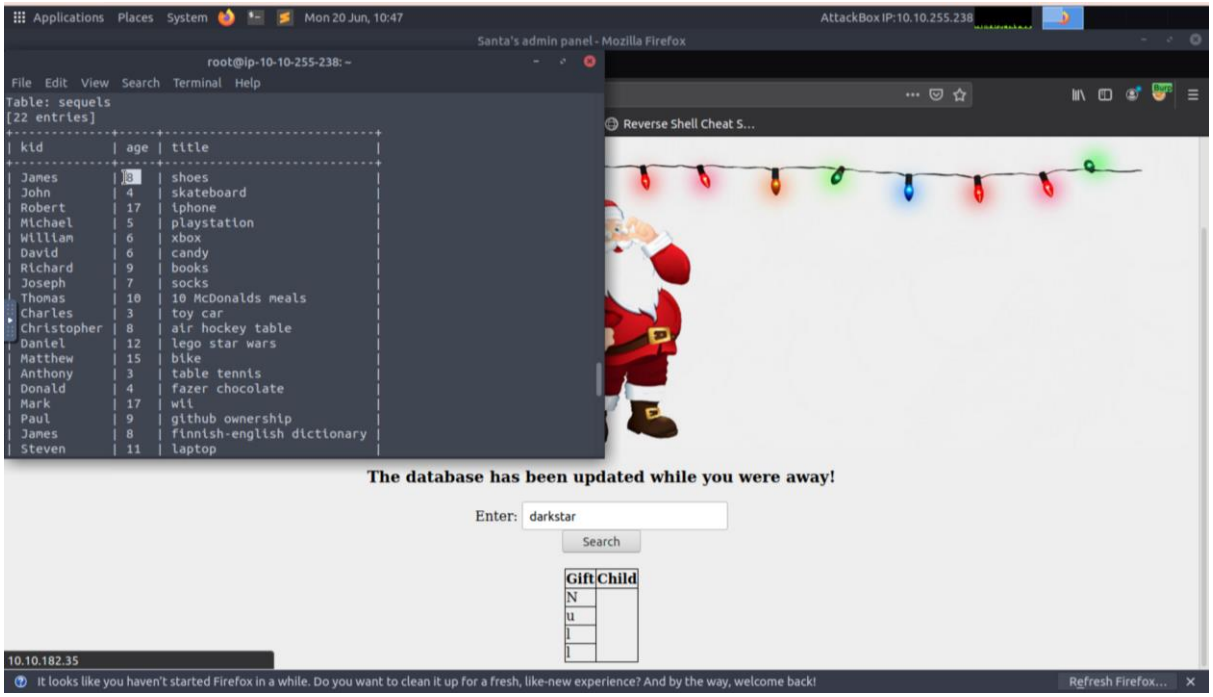
By using **sqlmap -r <filename> –tamper=space2comment –dump-all –dbms sqlite** on terminal, number of entries are shown above the table of 'sequels'.



Answer: **22**

Question 5: What is James' age?

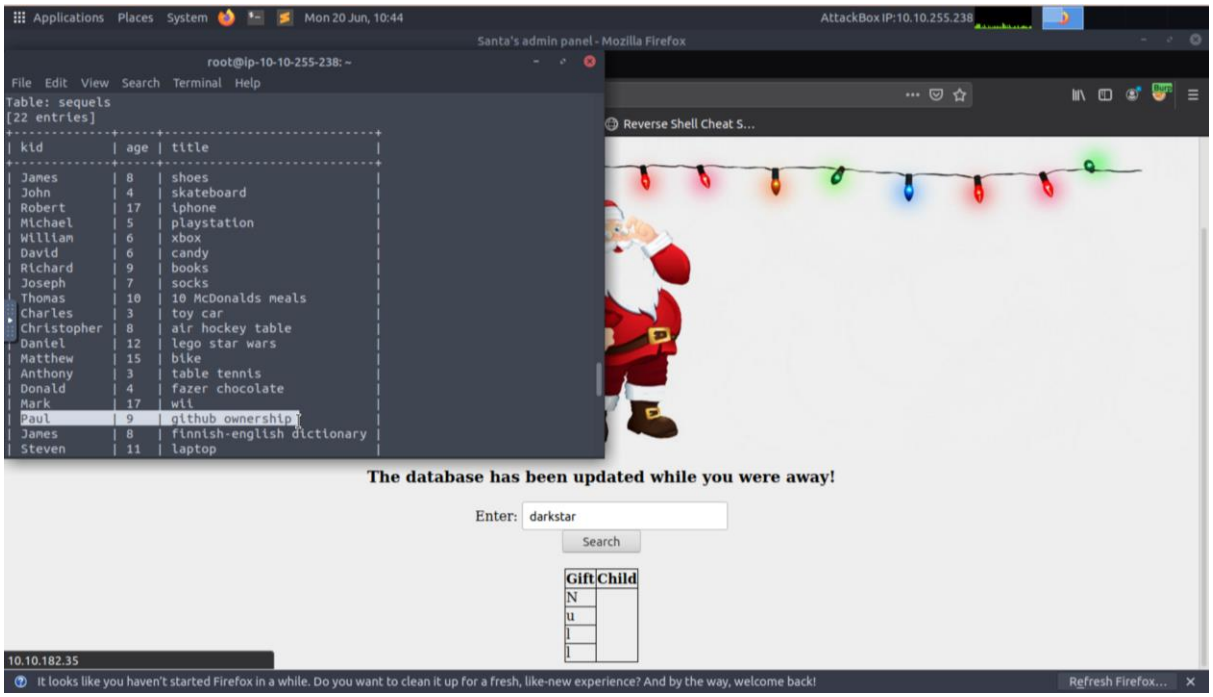
Doing the same step as Question 3, James' age can be obtained from the database shown on the terminal.



Answer: **8**

Question 6: What did Paul ask for?

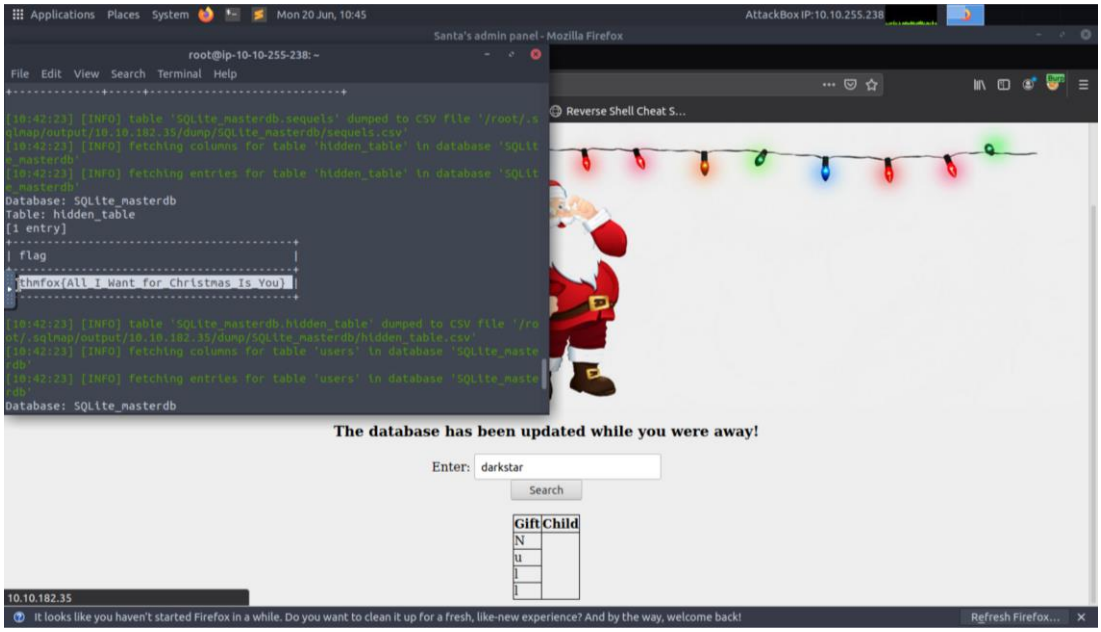
Based on the database obtained on the terminal, what Paul asked for is in the table given.



Answer: **github ownership**

Question 7: What is the flag?

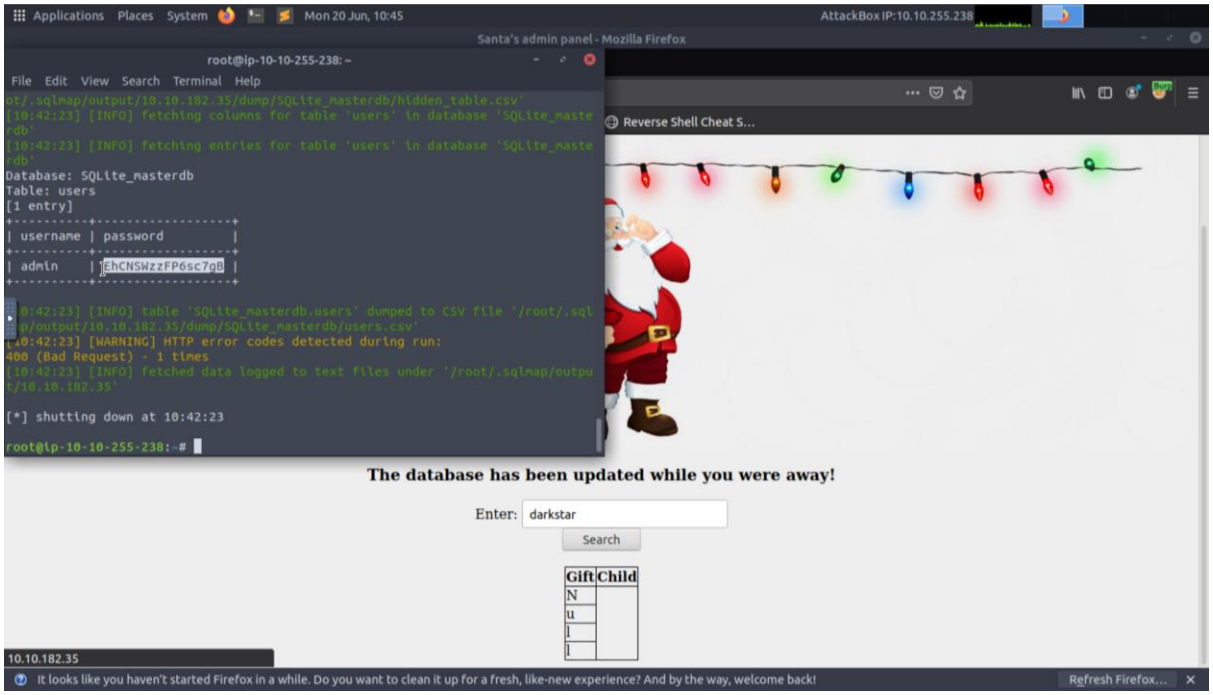
The flag is obtained from the database.



Answer: **thmfox{All_I_Want_for_Christmas_Is_You}**

Question 8: What is admin's password?

Admin's password is obtained from the database.



Answer: **EhCNSWzzFP6sc7gB**

Thought Process/Methodology:

Start AttackBox and click on the "Start Machine" on the task given to obtain IP address. Copy and paste IP address on the browser search bar and add the subdirectory **/santapanel** next to the IP address to see the Santa's Admin Panel page. Start BurpSuite and click on "Intercept is On" on the Proxy tab. Turn on the FoxyProxy on the browser to get the request. Open BurpSuite Application and go to the Proxy tab to see the request. Right click on the request and Send to Repeater and right click the request on the Repeater tab to save item. Name the item and save it on the Desktop. Then, open terminal and type **sqlmap -r <filename> –tamper=space2comment –dump-all –dbms sqlite** to see the database that has all the answers to the questions which are the admin's password, what Paul asked for, Jame's age and the name of the database used. Also, the flag can be obtained from the database shown.