Report PSP0201 T2130 - Tutorial Week 2

Group: **Marceline**

ID	Name	Role
1211100899	Muhammad Shahril Aiman	Leader
1211101533	Muhammad Aniq Fahmi	member
1211101303	Aiman Faris	member
1211102759	Muhammad Zaquan	member

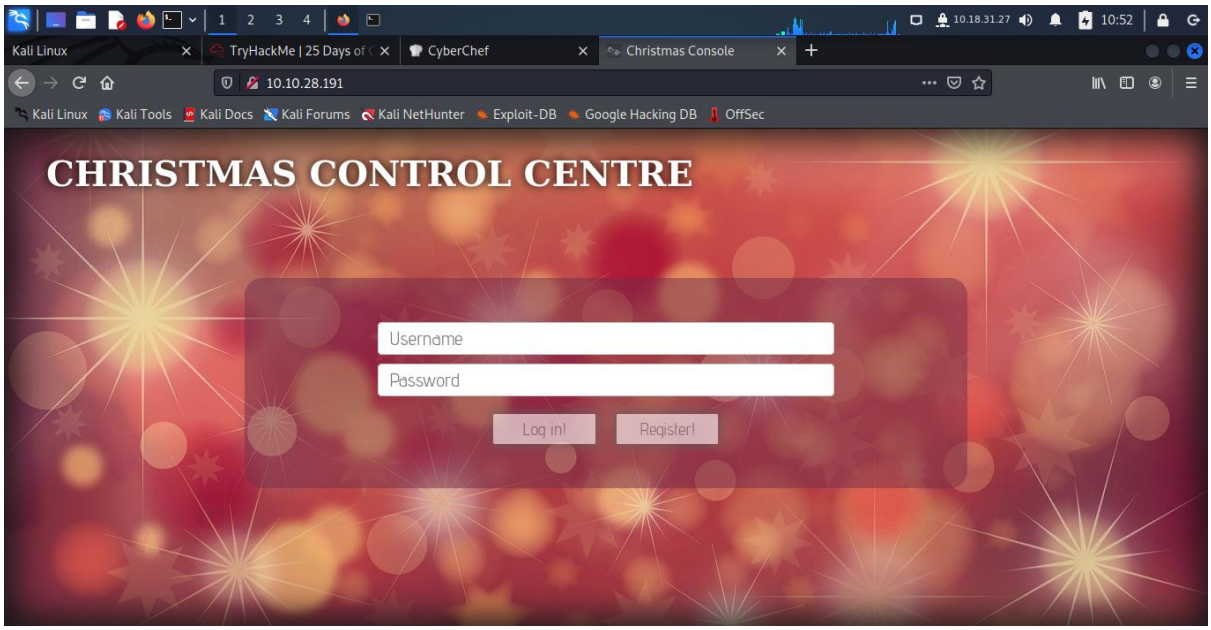
Day 1: Web Exploitation: A Christmas Crisis

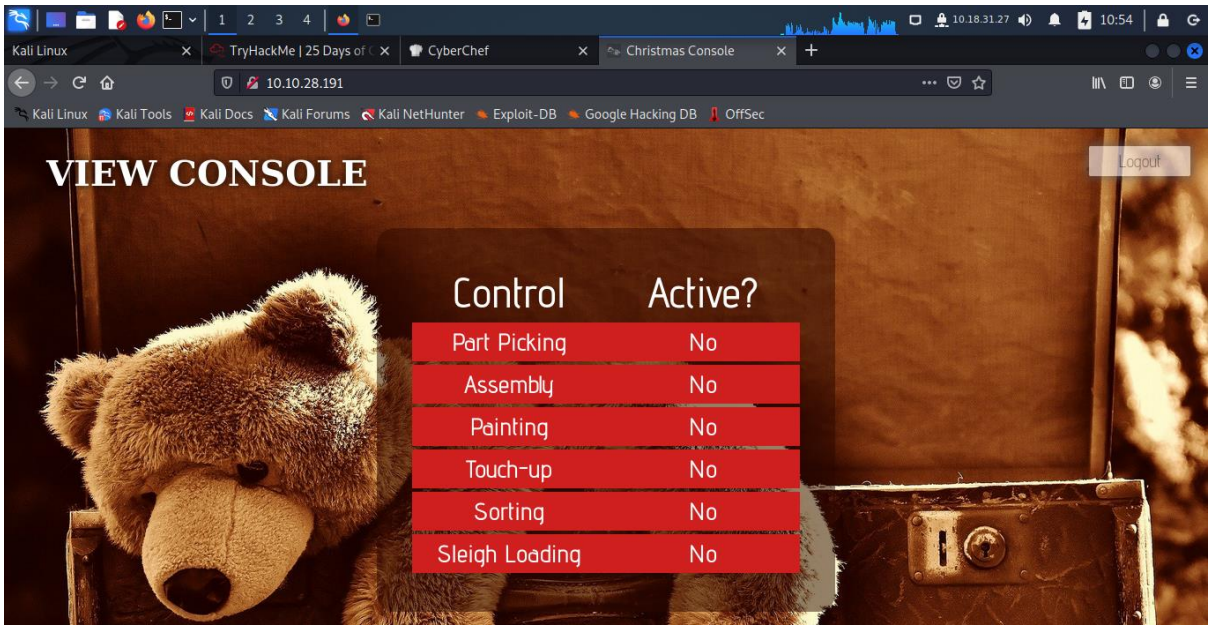
Tools used: Kali Linux, Firefox

Solution/Walkthrough:

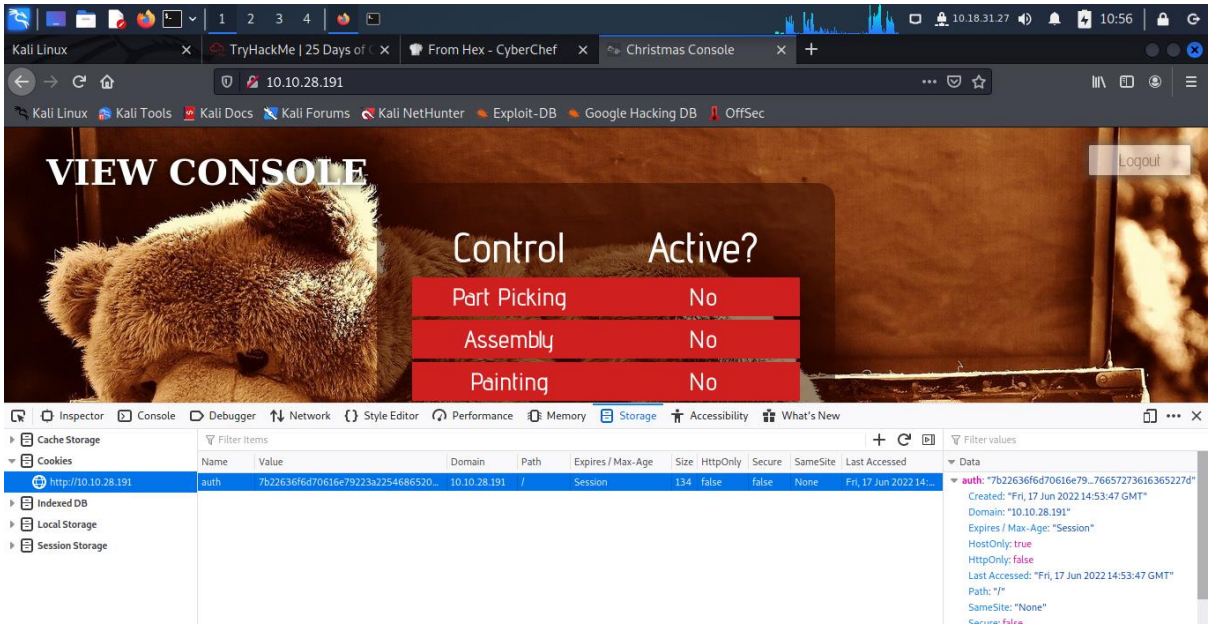
Question 1:

Registration and logging in to the Christmas Control Centre. No access to the control console.





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

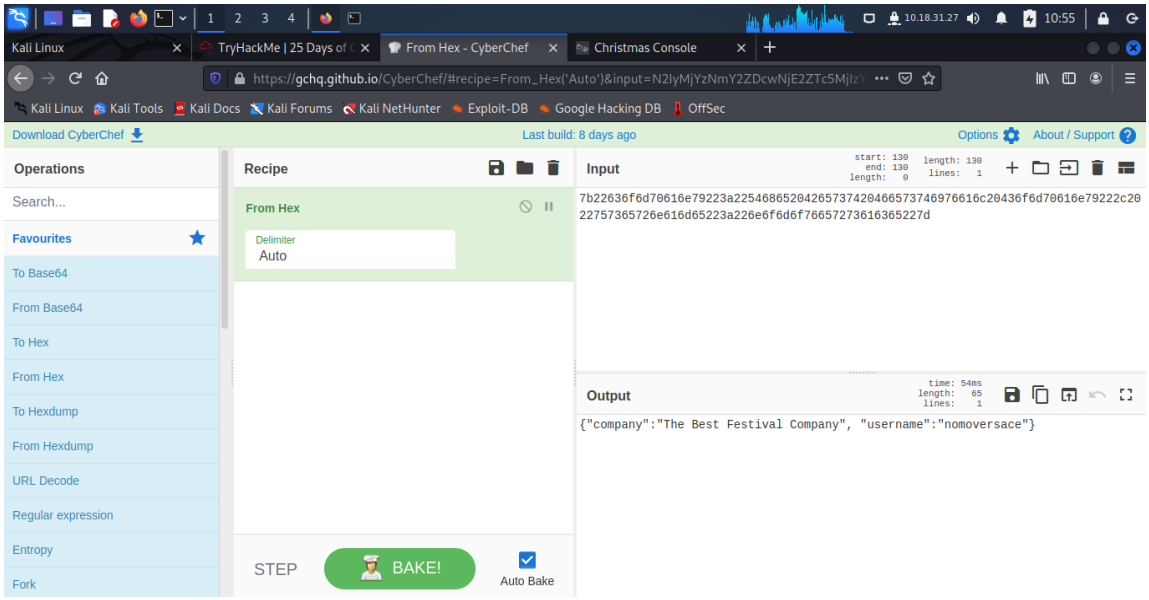


Question 2:

Obtain the value of the cookie.

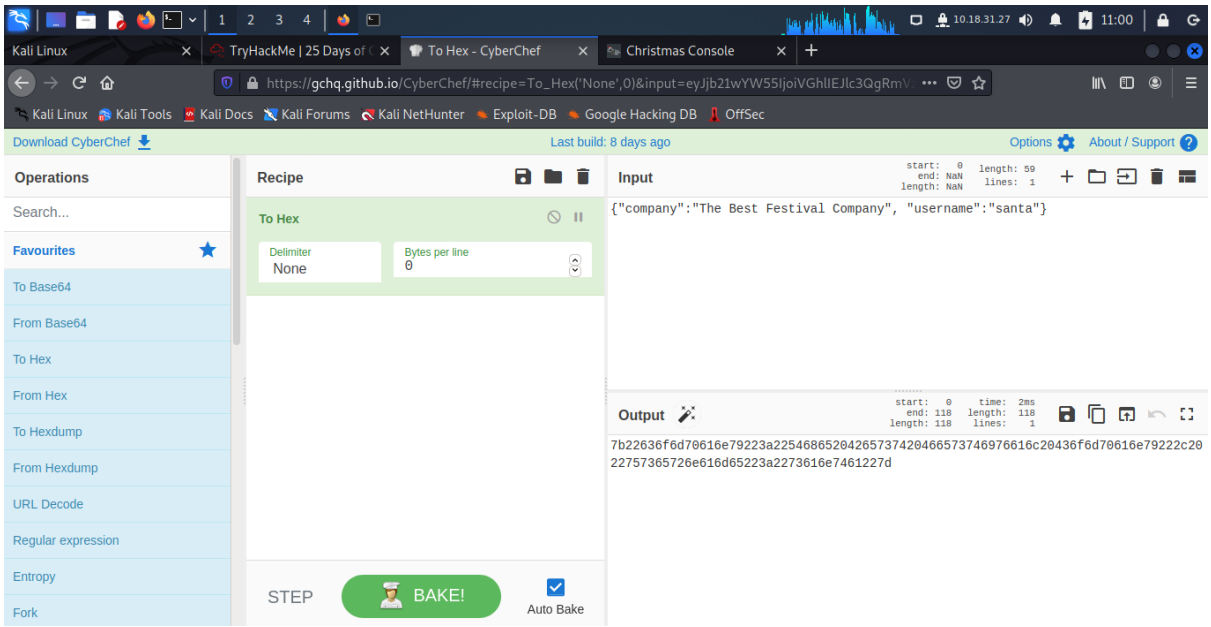
Question 3:

Using Cyberchef, convert the cookie value to string.



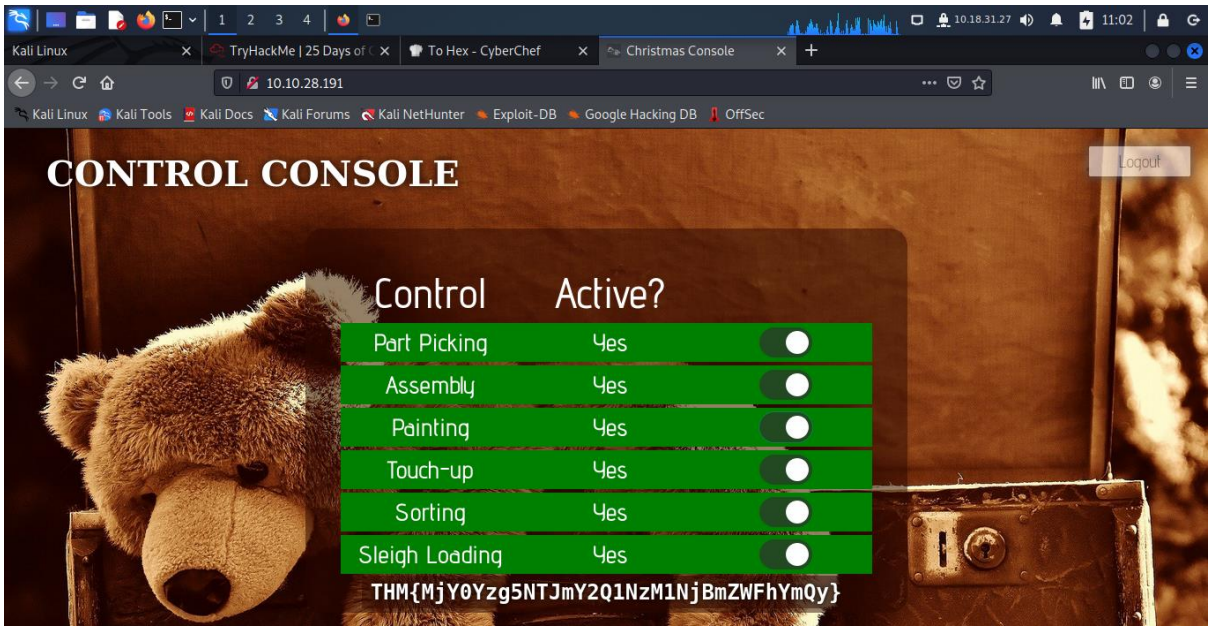
Question 4:

Changing the username to ‘santa’, convert the JSON statement to hex.



Question 5:

Now having access to the controls, switching on every control shows the flag.



METHODOLOGY:

When we started the machine, it gave us an Ip address that leads us to a login page which we have to register and login in order to obtain the first cookie by using browser developer tool by pressing f12, then we take the first cookie and bring it to cyber chef to change it from hexadecimals to text form or JSON statement. Then, we change the username that we created into “santa” and convert the JSON statement to hexadecimal form to get the value of santa’s cookie. After we obtain the value of the cookie, we went back to the log in page and use the developers’ tool to create a new cookie so that the system detects us as santa so we can log in as santa which is the administrator page that can enable every control. We enable every control in the page and obtain the flag that we need for the final question.

Day 2: Web Exploitation, The Elf Strikes Back!

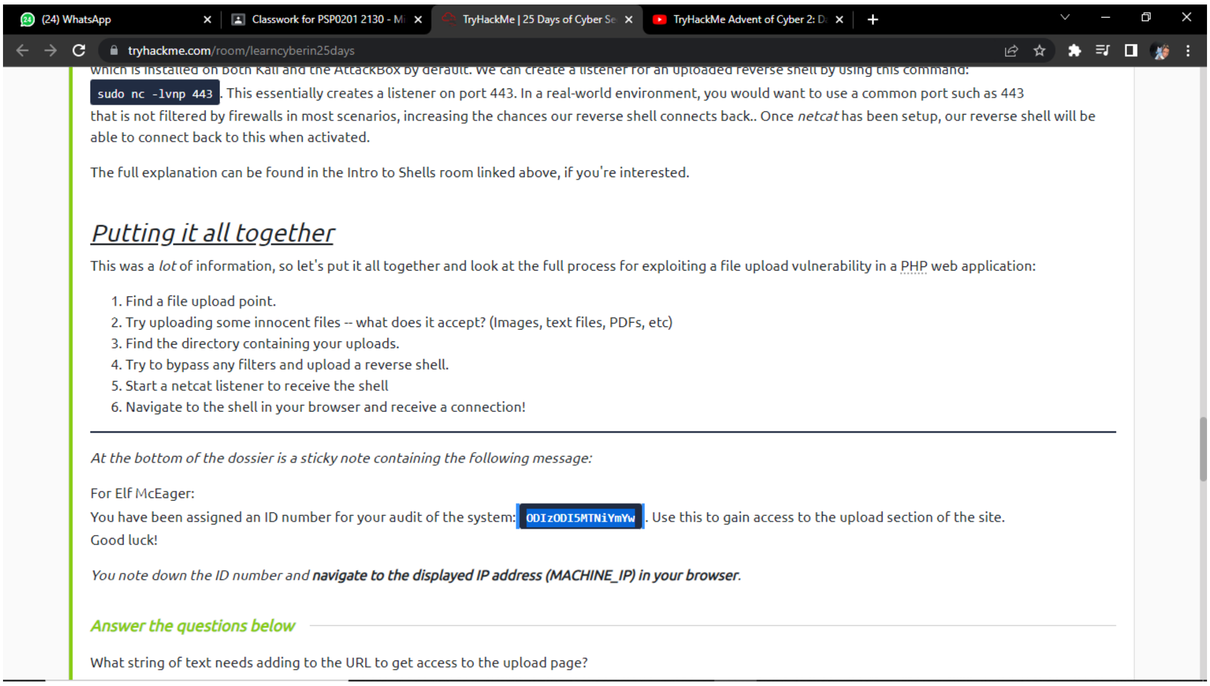
Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

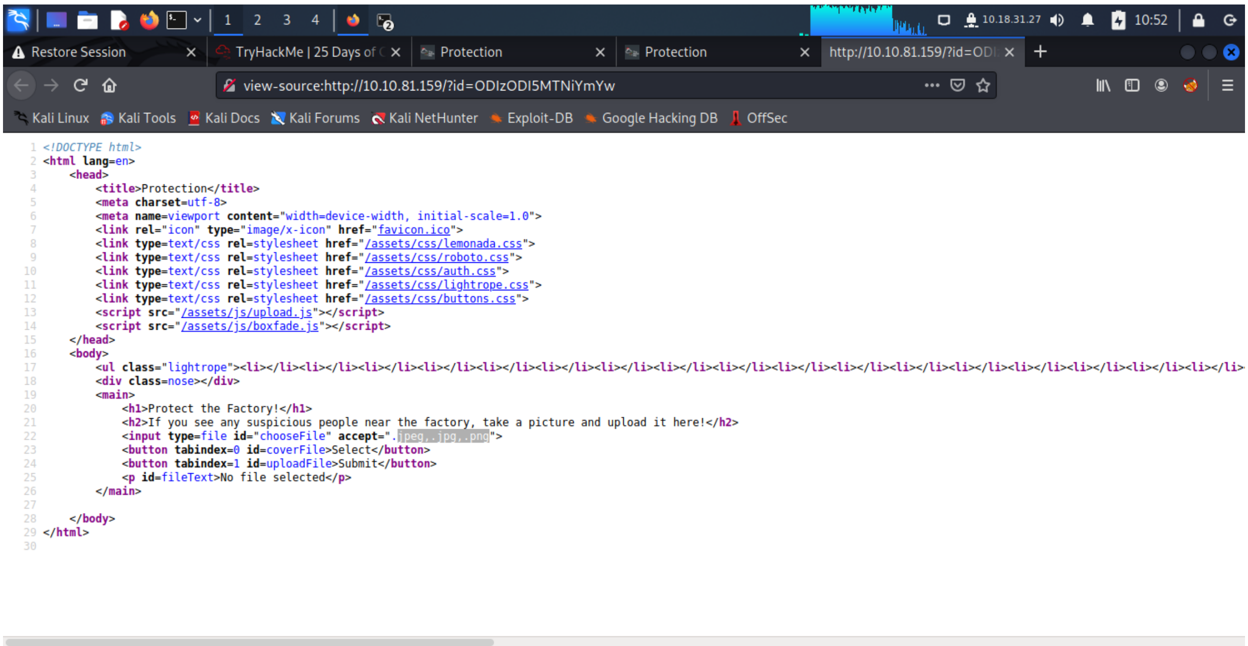
What string of text needs adding to the URL to get access to the upload page?

?id=ODIzODI5MTNiYmYw



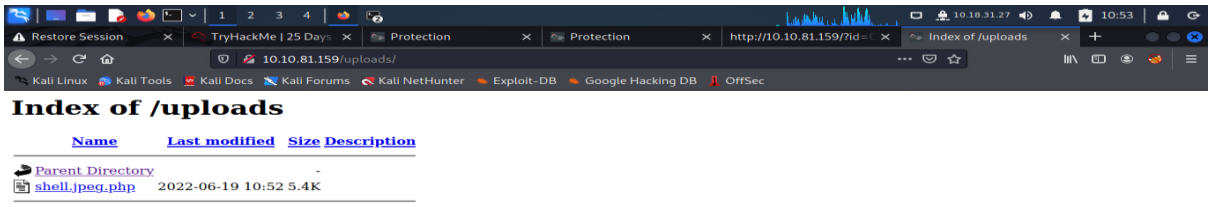
Question 2

What type of file is accepted by the site?



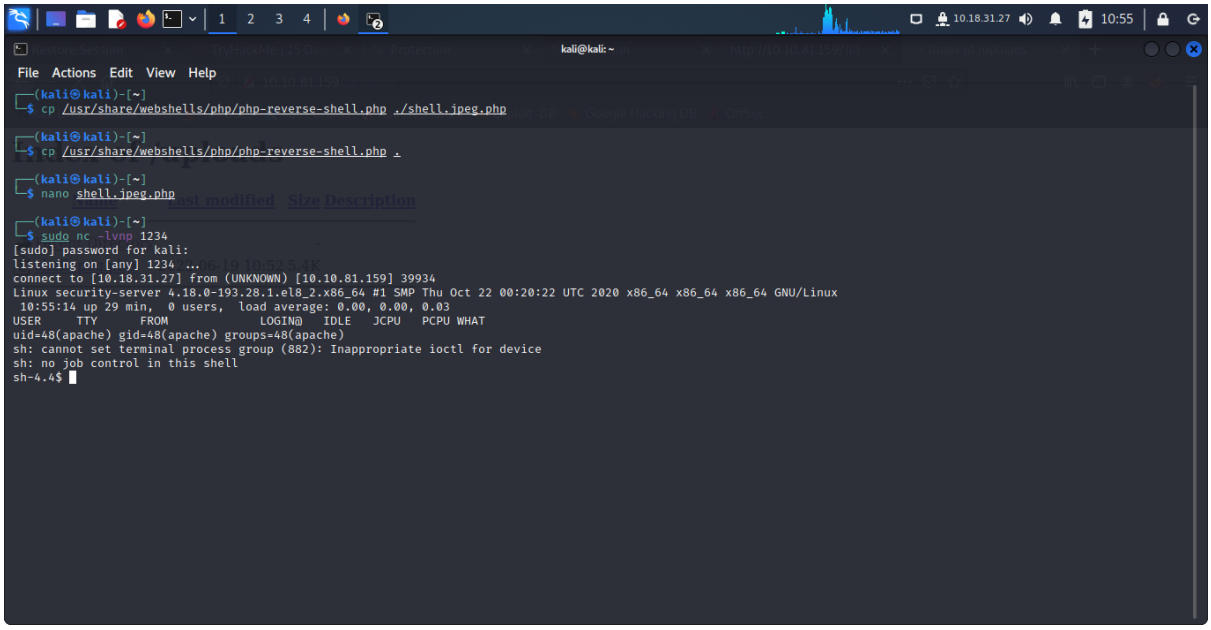
Question 3

In which directory are the uploaded files stored?



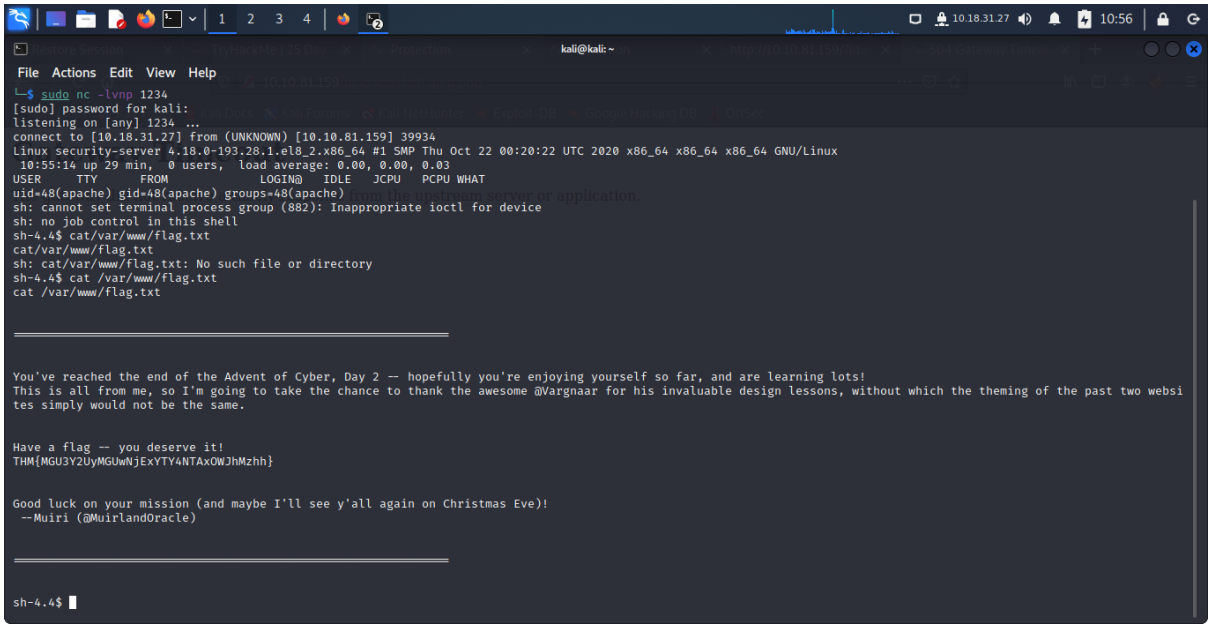
Question 4

Activate your reverse shell and catch it in a netcat listener!



Question 5

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



METHODOLOGY:

Firstly, we copy the Ip address that was given in Tryhackme and paste it another tab. We got a page that request our id to be put in to enter further in the page. We added this"? id=ODIzODI5MTNiYmYw" on our Ip address which gave us access to the page which now we have to upload a file in it. Then we save the reverse shell into our files by using the command "cp /usr/share/webshells/php/php-reverse-shell.php . After the file is saved, we used nano to change the ip address and port.After all has been changed we saved it and went straight to creating a listener called netcat to increase the chances of our reverse shell connecting back. We set up the netcat listener and then we upload the file that we saved earlier in the process to the page that request us the file. Once the upload is complete, we went to (*ip*/uploads) to check whether our file is there or not. Once we saw the file, we click on it and went back to the terminal to check if our listener is working. Finally, we entered cat /var/www/flag.txt to complete our final task and get the flag

Day 3: Web Exploitation, Christmas Chaos

Tools used: Kali Linux, Firefox, AttackBox

Solution/Walkthrough:

Question 1 & 2:

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

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

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):

Question 3:

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

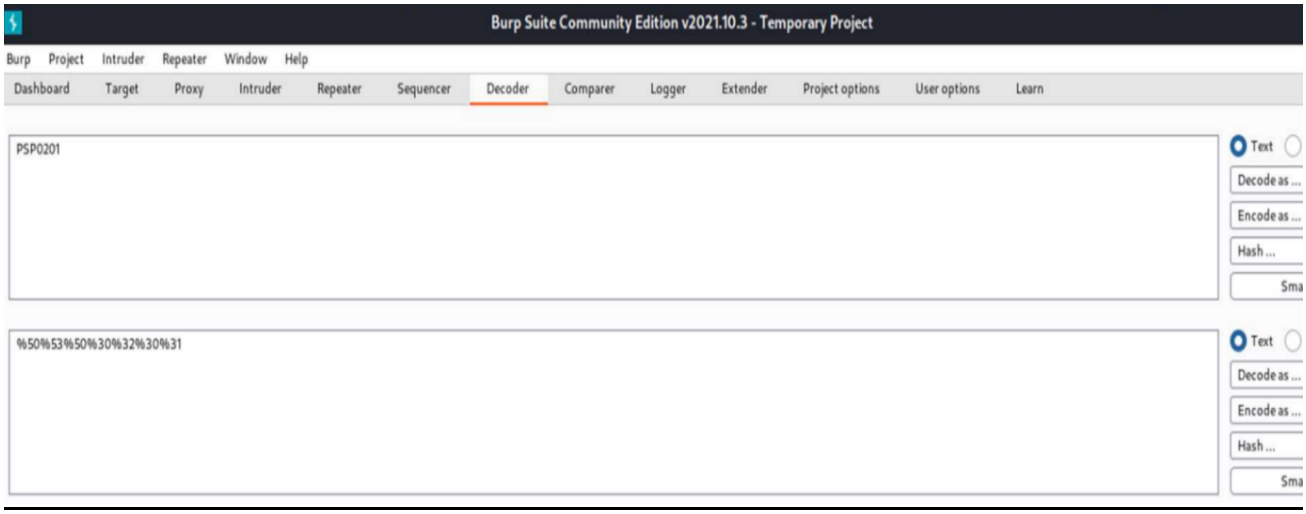
Question 4&5:

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

5.What is the proxy type?

Question 6:

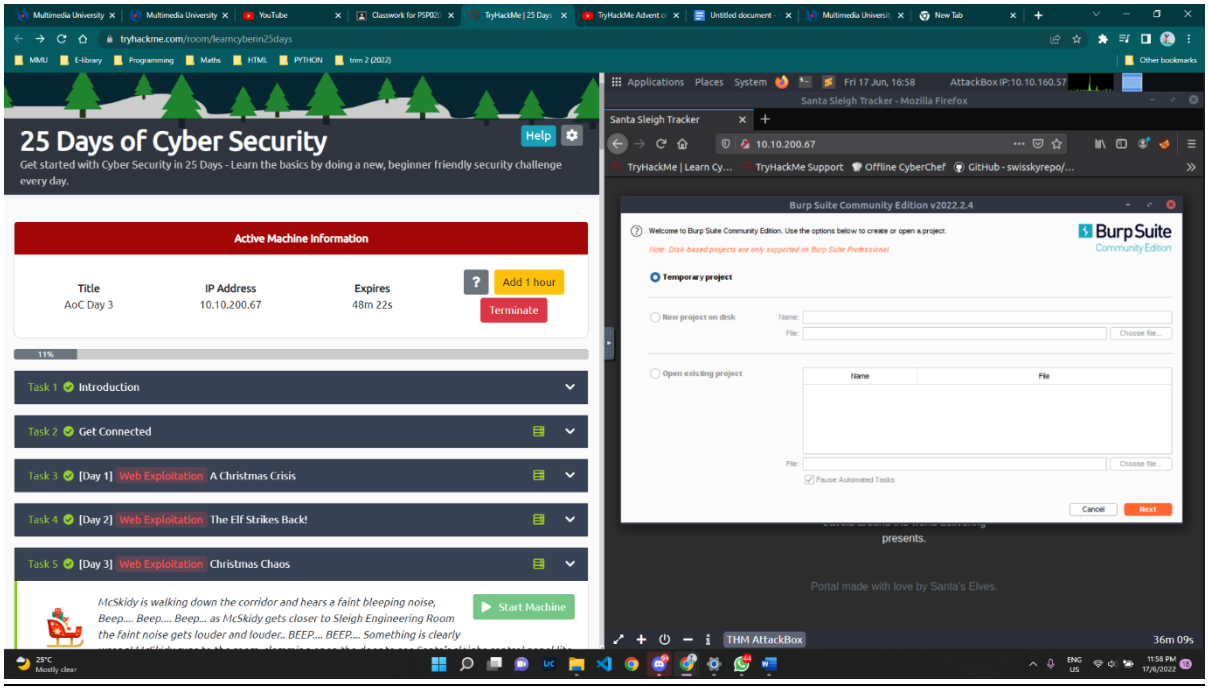
Experiment with decoder on Burp. What is the URL encoding for "PSP0201"?



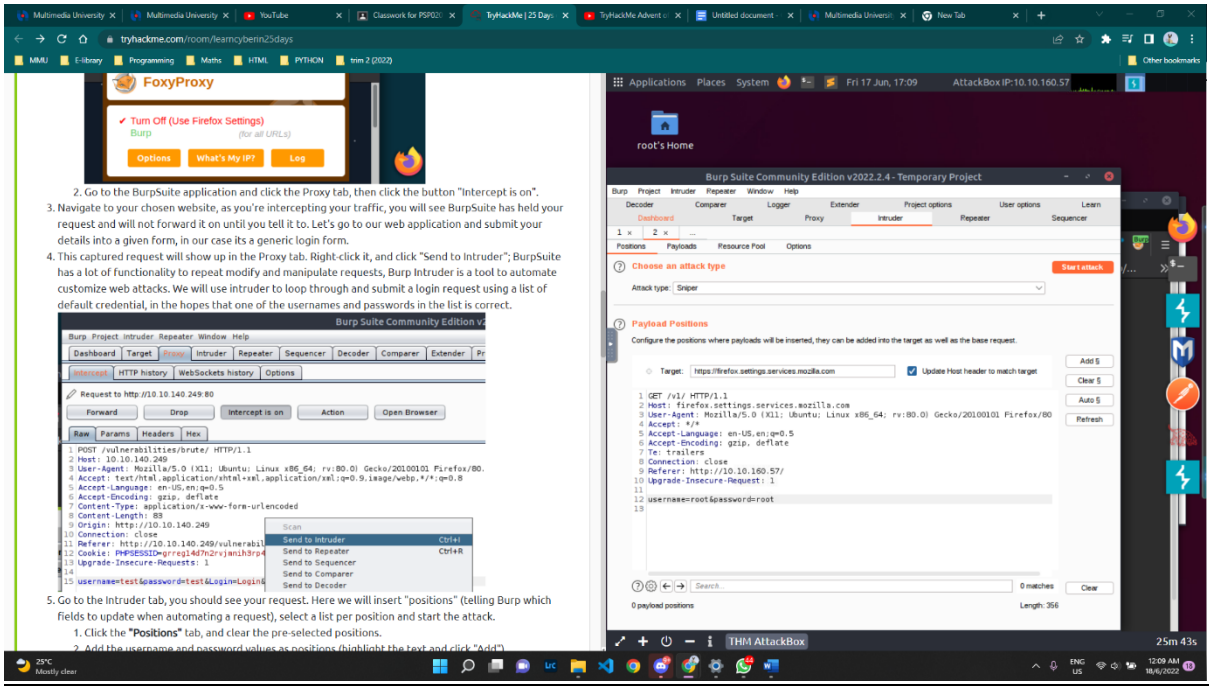
Question 8:

What is the flag?

Step 1



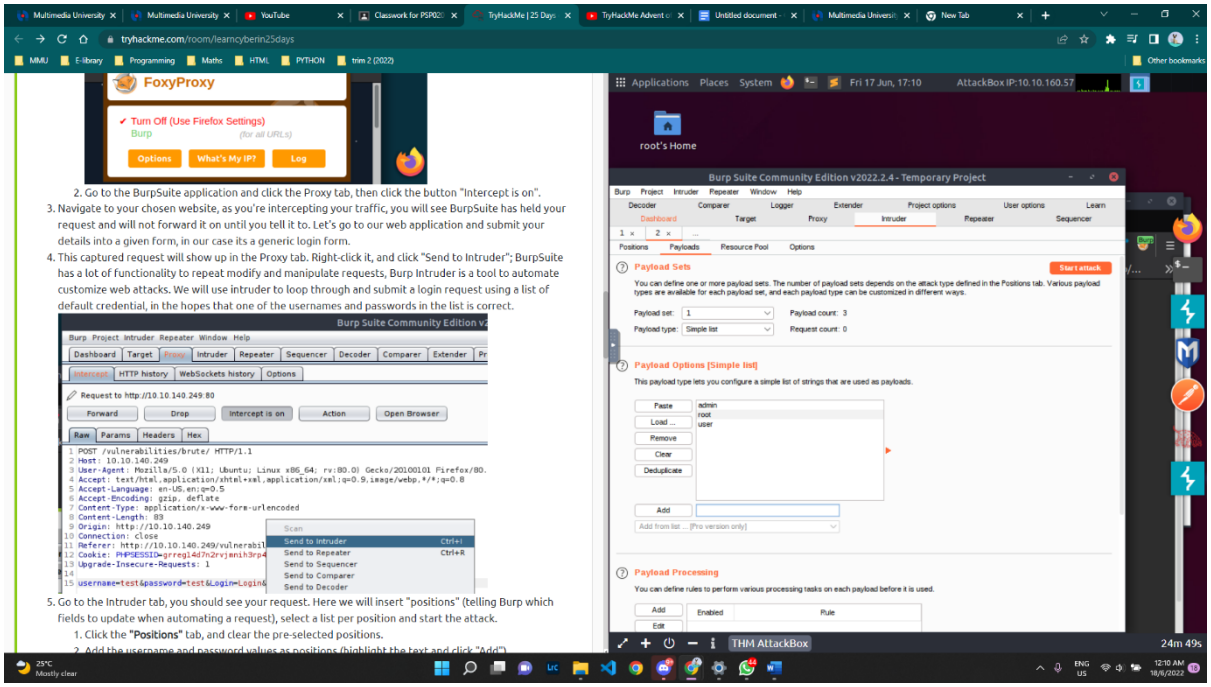
Step 2



2. Go to the BurpSuite application and click the Proxy tab, then click the button "Intercept is on".
3. Navigate to your chosen website, as you're intercepting your traffic, you will see BurpSuite has held your request and will not forward it on until you tell it to. Let's go to our web application and submit your details into a given form, in our case its a generic login form.
4. This captured request will show up in the Proxy tab. Right-click it, and click "Send to Intruder"; BurpSuite has a lot of functionality to repeat modify and manipulate requests, Burp Intruder is a tool to automate customize web attacks. We will use intruder to loop through and submit a login request using a list of default credential, in the hopes that one of the usernames and passwords in the list is correct.

5. Go to the Intruder tab, you should see your request. Here we will insert "positions" (telling Burp which fields to update when automating a request), select a list per position and start the attack.
    1. Click the **"Positions"** tab, and clear the pre-selected positions.
    2. Add the username and password values as positions (highlight the text and click "Add").

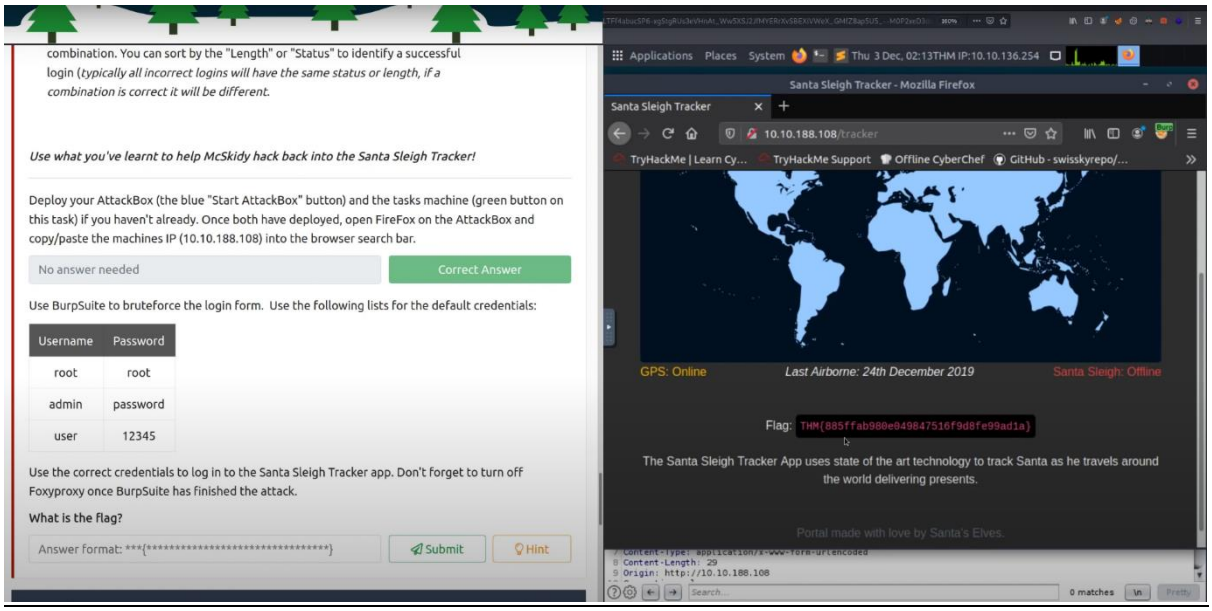
Step 3



2. Go to the BurpSuite application and click the Proxy tab, then click the button "Intercept is on".
3. Navigate to your chosen website, as you're intercepting your traffic, you will see BurpSuite has held your request and will not forward it on until you tell it to. Let's go to our web application and submit your details into a given form, in our case its a generic login form.
4. This captured request will show up in the Proxy tab. Right-click it, and click "Send to Intruder"; BurpSuite has a lot of functionality to repeat modify and manipulate requests, Burp Intruder is a tool to automate customize web attacks. We will use intruder to loop through and submit a login request using a list of default credential, in the hopes that one of the usernames and passwords in the list is correct.

5. Go to the Intruder tab, you should see your request. Here we will insert "positions" (telling Burp which fields to update when automating a request), select a list per position and start the attack.
    1. Click the **"Positions"** tab, and clear the pre-selected positions.
    2. Add the username and password values as positions (highlight the text and click "Add").

Step 4



METHODOLOGY:

When we started the machine, it gave us an Ip address that leads us to a login page which we have to register and login in order to obtain the first cookie by using browser developer tool by pressing f12, then we open the BurpSuite at the application and start to attack the website. After that, I open the FoxyProxy and the on to burp and start the work. I turn on the proxy intruder at the BurpSuite. Then, I go to the proxy and send to the intruder for attacking purposes. I go to the intruder positions to make sure the connection is closed. I write my username and password at the intruder section. Then I go the payloads to write the username and the password each of the account to attack them. After that I try to login with the account and got the flag for the Santa.

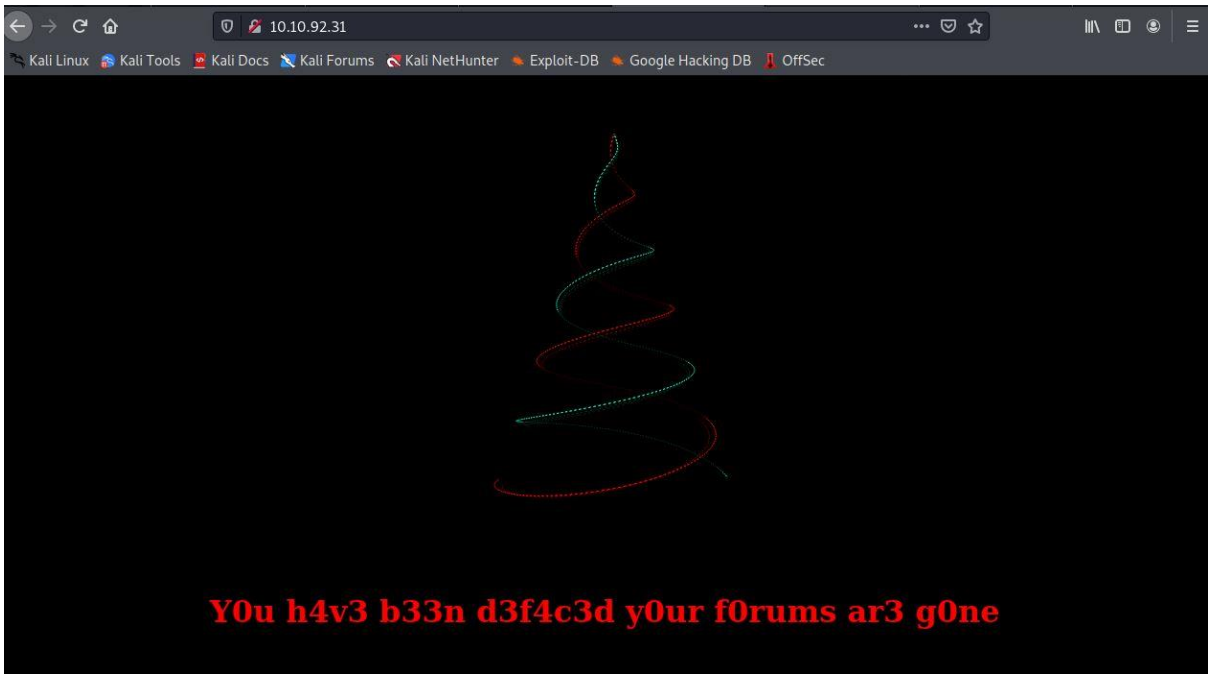
Day 4: Web Exploitation, Santa's Watching

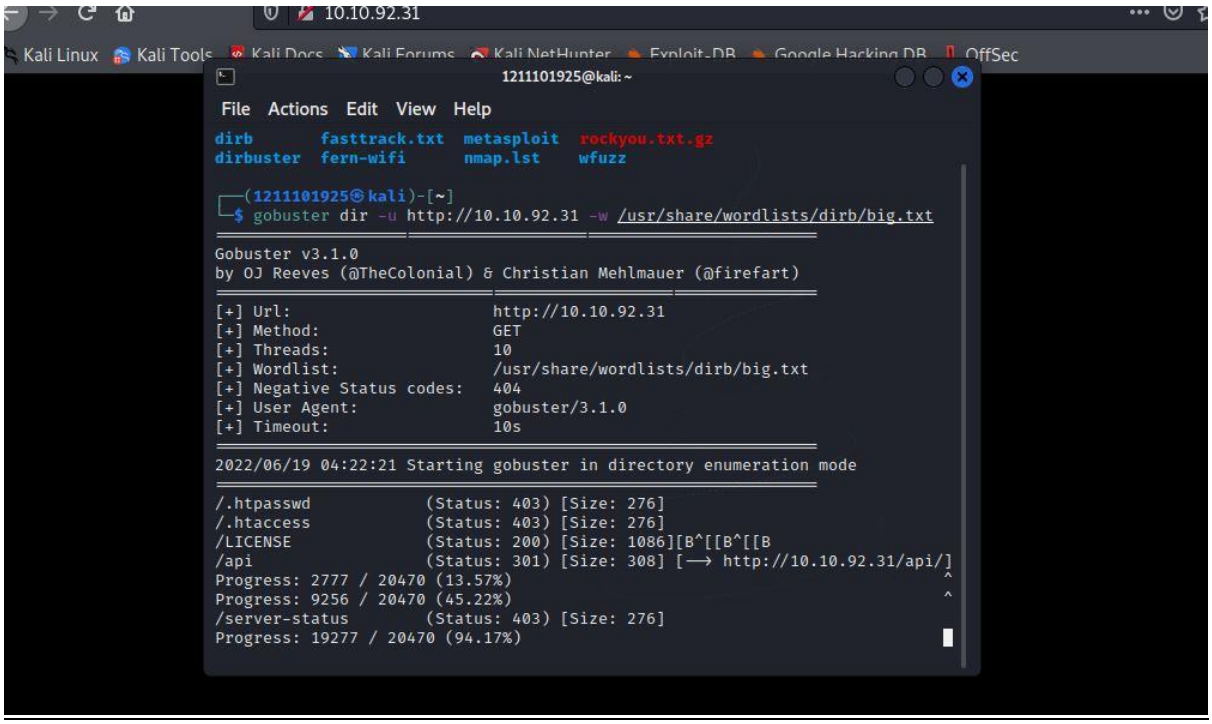
Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1:

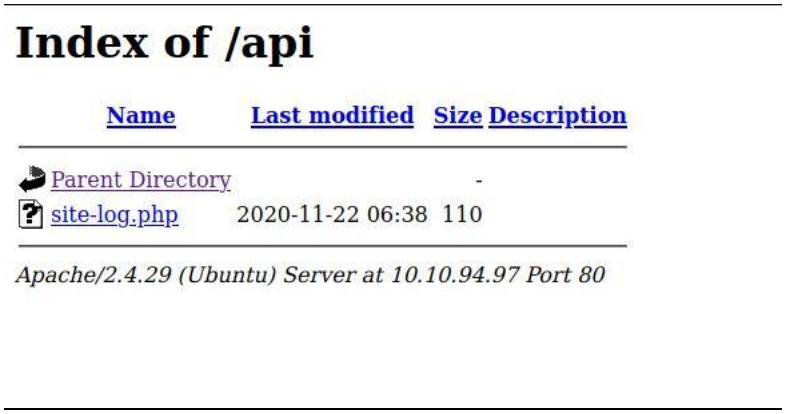
Given the URL "http://shibes.xyz/api.php", what would the entire wfuzz command look like to query the "breed" parameter using the wordlist "big.txt" (assume that "big.txt" is in your current directory)





Question 2:

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



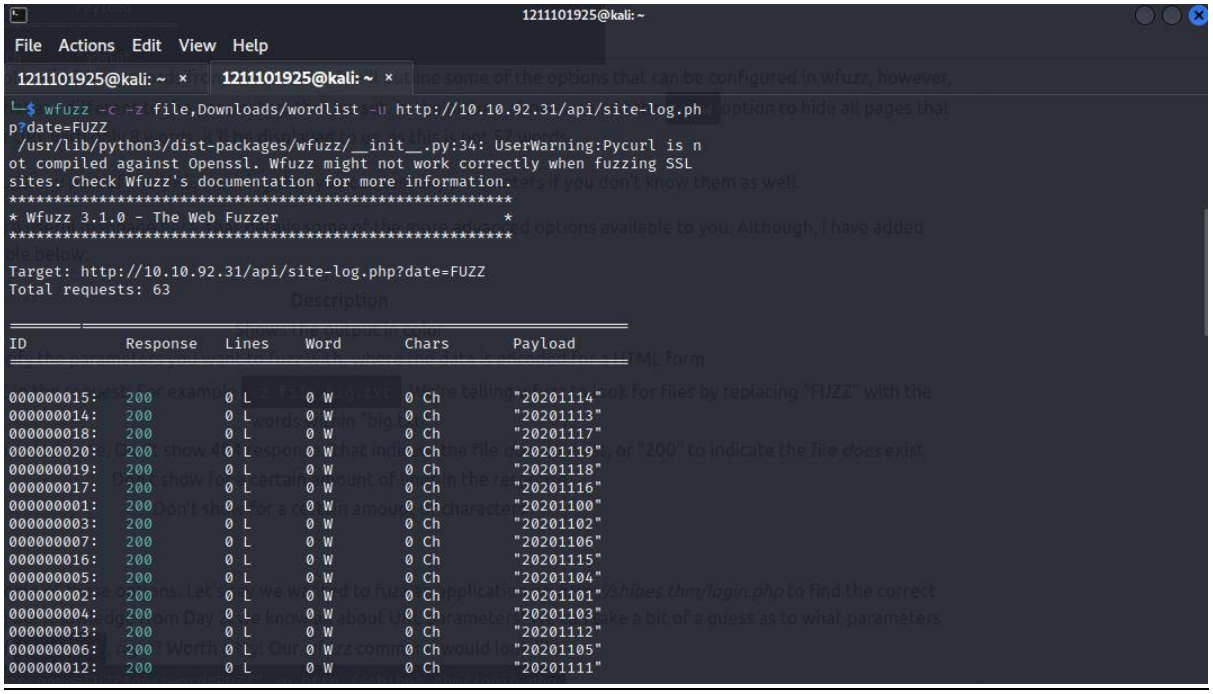
Index of /api

Name	Last modified	Size	Description
Parent Directory		-	
site-log.php	2020-11-22 06:38	110	

Apache/2.4.29 (Ubuntu) Server at 10.10.94.97 Port 80

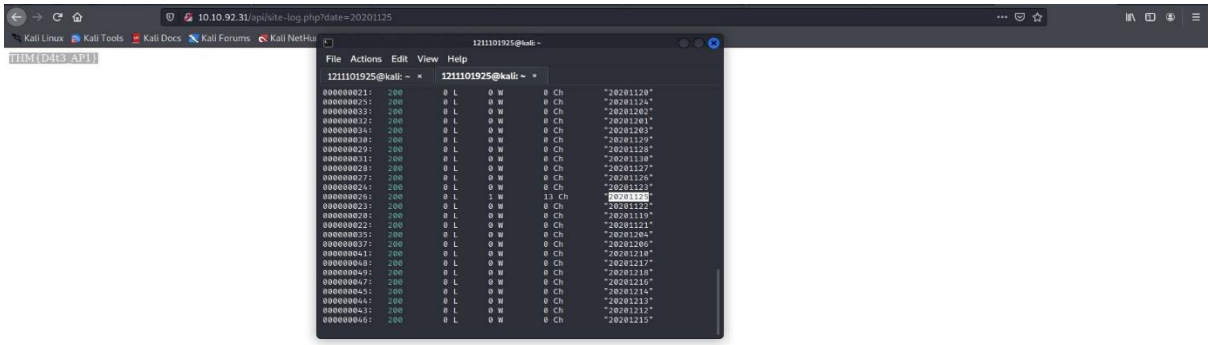
Question 3:

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



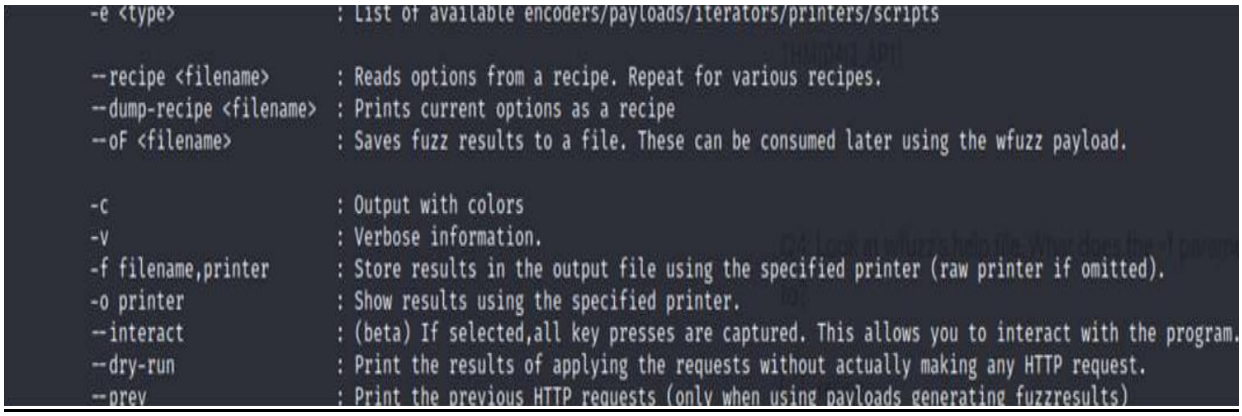
```
1211101925@kali: ~
File  Actions  Edit  View  Help
1211101925@kali: ~ ×   1211101925@kali: ~ ×
└─$ wfuzz -c -z file,Downloads/wordlist -u http://10.10.92.31/api/site-log.ph
p?date=FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is n
ot compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL
sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.92.31/api/site-log.php?date=FUZZ
Total requests: 63

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000015:   200        0 L      0 W        0 Ch        "20201114"
000000014:   200        0 L      0 W        0 Ch        "20201113"
000000018:   200        0 L      0 W        0 Ch        "20201117"
000000020:   200        0 L      0 W        0 Ch        "20201119"
000000019:   200        0 L      0 W        0 Ch        "20201118"
000000017:   200        0 L      0 W        0 Ch        "20201116"
000000001:   200        0 L      0 W        0 Ch        "20201100"
000000003:   200        0 L      0 W        0 Ch        "20201102"
000000007:   200        0 L      0 W        0 Ch        "20201106"
000000016:   200        0 L      0 W        0 Ch        "20201115"
000000005:   200        0 L      0 W        0 Ch        "20201104"
000000002:   200        0 L      0 W        0 Ch        "20201101"
000000004:   200        0 L      0 W        0 Ch        "20201103"
000000013:   200        0 L      0 W        0 Ch        "20201112"
000000006:   200        0 L      0 W        0 Ch        "20201105"
000000012:   200        0 L      0 W        0 Ch        "20201111"
```

Go to correct post for the flag.



Question 4:

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



METHODOLOGY:

When we started the machine, it gave us an Ip address that leads us to a login page which we have to register and login in order to obtain the first cookie by using browser developer tool by pressing f12. Then, we open the command prompt at kali and turn the vpn. we type “gobuster dir <rest of command>” to download the GoBuster. But before download the gobuster, we must make sure that the kali must have the wordlist. Then, I write the command “gobuster dir -u” ad put our Ip address to make sure it connected to the website. After we put the command, it will run and show the API. It shows “http://10.10.237.0”. Then, we copy and paste to other tab.it will show us the file what they have at that API directory. After we get the file at API directory, we use that to find the flag.

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

Tools used: Kali Linux, Firefox, BurpSuite

Solution/Walkthrough:

Question 1:

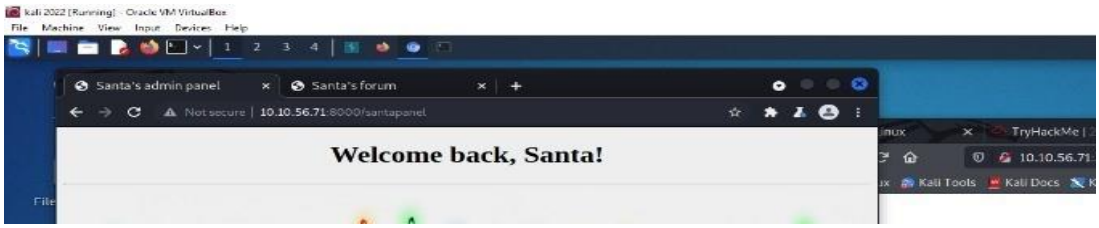
What is the default port number for SQL Server running on TCP?

Applies to: SQL Server (all supported versions)

This topic describes how to configure an instance of the SQL Server Database Engine to listen on a specific fixed port by using the SQL Server Configuration Manager. If enabled, the default instance of the SQL Server Database Engine listens on TCP port 1433. Named instances of the Database Engine and SQL Server Compact are configured for dynamic ports. This means they select an available port when the SQL Server service is started. When you are connecting to a named instance through a firewall, configure the Database Engine to listen on a specific port, so that the appropriate port can be opened in the firewall.

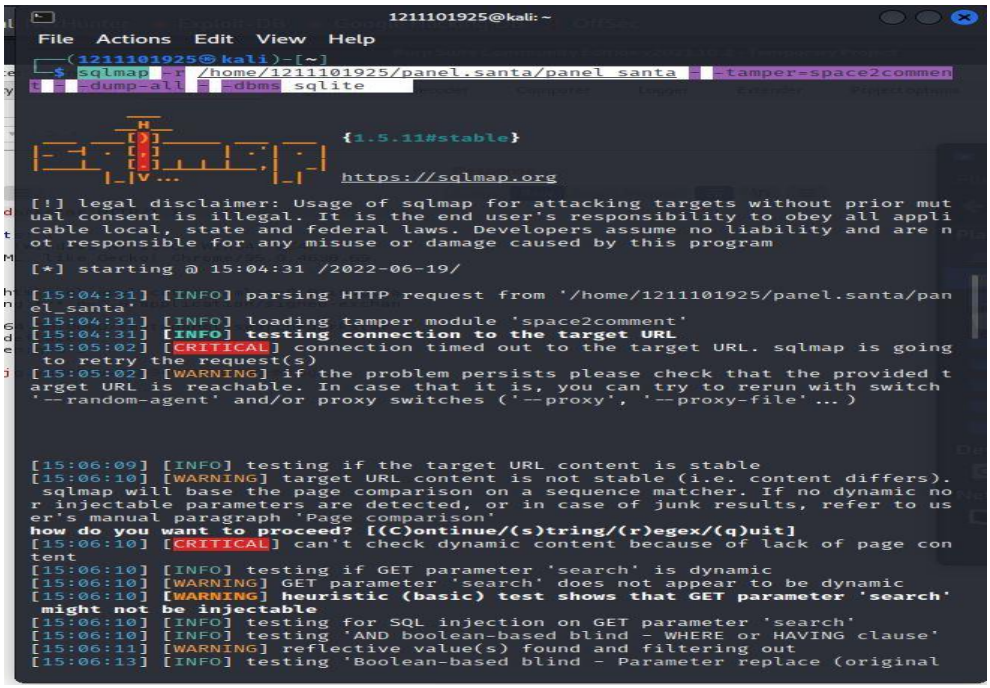
Question 2:

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



Question 3:

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



Question 4:

How many entries are there in the gift database?

```
[15:06:20] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/h
ome/1211101925/.local/share/sqlmap/output/10.10.164.58/dump/SQLite_masterdb/h
idden_table.csv'
[15:06:20] [INFO] fetching columns for table 'sequels'
[15:06:20] [INFO] fetching entries for table 'sequels'
Database: <current>
Table: sequels
[22 entries]
```

Question 5:

What is James' age?

kid	age	title
James	8	shoes
John	4	skateboard

Question 6:

What did Paul ask for?

Donald	4	fazer chocolate
Mark	17	wii
Paul	9	github ownership
James	8	finnish-english dictionary
Steven	11	laptop

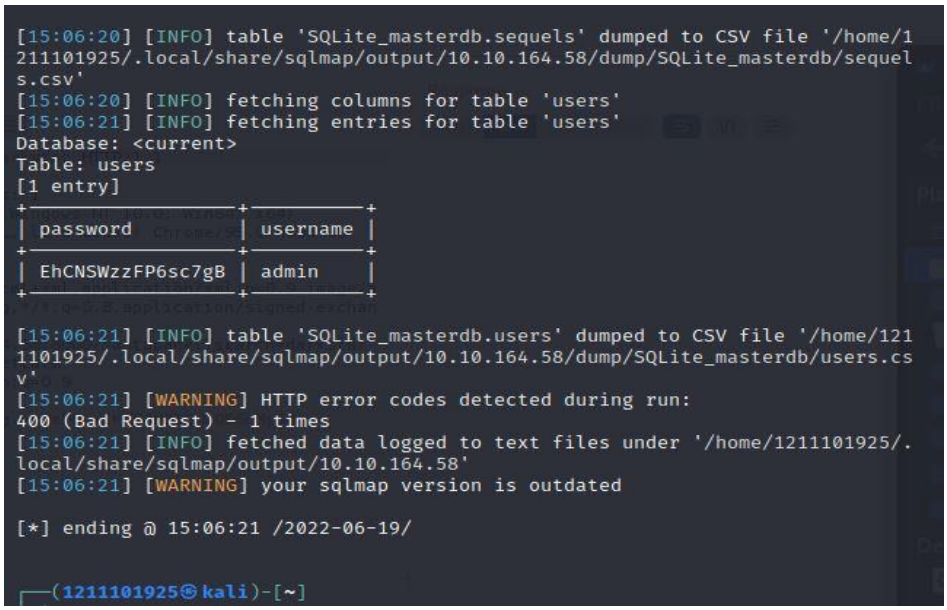
Question 7:

What is the flag?

```
1211101925@kali: ~
File  Actions  Edit  View  Help
[15:06:20] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+-----------------------------------+
| flag                              |
+-----------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----------------------------------+
```

Question 8:

What is admin's password?



METHODOLOGY:

To solve this problem, we need to go to the website. The panel consist of two words. After a few try and errors, the name of the secret panel is “santapanel”. After that, we were taken to a secret panel which says hello stranger. To log in, we use “admin” or “true - -“ for username and admin for the password. We were directed to the page that said “Welcome back, Santa” . Burp and intercept were on, we entered a name. then, we were directed to Burpsite and save the file. Afterwards, we use sql map command in our terminal to look at the file’s data. A list of 22 entries were displayed at santa’s sqlite database. After enough observations, we saw tha jame’s age is eight years old and paul wished for santa to give him github ownership. We also encountered with a hidden table with the flagand a table with a password and username for the page