PSP0201 Week 2 Writeup

Group Name: Gold
Members:

ID	Name	Role
1211101707	Nur’aina Binti Ikhwan Moeid	Leader
1211103984	Nur Afreen Junaidah Binti Noorul Mohamed Eliyas	Member
1211101519	Aisyah Binti Ahmad Komarolaili	Member
1211102590	Nur Hanisah Binti Mohd Pauzi	Member

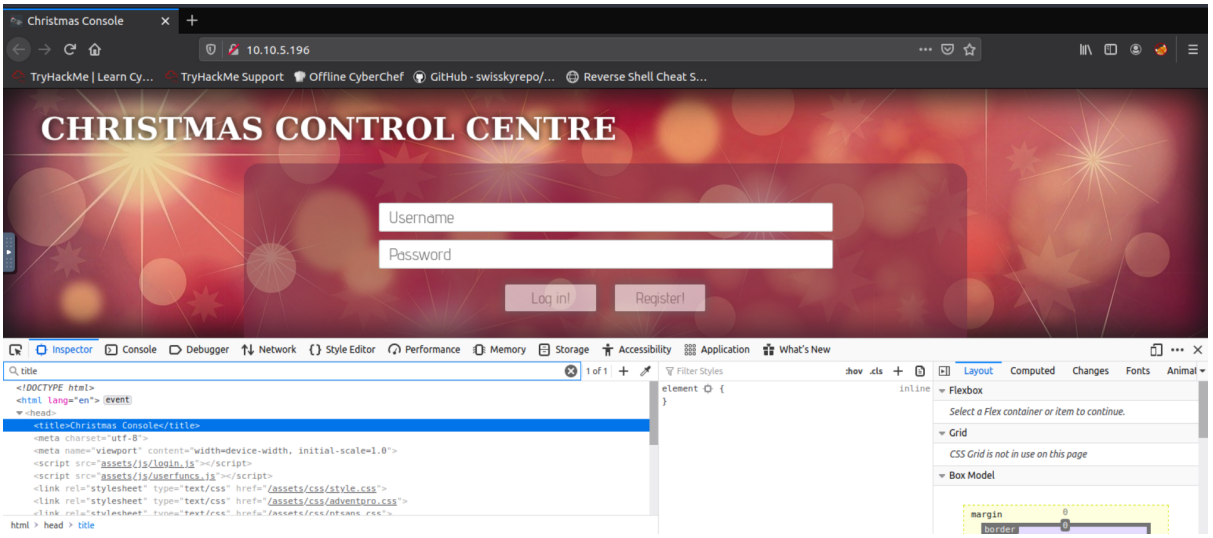
Day 1: Web Exploitation – A Christmas Crisis

Tools used: Kali Linux, Firefox

Solution/walkthrough:

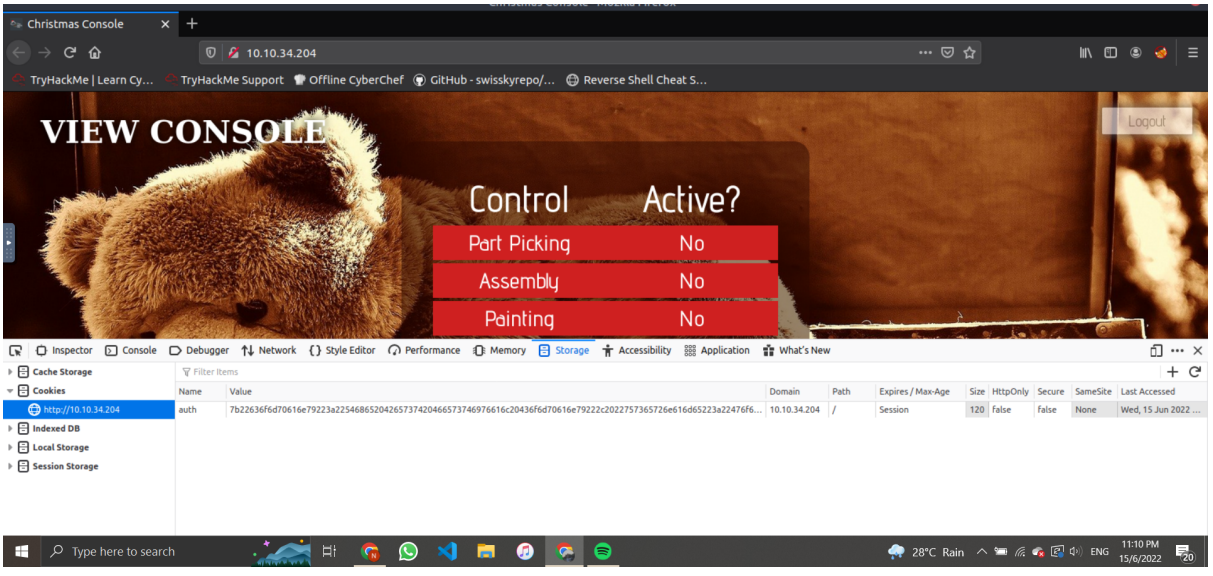
Question 1

Inspect the website. What is the title of the website? -Christmas Console



Question 2

What is the name of the cookie used for authentication? -auth



Question 3

In what format is the value of this cookie encoded? -hexadecimal

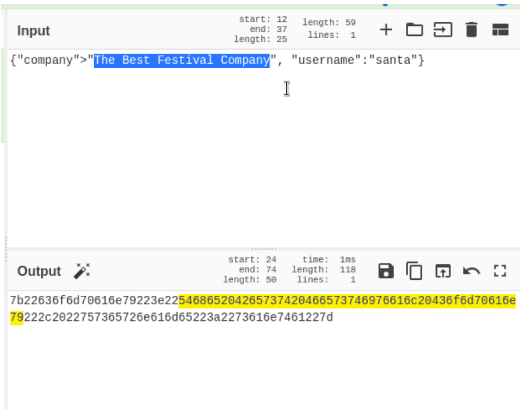
Question 4:

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

Question 5

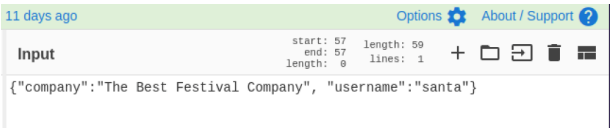
What is the value for the company field in the cookie?

-54686520426573742046657374697661 6c20436f6d70616e79



Question 6

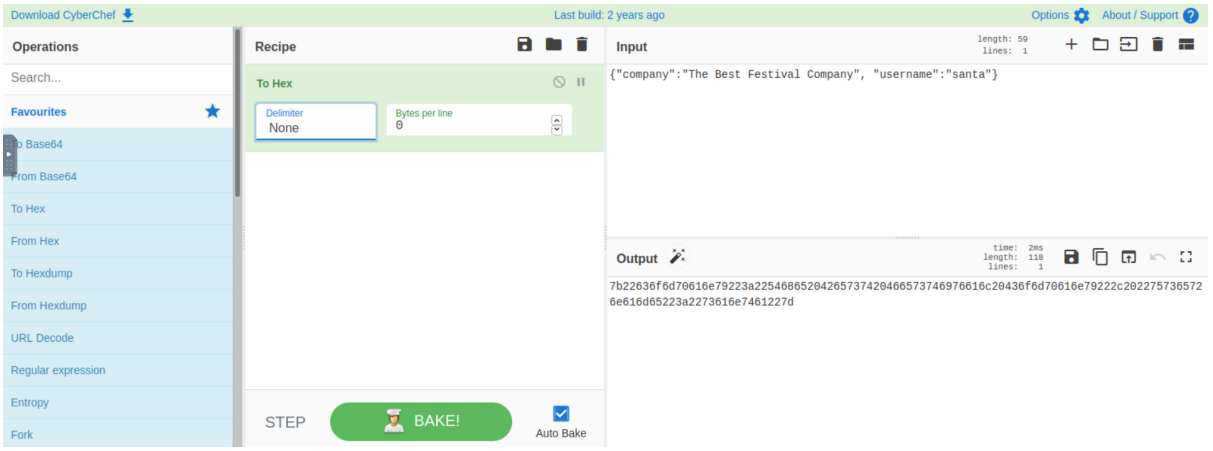
What is the other field found in the cookie? - username



Question 7

What is the value of Santa's cookie?

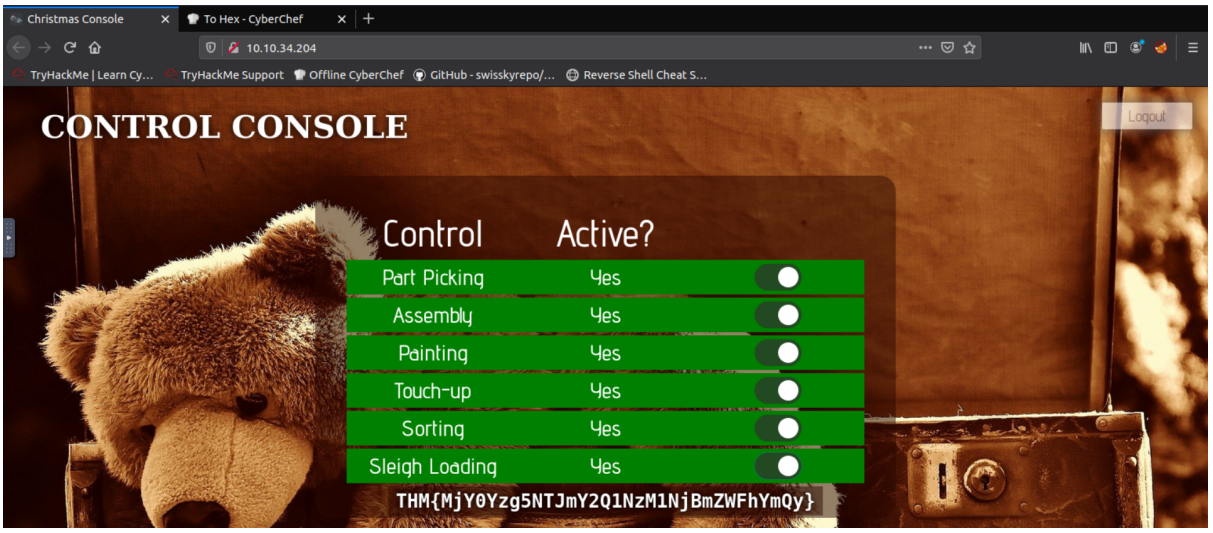
-7b22636f6d70616e79223a2254686520426573742046657374697661 6c20436f6d70616e79222c202757365726e616d65223a2273616e7461227d



Question 8

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

-THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}



Thought Process/ Methodology:

Firstly, we access the target machine where it brought us to a login/registration page. We create an account and login using the username and password we've created. After logging in, we inspect the website to get the tittle of the website. Then, we chose storage tab to view the site cookie. From there, we got the cookie value from the storage tab, with that we copy the value and open a new web browser, cyberchef. At cyberchef, we deduced the value to be a hexadecimal value and proceeded to convert it to text. Next, it state a JSON statement with username element where it is editable so we change the username from ours to santa's then convert it back to hexadecimal form. We decoded the new value we get after altered the username to santa's and replace the previous one at the storage tab. We refresh the page and get access into santa's account (administrator page) and enable all the controls and then the flag is shown.

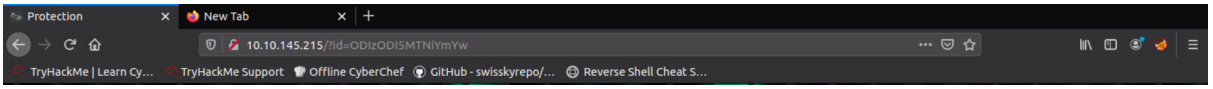
Day 2: Web Exploitation – The Elf Strikes Back!

Tools used: Kali Linux, Firefox

Solution/walkthrough:

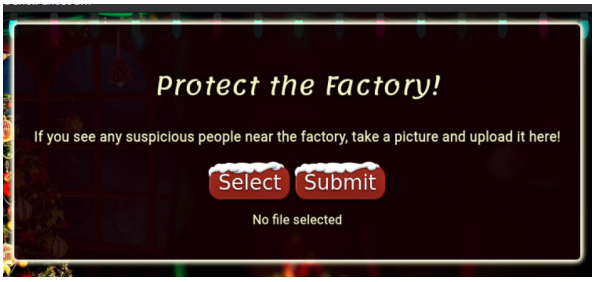
Question 1:

What string of text needs adding to the URL to get access to the upload page? -ODIzODI5MTNiYmYw



Question 2:

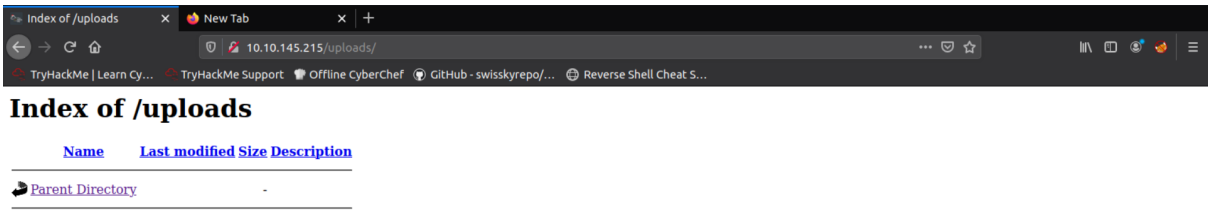
What type of file is accepted by the site? -Image




```
20          <h1>Protect the Factory!</h1>
21          <h2>If you see any suspicious people near the factory, take a picture and upload it here!</h2>
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>
```

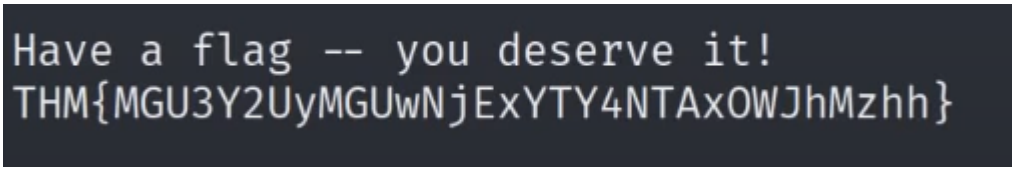
Question 3:

In which directory are the uploaded files stored? -uploads



Question 4:

What is the flag in /var/www/flag.txt? -THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}



Thought Process/ Methodology:

We connect to the vulnerable VM's upload page, by applying the assigned ID we're given earlier in the exercise and applying it in our URL. When we're going through the page, we found that this server only accepts images. Then, we take the php script used for establishing a reverse shell and make a copy, and change the reverse shell script with the relevant IP address and Port number. After that, we change the filetype to include a dot and jpeg to make the service accepting an image file. Then, we use /uploads/ tools by stating the ip address followed by /uploads/ in the web browser to figure out where in the directory that file has been placed. Next, we use the netcat on our AttackBox "listen" for the shell connection request from our script. When we we click the php script it simply activate it. Lastly, we use our reverse shell to navigate around and find the flag.

Day 3: Web Exploitation – Christmas Chaos

Tools used: Kali Linux, Firefox, Burpsuite

Solution/walkthrough:

Question 1:

What is the name of the botnet mentioned in the text that was reported in 2018? - Mirai

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:

How much did Starbucks pay in USD for reporting default credentials according to the text? -$250

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:

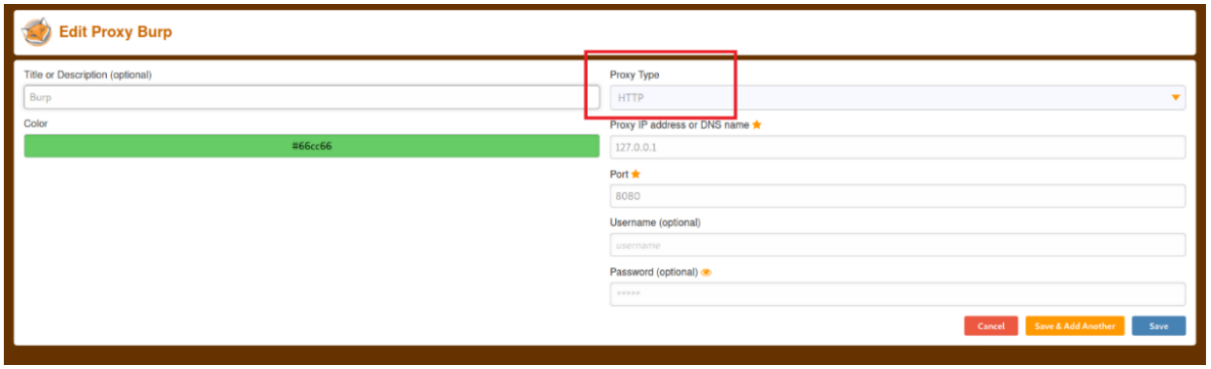
Read the report from Hackerone ID:804548 - who was the agent assigned from the Dept of Defense that disclosed the report on Jun 25th? - ag3nt-j1

Question 4:

Examine the options on FoxyProxy on Burp. What is the port number for Burp? - 8080

Question 5:

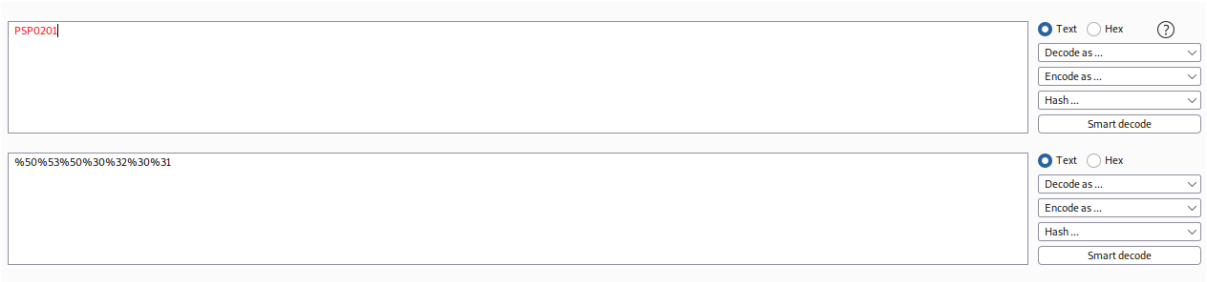
Examine the options on FoxyProxy on Burp. What is the proxy type? - HTTP



Question 6:

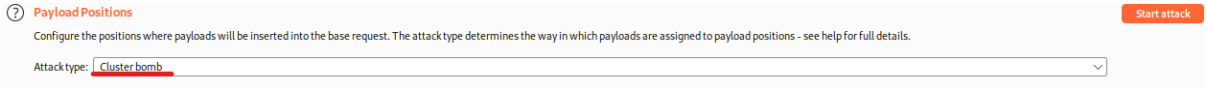
Experiment with decoder on Burp. What is the URL encoding for "PSP0201"? -

%50%53%50%30%32%30%31



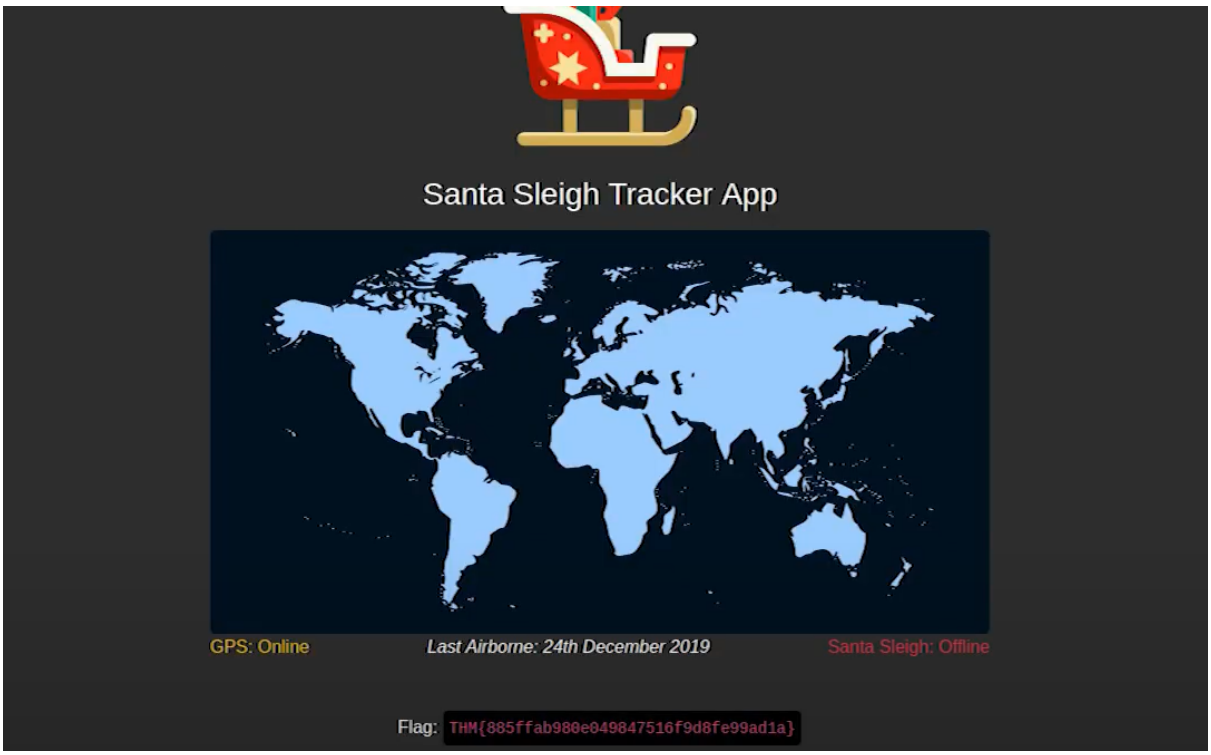
Question 7:

Look at the list of attack type options on intruder. Which of the following options matches the one in the description? - Cluster Bomb



Question 8:

What is the flag? - THM{885ffab980e049847516f9d8fe99ad1a}



Thought Process/ Methodology:

Firstly, we start the attackbox and launch the Burpsuite and then start Burp. at the same time, open firefox and put the IP address that was given in try hack me after that start loading. Next, click on the FoxyPoxy extension and select Burp.Back to the Burpsuite, click on Proxy and make sure that the intercept is on make sure just that this is pressed navigate to your chosen website. After that burp suite is waiting for us so we can see that we have our request here which is a normal to get request and we have to forward it in order for the web page to actually load. Then go back to the web application and try to fill the form. We go back to BurpSuite and forward all and let it stop proxing all the traffic . close the intercept and then go back to the website and then refresh it go back again to BurpSuite and on the intercept back. Then click on send to intruder. Next, click on positions and change the attack type to cluster bomb then go to payloads and adds the username and password that given then start attack and wait for the results. Now go back again to the website and fill the form with the username and password and click sign in and there's a flag showing below the kind of map picture and we are done.

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

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

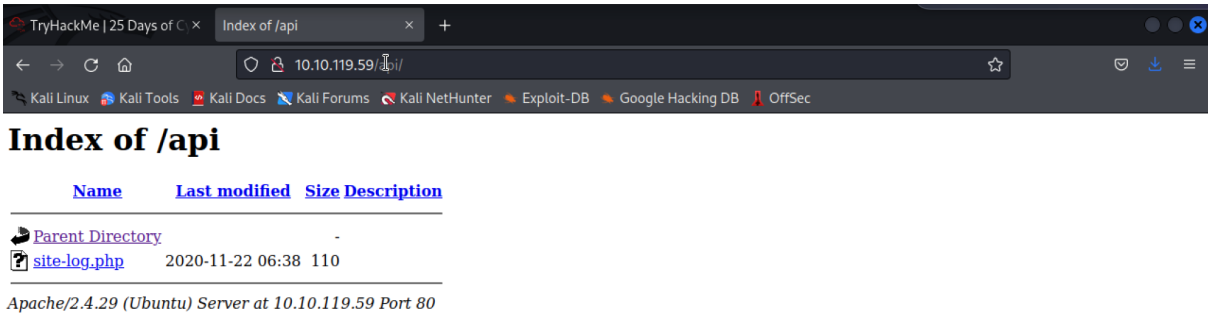
Let's bring this together and demonstrate some of these options. Let's say we wanted to fuzz an application on *http://shibes.thm/login.php* to find the correct credentials to the login form. After recalling our knowledge from Day 2, we know all about URL parameters! We can take a bit of a guess as to 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.

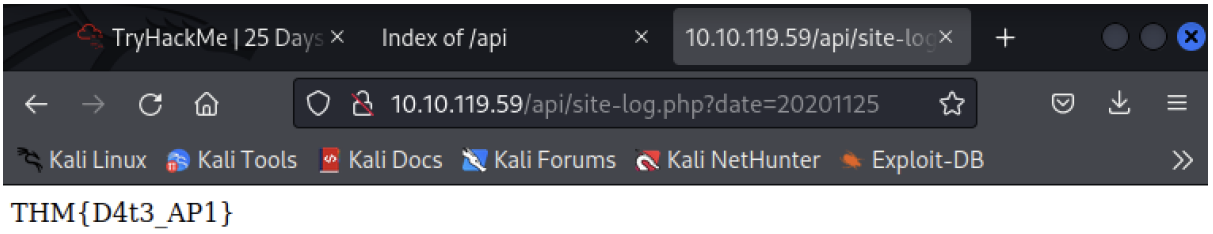
Question 2

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



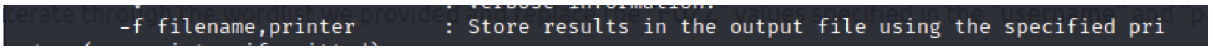
Question 3

Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post? - THM{D4t3_AP1}



Question 4

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



Thought Process/ Methodology:

Having accessed our target machines, we can see that our login page has been removed. But we can still find the API by using **goBuster** or **machines IP/api/** in our browser. After we found the file in the API directory, we can now **FUZZ** the date parameter. We can now use the date that we found, which in turn showed us the flag.

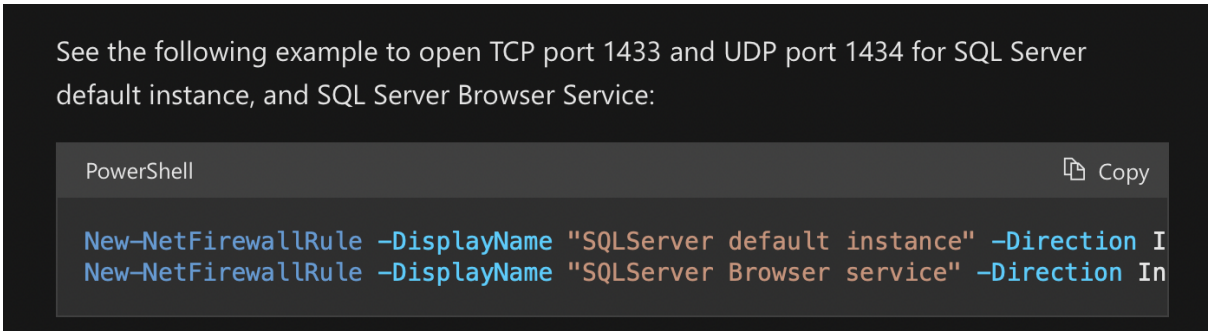
Day 5: Web Exploitation – Someone stole Santa's gift list!

Tools used: Kali Linux, Firefox

Solution/walkthrough:

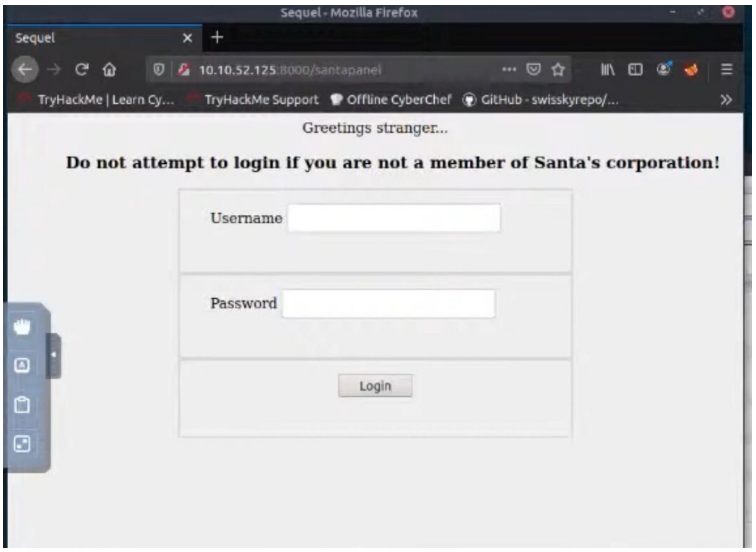
Question 1:

What is the default port number for SQL Server running on TCP? - 1433



Question 2:

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

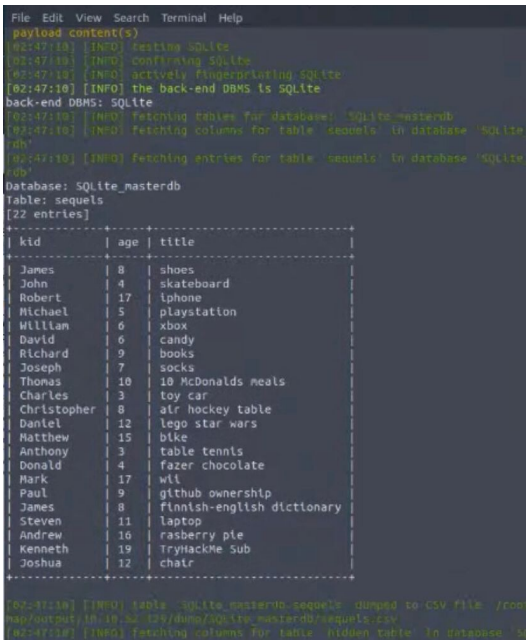


Question 3:

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? -22



Question 5:

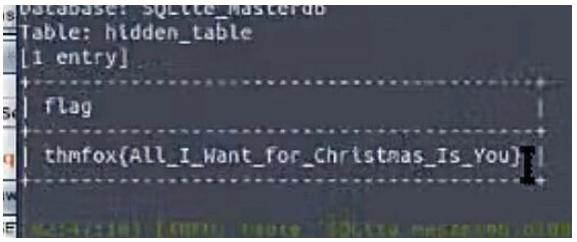
What is James' age? -8

Question 6:

What did Paul ask for? -github ownership

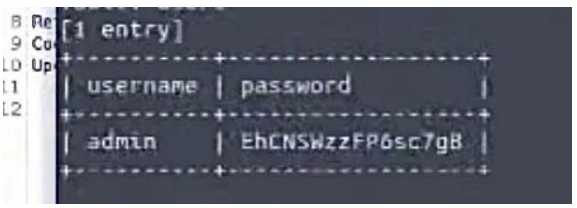
Question 7:

What is the flag? -thmfox{All_I_Want_for_Christmas_Is_You}



Question 8:

What is admin's password? -EhCNSWzzFP6sc7gB



Thought Process/ Methodology:

We start by typing in the IP address in the URL bar along with ":8000" which will bring us to Santa's Official Forum. Through the hint given in the question we can identify Santa's secret login panel which was "/santapanel". By adding this to the end of the URL, we are brought to the login page of Santa's panel. After typing in admin' or true– in the username section and admin in the password section we are able to login as santa. Using Burp Suite with proxy turned on, we can get request for the information we need to access the database in the terminal.