PSP0201

Week 2

Writeup

Group Name: CyberQuest

Members

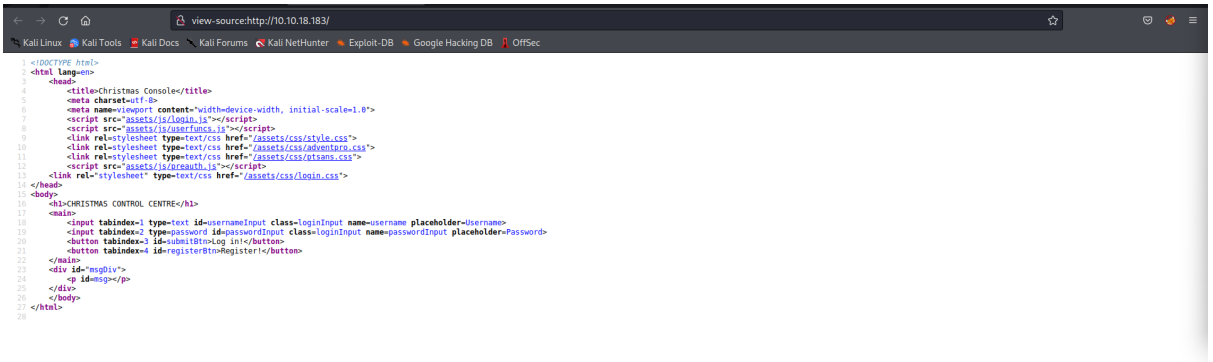
ID	Name	Role
1211102409	CHUA KAI ZHENG	Leader
1211102696	LEE JIA MENG	Member
1211100917	NATALIE TAN LI YI	Member

Day 1:Web Exploitation - A Christmas Crisis

Tools used: Kali Linux, Firefox

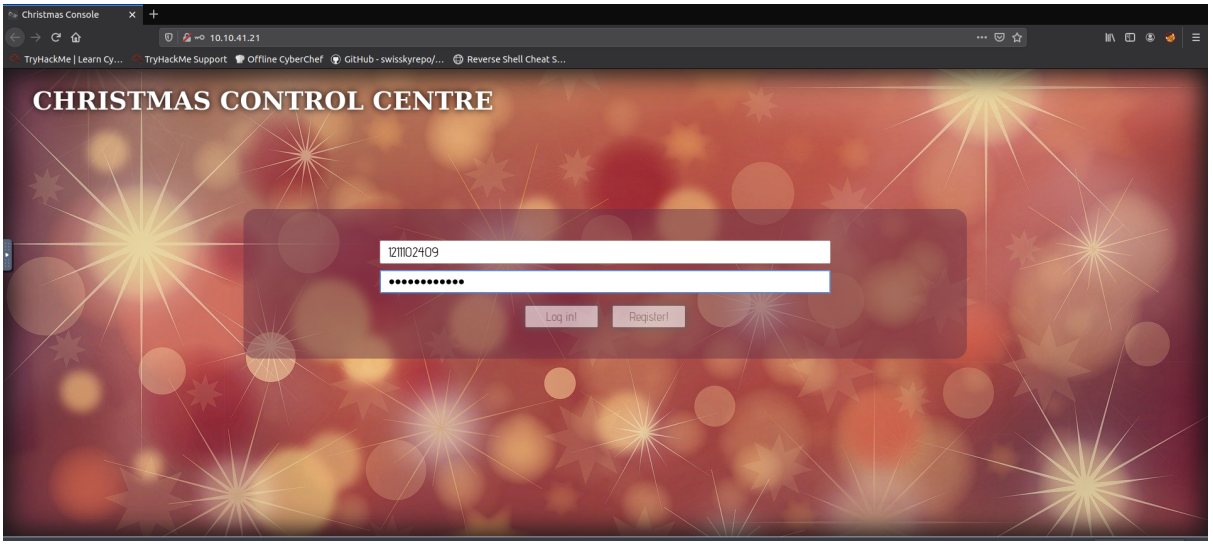
Question 1

Right-click and select “View Page Source”.The HTML code will show

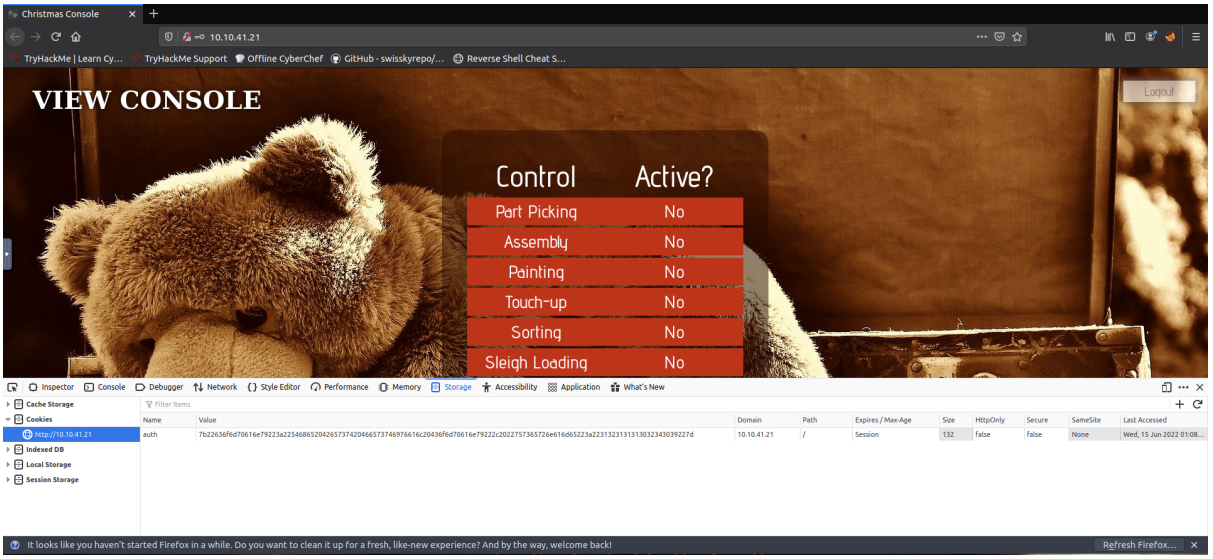


Question 2

Register to an account, then log in to the view console page.



Open the Browser Developer Tools and navigate to the storage to check on the cookies



Question 3

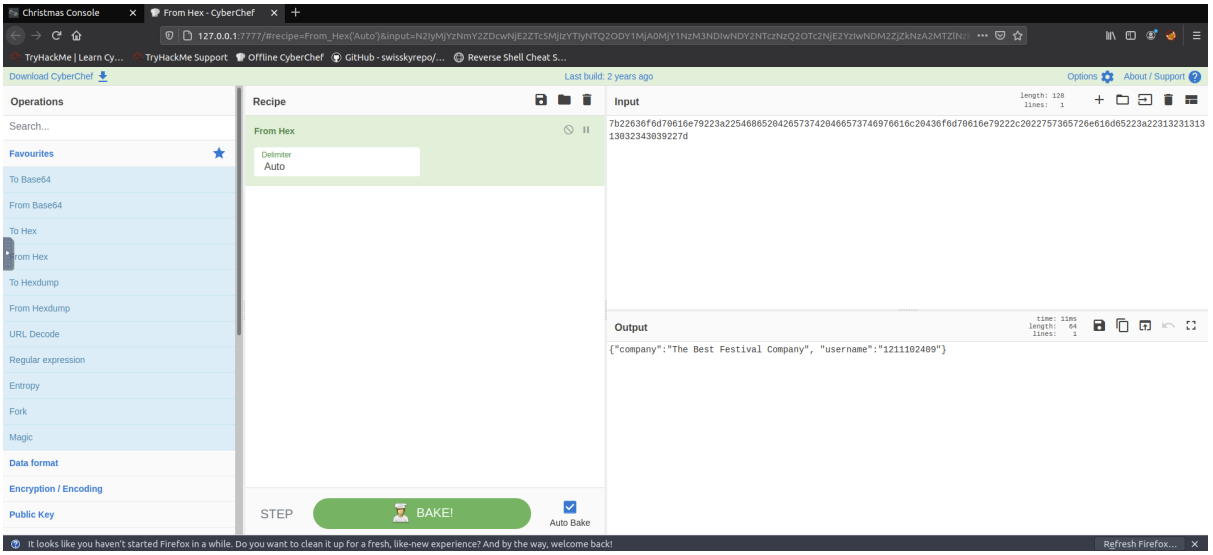
Discover the Value beside the Name

Value

```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a22313231313130323430392 27d
```

Question 4

Used CyberChef to decode the value



Question 5

Determine the value for the company field

```
{"company":"The Best Festival Company",
```

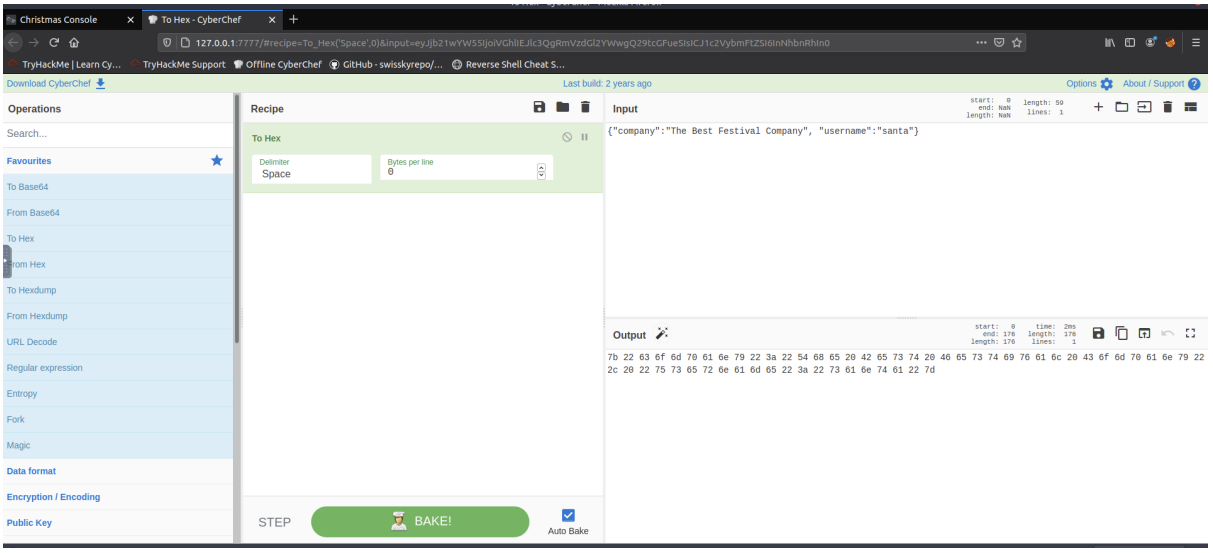
Question 6

Determine the other field found

```
"username":"1211102409"}
```

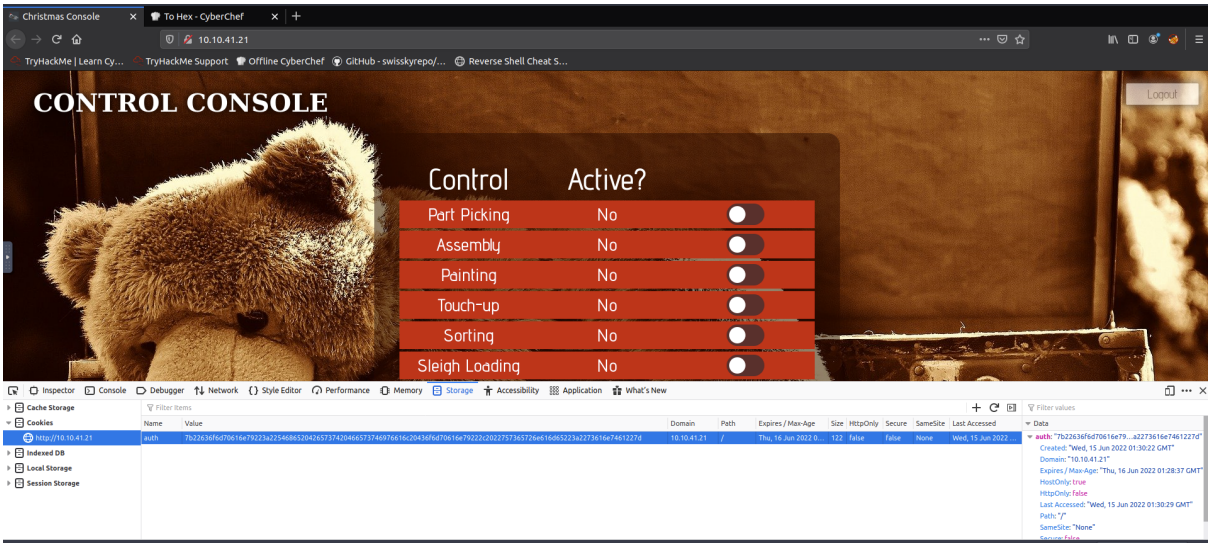
Question 7

Change the username to Santa, then convert it to Hex with CyberChef

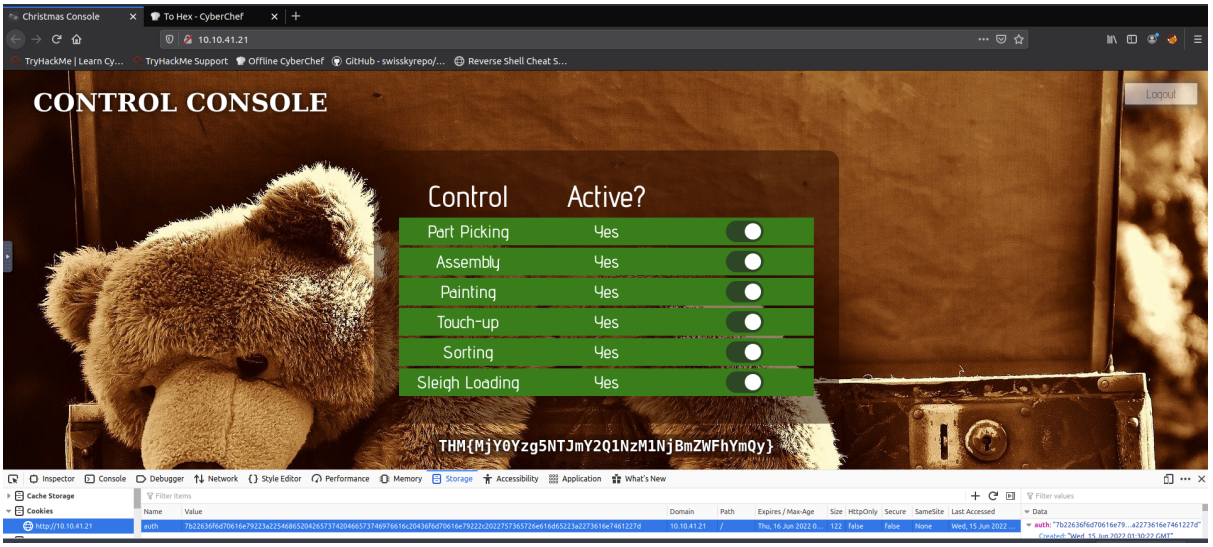


Question 8

Add new cookie with the new Hex value then refresh the page



Reactive all assembly line



Thought Process/Methodology

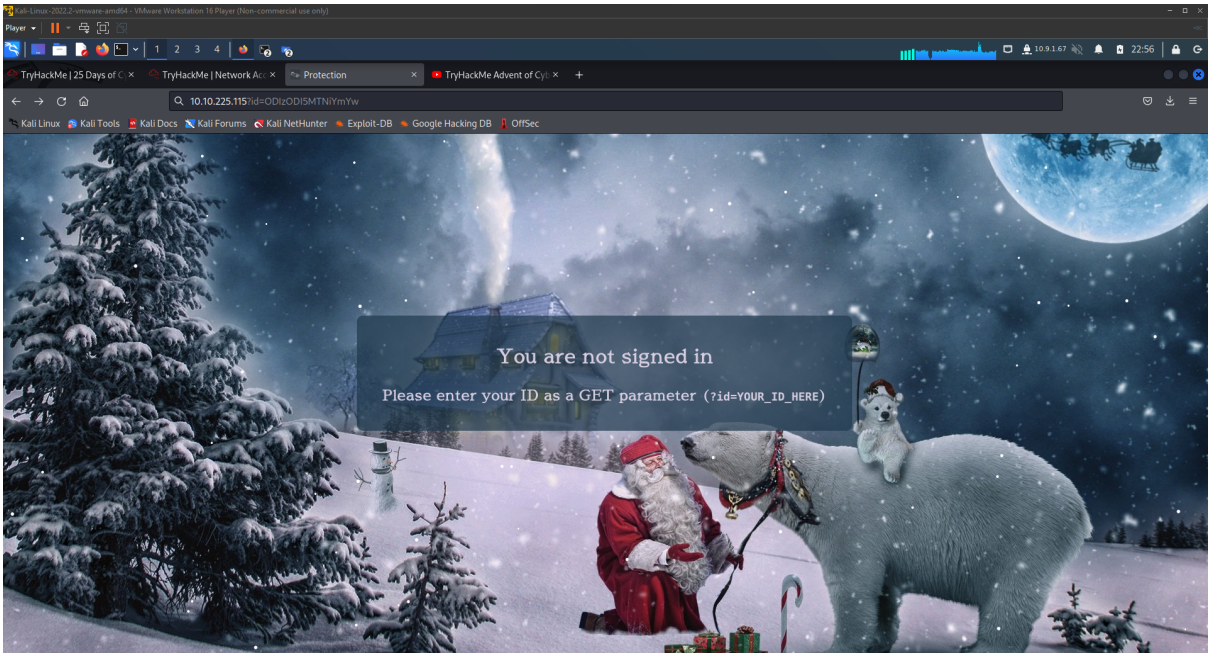
After gaining access to the target computer, a login/registration page called "Christmas Control Center" is shown. Then, we register an account and log in to the view console page. We press F12 to open the Browser Developer Tools and check the cookie at the storage tab. Looking at the cookie value shown, we deduced it as a hexadecimal cookie and convert it to string with the CyberChef Website. The string that show out was JSON statement with a username element. Next, we change the username to 'Santa' and convert it back to the hexadecimal value with CyberChef.After getting the value, we back to the machine tab to replace the value with the new one. We refresh the page and now we have shown with the administrator page and allowed to reactive all assembly lines, which in turn showed the flag.

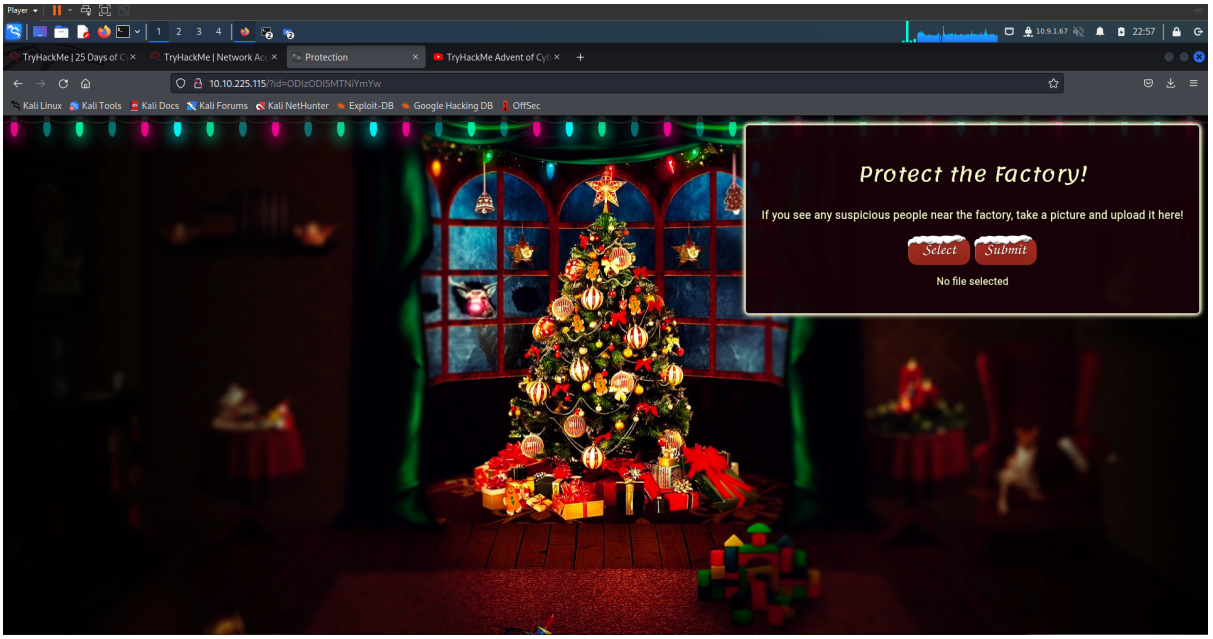
Day 2:Web Exploitation -The Elf Strikes Back!

Tools used: Kali Linux, Firefox, Terminal

Question 1

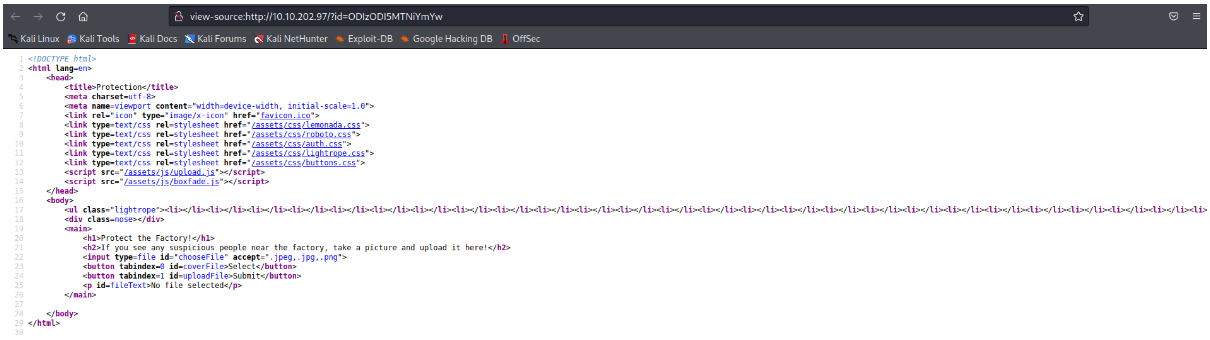
Insert ?id=ODIzODI5MTNiYmYw behind the IP address to enter the website





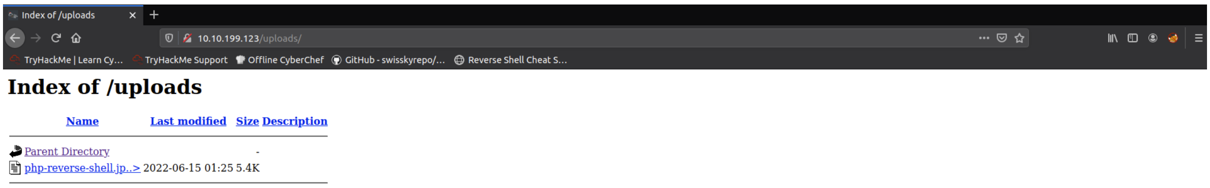
Question 2

Check at the source code to look at the type of file accepted



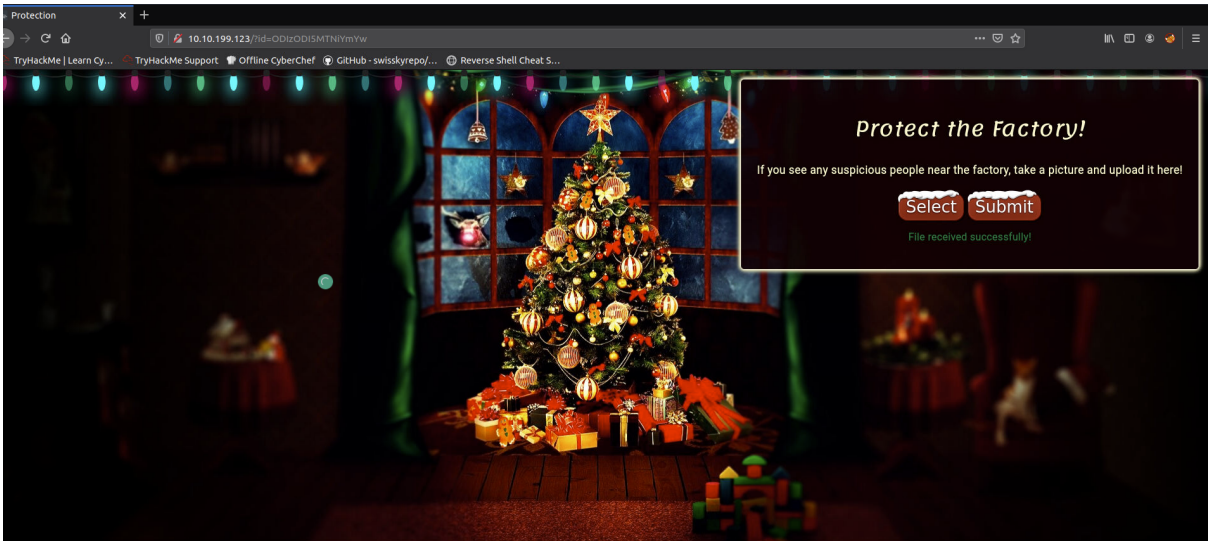
Question 3

Try /uploads, /images, /media, or /resources to get the directory and works on uploads

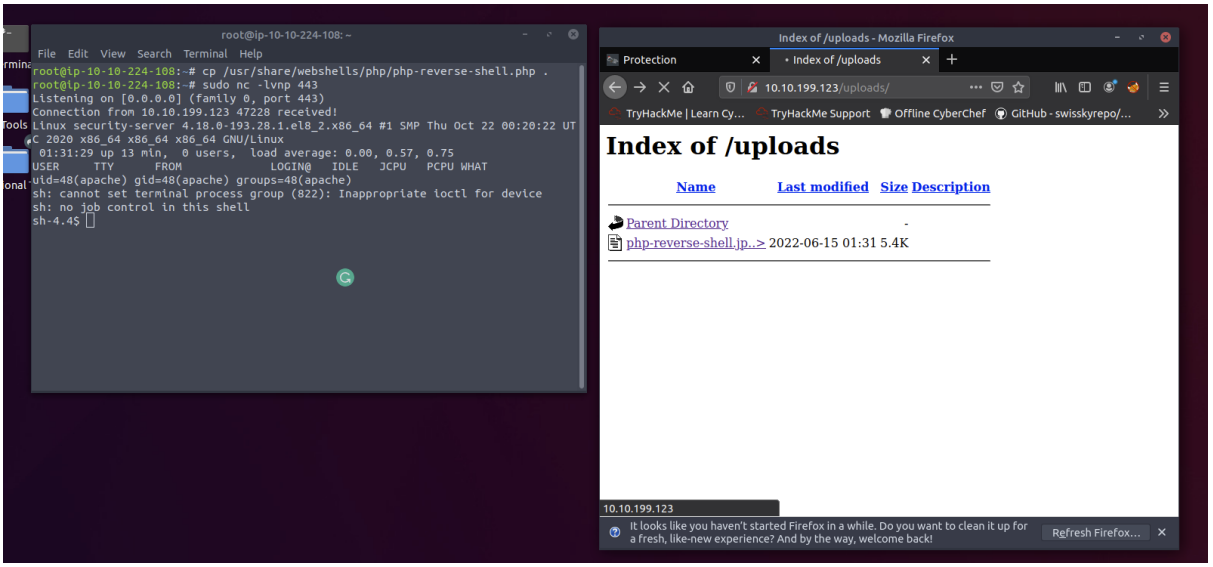


Question 4 (Tryhackme)

Bypass the filter with .jpeg.php and upload the reverse shell

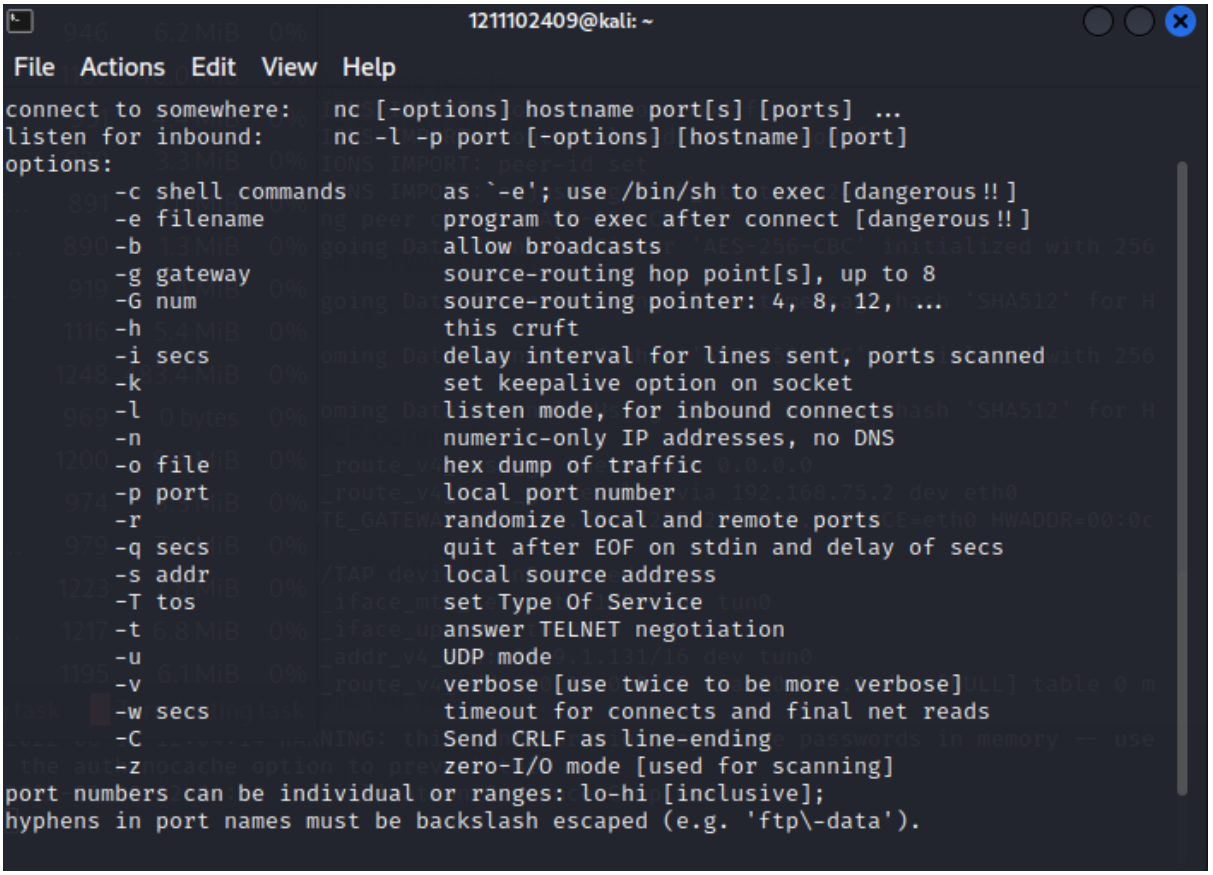


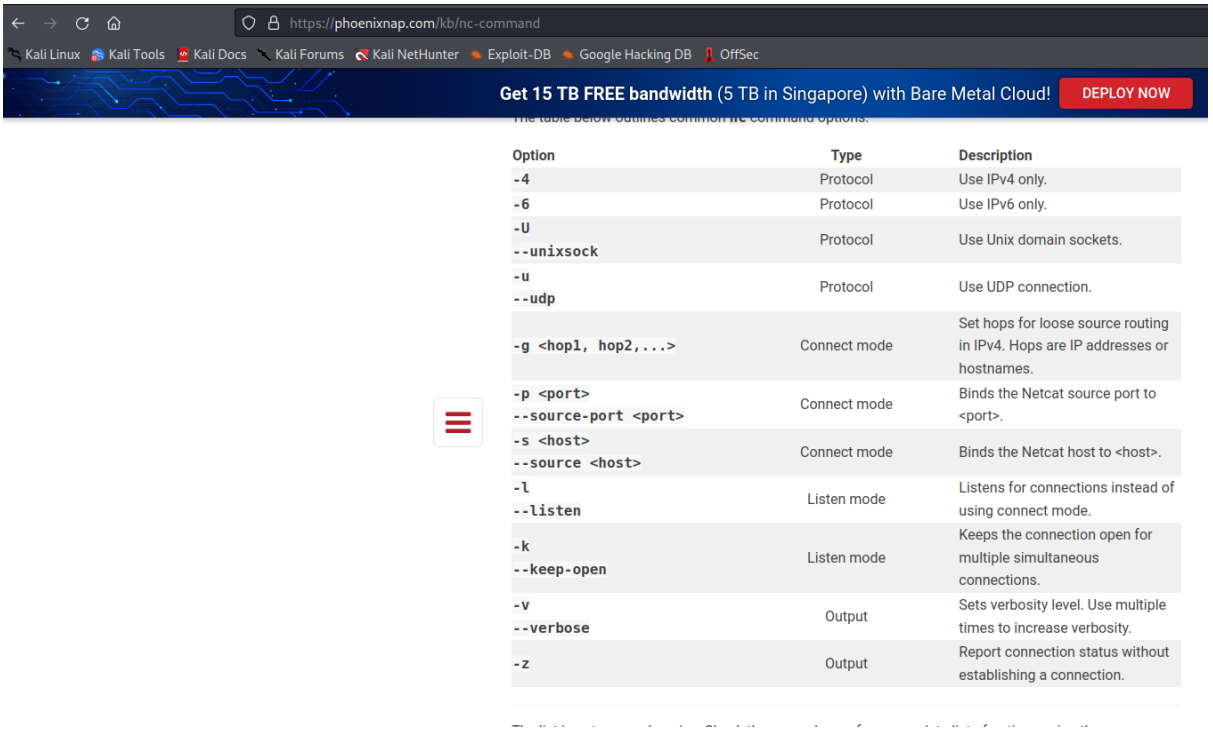
Start a Netcat listener and go to upload page, click the file,then the netcat listener will catch the shell



Question 4 (Google form)

Find the netcat's parameter explanations with -help and google

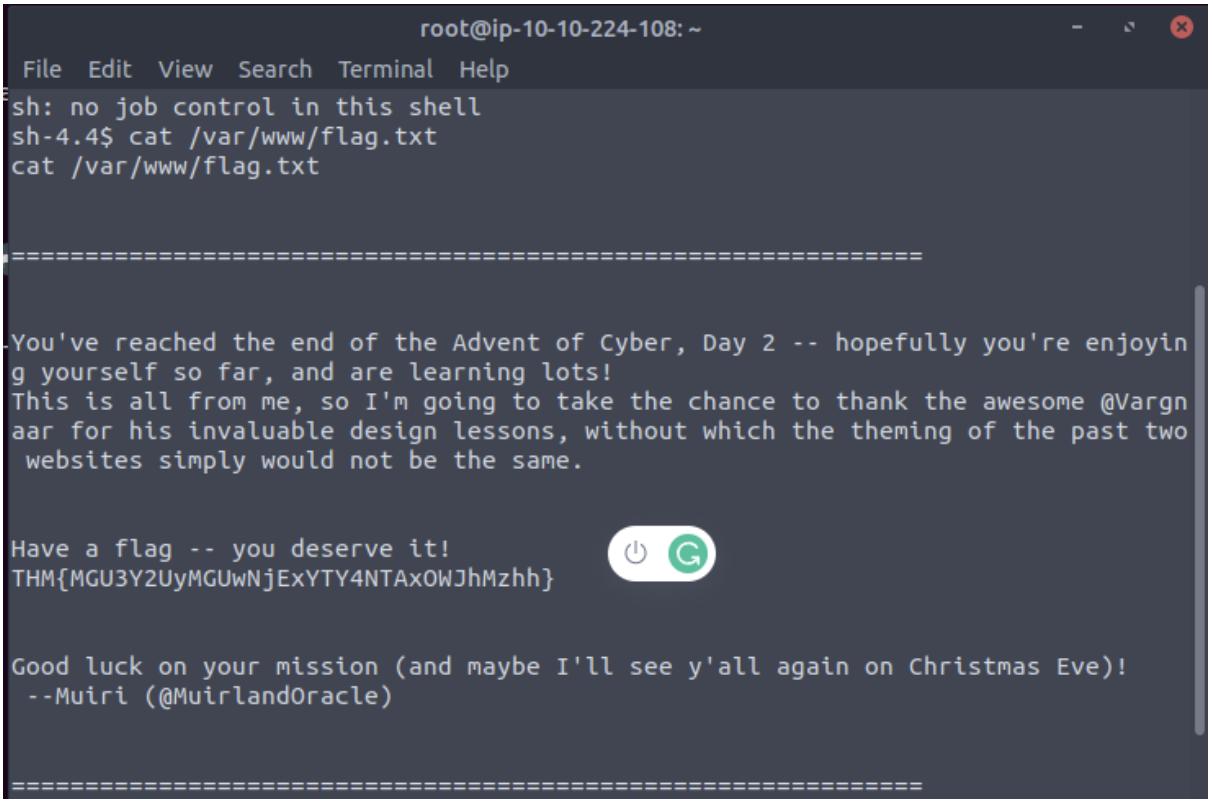




Option	Type	Description
`-4`	Protocol	Use IPv4 only.
`-6`	Protocol	Use IPv6 only.
`-U` `--unixsock`	Protocol	Use Unix domain sockets.
`-u` `--udp`	Protocol	Use UDP connection.
`-g <hop1, hop2,...>`	Connect mode	Set hops for loose source routing in IPv4. Hops are IP addresses or hostnames.
`-p <port>` `--source-port <port>`	Connect mode	Binds the Netcat source port to <port>.
`-s <host>` `--source <host>`	Connect mode	Binds the Netcat host to <host>.
`-l` `--listen`	Listen mode	Listens for connections instead of using connect mode.
`-k` `--keep-open`	Listen mode	Keeps the connection open for multiple simultaneous connections.
`-v` `--verbose`	Output	Sets verbosity level. Use multiple times to increase verbosity.
`-z`	Output	Report connection status without establishing a connection.

Question 5

Cat /var/www/flag.txt with terminal



Thought Process/Methodology

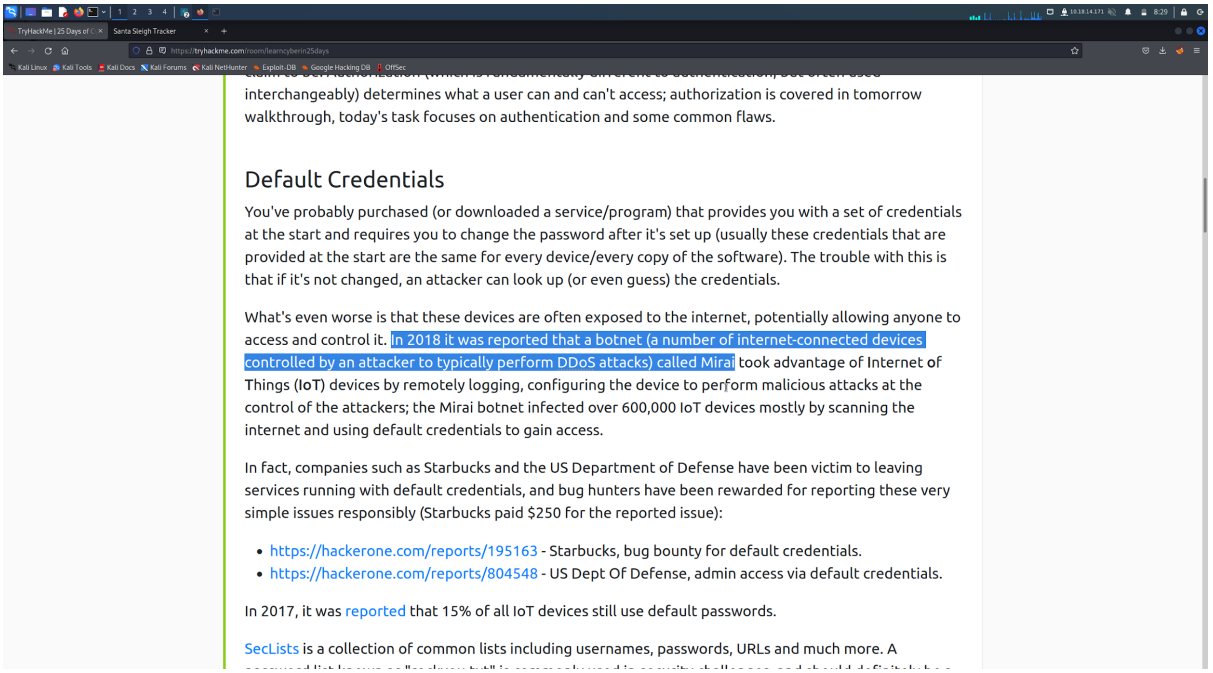
Before starting the machine we copy the PHP reverse shell script into the current directory and change the $ip and $port.After that we continue with entering the machine IP address, A page with “You are not assigned” is shown. We add the GET parameter(?id=ODIzODI5MTNiYmYw) given behind the IP address and page with the select and submit button shown. Then, we right-click the mouse and select view page source to check the source code.We realised the page accept image(.jpeg .jpg .png) upload to the webserver.Next, we try to bypass the reverse shell by changing it to a double-barrelled extension(.jpg.PHP) and upload the file by clicking on the submit button. After that, we start the Netcat listener and let it catch the shell by clicking the reverse shell uploaded at the upload page. In the end, we type the command cat /var/www/flag.txt and the flag appears.

Day 3:Web Exploitation Christmas Chaos

Tools used: Kali Linux, Firefox, Terminal, Burp Suite

Question 1

Read through the Default Credentials.



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):

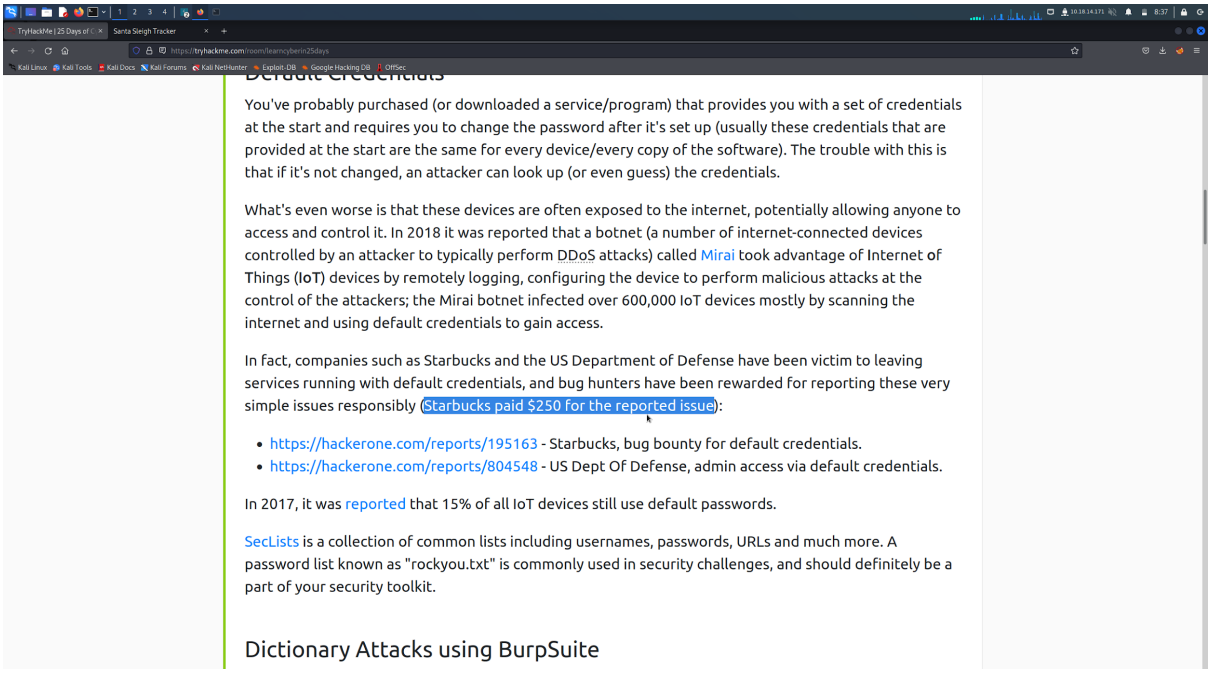
- https://hackerone.com/reports/195163 - Starbucks, bug bounty for default credentials.
- https://hackerone.com/reports/804548 - US Dept Of Defense, admin access via default credentials.

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

Question 2

Continuing to read through the text under 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

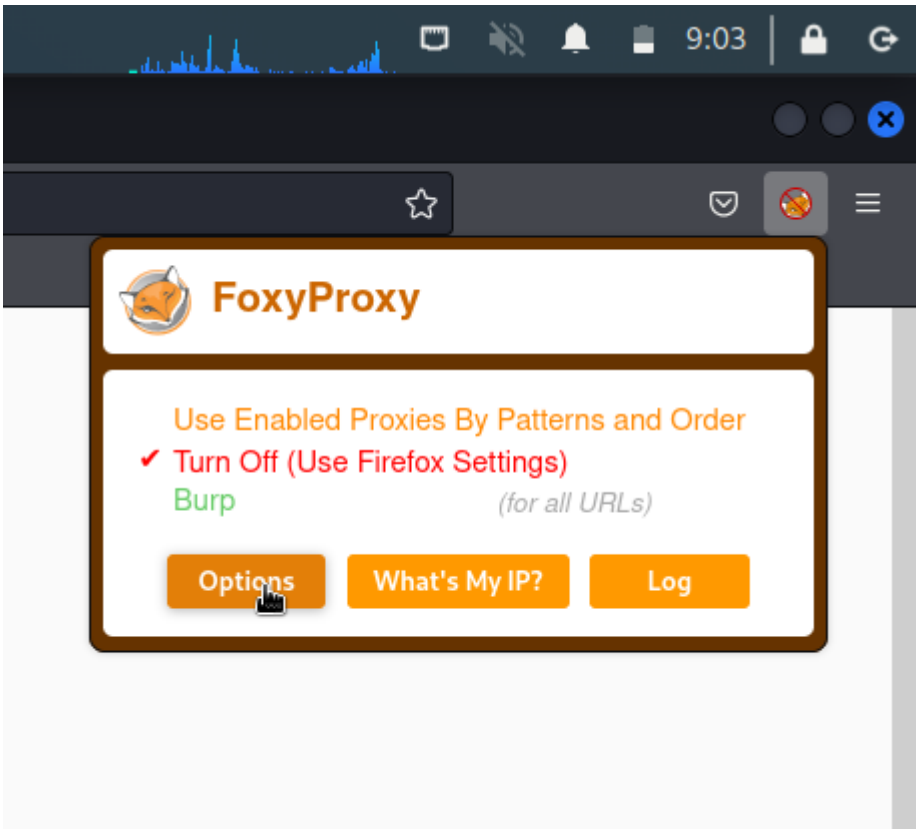
Question 3

Click onto the link provided in the text under Default Credentials. Then, read through and search for the agent.

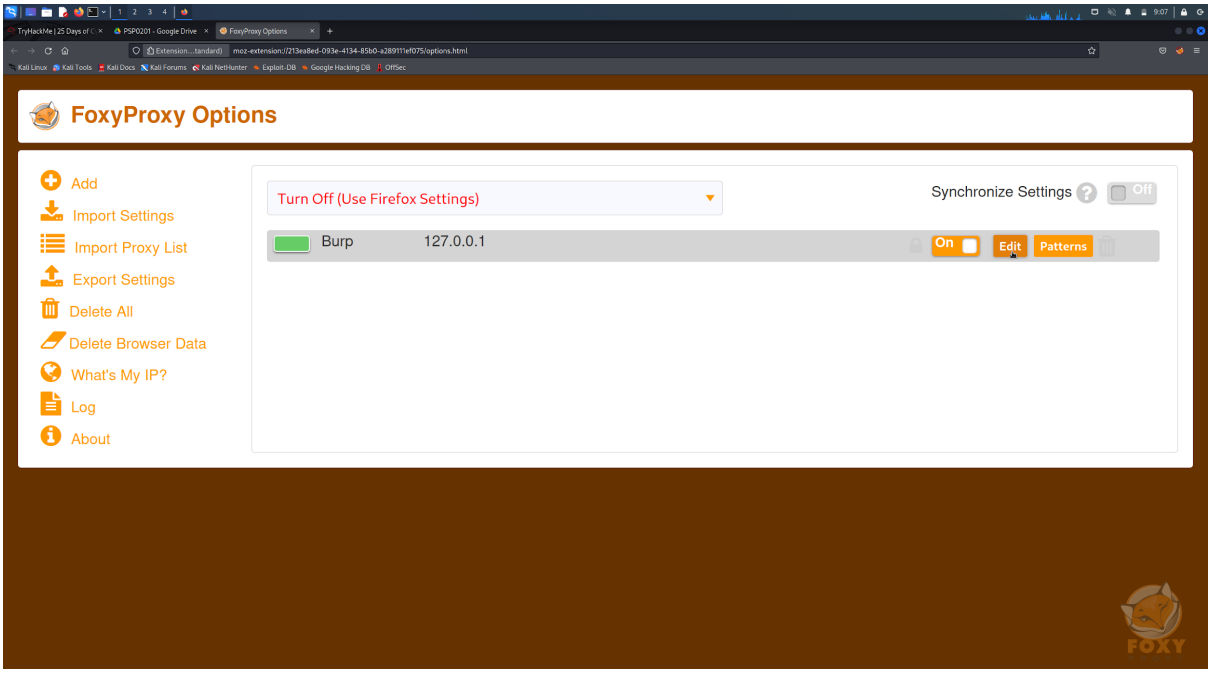
ag3nt-j1 U.S. Dept Of Defense staff agreed to disclose this report. Jun 25th (2 years ago)

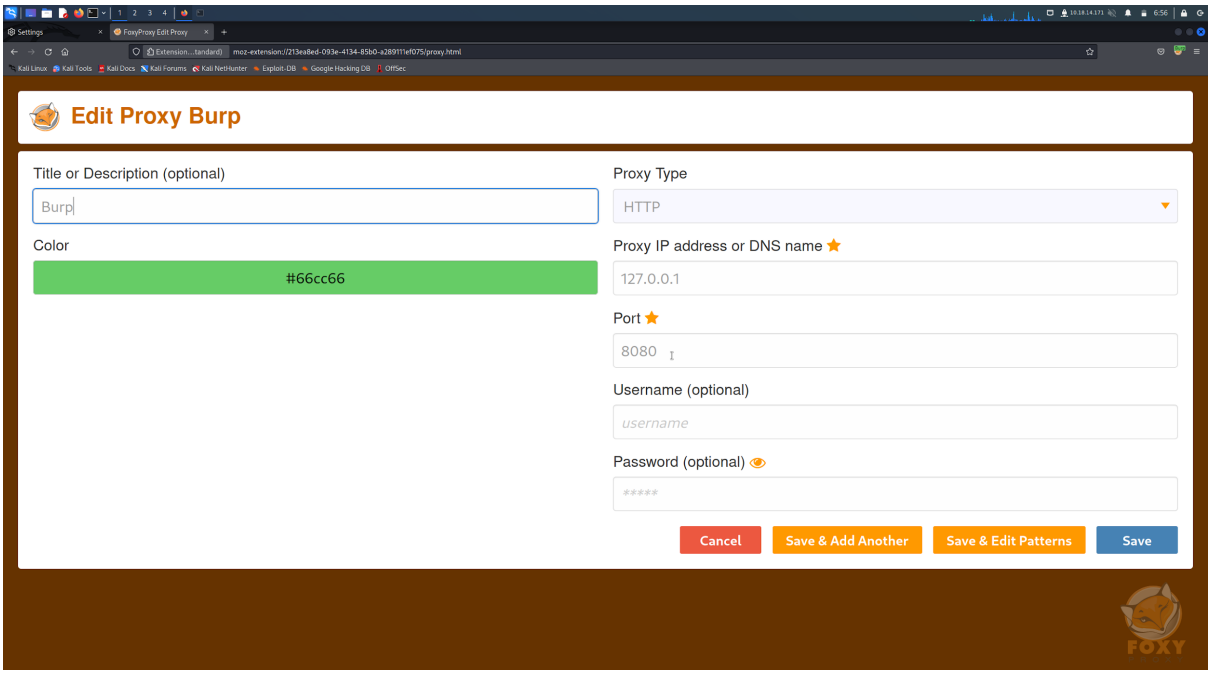
Question 4 & Question 5

Click on the FoxyProxy extension in Firefox. Then, click “option”.



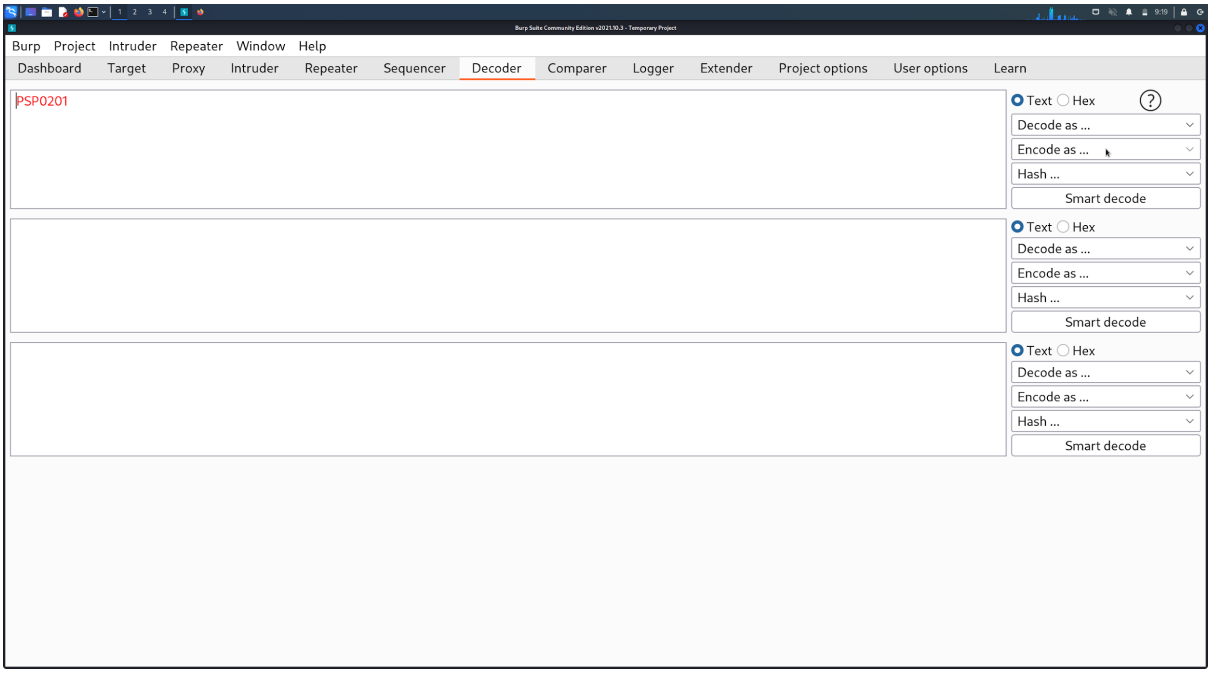
Then, click on the “Edit” button.



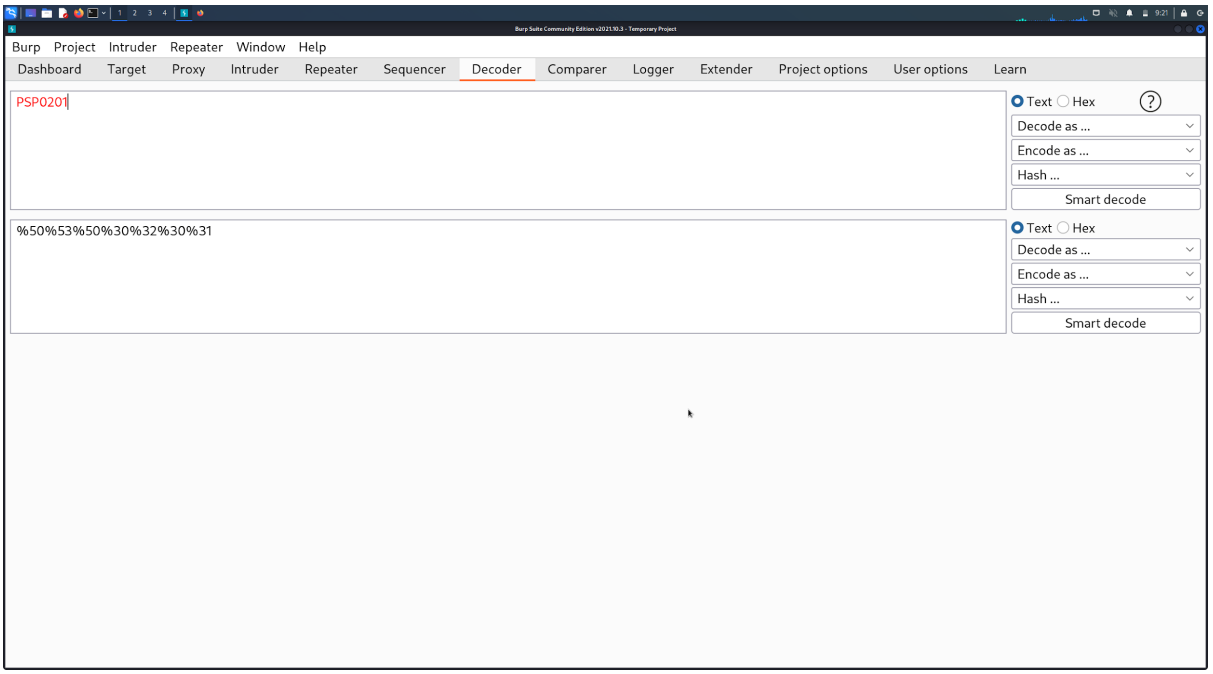


Question 6

Open BurpSuite, Click the “Decoder” tab. Then, type in “PSP0201”.



Then, press “Encode as URL”



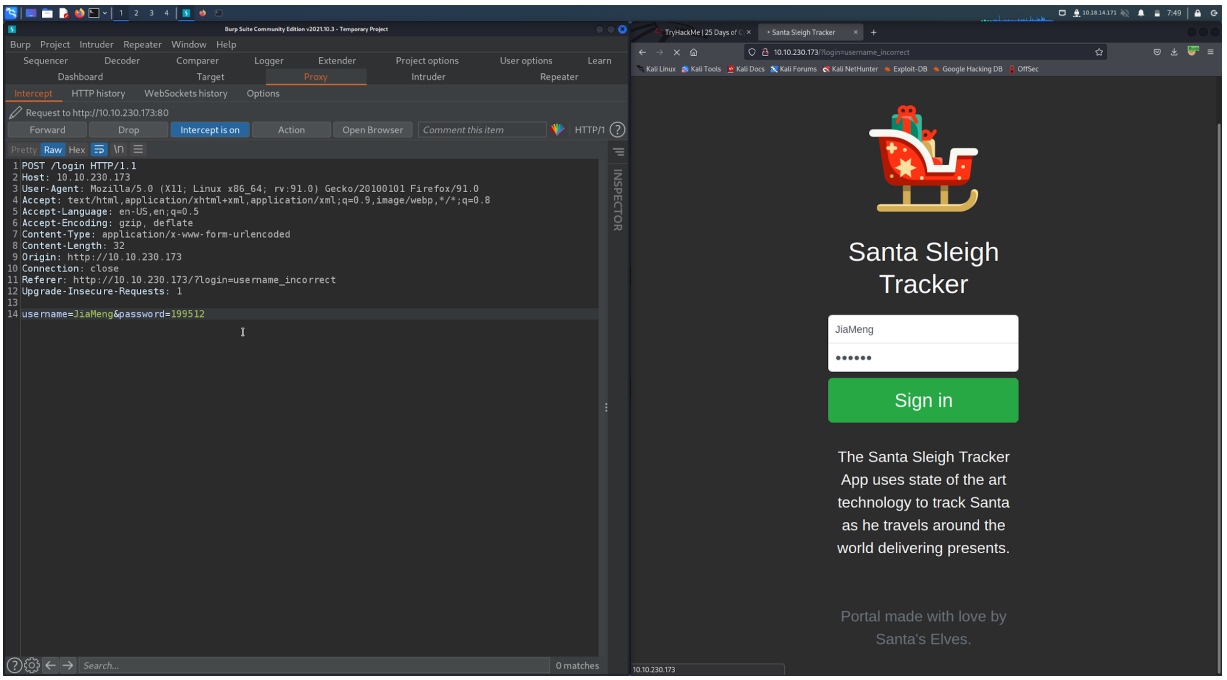
Question 7

Attack type that matches the description is **Cluster Bomb.**

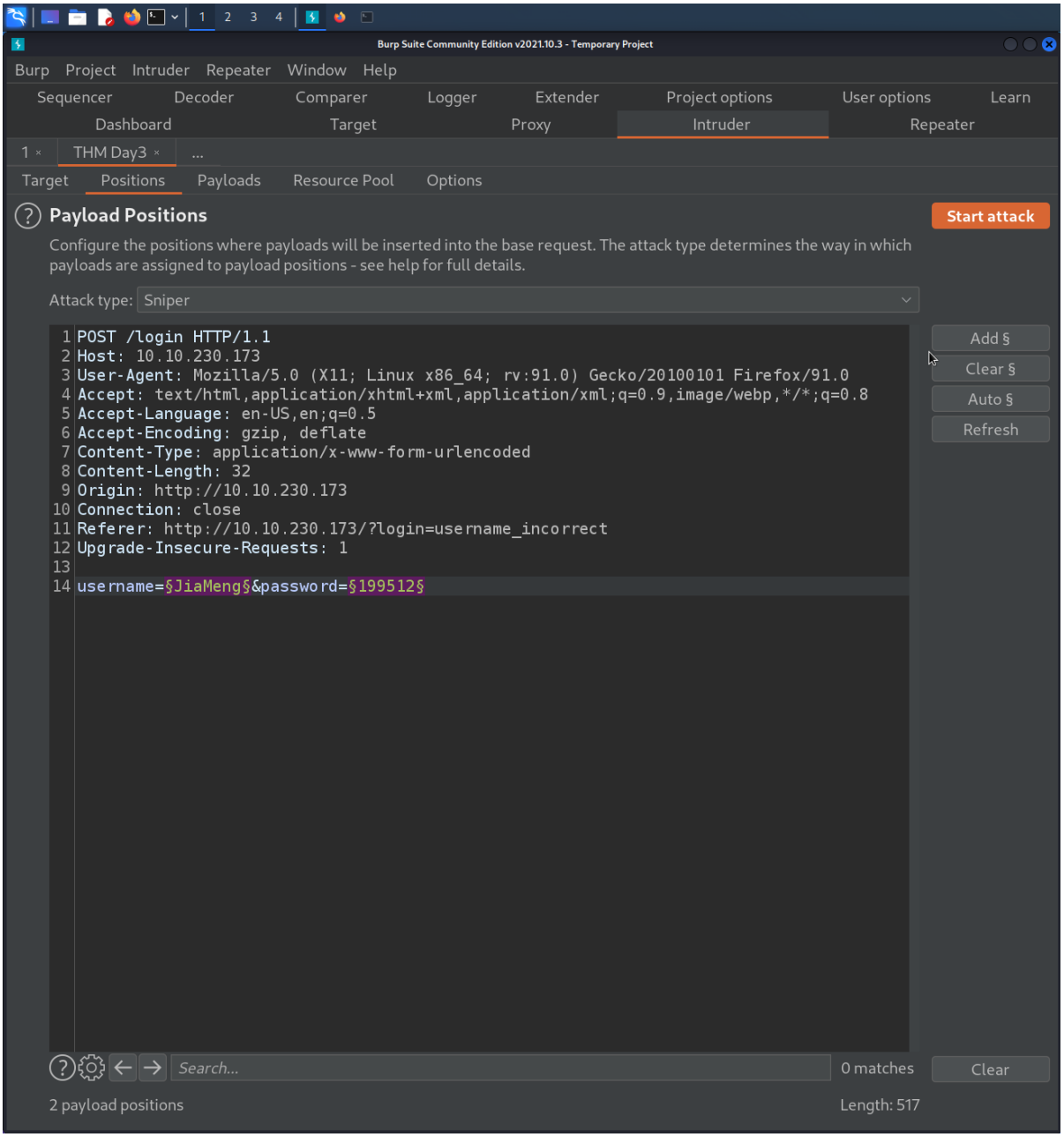
Select "Cluster Bomb" in the Attack type dropdown menu; this attack type iterates through each payloads sets in turn, so every combination of each set is tested.

Question 8

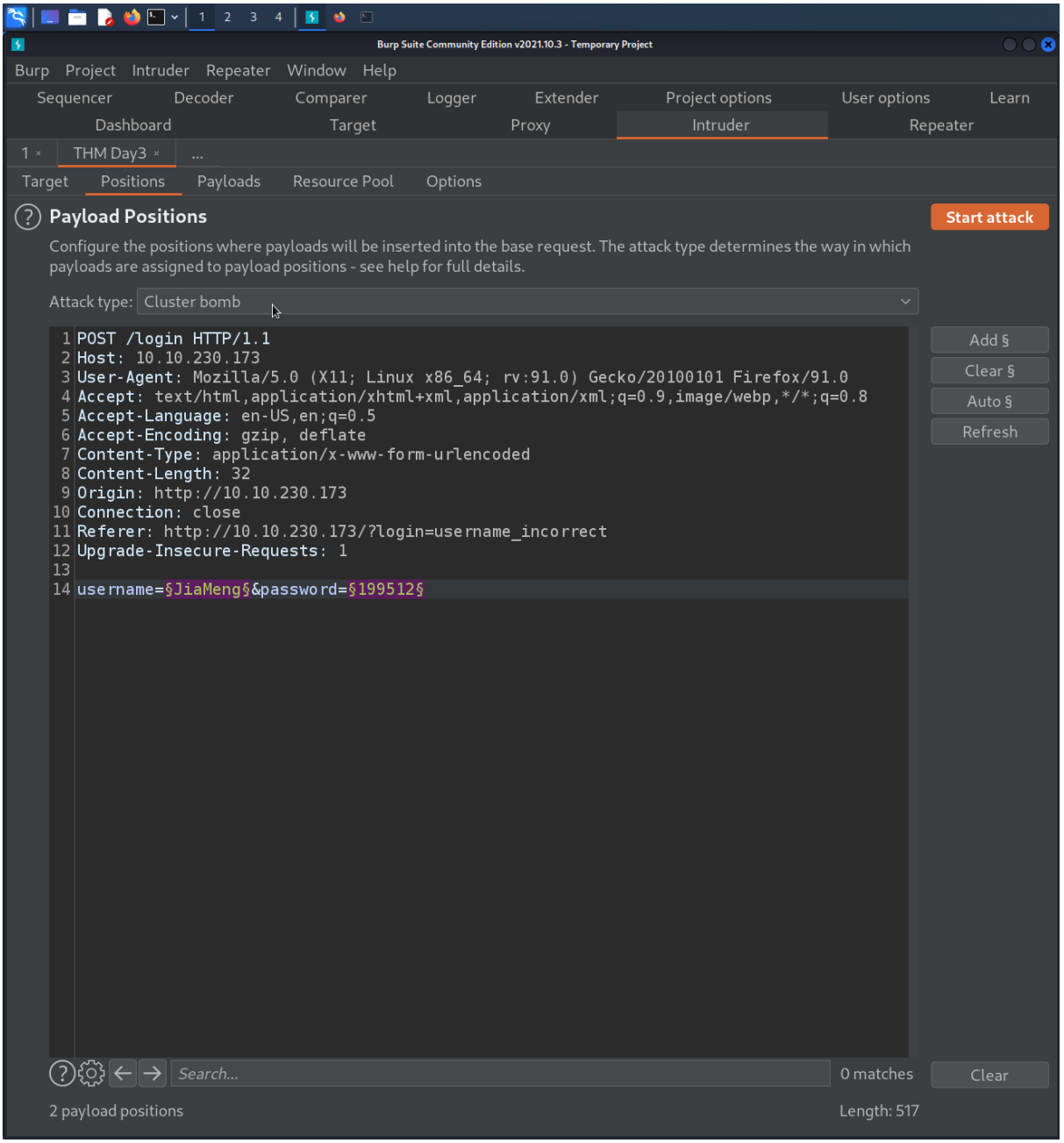
Access the website by entering the IP address. Submit the **username** and **password.** In BurpSuite, captured request will show up in intercept.



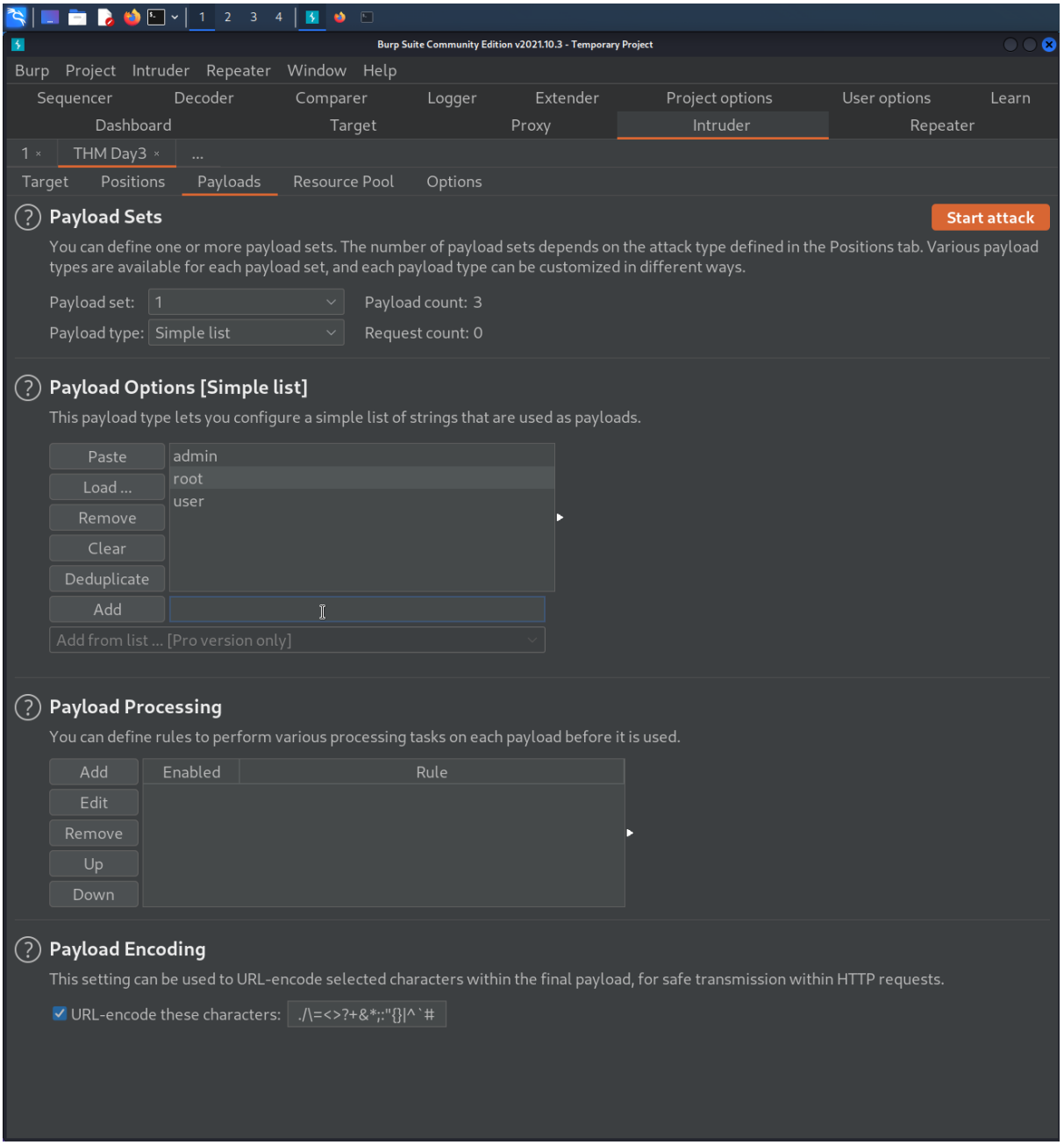
Click “Add” on the highlighted **username** and **password**.

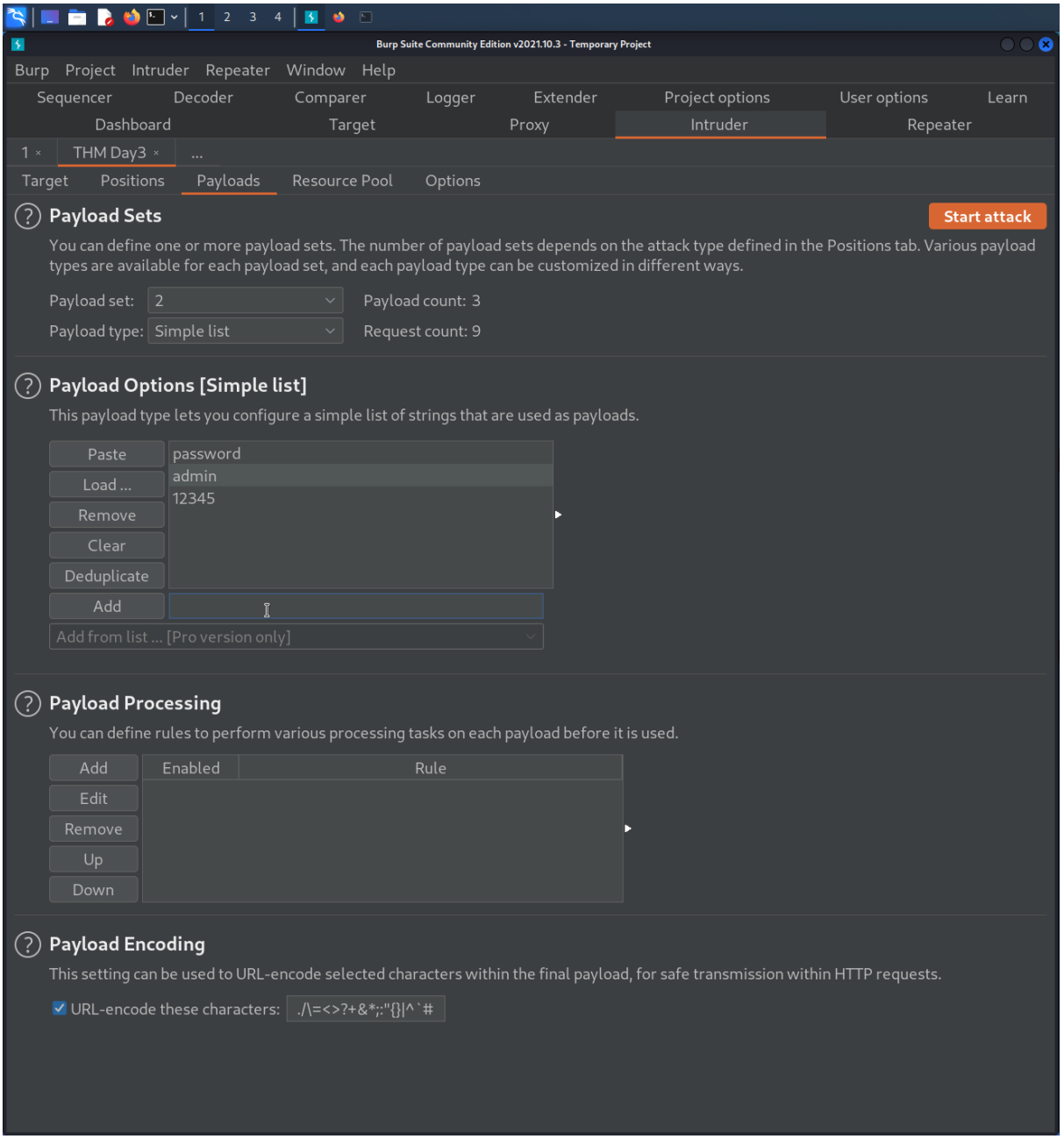

Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
1 THM Day3 ...
Target Positions Payloads Resource Pool Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
1 POST /login HTTP/1.1
2 Host: 10.10.230.173
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 32
9 Origin: http://10.10.230.173
10 Connection: close
11 Referer: http://10.10.230.173/?login=username_incorrect
12 Upgrade-Insecure-Requests: 1
13
14 username=§JiaMeng§&password=§199512§
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear
2 payload positions
Length: 517

Change the attack type to “Cluster Bomb”.

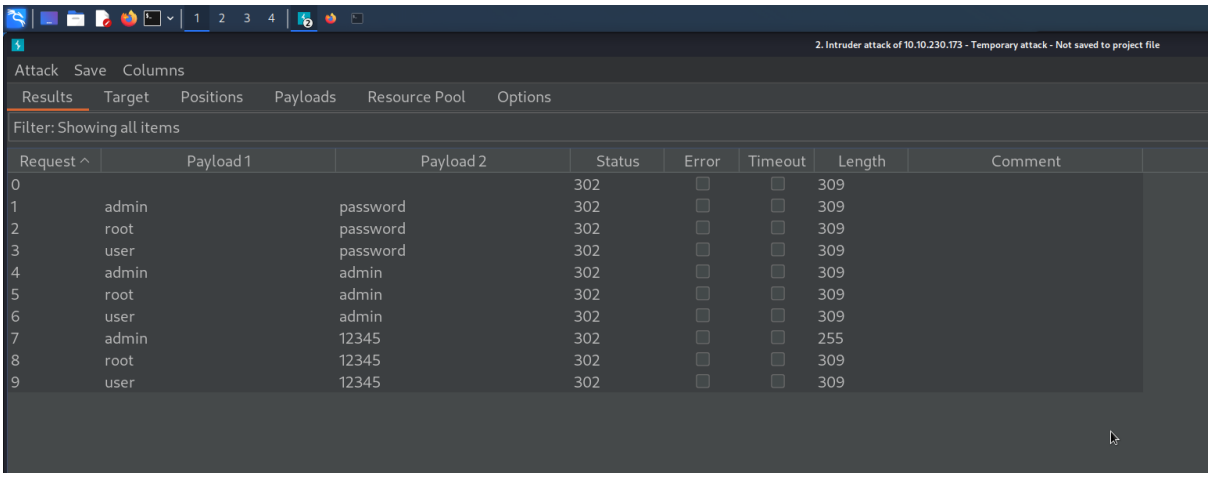


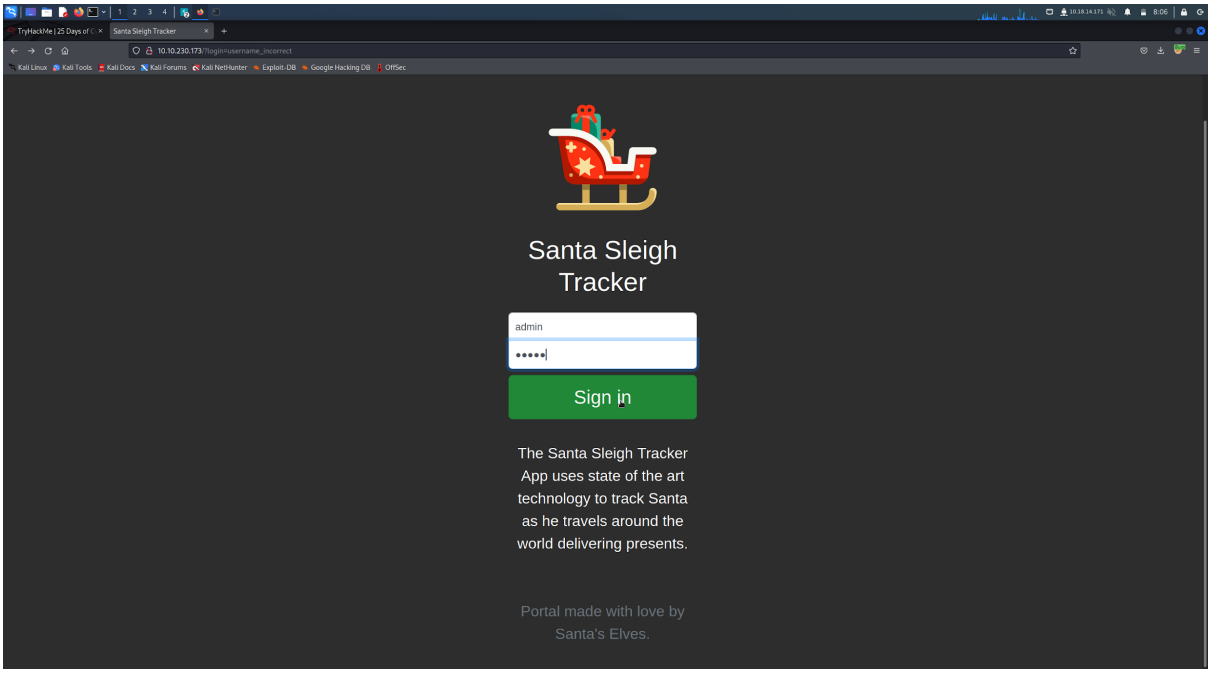
In set 1, add “admin”, “root” and “user” under the payloads of the **Intruder** tab. Repeat the same process for set 2, by adding “password’, “admin” and “12345”.

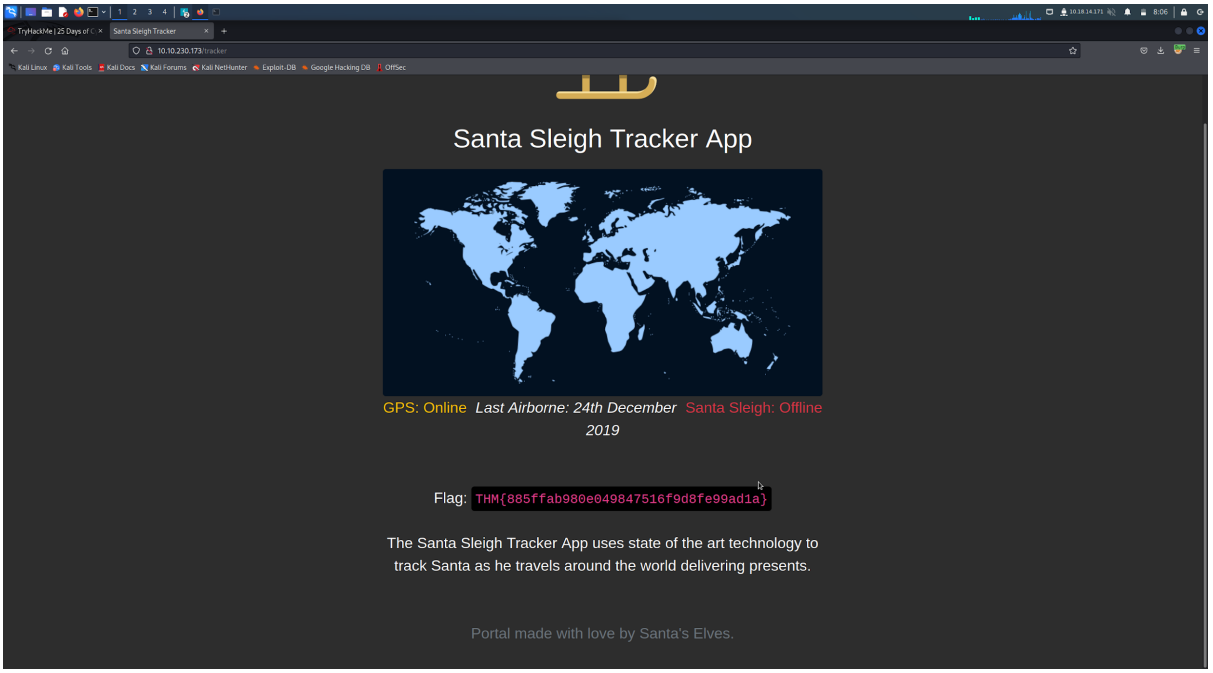



Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
1 THM Day3 ...
Target Positions Payloads Resource Pool Options
Payload Sets
Start 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
Add
password
admin
12345
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters: ./\=<>?+&*;:"{}|^`#

Start the attack. The odd out one will be the correct username and password to sign into the website.







Thought Process/Methodology

Having access to the target machine, a sign in page was presented. Then, we proceeded to sign in with our own username and password. We would not be able to successfully access and obtain the flag. Thus, we need to head to BurpSuite to send the captured request to the intruder and repeater. We can see the request being sent to the ***Intruder*** tab. We then need to clear the pre-selected values under the ***positions*** tab and add both the username and password values as positions. We then need to select "**Cluster Bomb**" as our attack type. Next up, we need to add in a few common default usernames such as "admin", "root', and "user" in Set 1 in the ***Payload*** tab. Repeat the process but for set 2 and add common default passwords like "password", "admin", and "12345". We can then start the attack which we will be able to catch the odd one out. That pair of username and password will be used to sign in and in return, show the flag.

Day 4:Web Exploitation: Santa's watching

Tools used : Kali Linux, Firefox, Terminal

Question 1

Creating command using URL "http://shibes.xyz/api.php", "breed" parameter and wordlist "big.txt". Following the text from picture given below, the output is :

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

some of the more useful options into the table below:

Options	Description
-c	Shows the output in color
-d	Specify the parameters you want to fuzz with, where the data is encoded for a HTML form
-z	Specifies what will replace FUZZ in the request. For example `-z file,big.txt`. We're telling wfuzz to look for files by replacing "FUZZ" with the words within "big.txt"
--hc	Don't show certain http response codes. I.e. Don't show **404** responses that indicate the file *doesn't* exist, or "**200**" to indicate the file *does* exist
--hl	Don't show for a certain amount of lines in the response
--hh	Don't show for a certain amount of characters

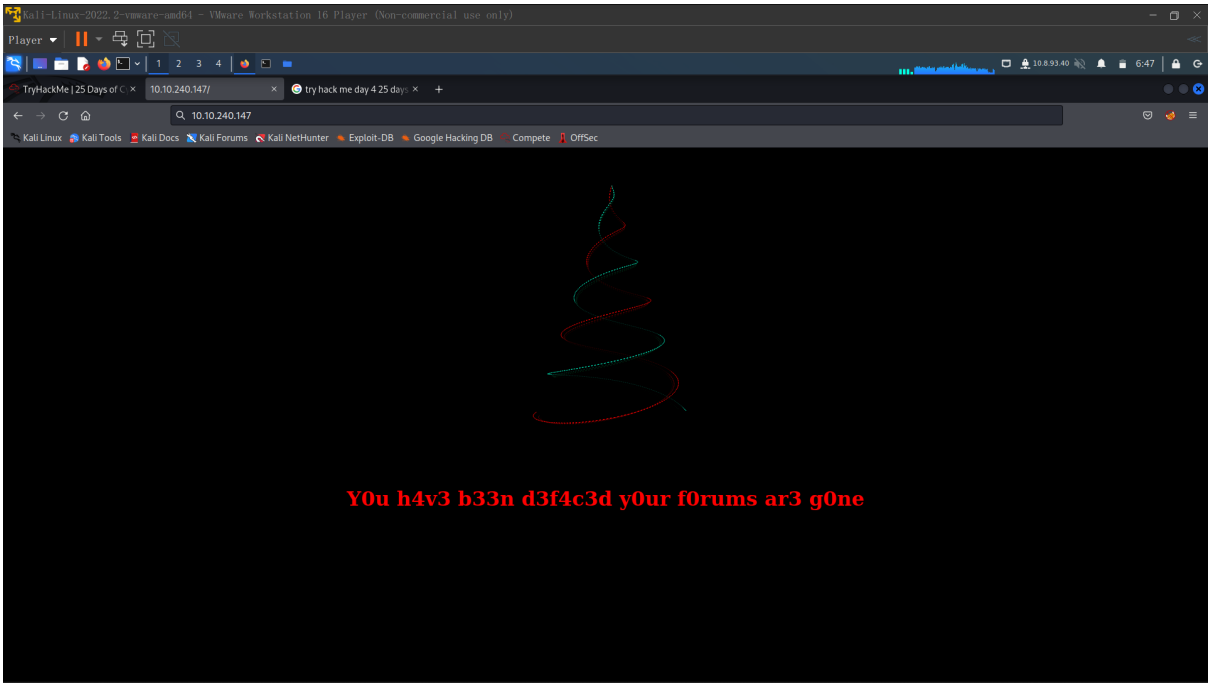
Let's bring this together and demonstrate some of these options. Let's say we wanted to fuzz an application on *http://shibes.thm/login.php* to find the correct credentials to the login form. After recalling our knowledge from Day 2, we know all about URL parameters! We can take a bit of a guess as to what parameters the login form may be using `username` and `password`, right? Worth a try! Our wfuzz command would look like so:

```
wfuzz -c -z file,mywordlist.txt -d "username=FUZZ&password=FUZZ" -u http://shibes.thm/login.php
```

Where wfuzz will now iterate through the wordlist we provided and replace the "FUZZ" values specified in the "username" and "password" parameters.

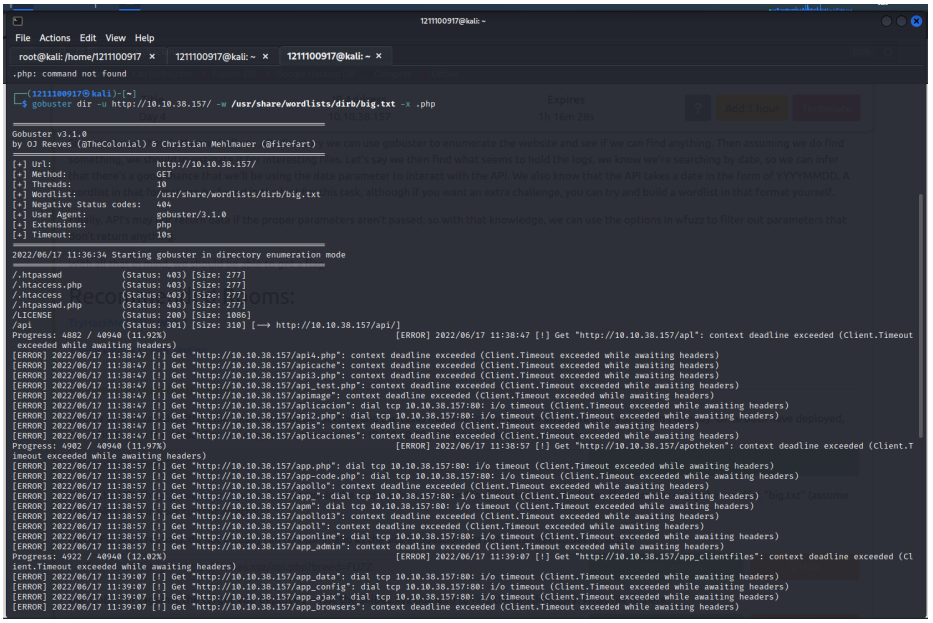
Question 2

Insert IP address to access website



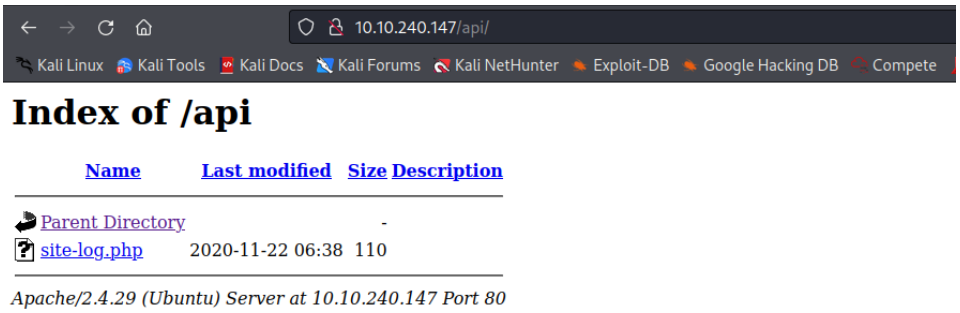
Question 3

Use terminal to find API to access website



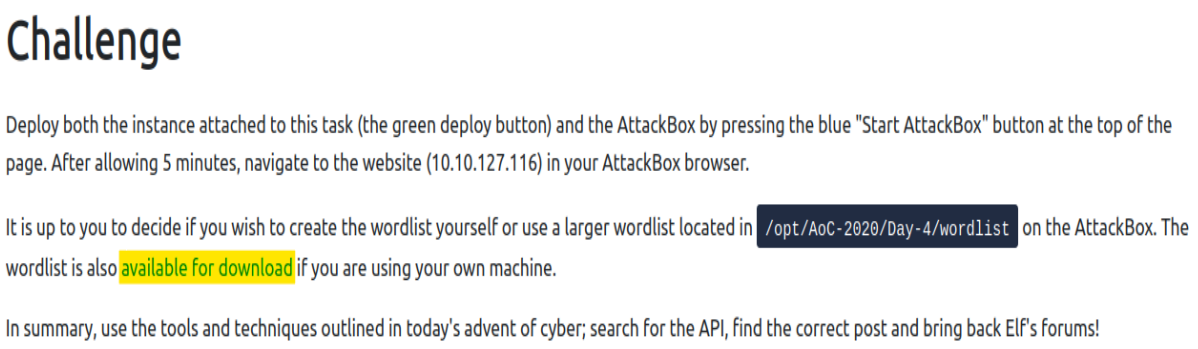
Question 4

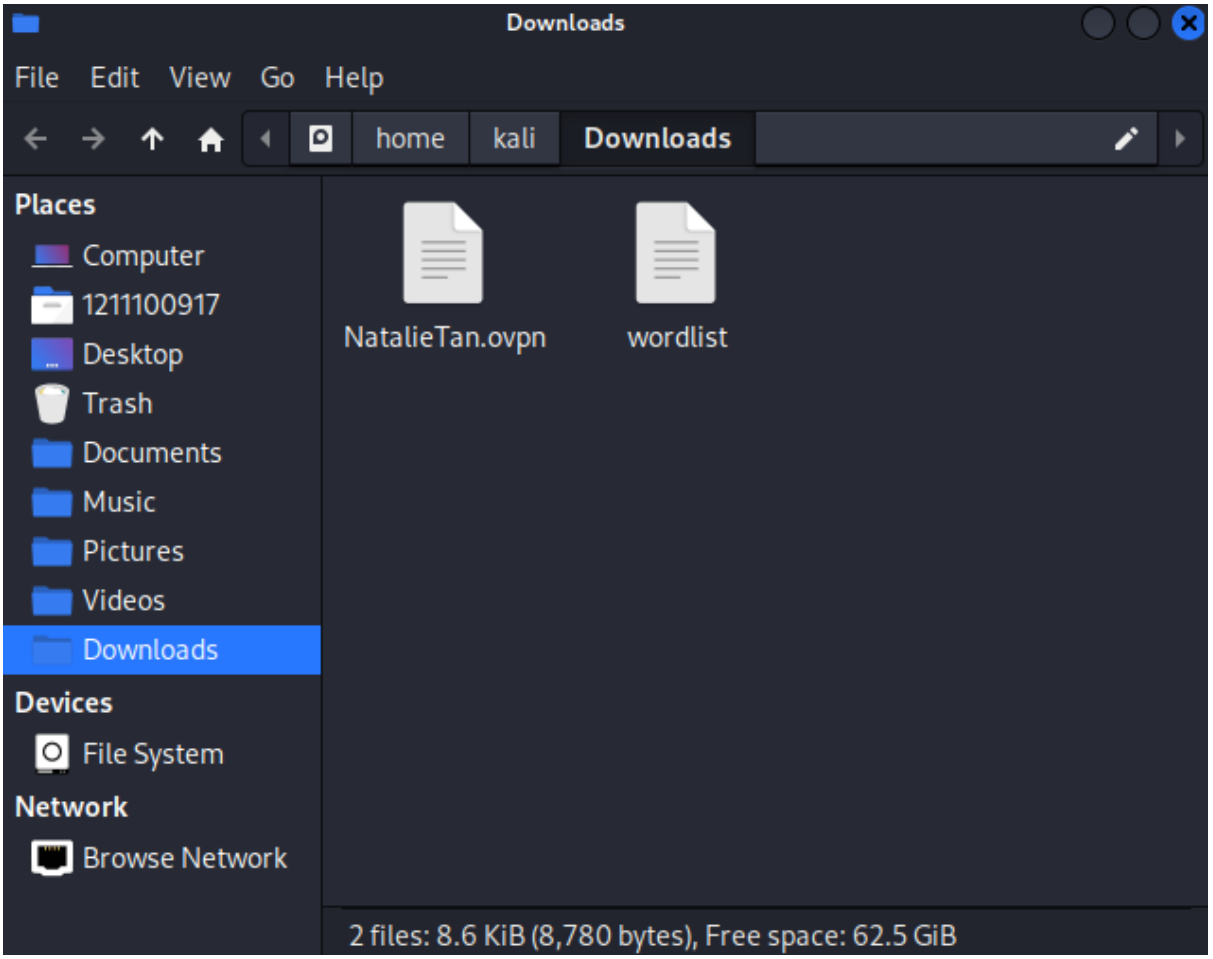
Access website by inserting API address found in the terminal



Question 5

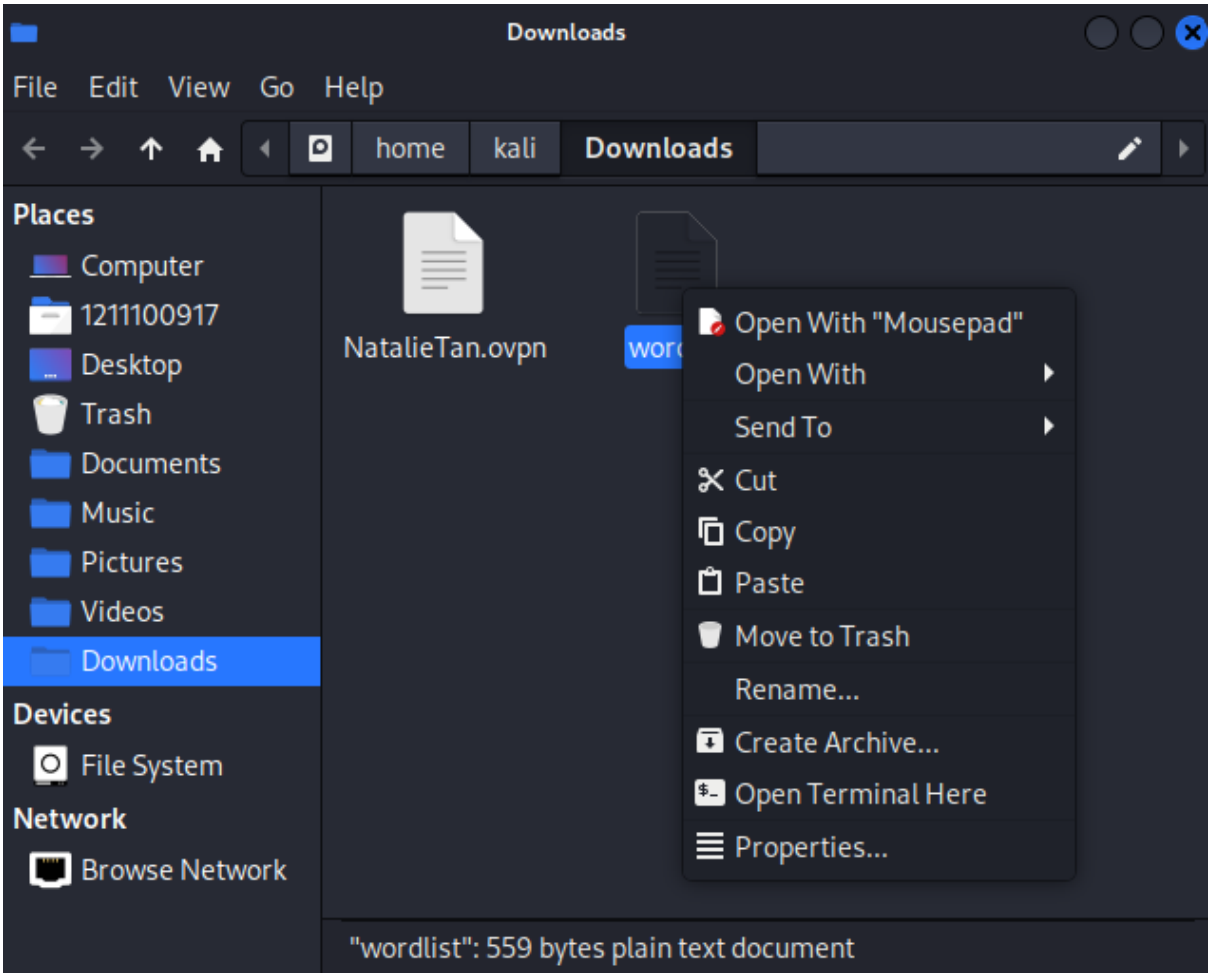
Download wordlist file from THM website





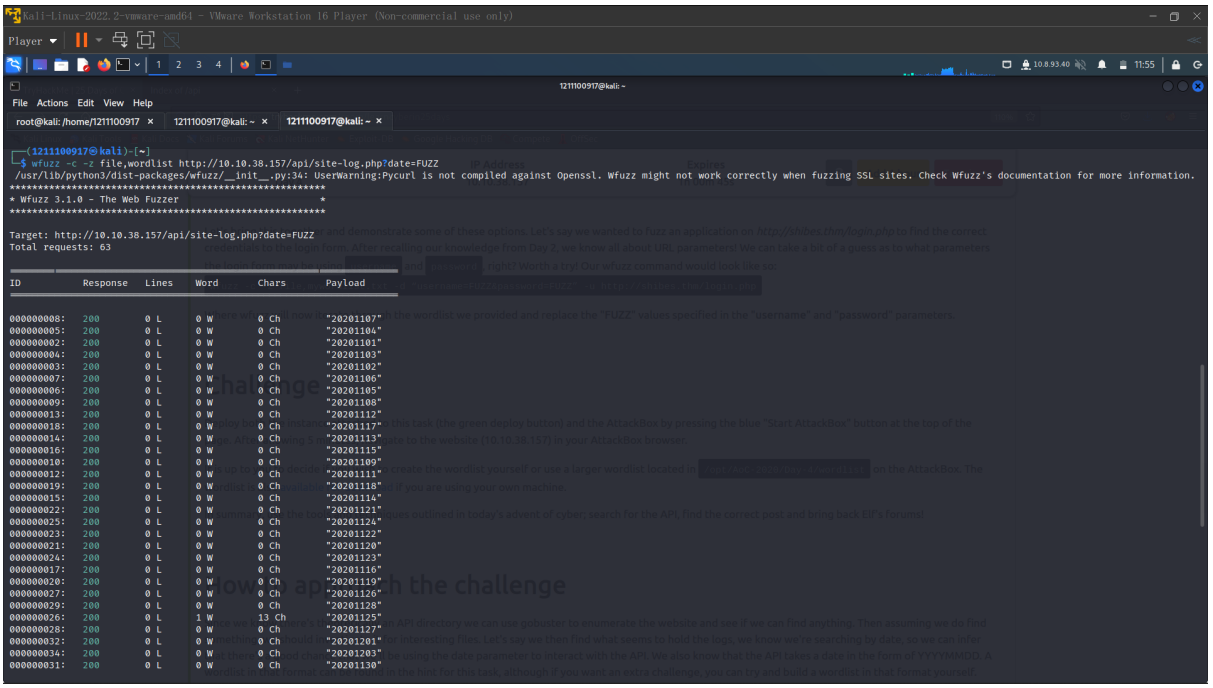
Question 6

Copy path of the file



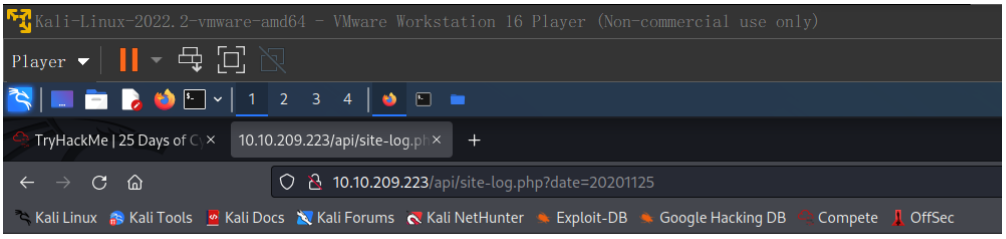
Question_7

Use “wfuzz” to check the dates from wordlist file



Question 8

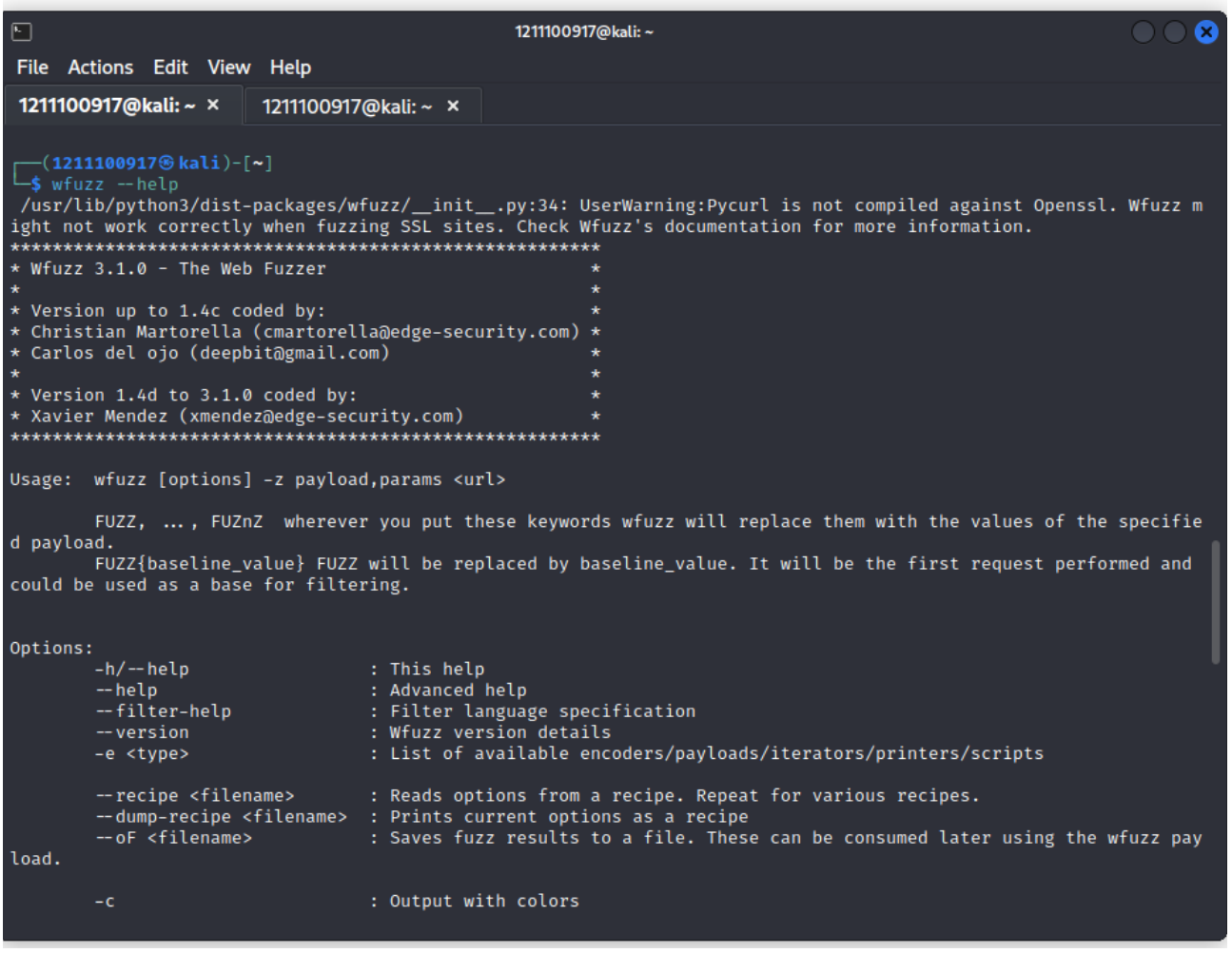
Insert date behind the website to get flag



THM{D4t3_AP1}

Question 9

Using wfuzz-help to find what is stored in -f parameter



Question 10

-f parameter store result

```
********************************************************

Usage:  wfuzz [options] -z payload,params <url>

        FUZZ, ... , FUZnZ  wherever you put these keywords wfuzz will replace them with the values of the specifie
d payload.
        FUZZ{baseline_value} FUZZ will be replaced by baseline_value. It will be the first request performed and
could be used as a base for filtering.


Options:
        -h/--help                : This help
        --help                   : Advanced help
        --filter-help            : Filter language specification
        --version                : Wfuzz version details
        -e <type>                : List of available encoders/payloads/iterators/printers/scripts

        --recipe <filename>      : Reads options from a recipe. Repeat for various recipes.
        --dump-recipe <filename> : Prints current options as a recipe
        --oF <filename>          : Saves fuzz results to a file. These can be consumed later using the wfuzz pay
load.

        -c                       : Output with colors
        -v                       : Verbose information.
        -f filename,printer      : Store results in the output file using the specified printer (raw printer if
omitted).
```

Thought Process/Methodology

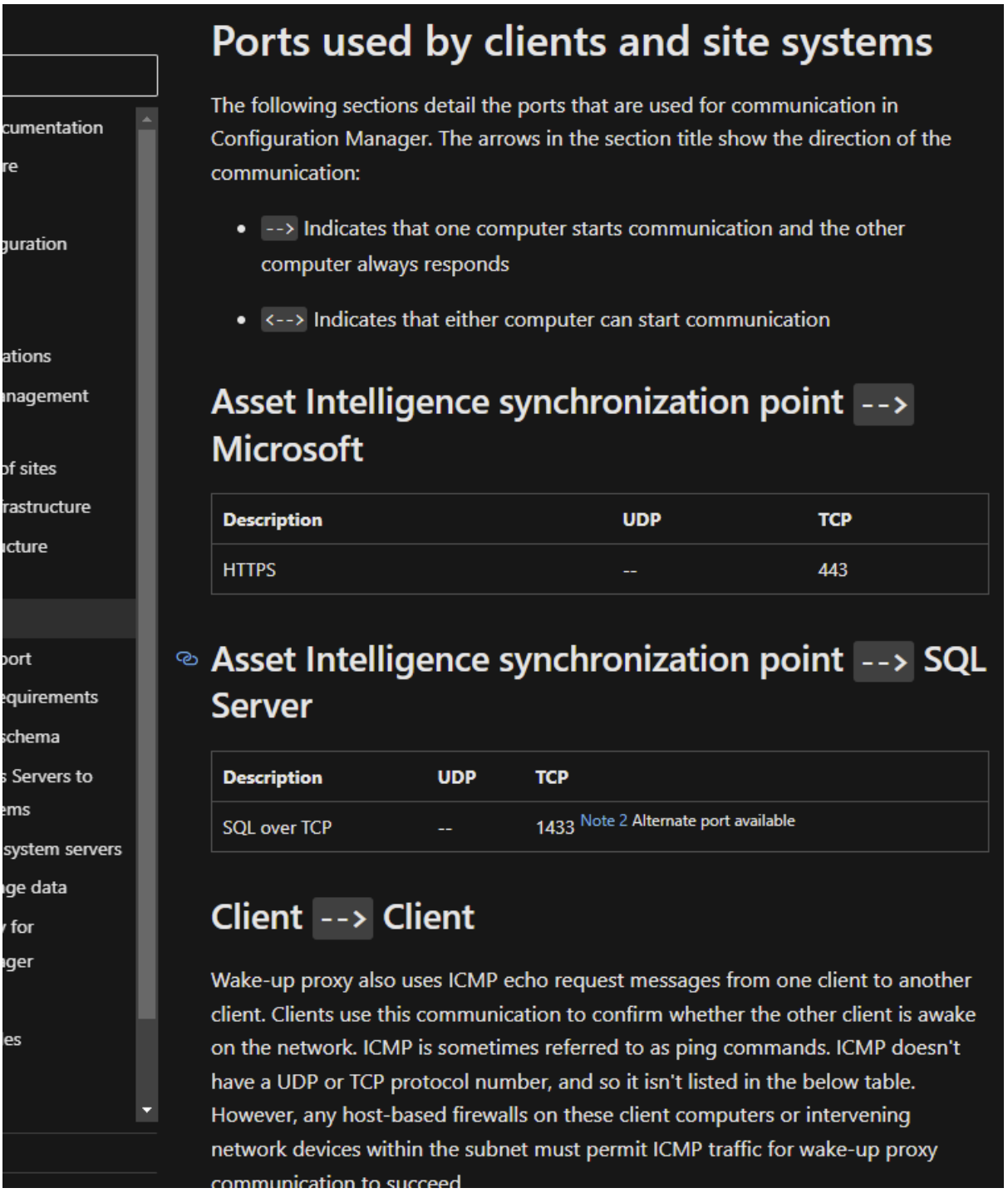
In order to find the custom wfuzz command, we would refer to the Try Hack Me website's explanation to figure out the placing to form the command. After gaining access to the target computer by pasting the IP address(10.10.240.147) in the address bar , a page with " You have been defaced, your forums are gone" is shown. Then, use gobuster's directory to find the API to access the webpage. Paste the API address to the address bar. From there we can see the index of the API. Later on, download the "wordlist" file from Try Hack Me website and copy its name. Using "wfuzz", we would paste "wordlist" to the wfuzz command,insert the path of "site-log" from the API website and insert date parameter. Next, insert the get date parameter with the date behind the API address to get the flag. Then, type "wfuzz-help" to find the -f parameter store result.

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

Tools used: Linux, Firefox, Terminal, Burpsuite, SQLMap

Question 1

Refer to the Microsoft documentation



Ports used by clients and site systems

The following sections detail the ports that are used for communication in Configuration Manager. The arrows in the section title show the direction of the communication:

- `-->` Indicates that one computer starts communication and the other computer always responds
- `<-->` Indicates that either computer can start communication

Asset Intelligence synchronization point `-->` Microsoft

Description	UDP	TCP
HTTPS	--	443

Asset Intelligence synchronization point `-->` SQL Server

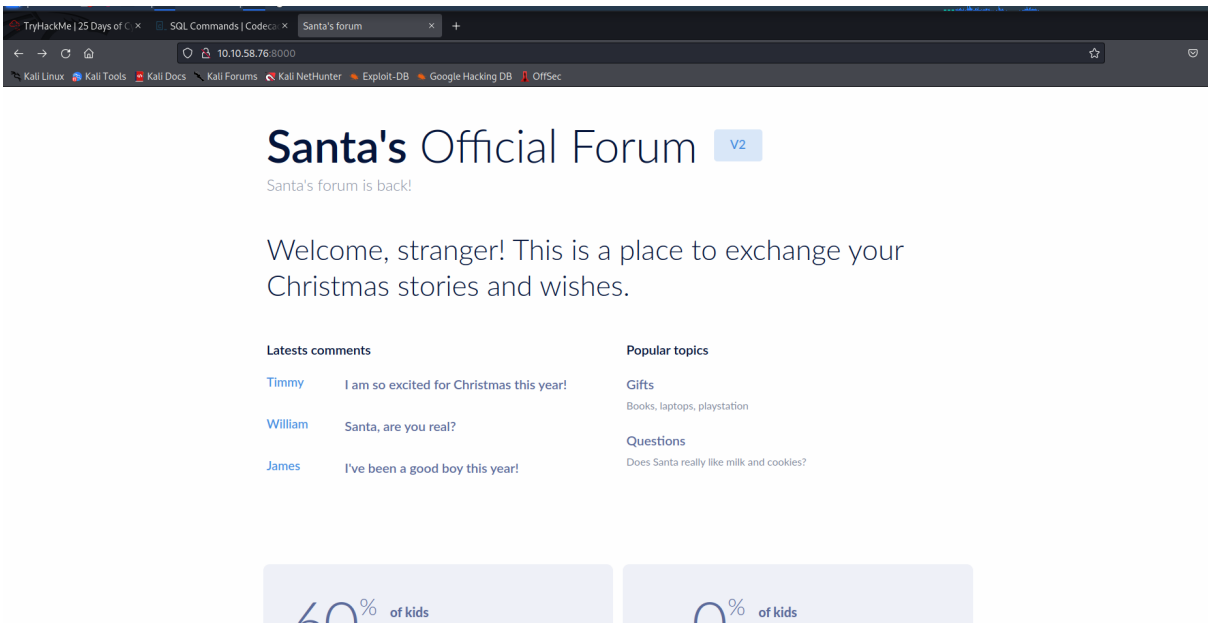
Description	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

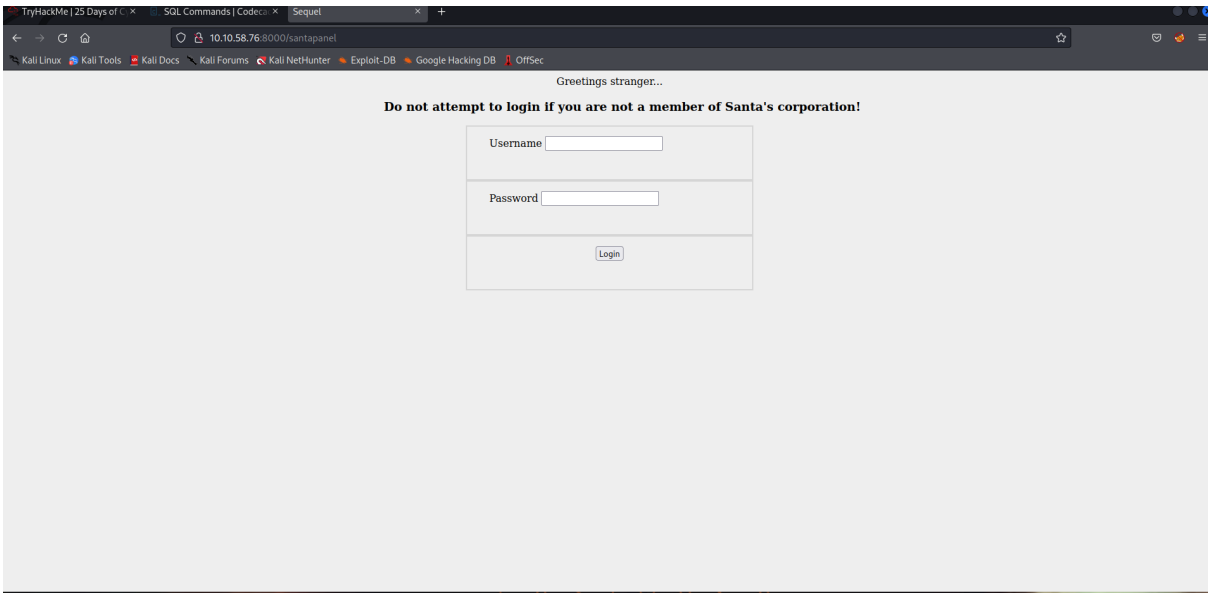
Client `-->` Client

Wake-up proxy also uses ICMP echo request messages from one client to another client. Clients use this communication to confirm whether the other client is awake on the network. ICMP is sometimes referred to as ping commands. ICMP doesn't have a UDP or TCP protocol number, and so it isn't listed in the below table. However, any host-based firewalls on these client computers or intervening network devices within the subnet must permit ICMP traffic for wake-up proxy communication to succeed

<u>Question 2</u>

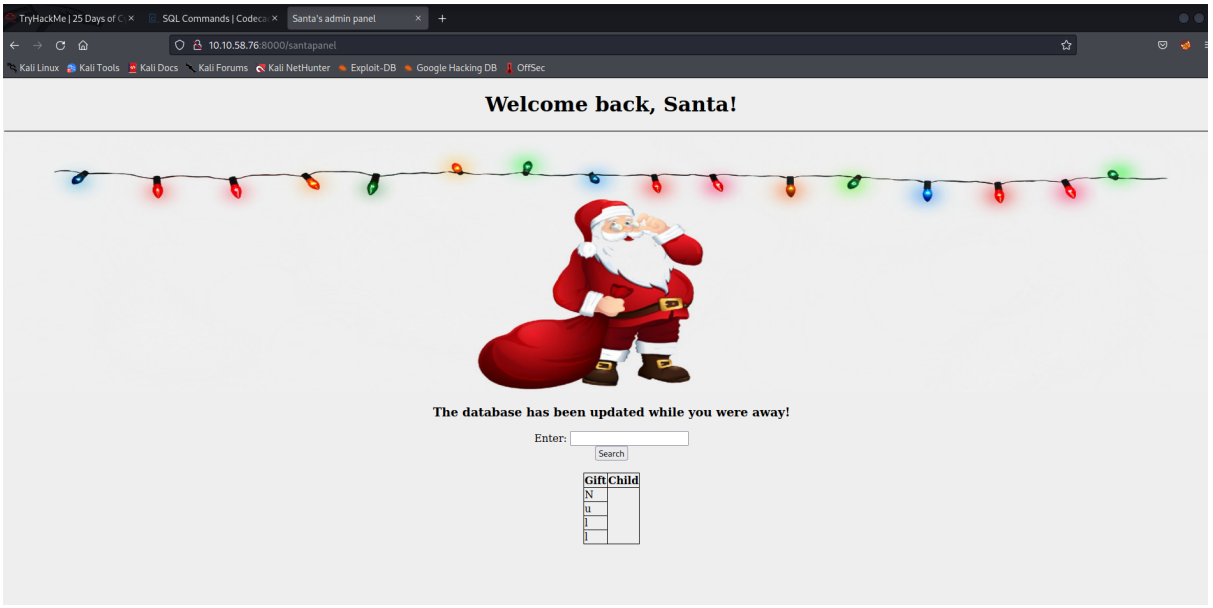
Enter Santa's secret login panel by adding /santapanel behind the IP address





Question 2(Tryhackme)

Enter Santa's admin panel page with SQLi



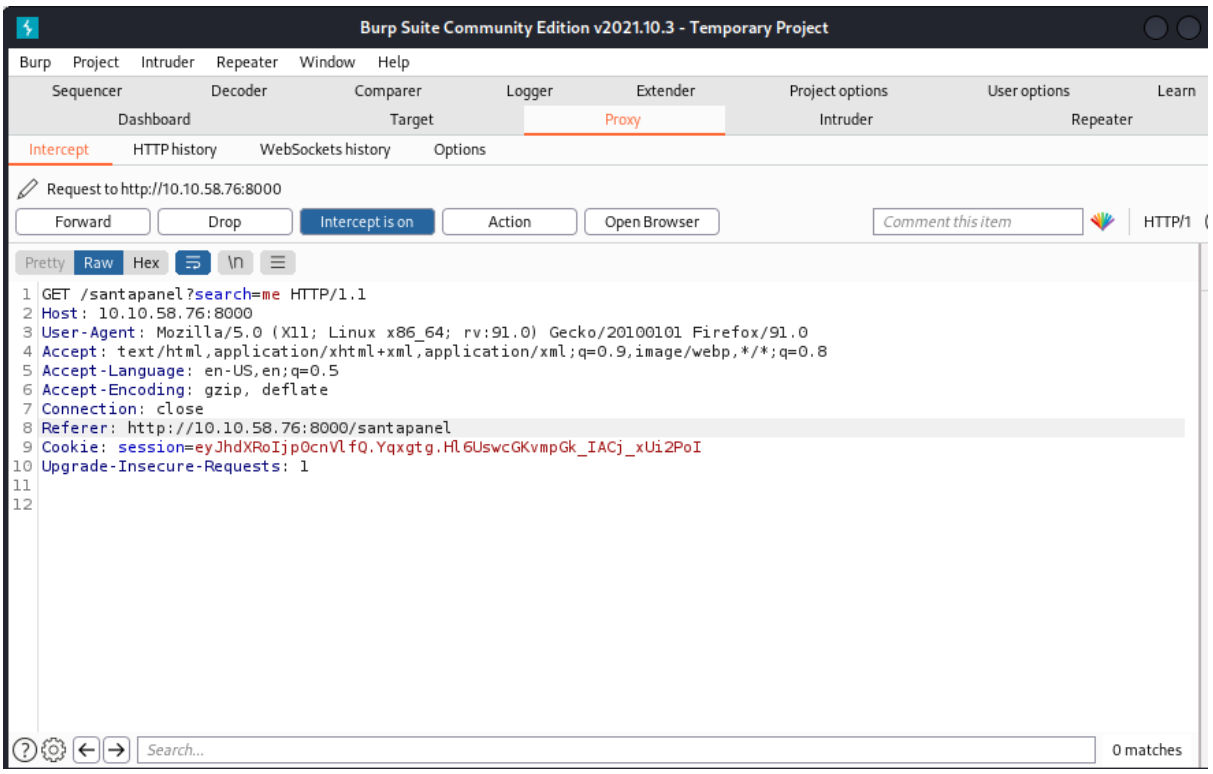
Question 3

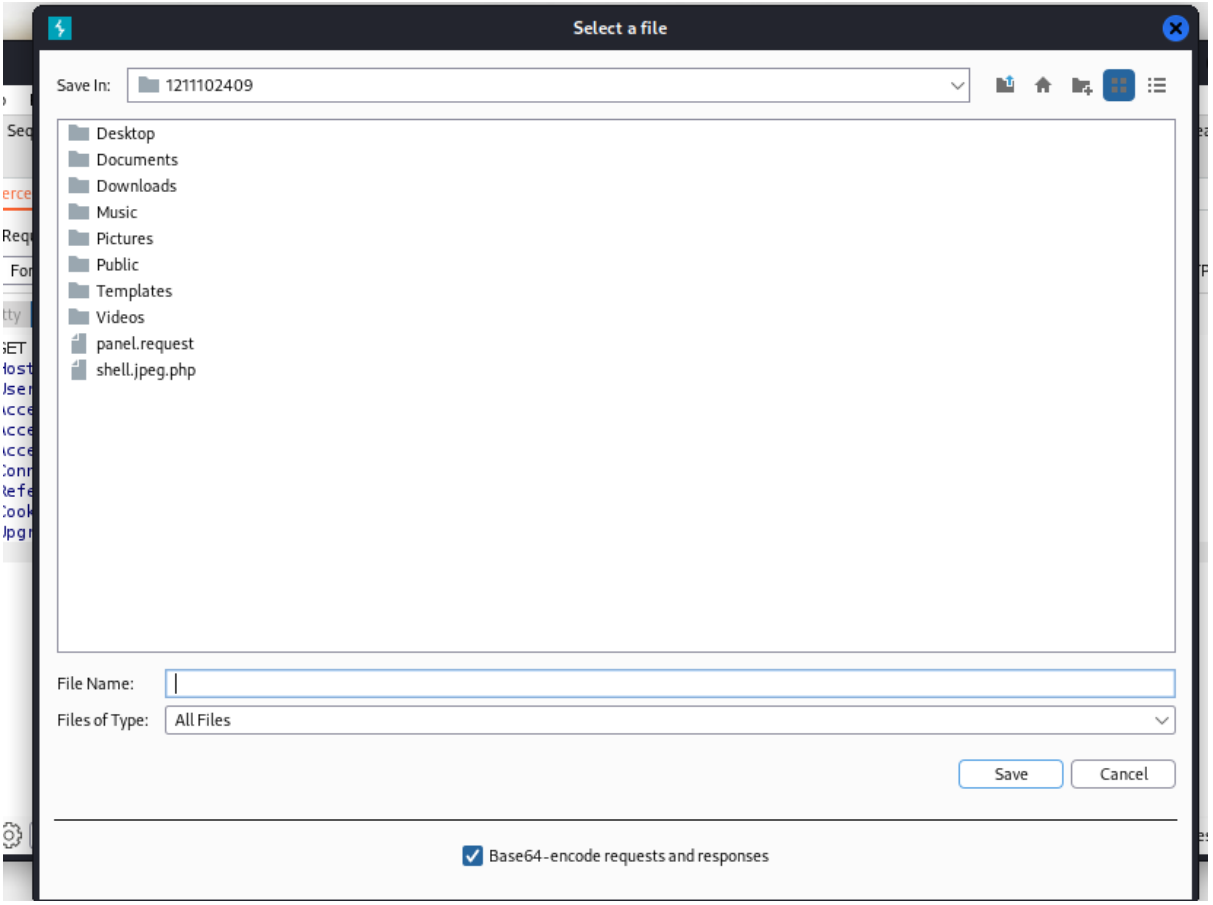
Finds at the tryhackme day 5 Challenge

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

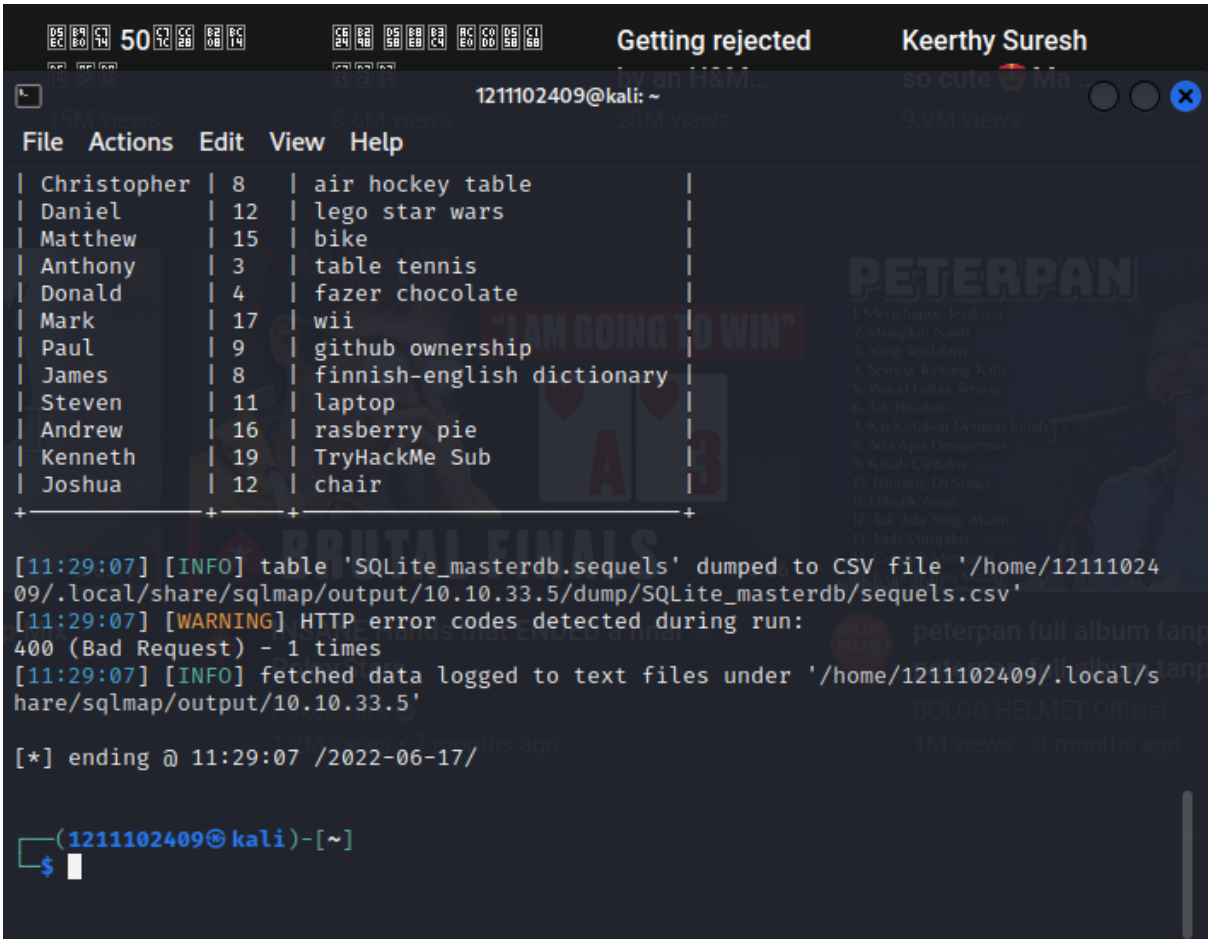
Question 4

Open foxyproxy and burp fill in something in the blank. Send the proxy to the repeater and save it.


Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Request to http://10.10.58.76:8000
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex \n
1 GET /santapanel?search=me HTTP/1.1
2 Host: 10.10.58.76:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.58.76:8000/santapanel
9 Cookie: session=eyJhdXRoIjp0cnVlfQ.Yqxgtg.Hl6UswcGKvmpGk_IACj_xUi2PoI
10 Upgrade-Insecure-Requests: 1
11
12
Search...
0 matches

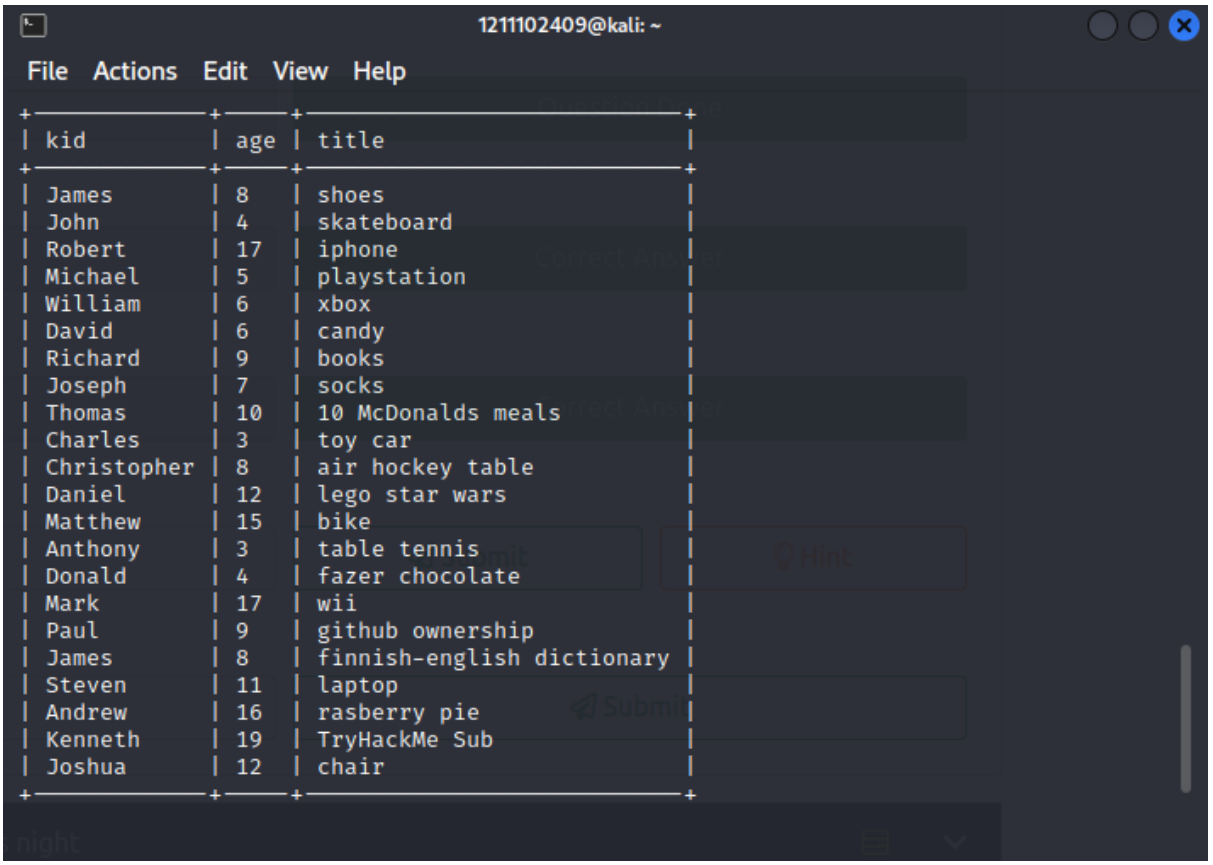

Select a file
Save In: 1211102409
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
panel.request
shell.jpeg.php
File Name:
Files of Type: All Files
Save
Cancel
Base64-encode requests and responses

Find the gift database using SQLmap



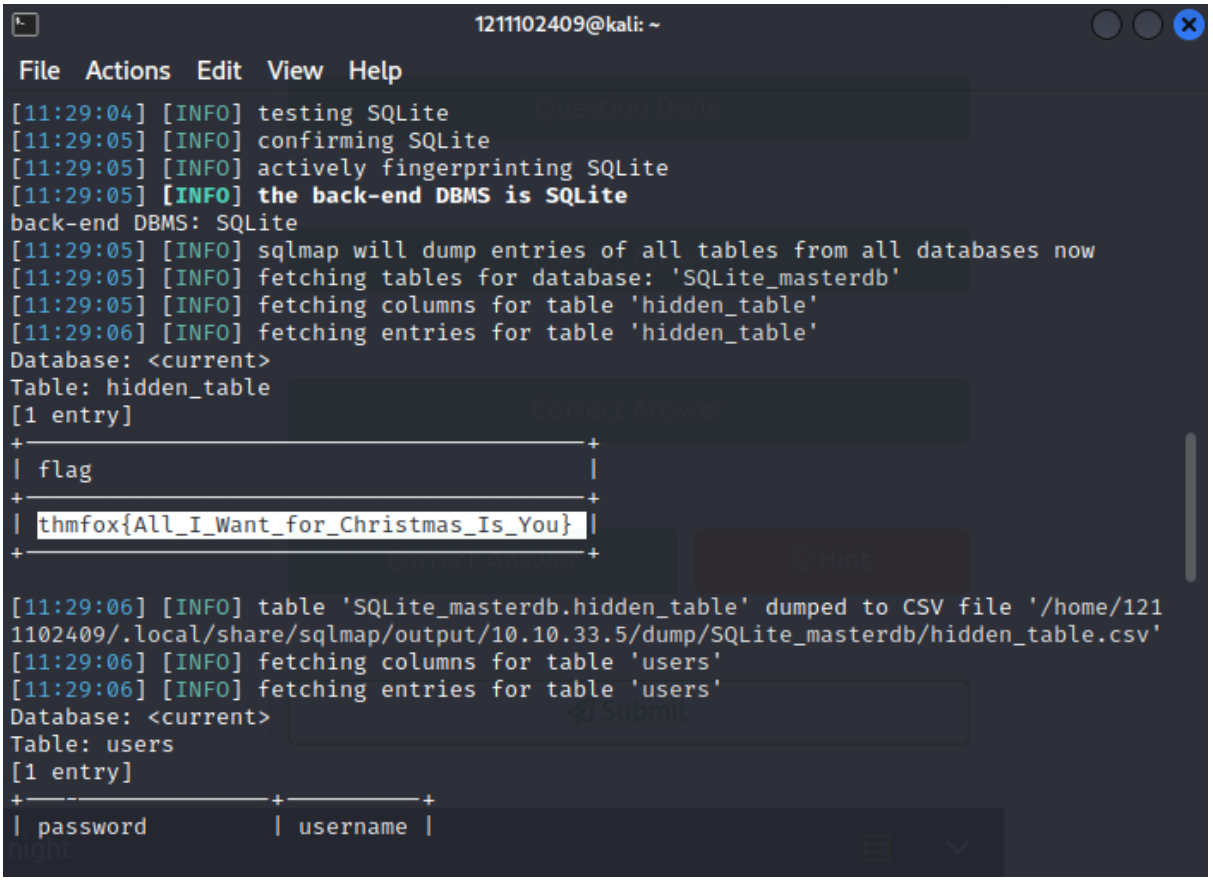
Question 5&6

Check the age of the kid name James. Check the title for the kid name Paul



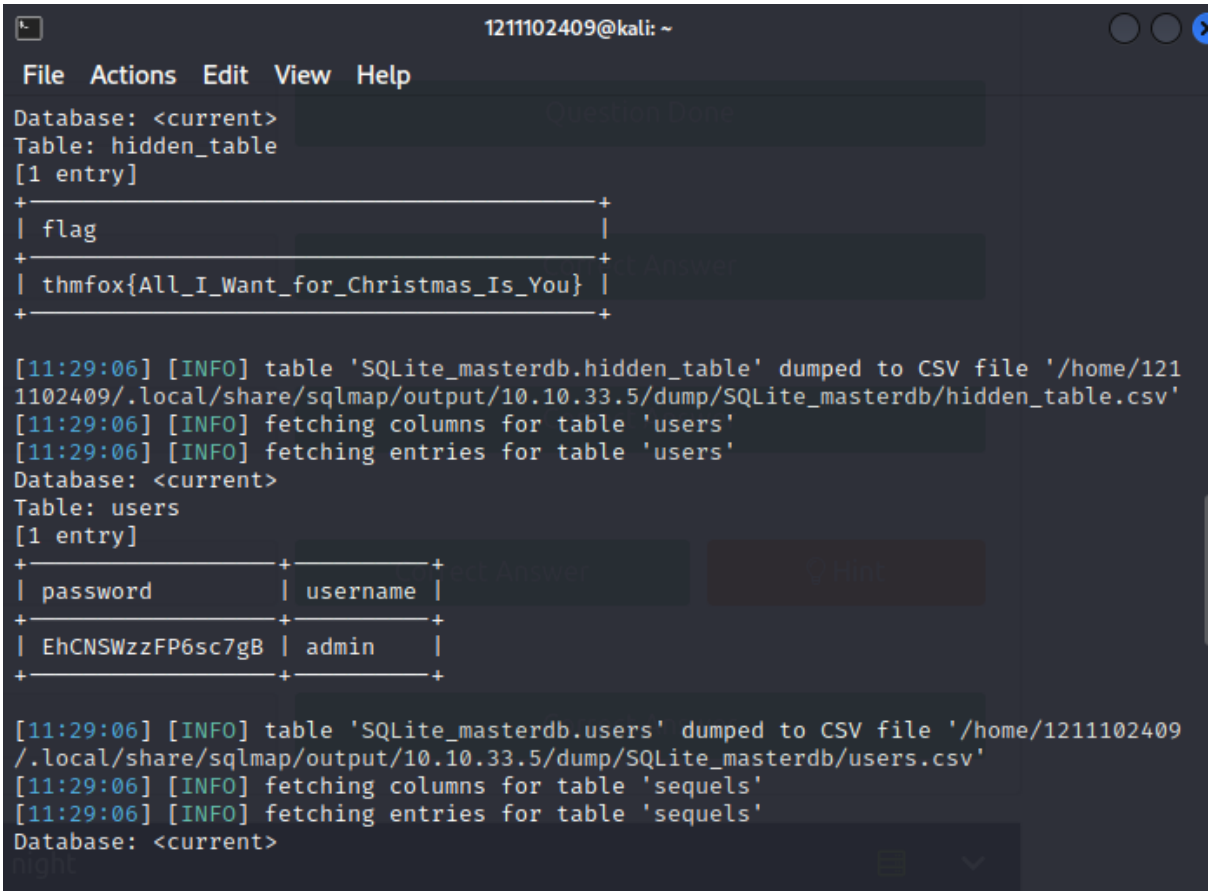
Question 7

Find the flag in the database



Question 8

Get the admin's password from the database



Thought Process/Methodology

After entering the IP address with port 8000, Santa's Official Forum v2 was shown. To enter Santa's secret login panel we insert /santapanel behind the IP address. After that, we login bypass to Santa's admin panel page with SQL Injection(input ' or true –). Then, we try to get the gift database by using SQLMap&BurpSuite.The database shows out in the terminal. Now, we can check for the kid's name with the present, flag, and username with password.