PSP0201

Week 2

Writeup

Group Name: F4urDeveloper

Members:

ID	NAME	ROLE
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	LEADER
1211104237	ALIA MAISARA BINTI SHAHRIN	MEMBER
1211102287	TERRENCE CHENG	MEMBER
1211101153	MISCHELLE THANUSHA JULIUS	MEMBER

Day 1: Web Exploitation – A Christmas Crisis

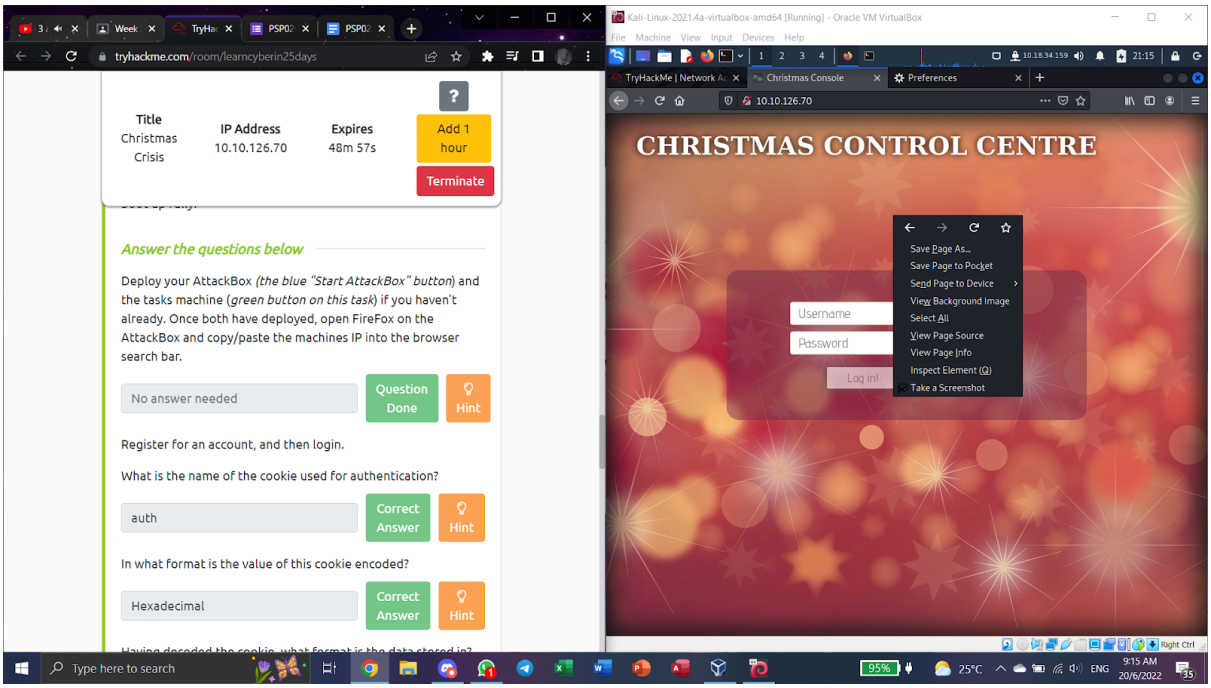
Tools used: Kali Linux, Firefox

Solution/Walkthrough:

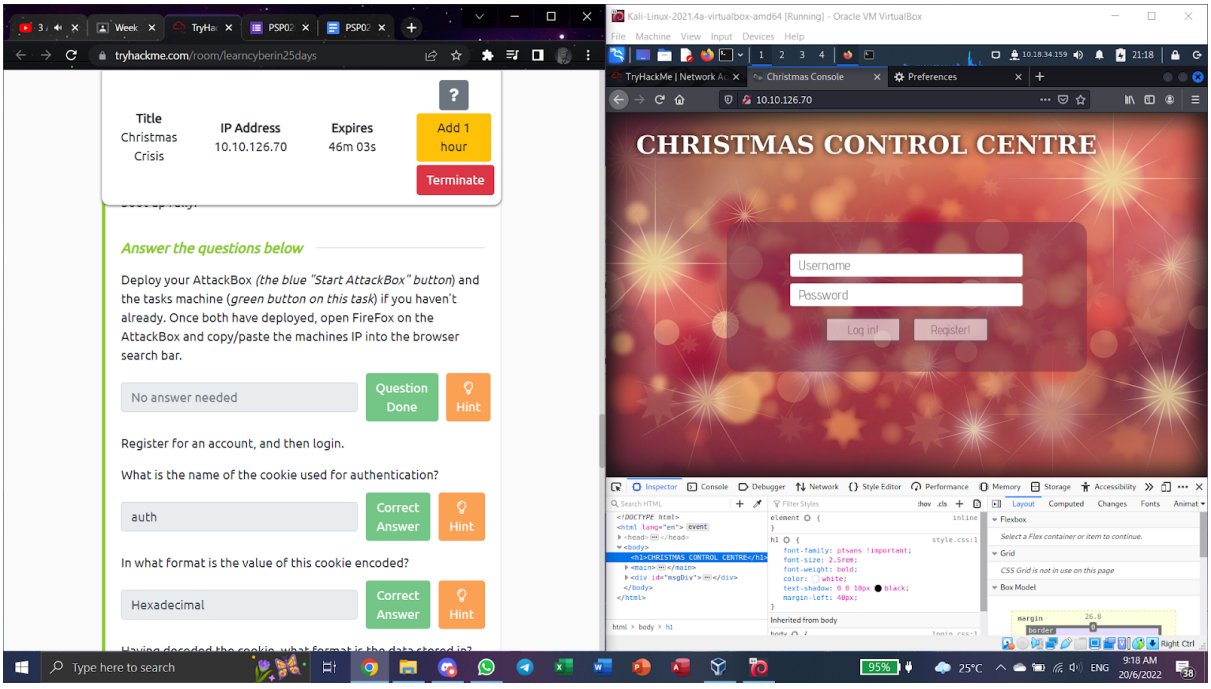
Question 1

Inspect the website. What is the title of the website?

Having access to the main page of the website as shown in the image below after typing in the given IP address, right click on the website and click ‘Inspect Element’ to find the title for the website.



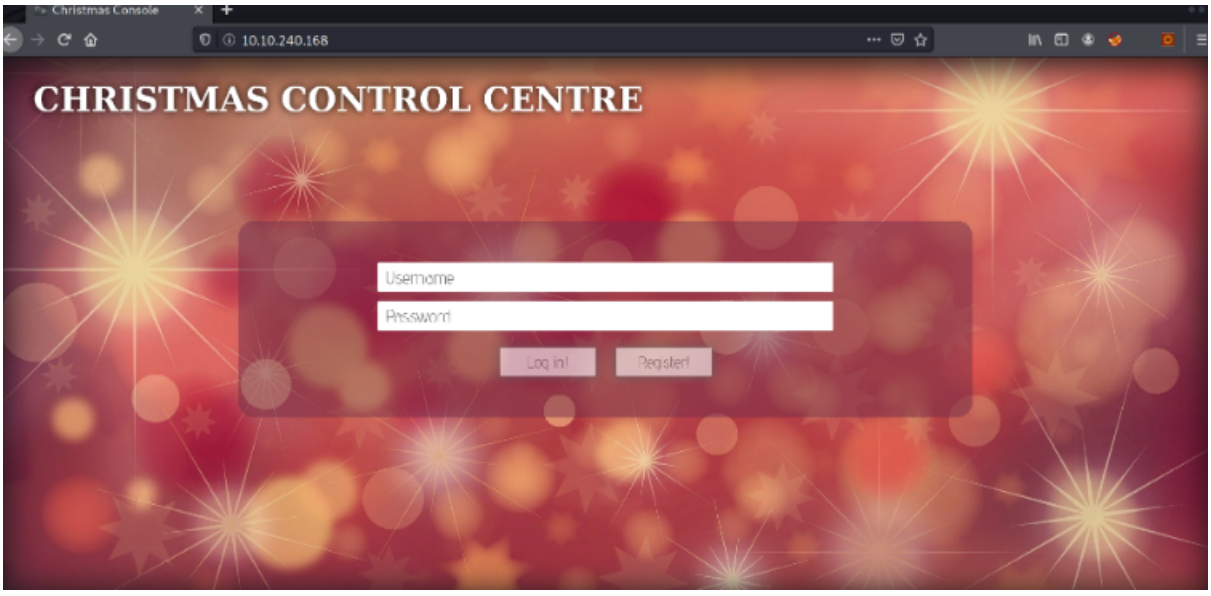
After clicking the ‘Inspect Element’ option, the title of the website can be identified at the top left bottom of the page on the <h1> tag (highlighted in blue for viewing purposes).

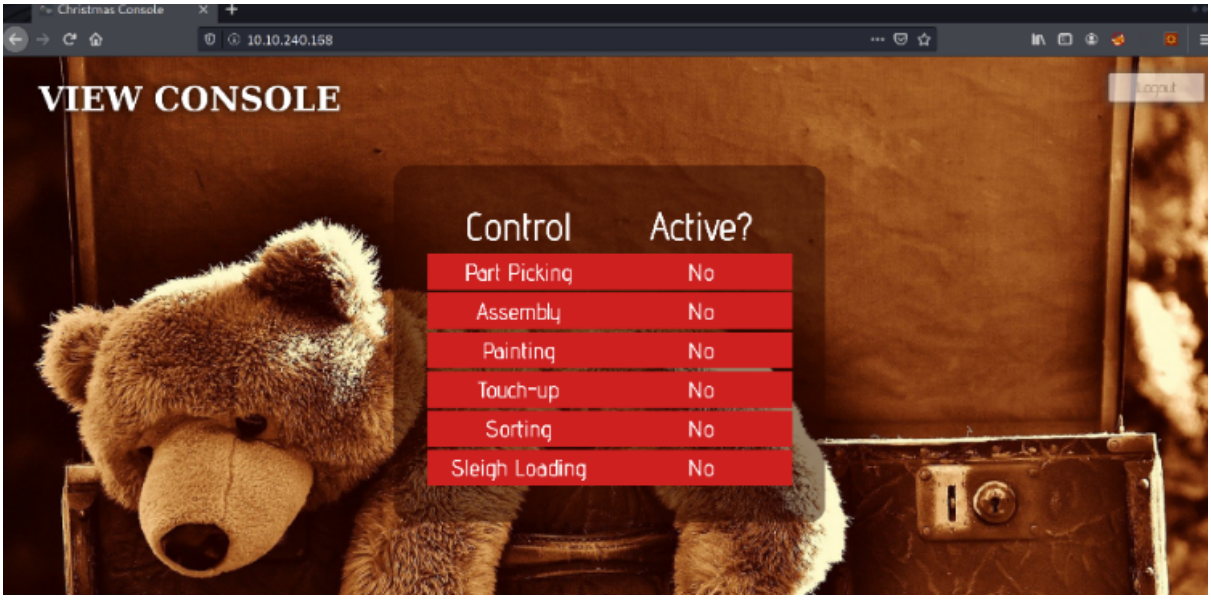


Question 2

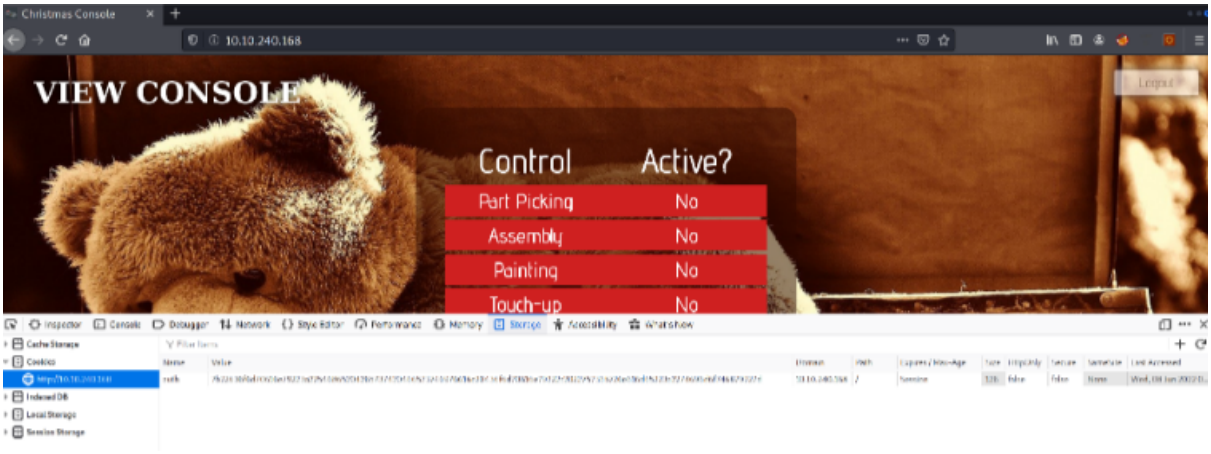
What is the name of the cookie used for authentication?

Register your own credentials and log in to the Christmas Control Centre. After doing so, it should lead you to the next page of the website titled ‘View Console’.





Open up the browser developer tools by right clicking the page and click the ‘Inspect Element’ option. After doing so, go to the ‘Storage’ tab to identify the value of the cookie used for authentication.



Question 3

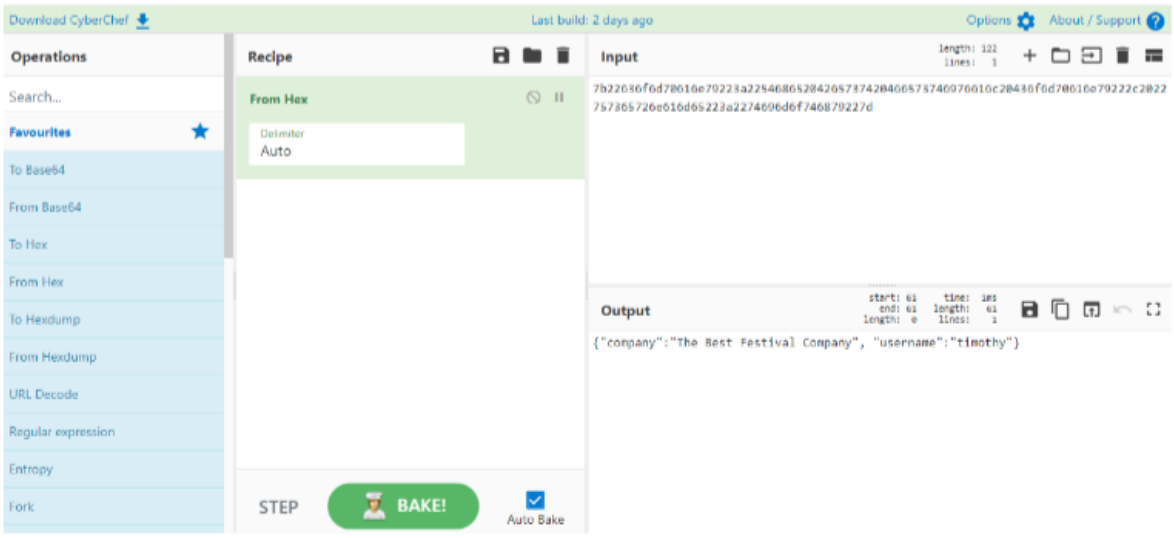
In what format is the value of this cookie encoded?

The answer for this particular question is obtainable via Binary 101 knowledge. As we can tell, base 2 and base 10 are not the correct format used for the cookie from previous question. Therefore, the only possible answer is base 16 which is ‘Hexadecimal’.

Question 4

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

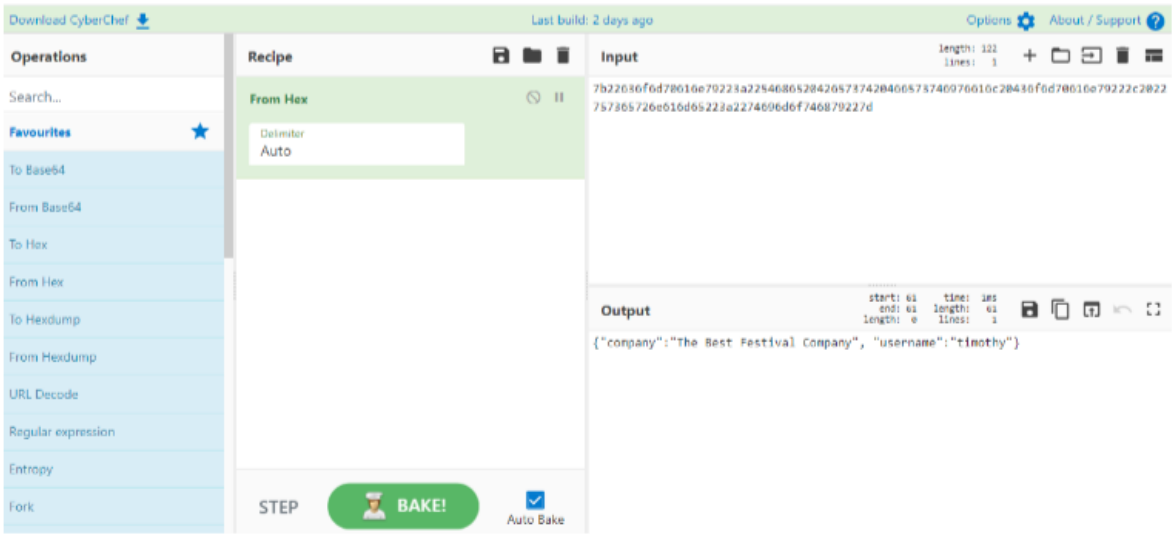
With the idea of the cookie’s value being hexadecimal, go to the Cyberchef website to decode the cookie and identify the format the data is stored in. Choose the ‘From Hex’ option and paste in the cookie’s value into the ‘Input’ section. The output should be the same as the image below. The opening and closing curly brackets with a key sets to a specific value tells us that the format the data is stored in is Javascript or JSON.



Question 5

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

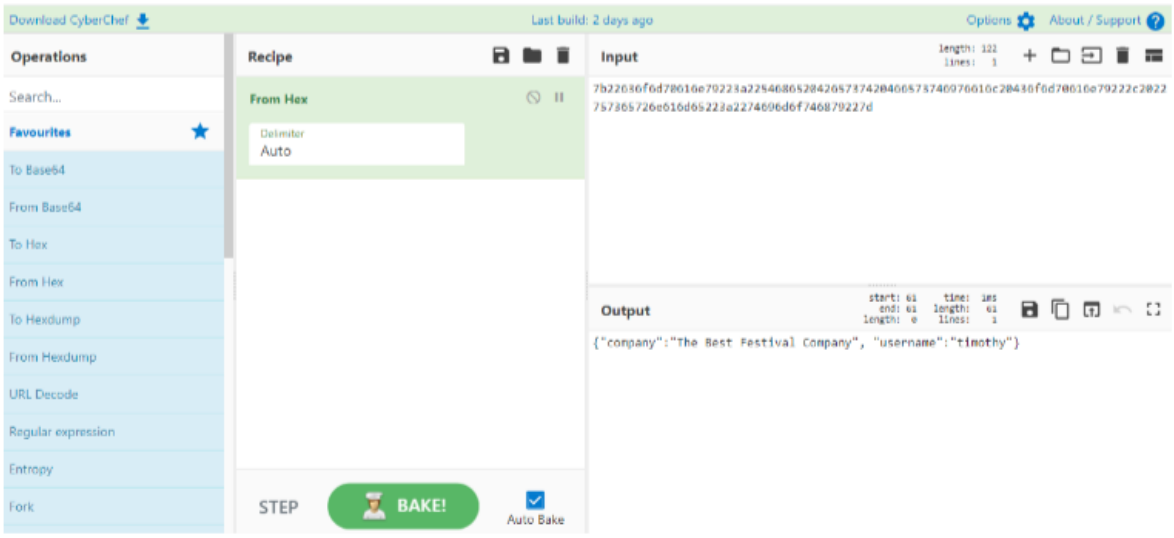
After decoding the cookie's value and identifying the format the data is stored in, the answer can be found on company (key) which is set to The Best Festival Company (value).



Question 6

What is the other field found in the cookie?

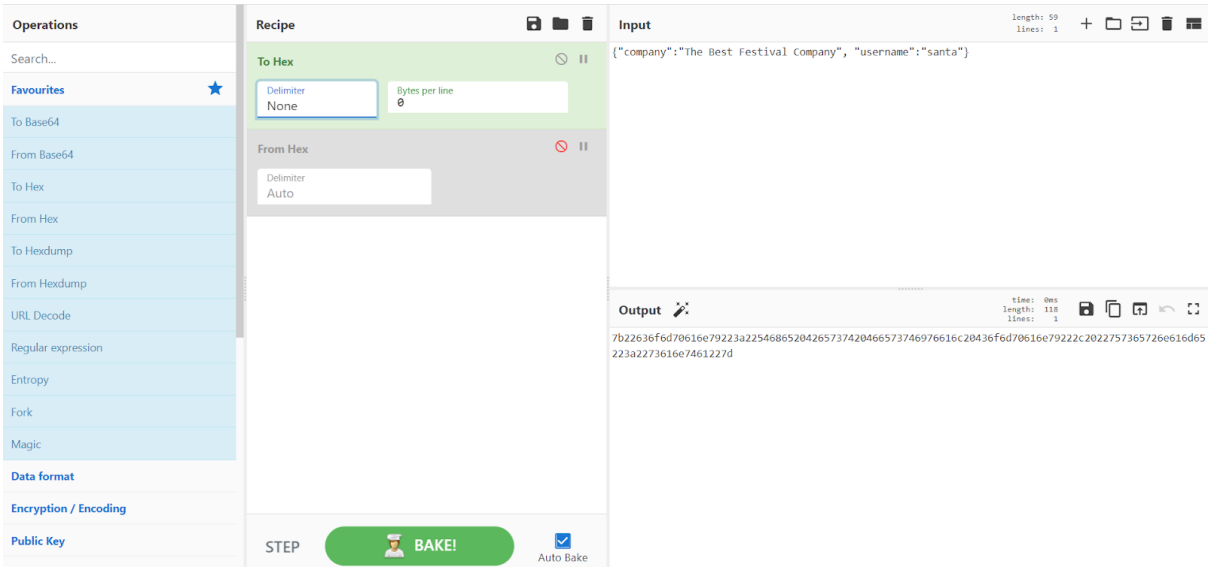
The other field can be identified by looking at the second key involved in the output. In this case, the second key should be 'username'.



Question 7

What is the value of Santa's cookie?

Still using Cyberchef, drag the 'To Hex' option to the recipe section and disable the 'From Hex' option to avoid any error for the value of Santa's cookie later. Copy the output from previous question and paste it inside the 'input' section. Change the username to santa to gain the value of Santa's cookie. By default, the delimiter is set to 'space' so changing it to 'none' is vital to get the value of Santa's cookies. The value can be seen in the 'output' section if every steps mentioned is done correctly.



Question 8

What is the flag you are given when the line is fully active?

After logging in and such, you should be given access to the controls, switch every controls you see on the page on and the flag should appear at the bottom of the page.

Thought Process/Methodology:

After typing in the IP address for the website titled Christmas Control Centre, we are able to inspect the website and identify the title for it. After that, we are able to register our own credentials and log into the website to gain access to the next page titled Control Console. Opening up the browser developer tools allows us to identify the cookie's value which is located under the Storage tab. Using our Binary 101 knowledge, we can deduce the value to be base 16 or hexadecimal. The value then can be converted using Cyberchef to identify the format of the data that is being stored in which is Javascript or JSON. Still using Cyberchef, to find the value of Santa's cookie, we can just change the username from our credentials to the word 'santa'. The final step for us to do is to enable every controls on the website page to let us identify the flag.

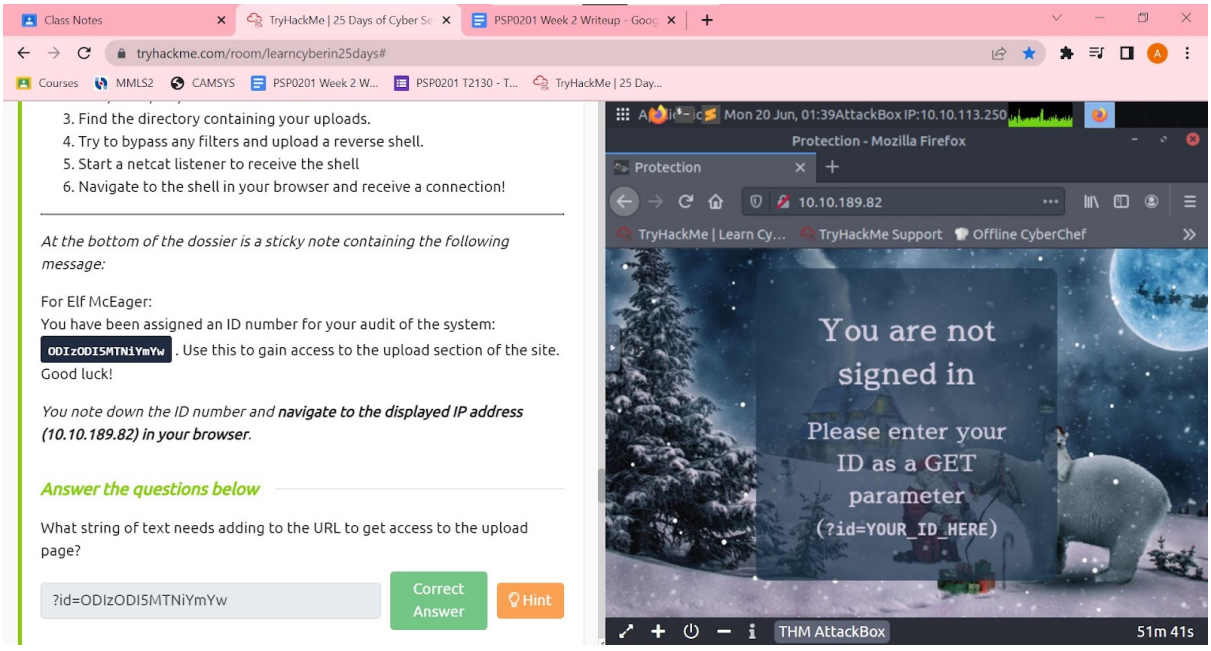
Day 2 : Web Exploitation - The Elf Strikes Back!

Tools use : THM Attackbox

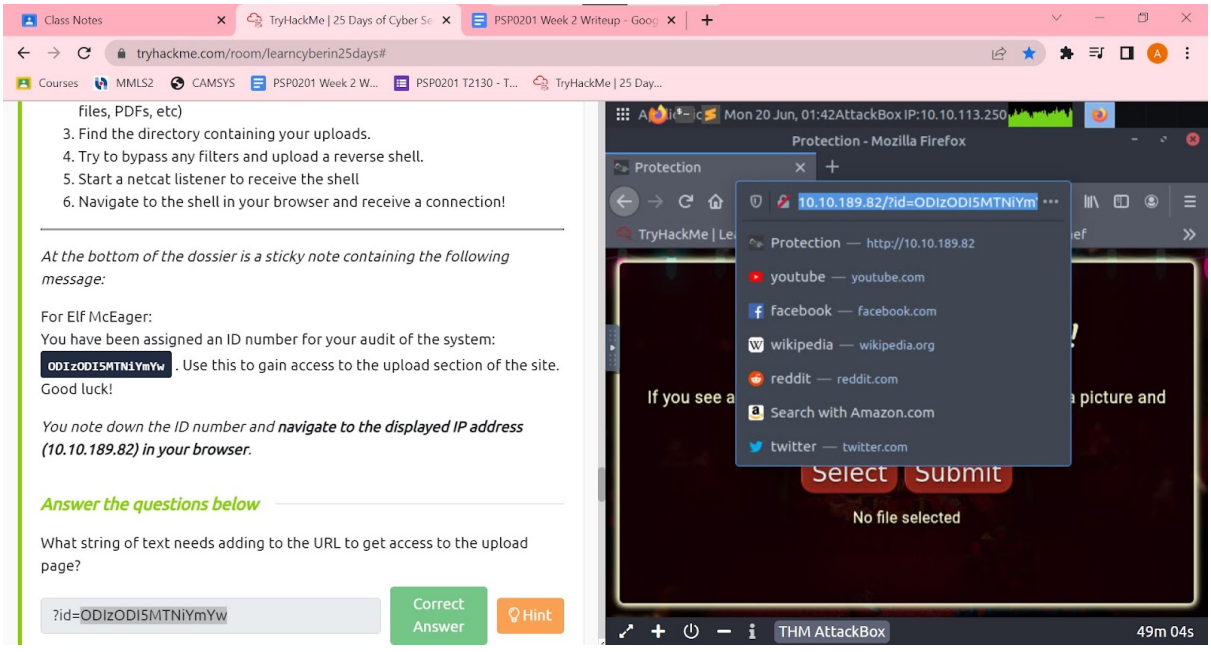
Solution/Walkthrough:

Question 1:

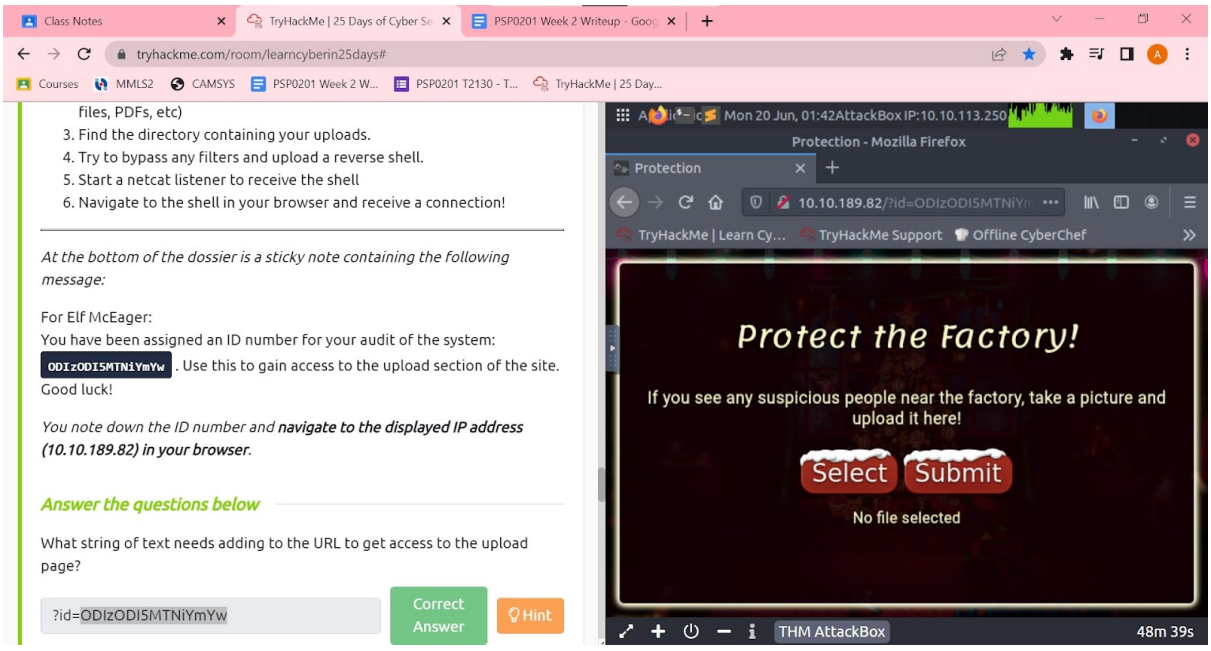
What string of text needs adding to the URL to get access to the upload page?



Insert the ip address of the victim

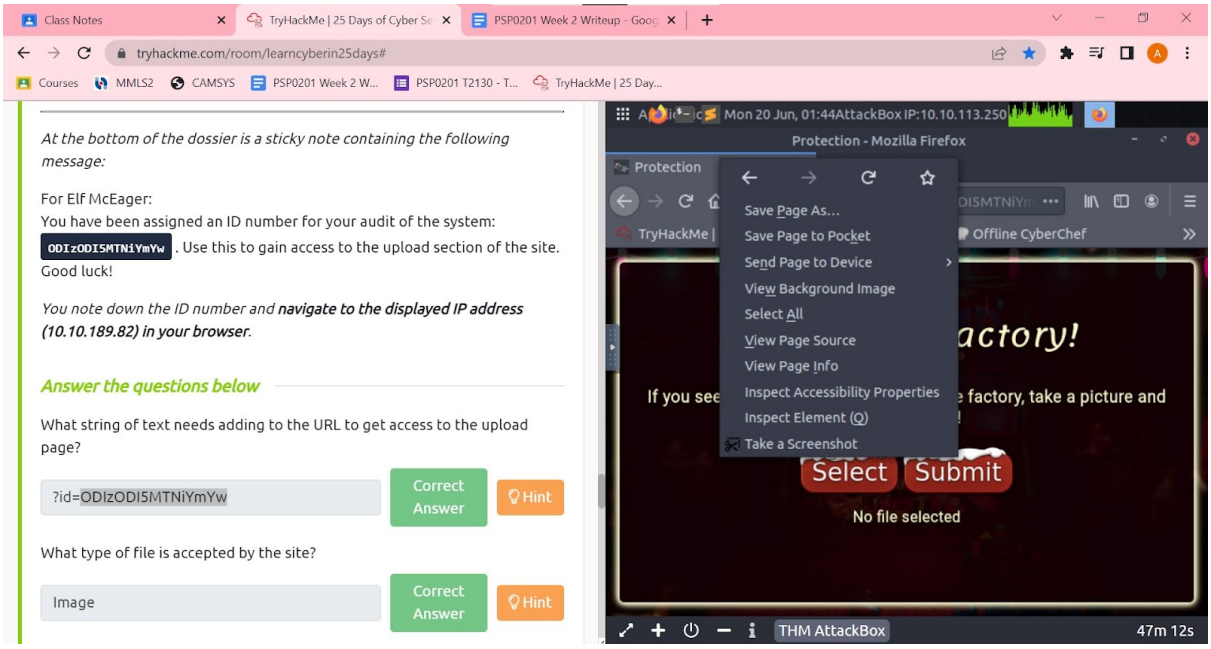


Insert the id number given by the website which is ?id=ODIzODI5MTNiYmYw after the victim's ip adress to get access to the upload page

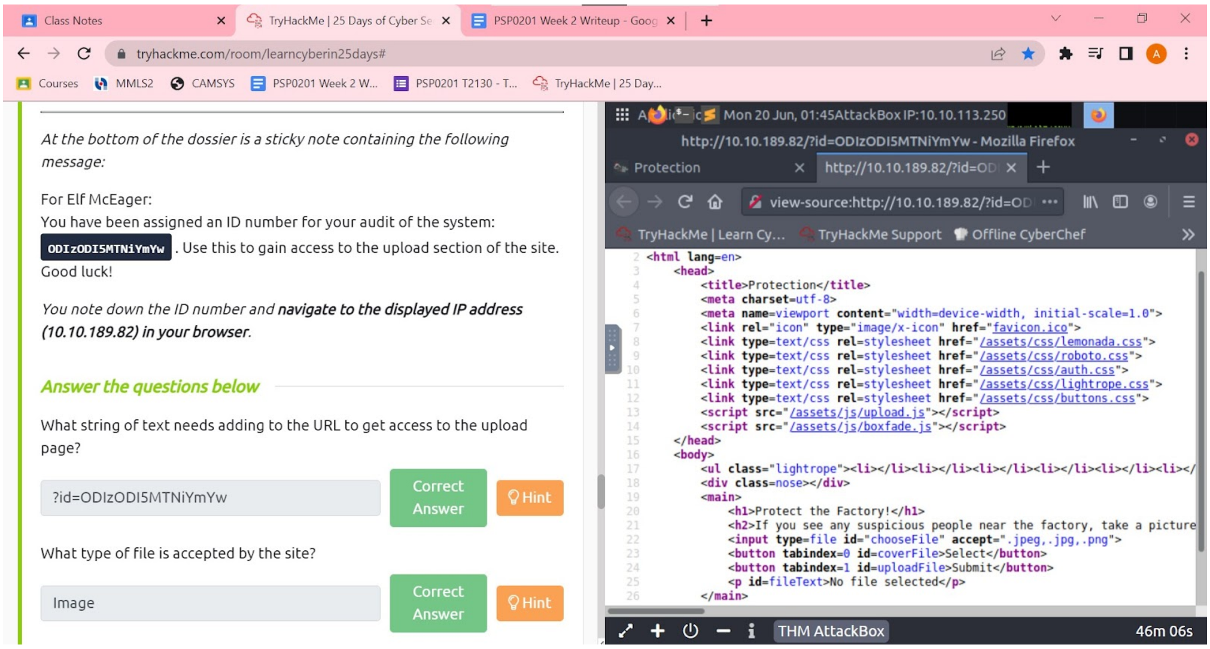


Question 2 :

What type of file is accepted by the site?



Double click the website and click on View Page Source

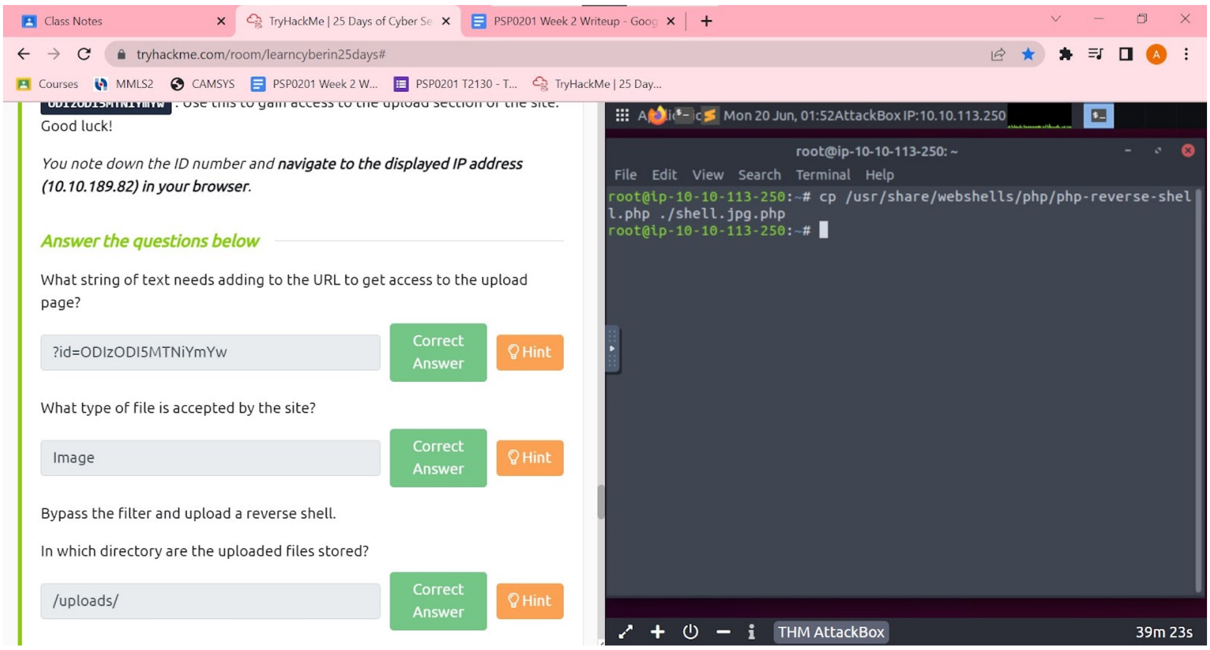


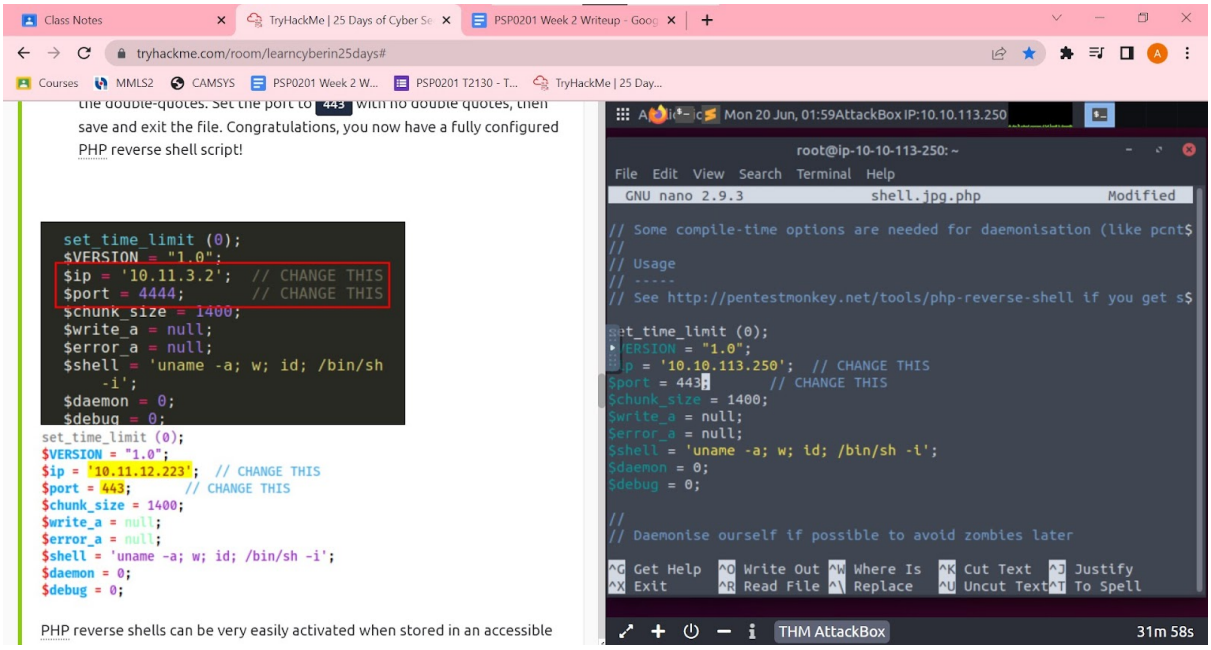
From the Page Source, we can see that the format of the file accepted is .jpeg , .jpg , .png , so the type of file accepted is image

Question 3:

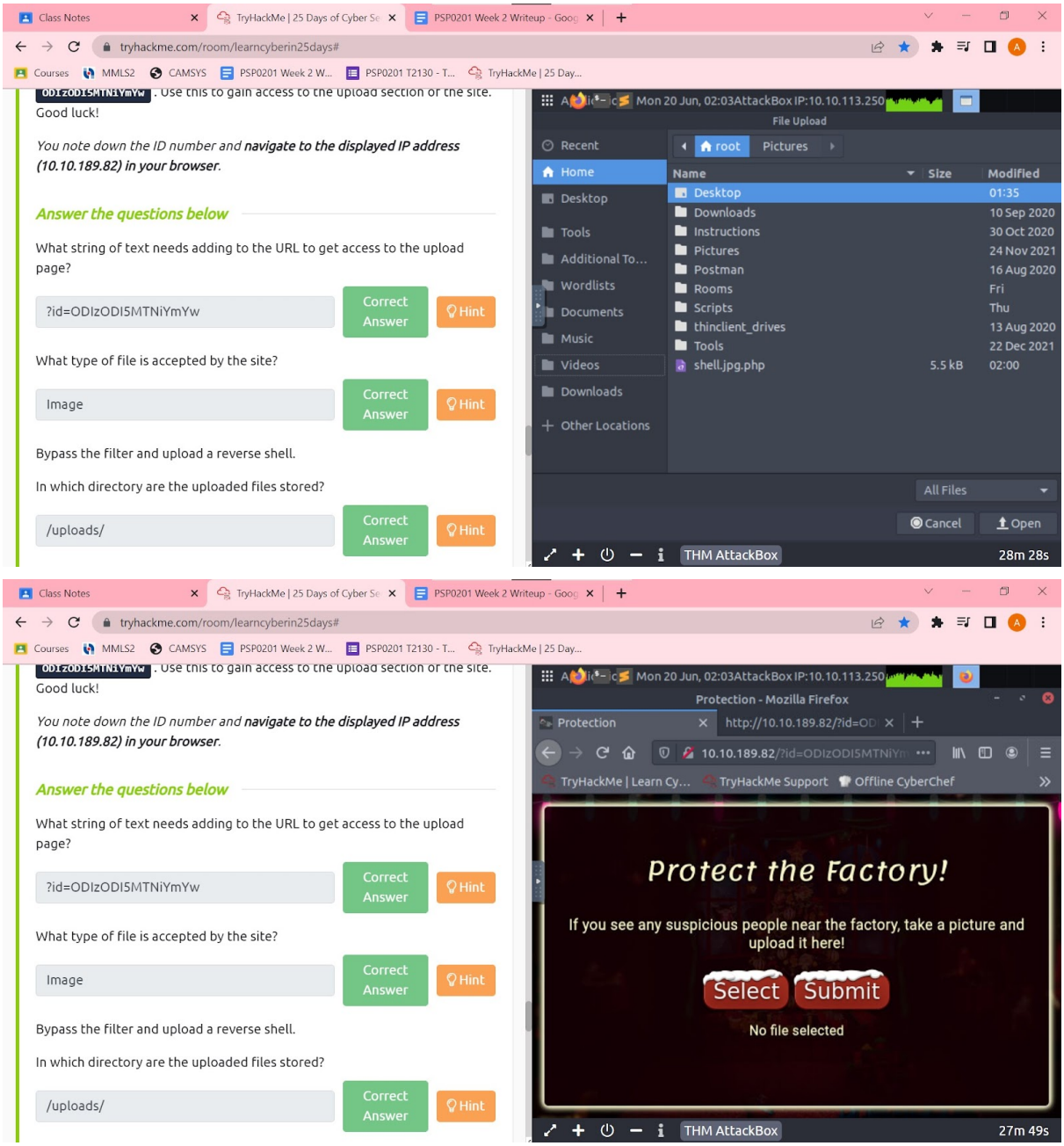
Bypass the filter and upload a reverse shell.

In which directory are the uploaded files stored?

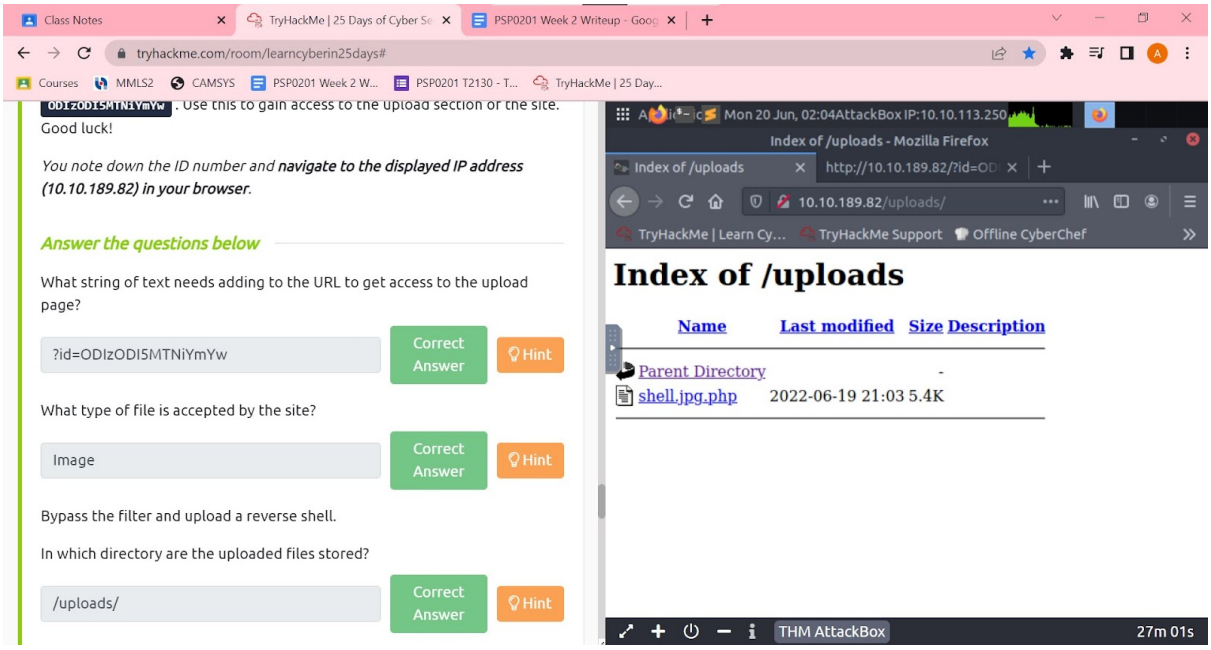




Change the $ip to the attacker’s ip address, and change the $port to 443, reverse shell is done



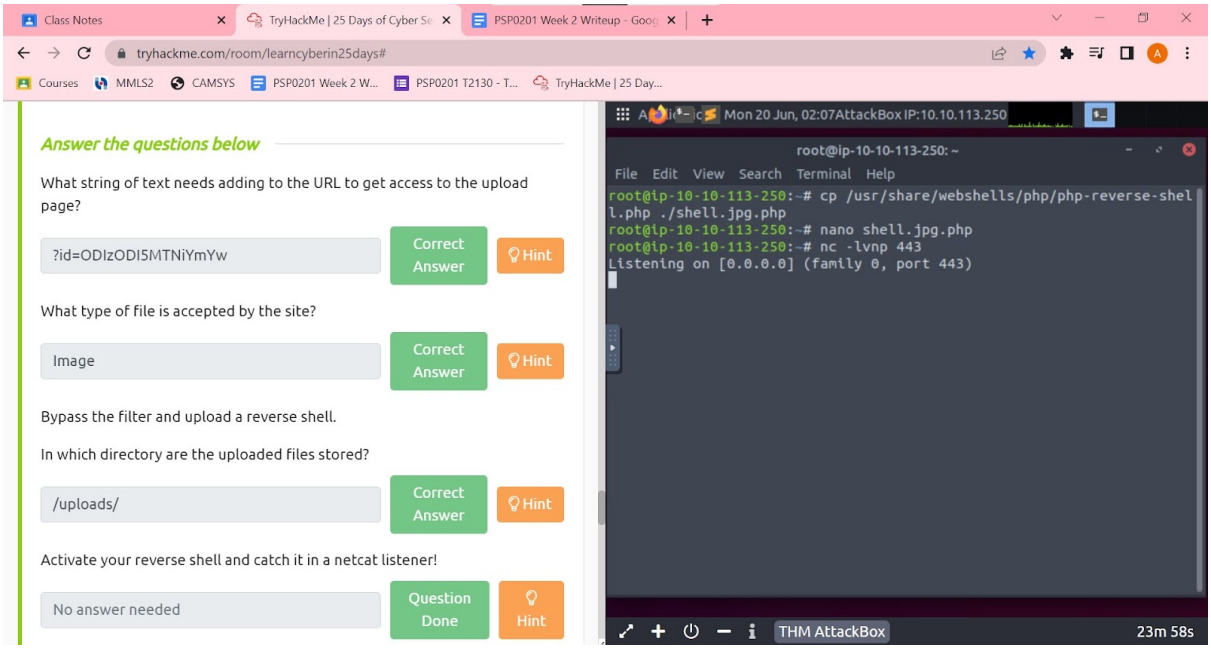
Upload the file that we want, in this case it’s shell.jpg.php

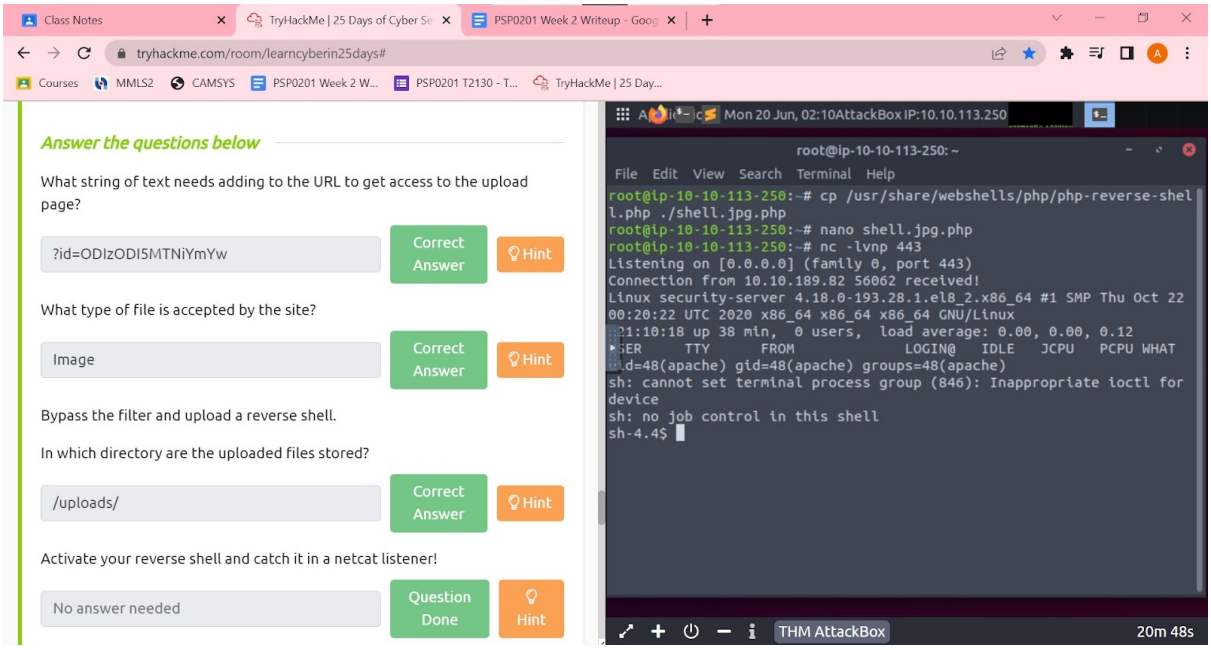


Try out some common directory for most websites, in this case the directory the uploaded file are stored by the site is /uploads/

Question 4 :

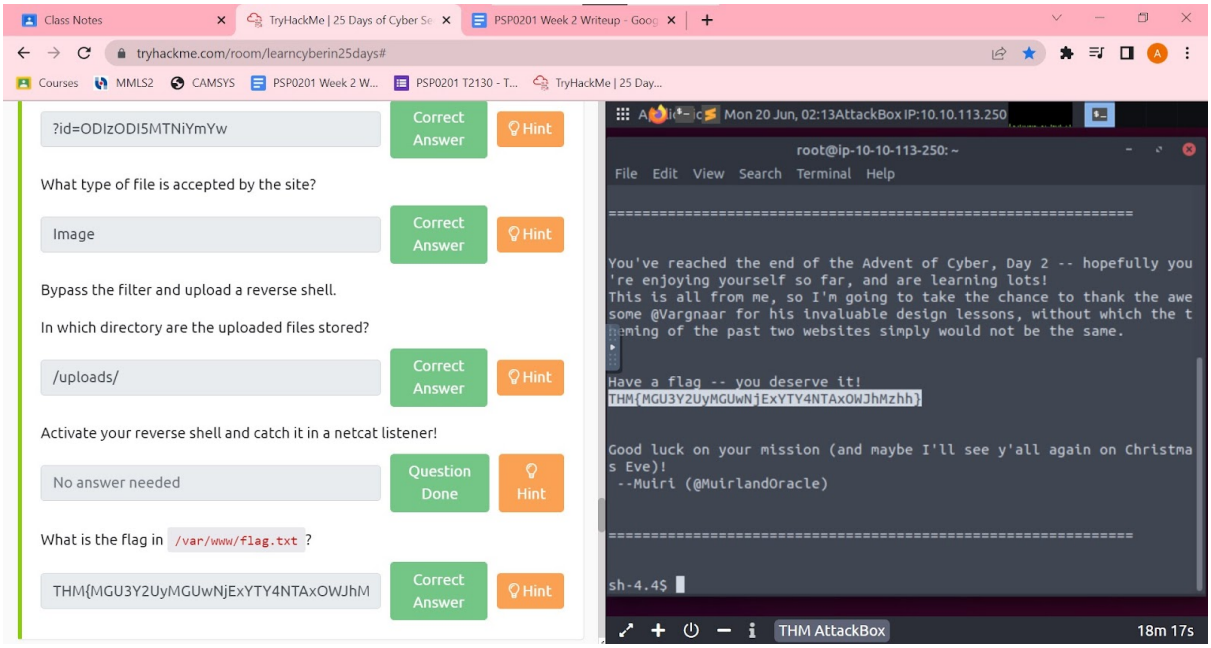
Activate your reverse shell and catch it in a netcat listener!





Question 5 :

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



Thought Process/Methodology:

We were given the GET parameter to access the website file upload point. To know what type of file that the website accepts, we opened Page Source and started analysing the type of file that can be uploaded, in this case it is image. It is also common that most websites use the same common upload file directory which is /uploads/ . After that, we bypassed the filters and uploaded a reverse shell. We also started a netcat listener to receive the reverse shell.

Day 3:Web Exploitation - Christmas Chaos

Solution/walkthrough

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

- Bypass a login form using BurpSuite

Authentication

Authentication is a process of verifying a users' identity, normally by credentials (such as a username, user id or password); to put simply, authentication involves checking that somebody really is who they claim to be. Authorization (which is fundamentally different to authentication, but often used interchangeably) determines what a user can and can't access; authorization is covered in tomorrow walkthrough, today's task focuses on authentication and some common flaws.

Default Credentials

You've probably purchased (or downloaded a service/program) that provides you with a set of credentials at the start and requires you to change the password after it's set up (usually these credentials that are provided at the start are the same for every device/every copy of the software). The trouble with this is that if it's not changed, an attacker can look up (or even guess) the credentials.

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

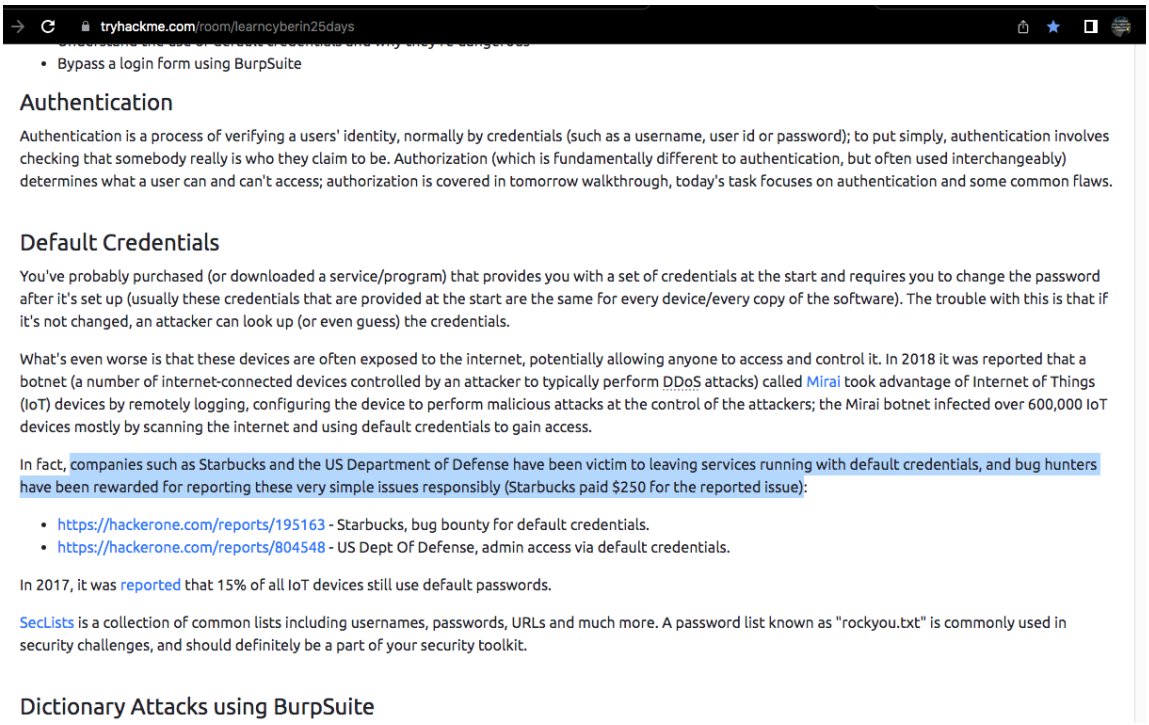
In fact, companies such as Starbucks and the US Department of Defense have been victim to leaving services running with default credentials, and bug hunters have been rewarded for reporting these very simple issues responsibly (Starbucks paid $250 for the reported issue):

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

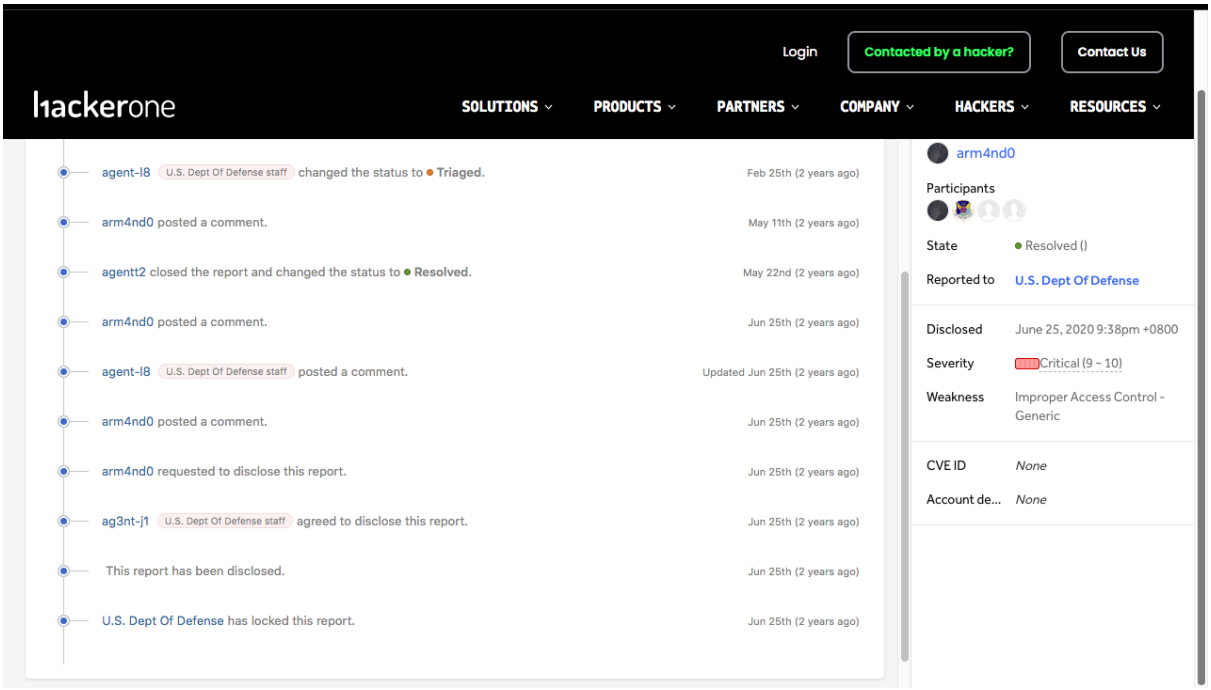
In 2017, it was reported that 15% of all IoT devices still use default passwords.

SecLists is a collection of common lists including usernames, passwords, URLs and much more. A password list known as "rockyou.txt" is commonly used in security challenges, and should definitely be a part of your security toolkit.

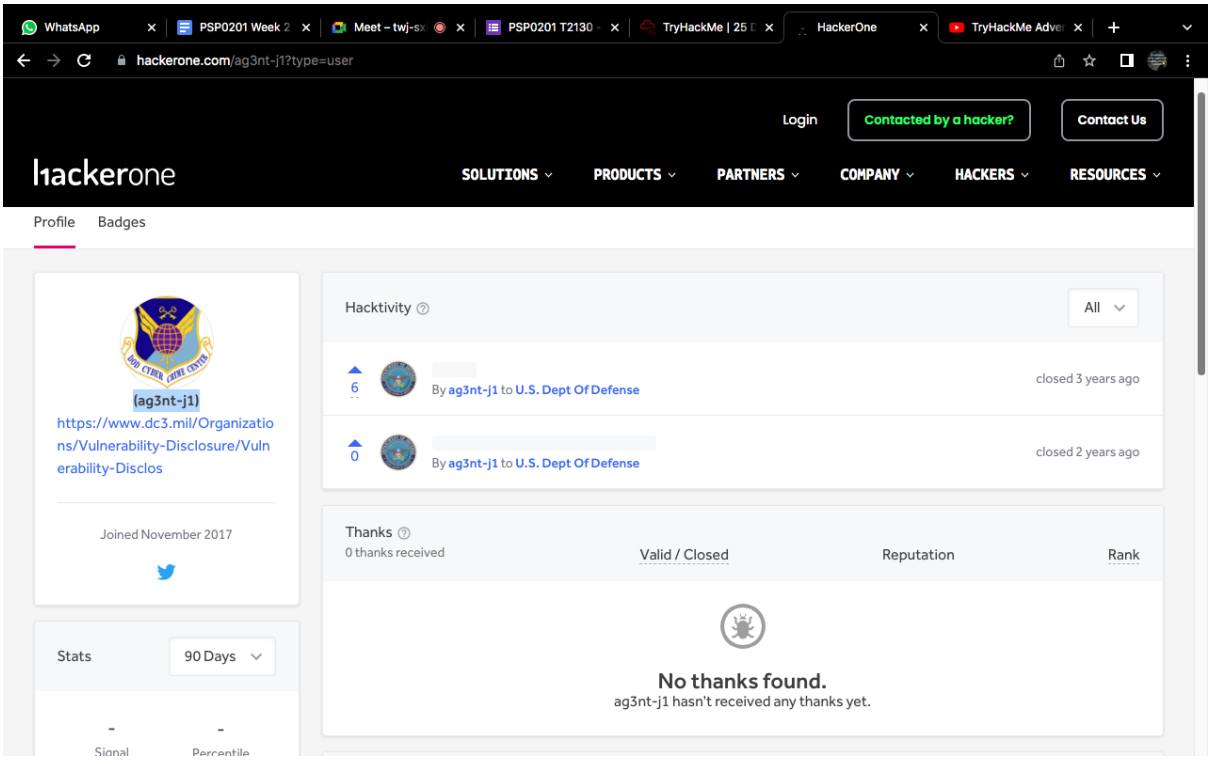
2.How much did Starbucks pay in USD for reporting default credentials according to the text?



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?

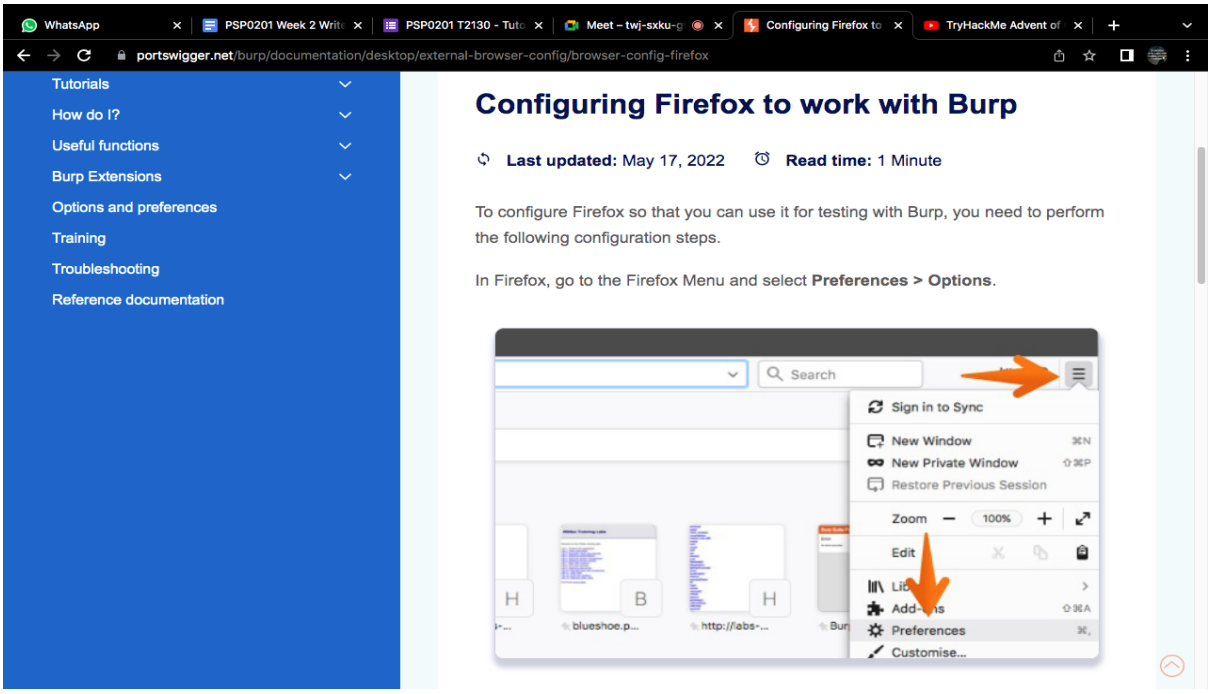


Go to this website https://hackerone.com/reports/804548 and search for Depth of Defense.

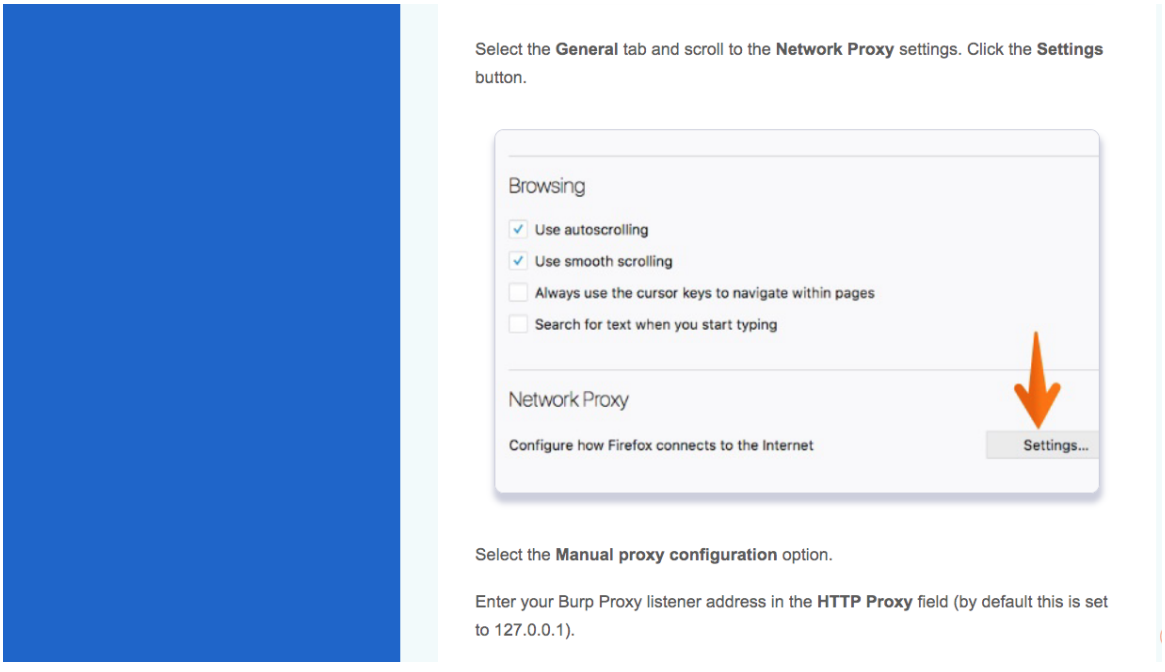


Select the Depth of Defence that was disclosed the report on 25th June

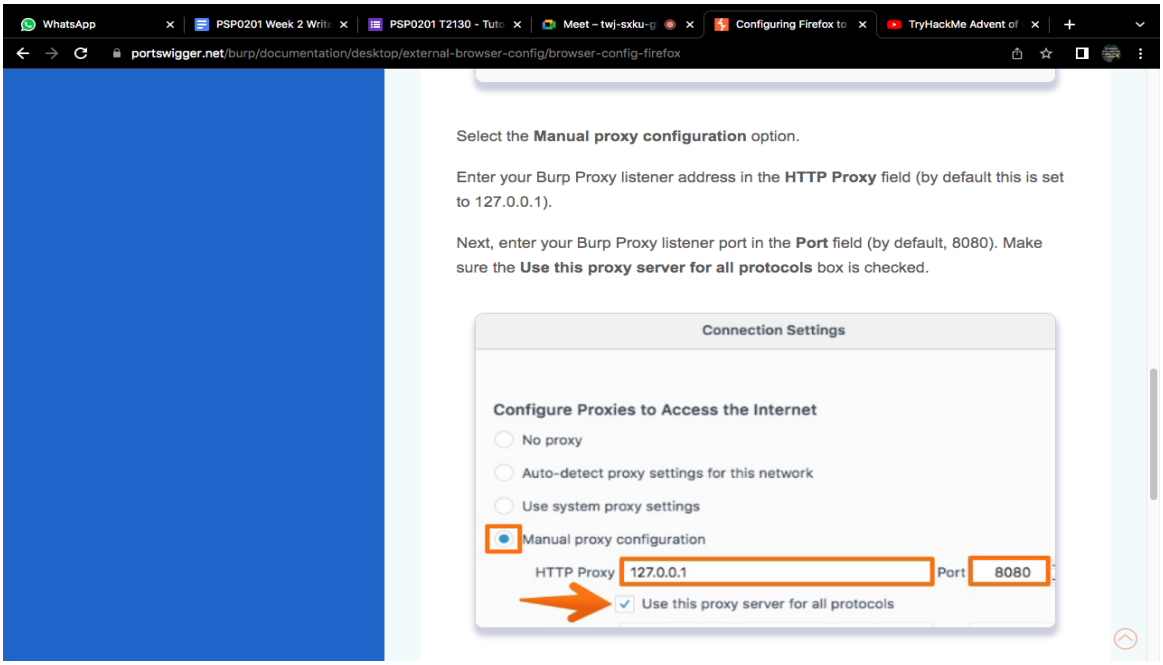
4.Examine the options on FoxyProxy on Burp. What is the port number for Burp?



After entering Burp, click the preferences button

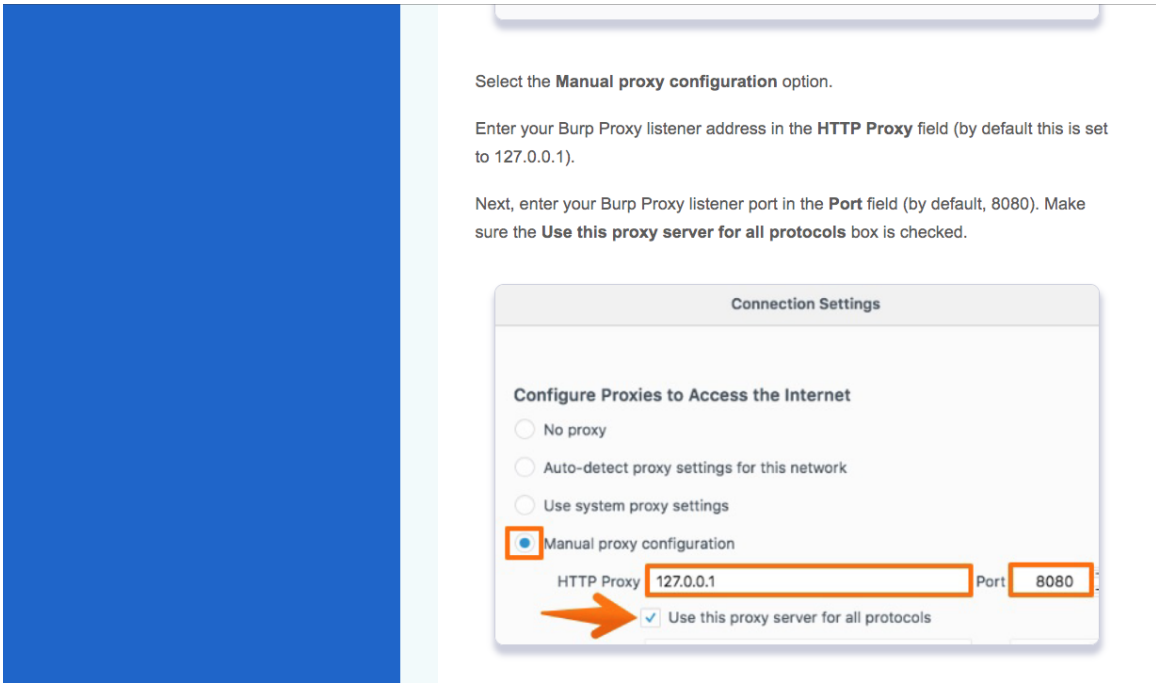


After clicking the preferences button go to settings to find out the port number.



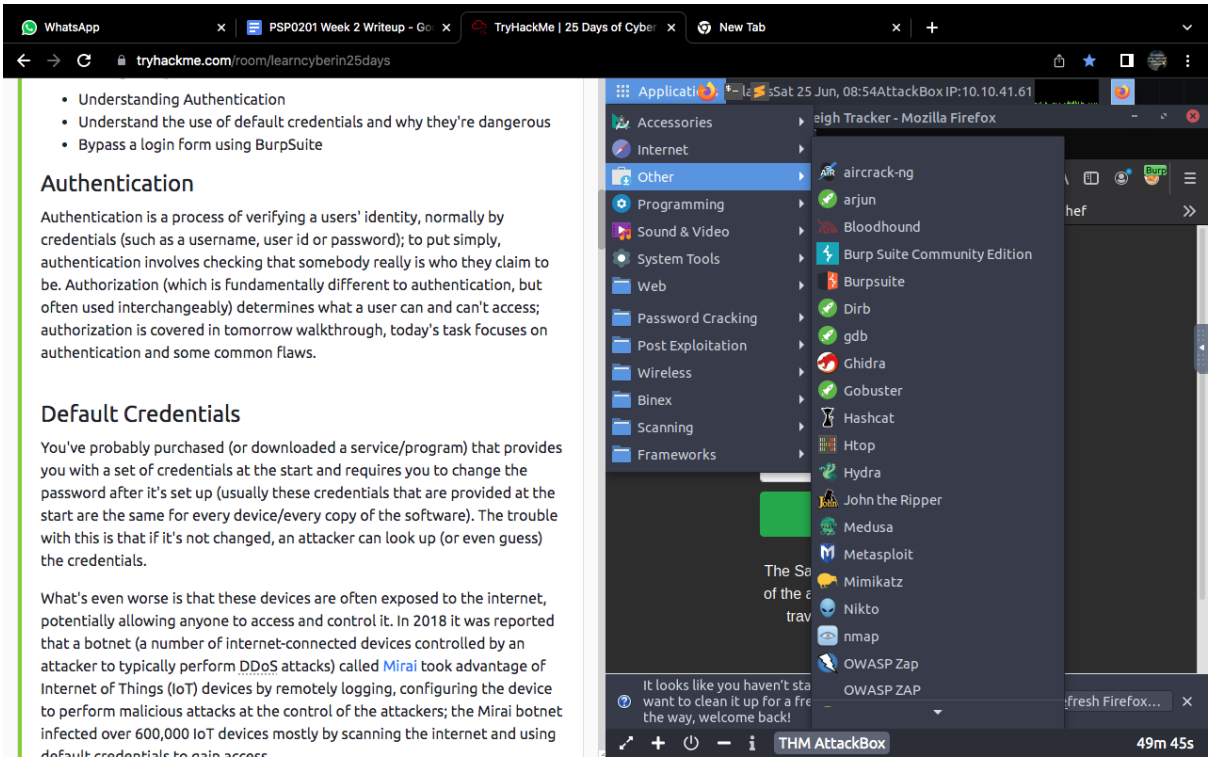
And under the connection settings we can know the port number which is 8080.

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

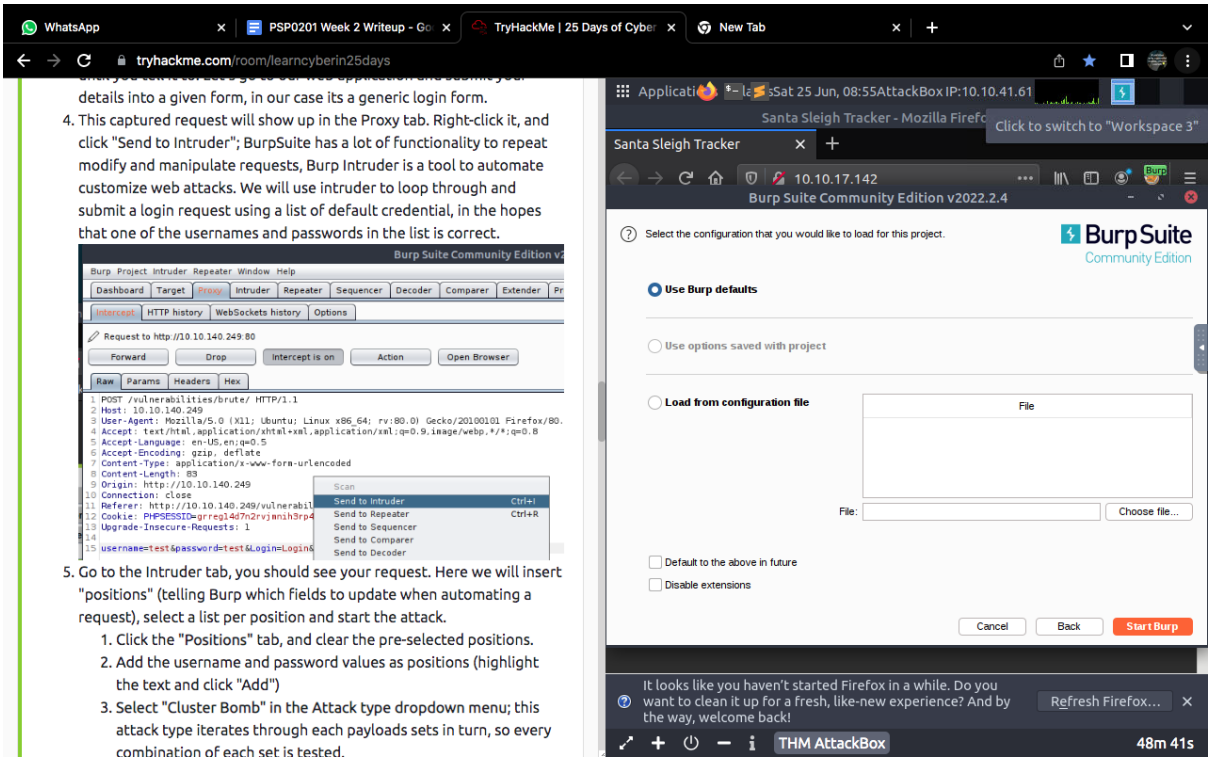


We will be able to find the proxy type beside the port number under connection settings.

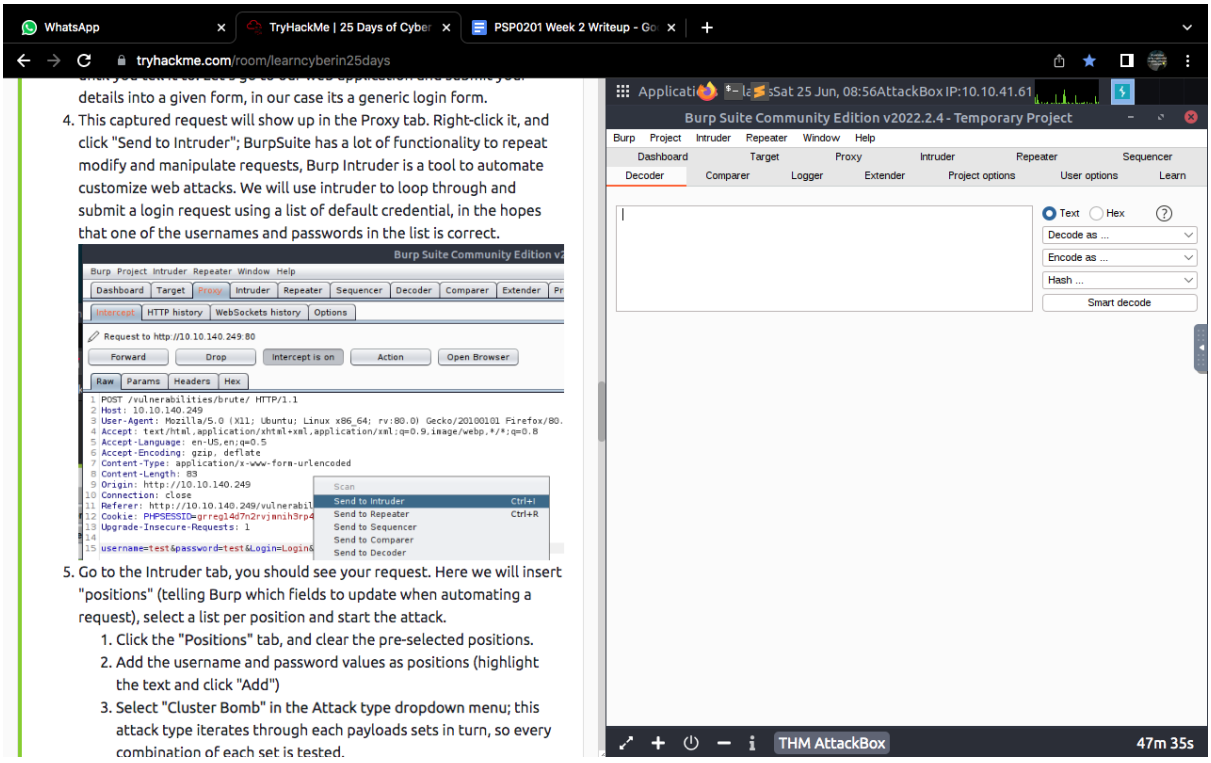
6.Experiment with decoder on Burp. What is the URL encoding for "PSP0201"?



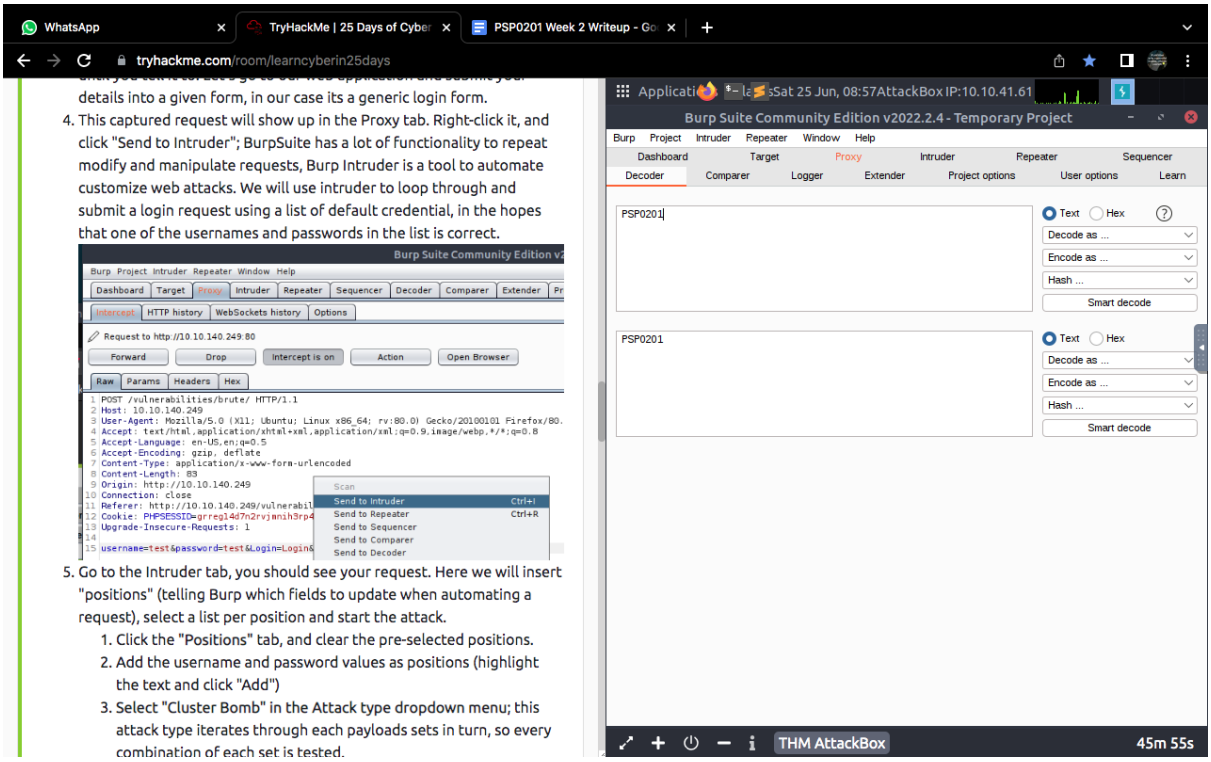
Open application and choose Burp suite Community Edition.



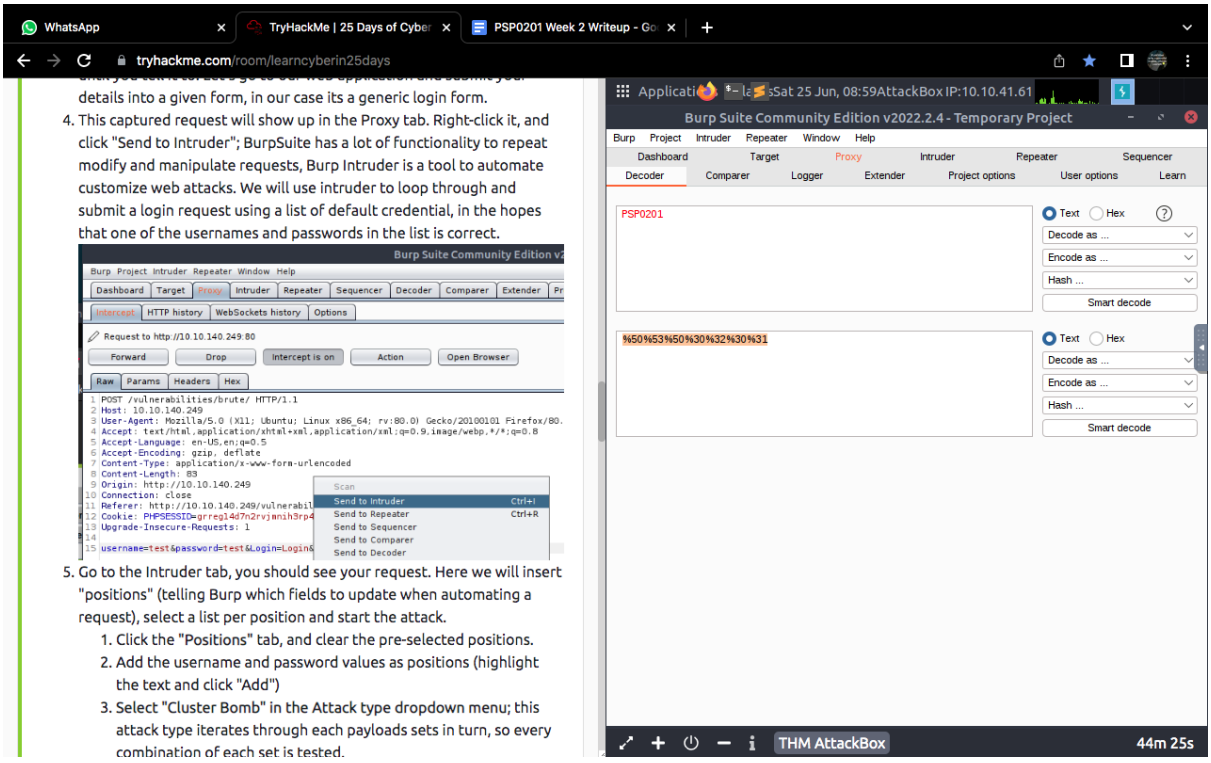
After opening Burp Suite, click start Bump.



Next, choose decoder to decode the word .

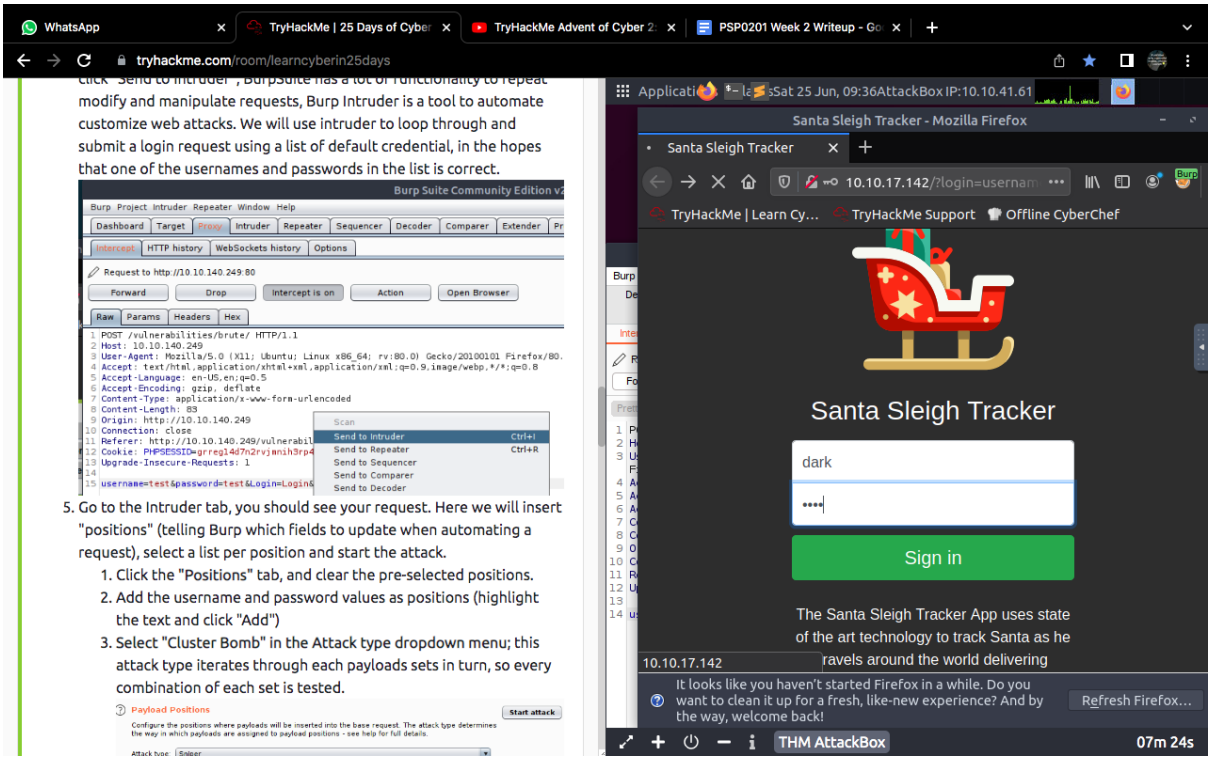


Type in the word PSP0201 in the given space

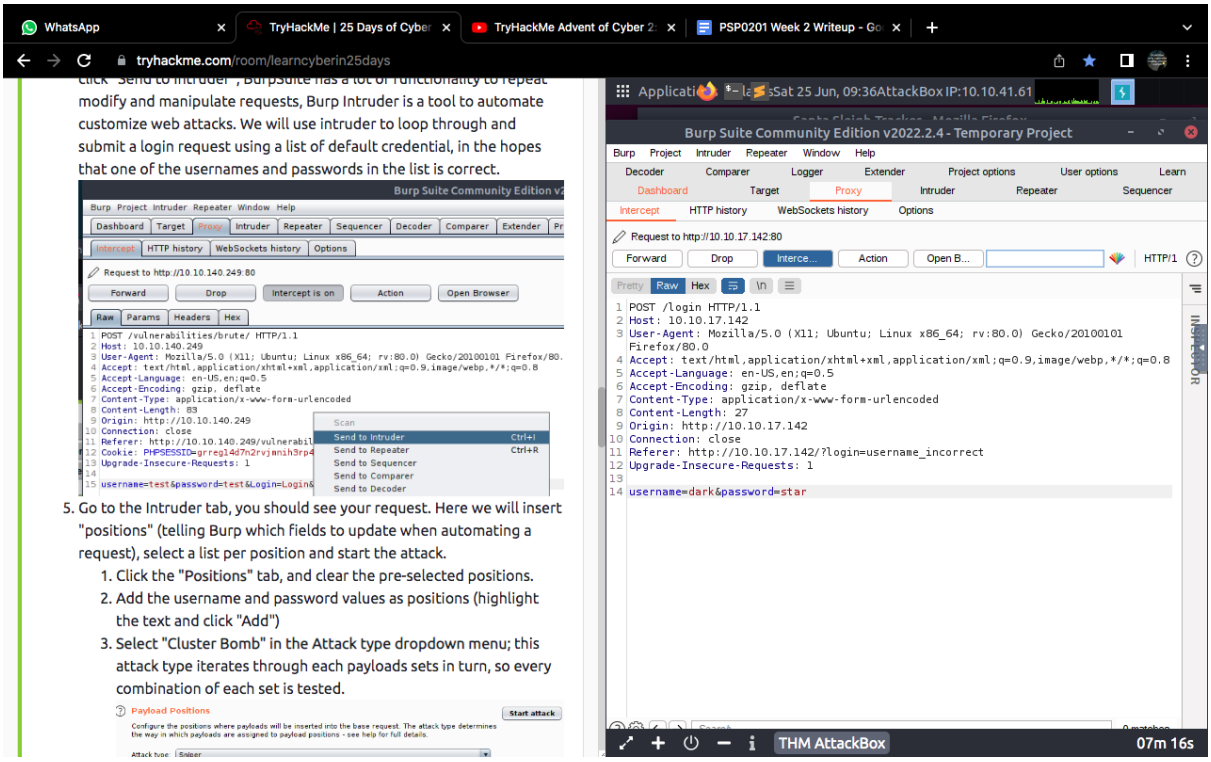


Encode to URL and then we can see the URL for the word that we have type in .

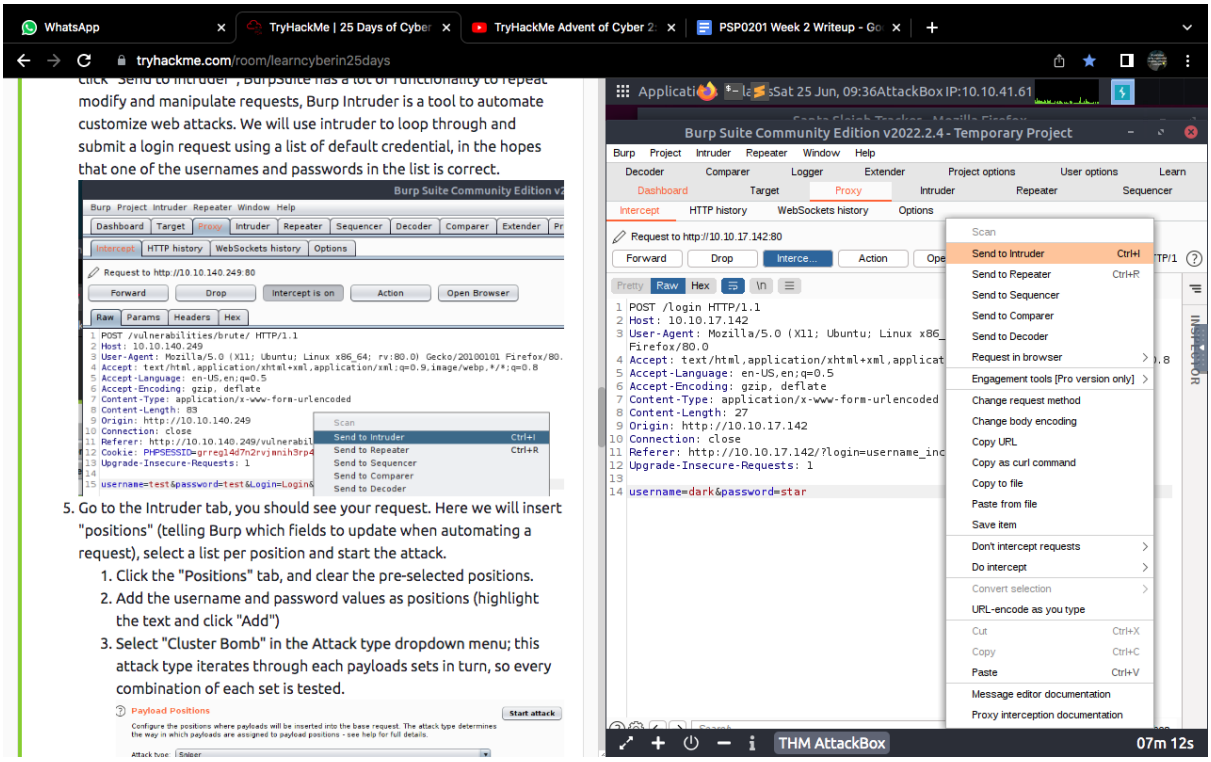
7.Look at the list of attack type options on intruders. Which of the following options matches the one in the description?



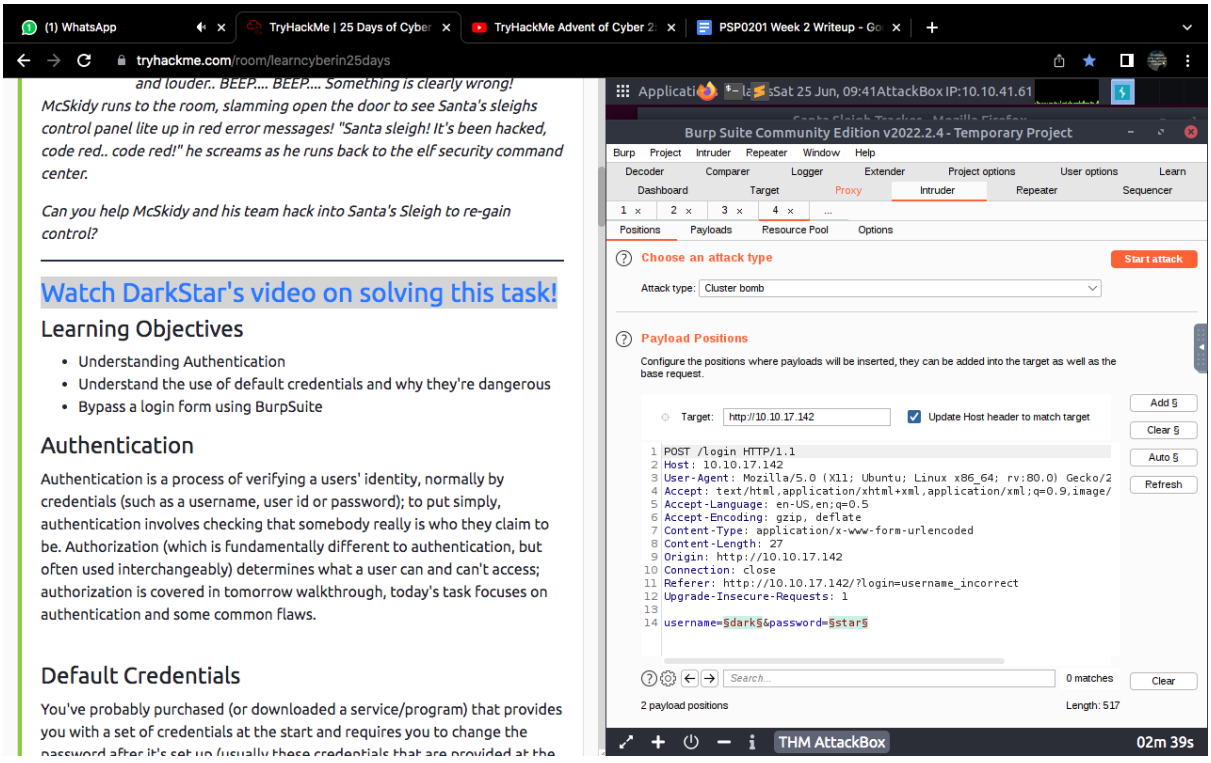
As for this question, forward proxy till the page is empty, refresh again the website and type in and username and password in the given place.



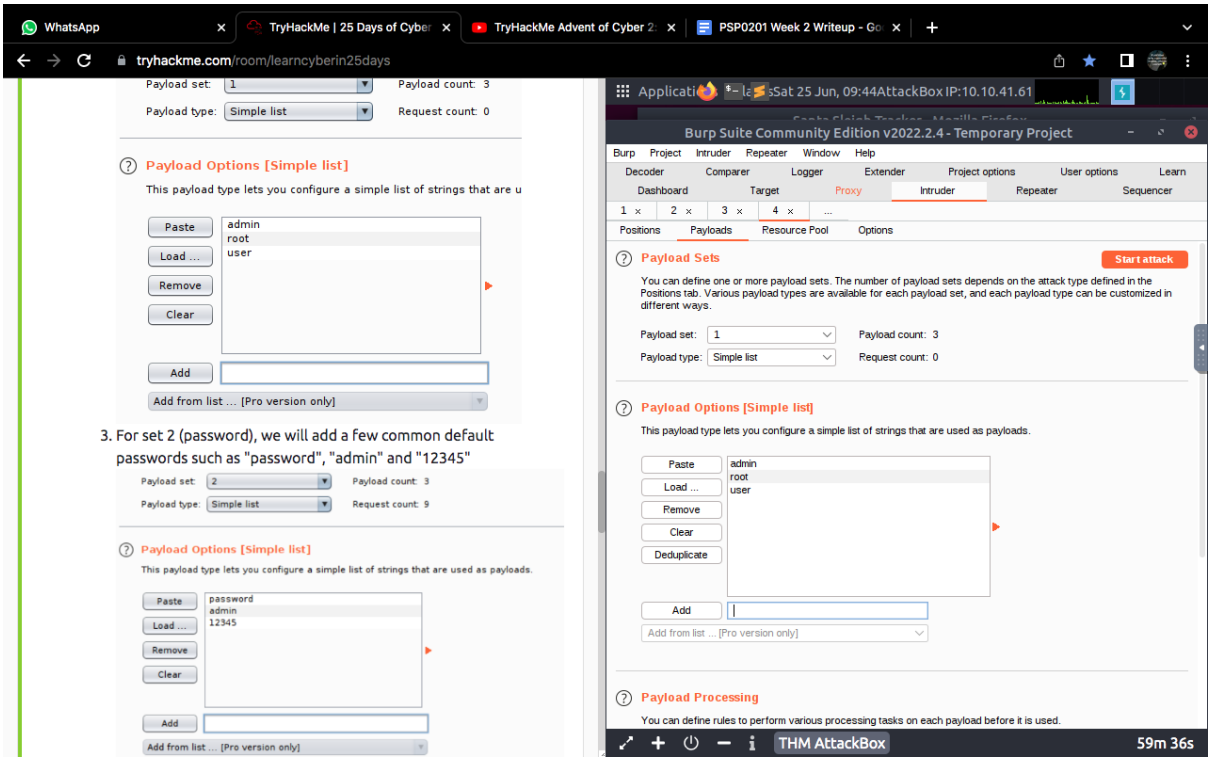
As in the picture above the username and password is highlighted



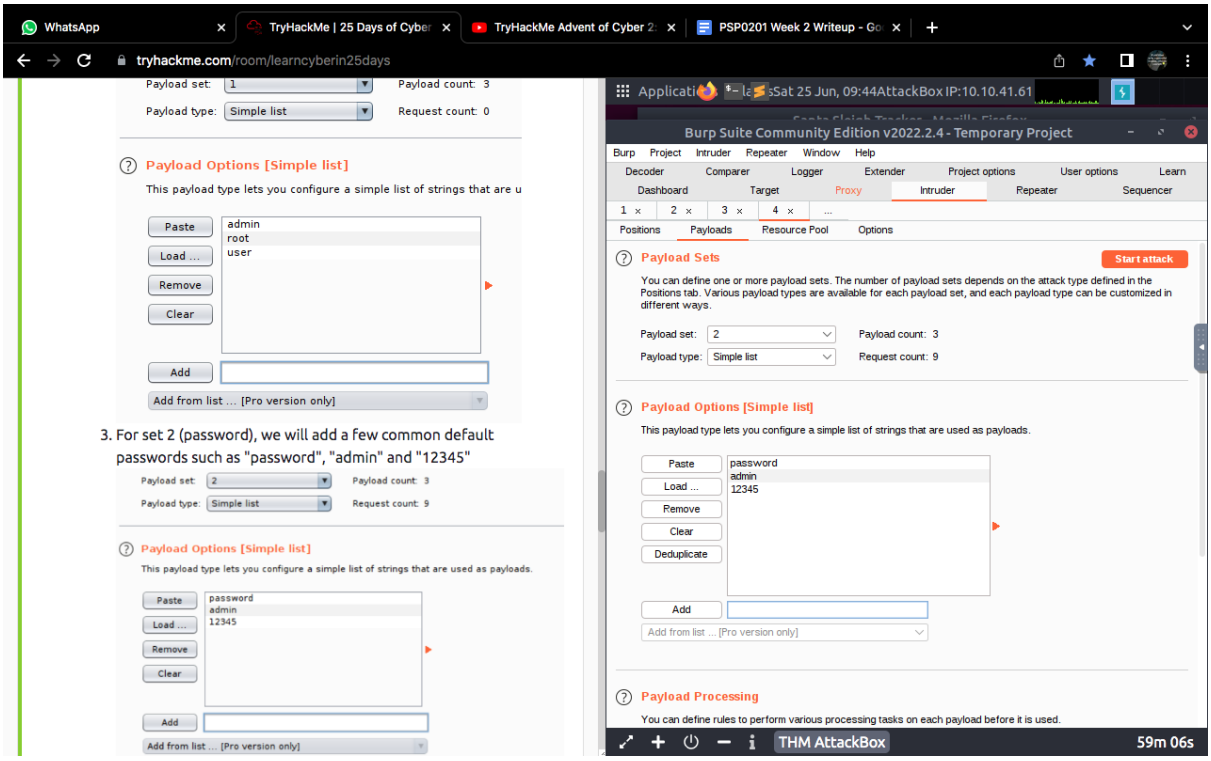
Right click on the page and click send to intruder.



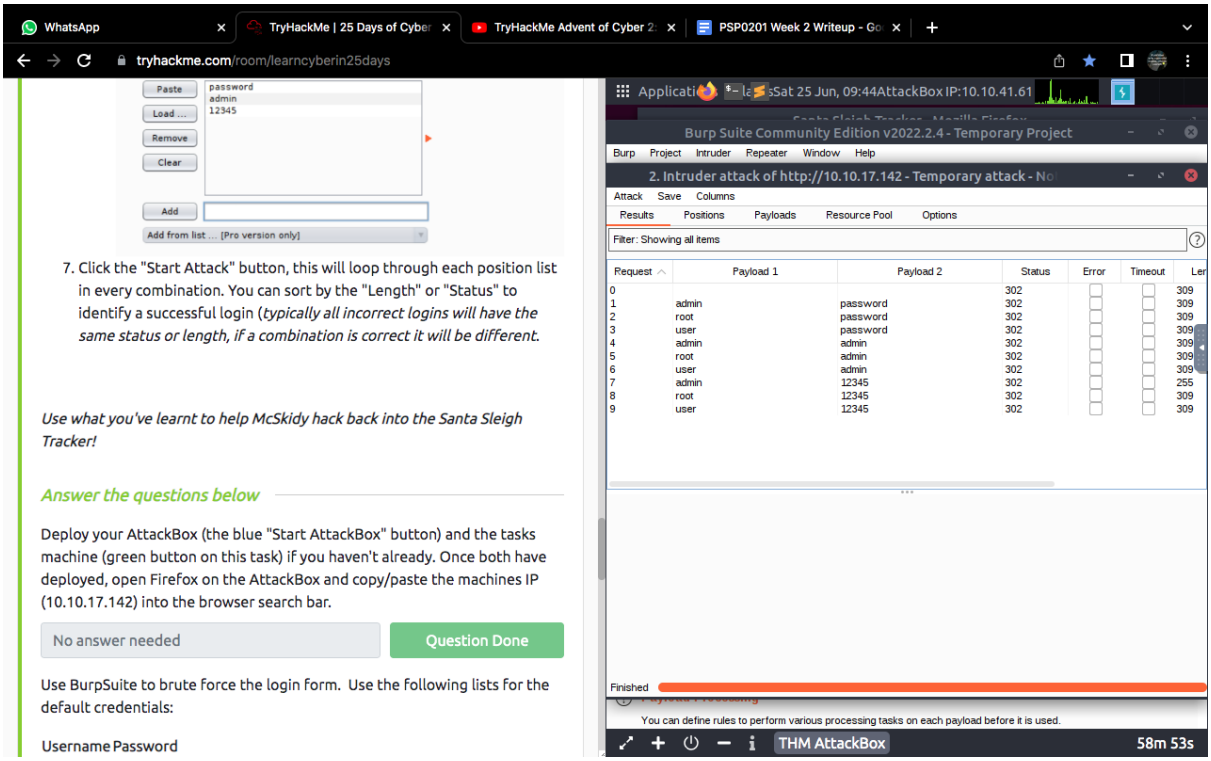
After sending to intruder, change the attack type to cluster bom and click start attack.



After we start attack go to Payloads and fill in the first box for username

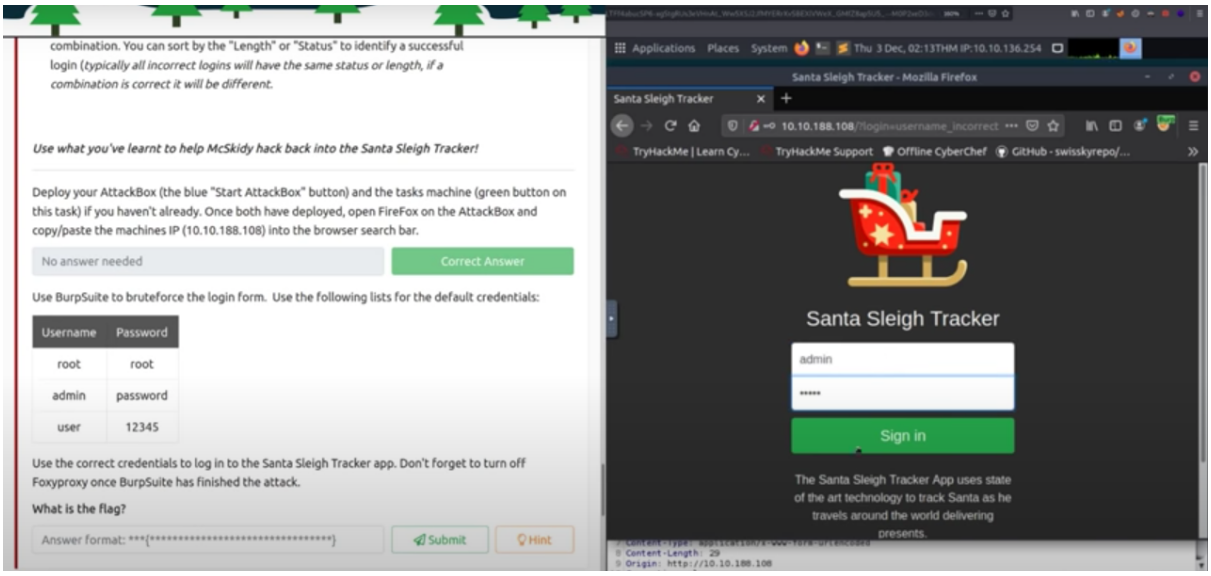


As for the second box, change the payload set to 2 and fill in the passwords.

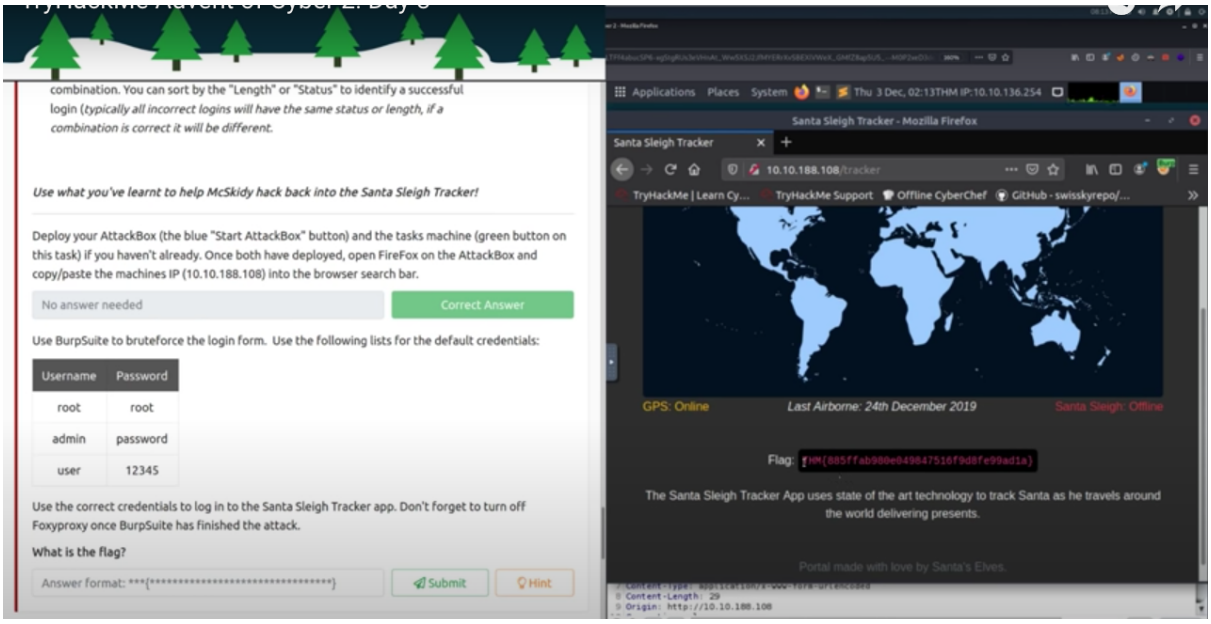


Lastly, we will able to see list of attack type options on intruders

8. What is the flag?



Type in the username “admin” and the password “12345” and sign in.



After signing in, we will be able to see the flag for this web exploitation.

Thought Process/Methodology:
As for question 1 and 2 the answers are in the website itself that had been highlighted . For question 3, go to this website https://hackerone.com/reports/804548 and search for Depth of Defence and select the Depth of Defence that was disclosed the report on 25th June. Next for the 4th question, after entering Burp, click the preferences button and click the preferences button go to settings to find out the port number.For

question number 5, under the connection settings we can know the port number which is 8080.As for question 6, open application and choose Burp suite Community Edition.After opening Burp Suite, click start Bump.Next, choose decoder to decode the word .Type in the word PSP0201 in the given space.Encode to URL and then we can see the URL for the word that we have type in . Next is question 7, ss for this question, forward proxy till the page is empty, refresh again the website and type in and username and password in the given place.As in the picture above the username and password is highlighted.Right click on the page and click send to intruder.After sending to intruder, change the attack type to cluster bom and click start attack.After we start attack go to Payloads and fill in the first box for username.As for the second box, change the payload set to 2 and fill in the passwords.Lastly, we will able to see list of attack type options on intruders. For the last question, type in the username "admin" and the password "12345" and sign in.After signing in, we will be able to see the flag for this web exploitation.

Day 4 : Web Exploitation - Santa's watching

Tools used: Kali Linux/Mozilla Firefox/Gobuster

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)

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:

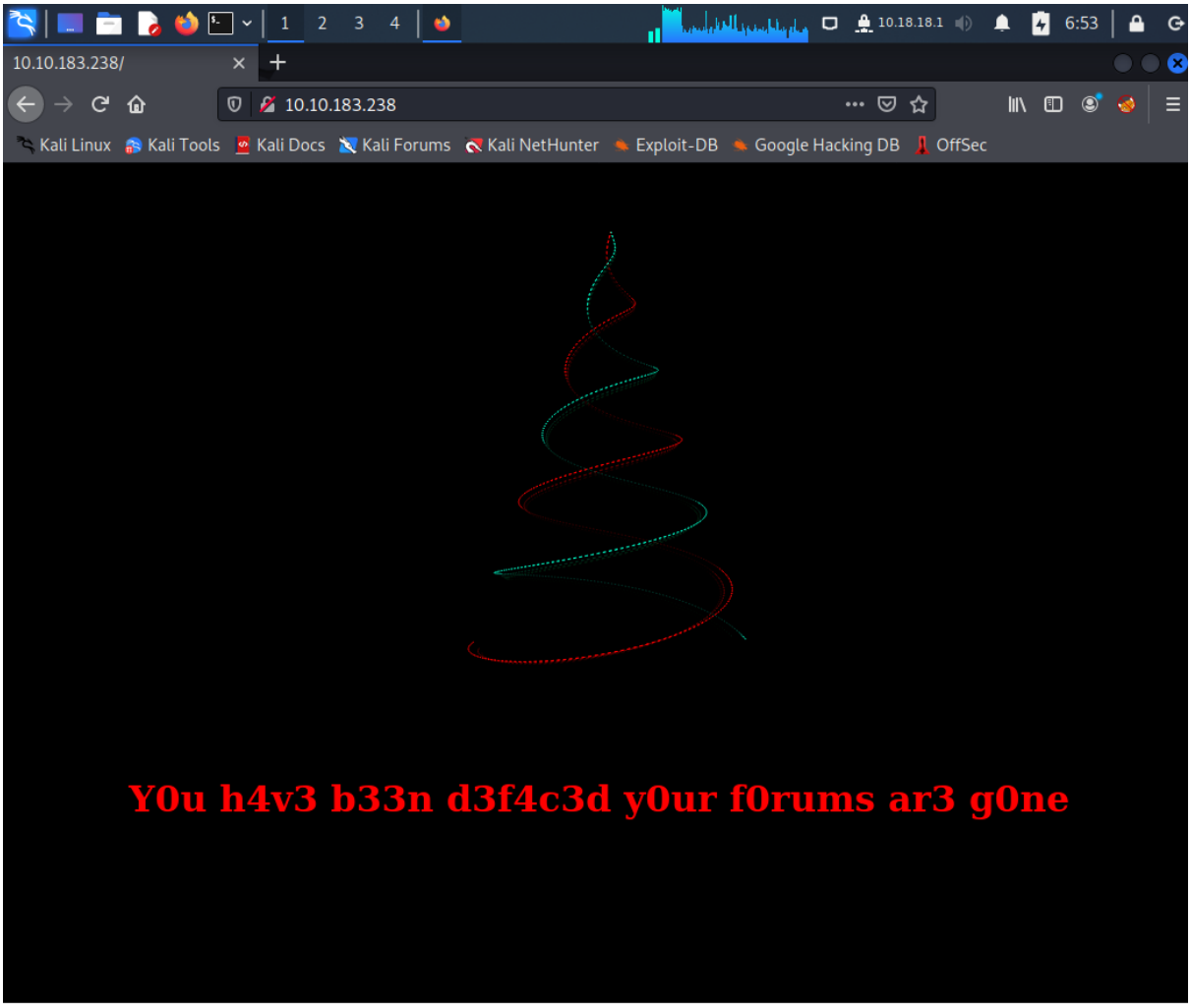
```
wfuzz -c -z file,mywordlist.txt -d "username=FUZZ&password=FUZZ" -u
http://shibes.thm/login.php
```

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

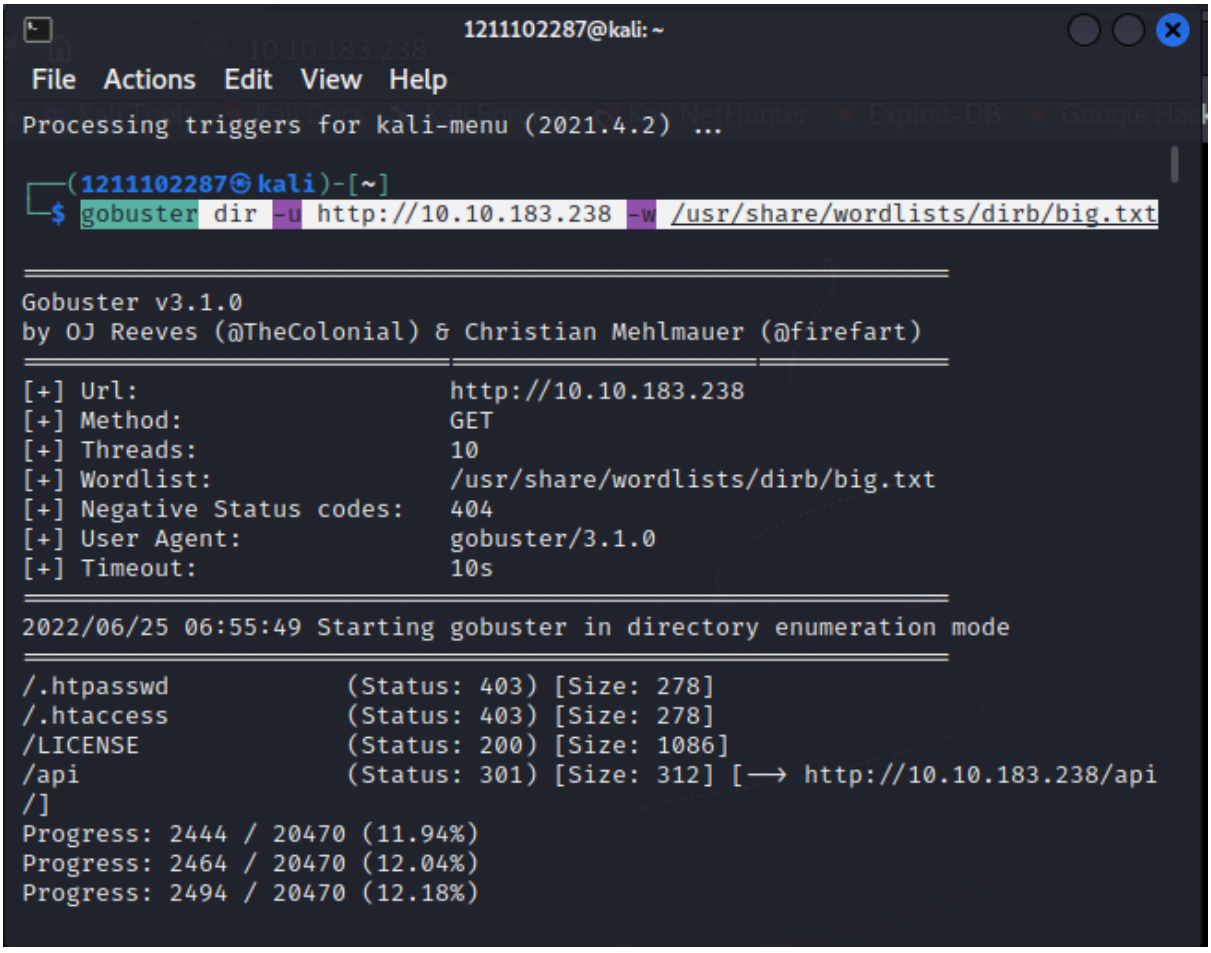
By using the highlighted command's materials from THM, our wfuzz command would look like: **wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ**

Question 2

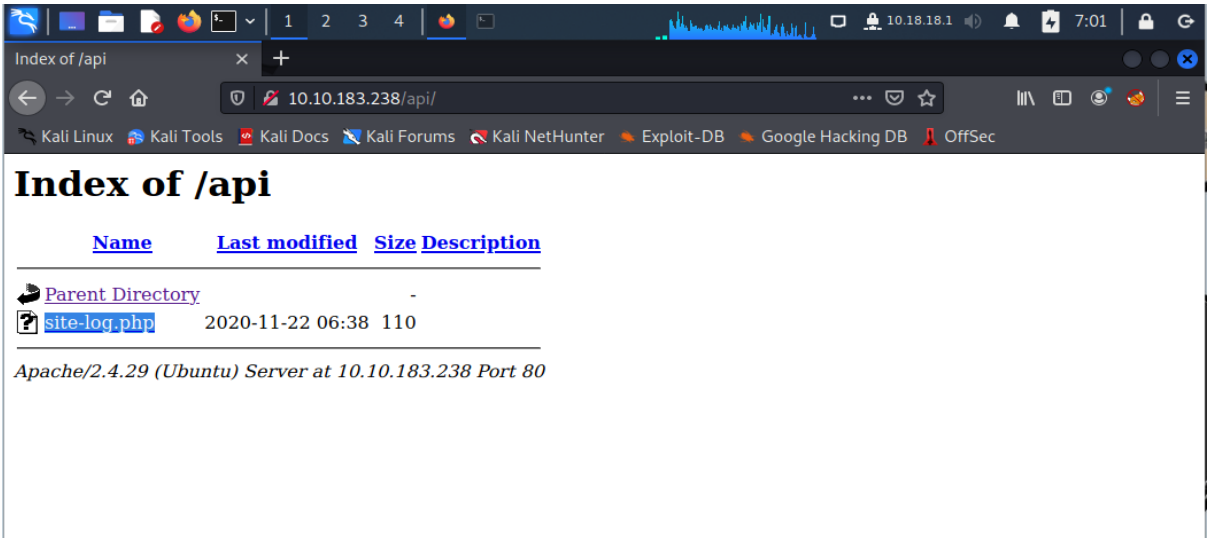
Use GoBuster (against the target you deployed -- not the shibes.xyz domain) to find the API directory. What file is there?



Place your IP address in your browser



Start Gobuster by typing the following commands in the terminal and we can find the API directory there which is “/api” in the commands.



By adding /api after the website’s IP address in the search bar, we can see that the file shown in the API directory is shown which is **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?

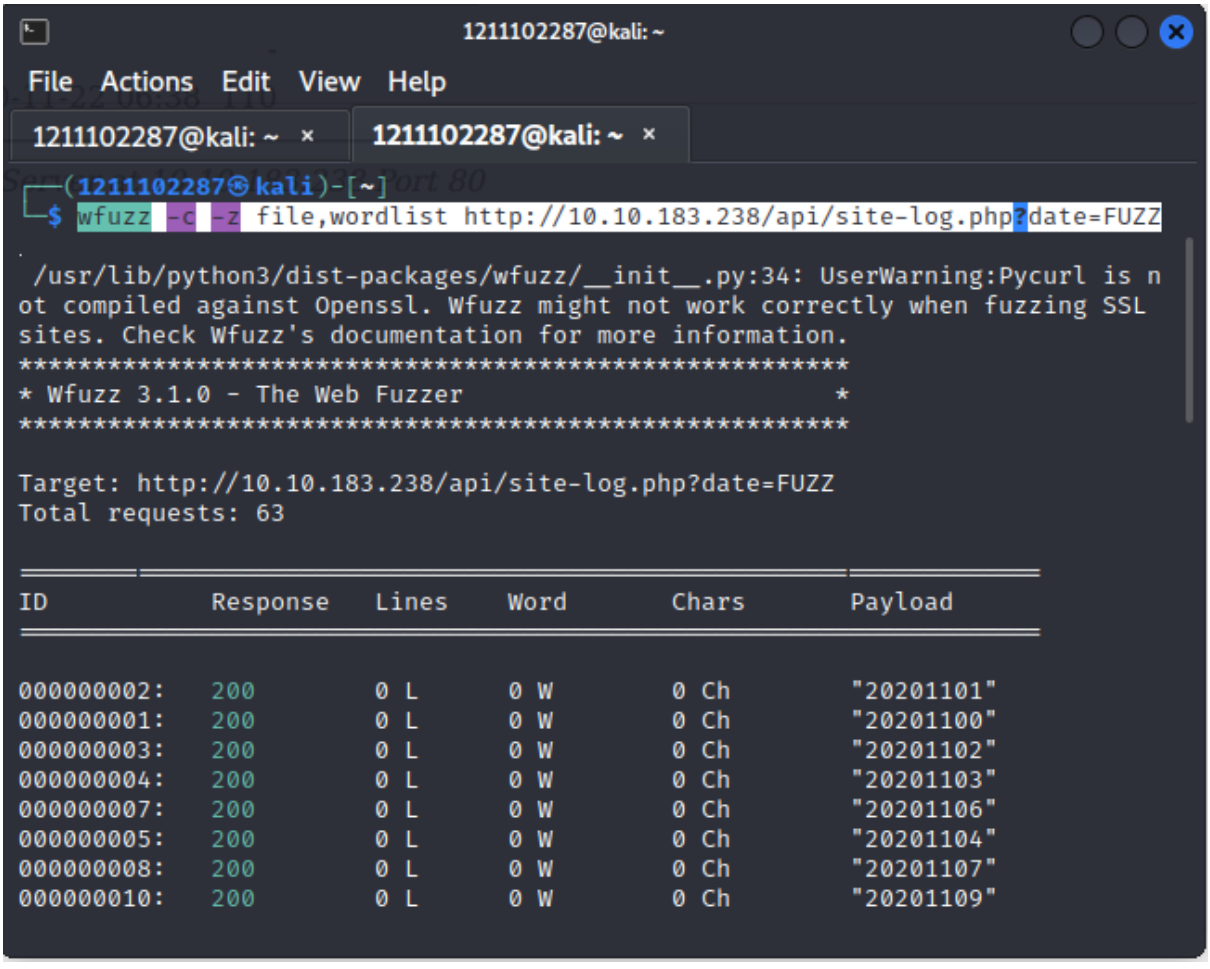
Challenge

Deploy both the instance attached to this task (the green deploy button) and the AttackBox by pressing the blue "Start AttackBox" button at the top of the page. After allowing 5 minutes, navigate to the website (10.10.183.238) in your AttackBox browser.

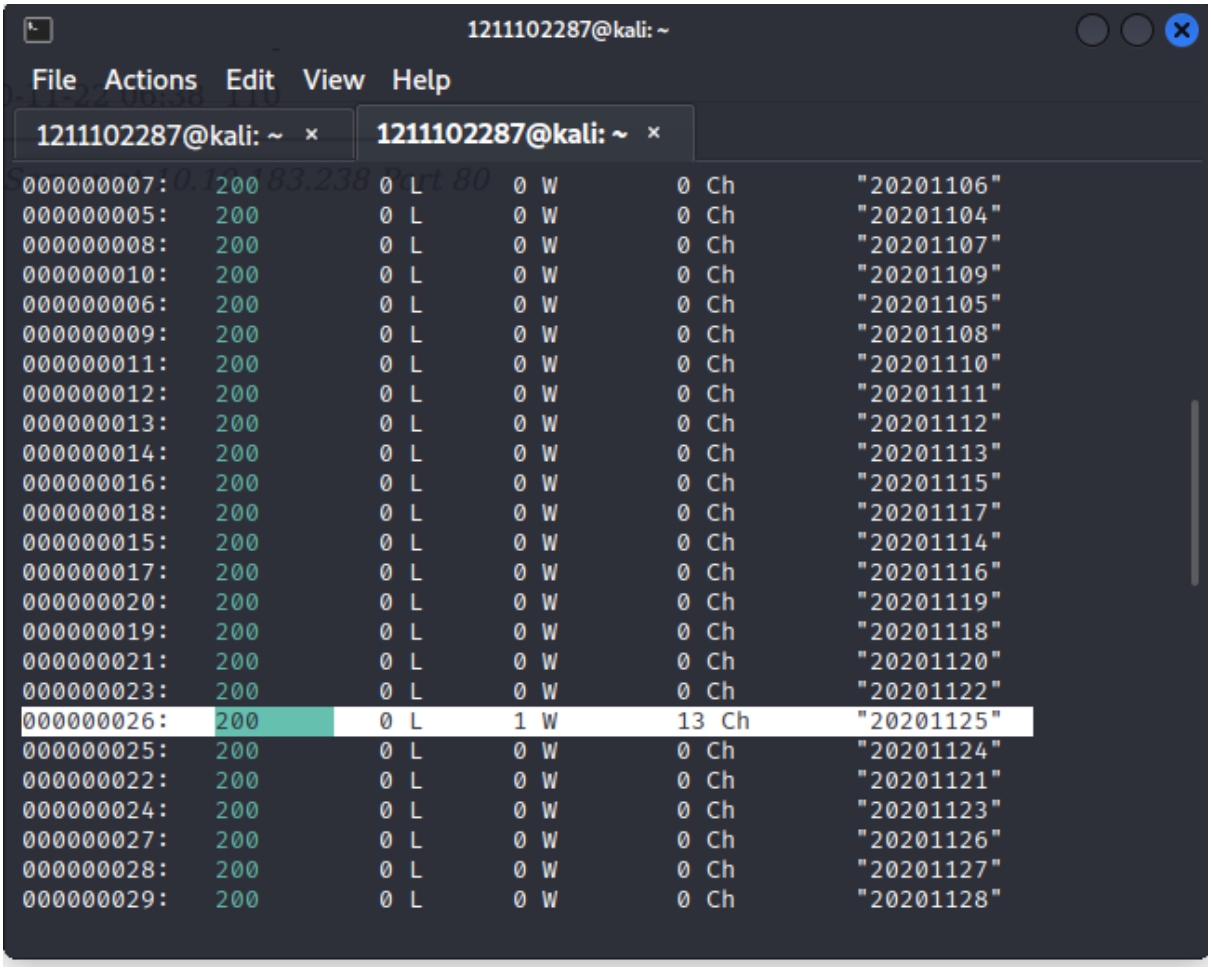
It is up to you to decide if you wish to create the wordlist yourself or use a larger wordlist located in `/opt/AoC-2020/Day-4/wordlist` on the AttackBox. The wordlist is also available for download if you are using your own machine.

In summary, use the tools and techniques outlined in today's advent of cyber; search for the API, find the correct post and bring back Elf's forums!

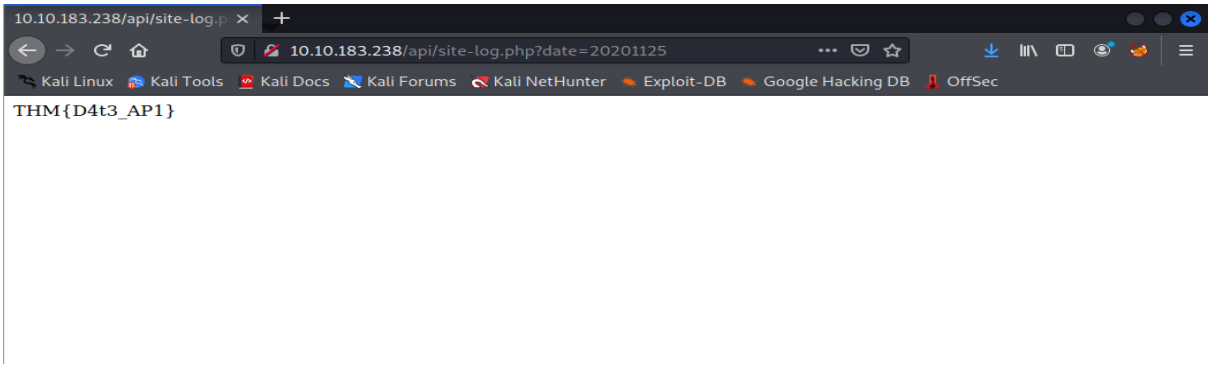
Download the “wordlist” text file from the blue highlighted link from the picture below.



Enter the highlighted code in the terminal to make the run of Wfuzz



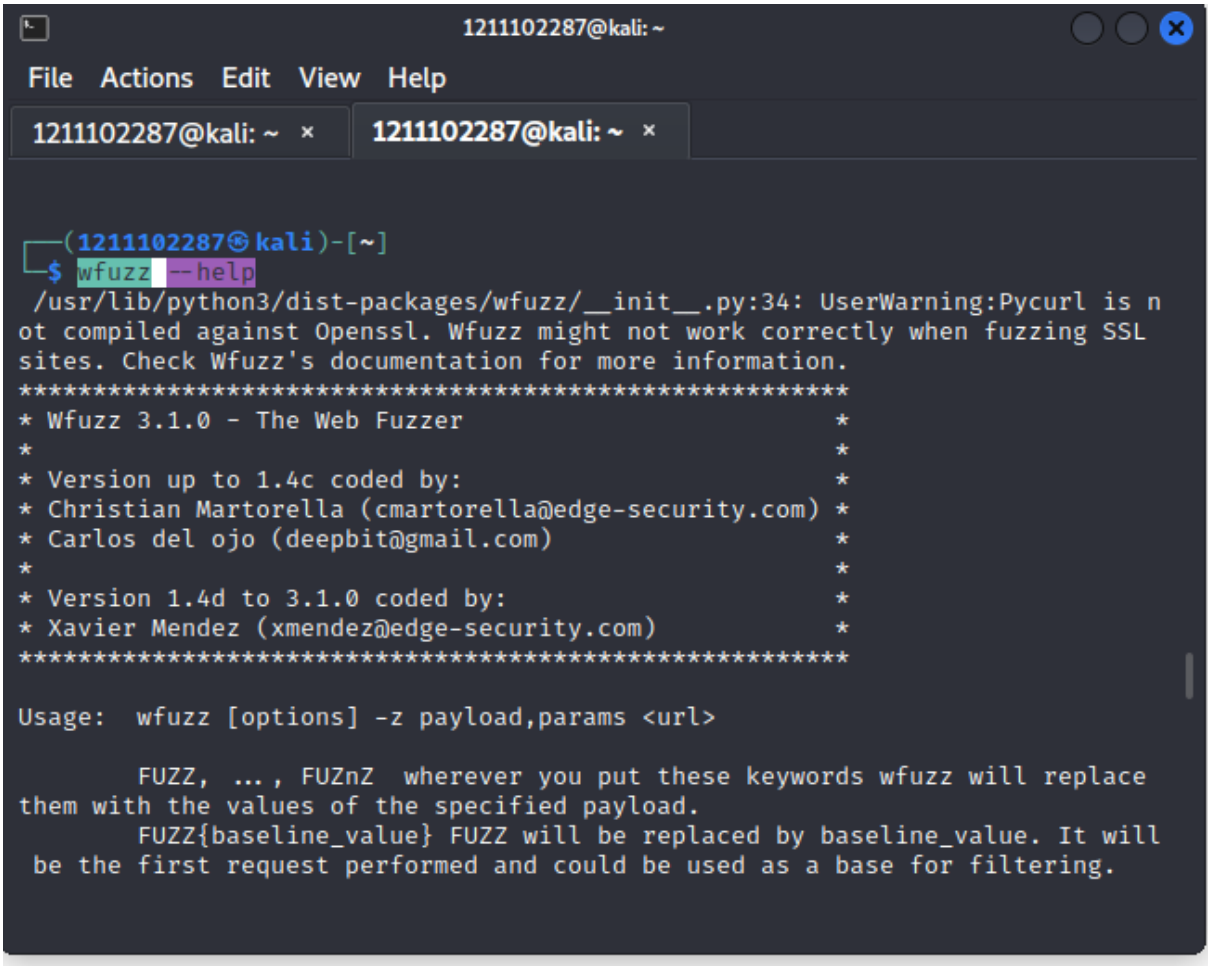
Under the Word section, there is one word which is different from the others (1W), while under the Channel Section, there is one channel which is different from others (13 Ch). Copy the Payload number (20201125) from the same row on the right.

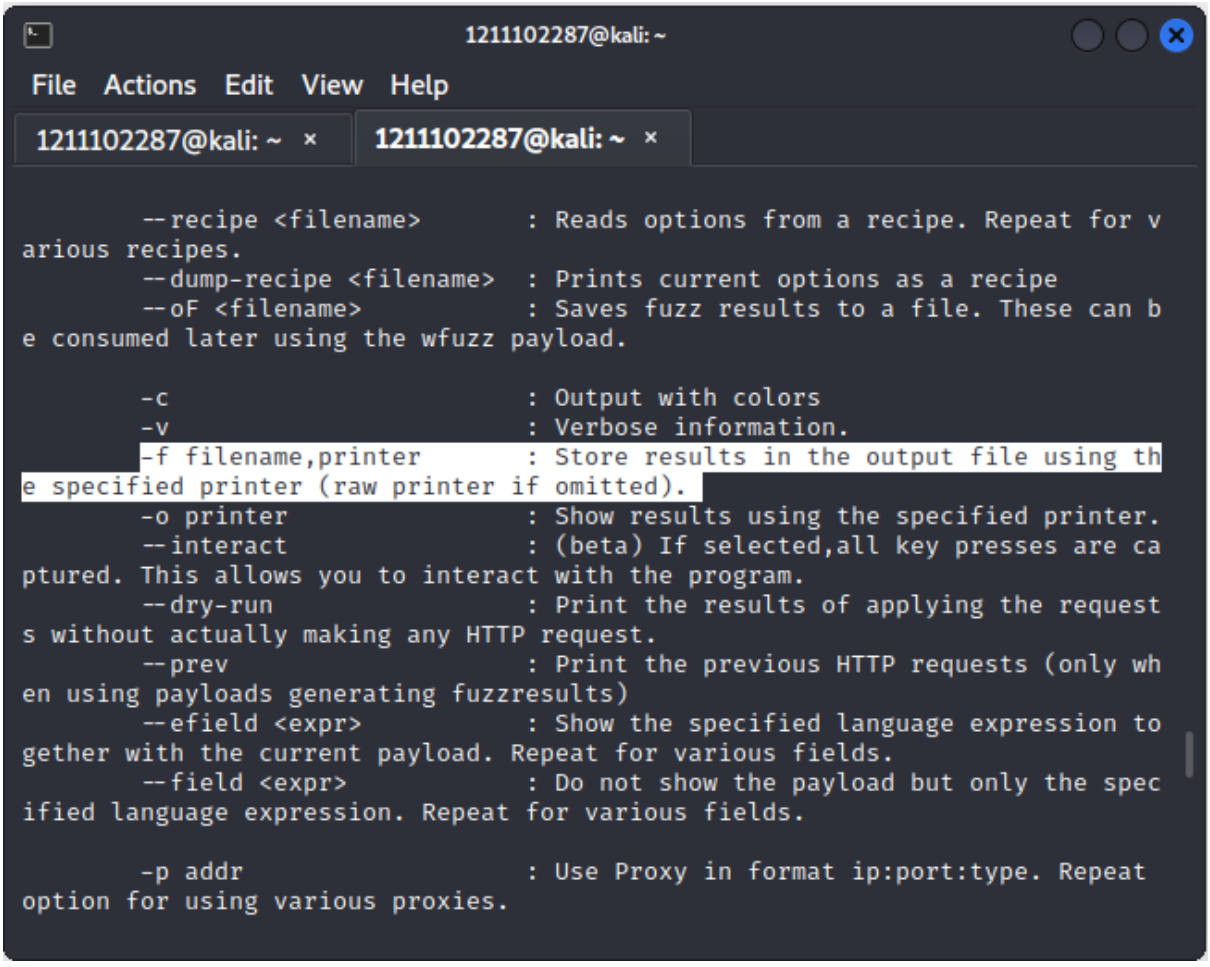


Add “site-log.php?date=20201125” after the website’s URL. It will lead us to another website which has the Flag in it. The flag **THM{D4t3_AP1}** can be seen on the website.

Question 4

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





Insert “wfuzz –help” in the terminal. Scroll down and find the Function of the -f parameter. It is shown that the -f parameter store results to **filename, printer**.

Thought Process/Methodology:

After typing the IP address in the browser and accessing the picture of Christmas Tree with words below it, we are required to type in a line of commands with the usage of Gobuster in the terminal window to find the API directory of the website. With our Gobuster command options’ knowledge, to specify the wordlist, -u and -w is being used. The API directory is shown by adding /api after the IP address in the browser bar. A file “site-log.php” which is a blank and empty file, could be found in the website. Download the file which is called “wordlist” in the Challenge description so that we could access the file for further information. By entering the wfuzz command, the parameter -z is used to look for the file, which is the “wordlist” text file, by replacing "FUZZ" with the words within "big.txt". The text in the file is shown in the terminal window and we have to find the row with the context which is different from the others. A date in the right of the row could be found which is “20201125”. Add “site-log.php?date=20201125” after the website’s URL, replacing the actual date with the FUZZ word. It will lead us to a website with a Flag on it. Insert the command “wfuzz –help” and scroll down the commands to find the function of the -f parameter.

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

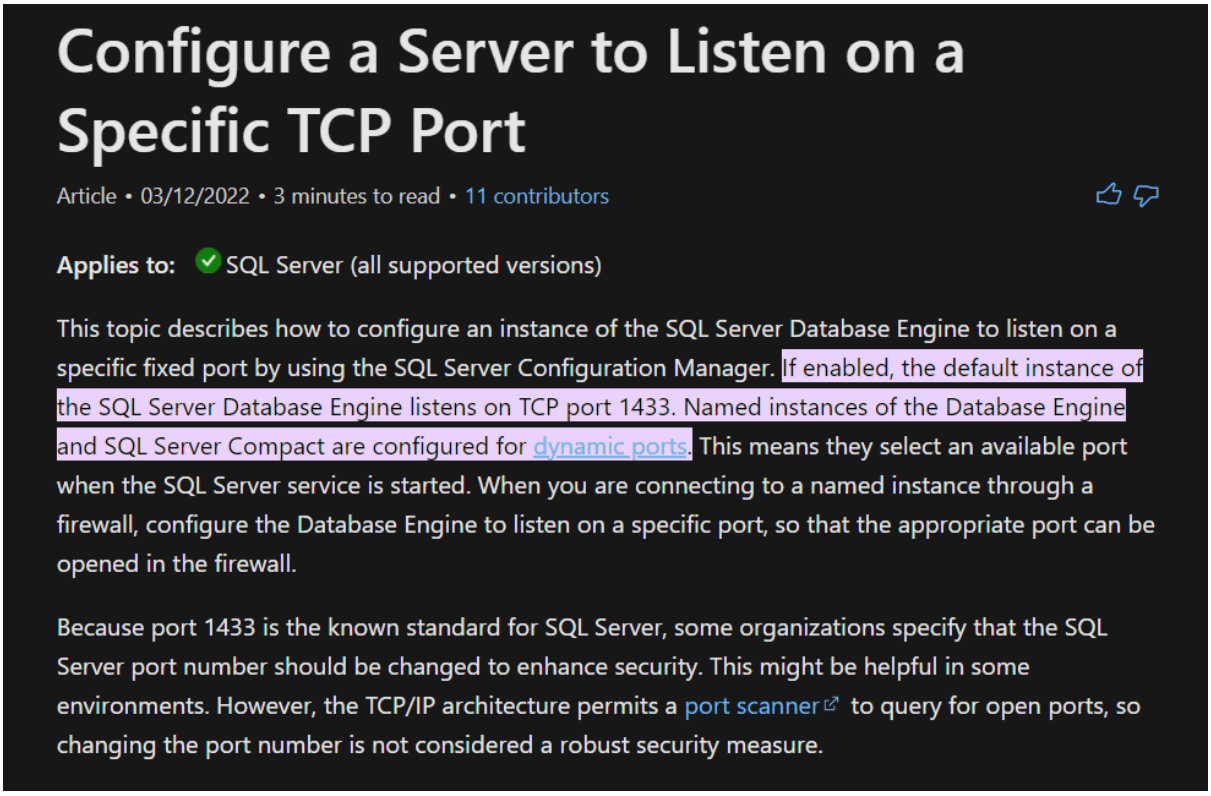
Tools used: THM Attackbox/Mozilla Firefox

Solution/Walkthrough:

Question 1

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

After referring to the Microsoft's documentation, it can be deduced that the default port number for SQL server running on TCP is 1433 (highhlighted for viewing purposes).



Configure a Server to Listen on a Specific TCP Port

Article • 03/12/2022 • 3 minutes to read • 11 contributors

Applies to: SQL Server (all supported versions)

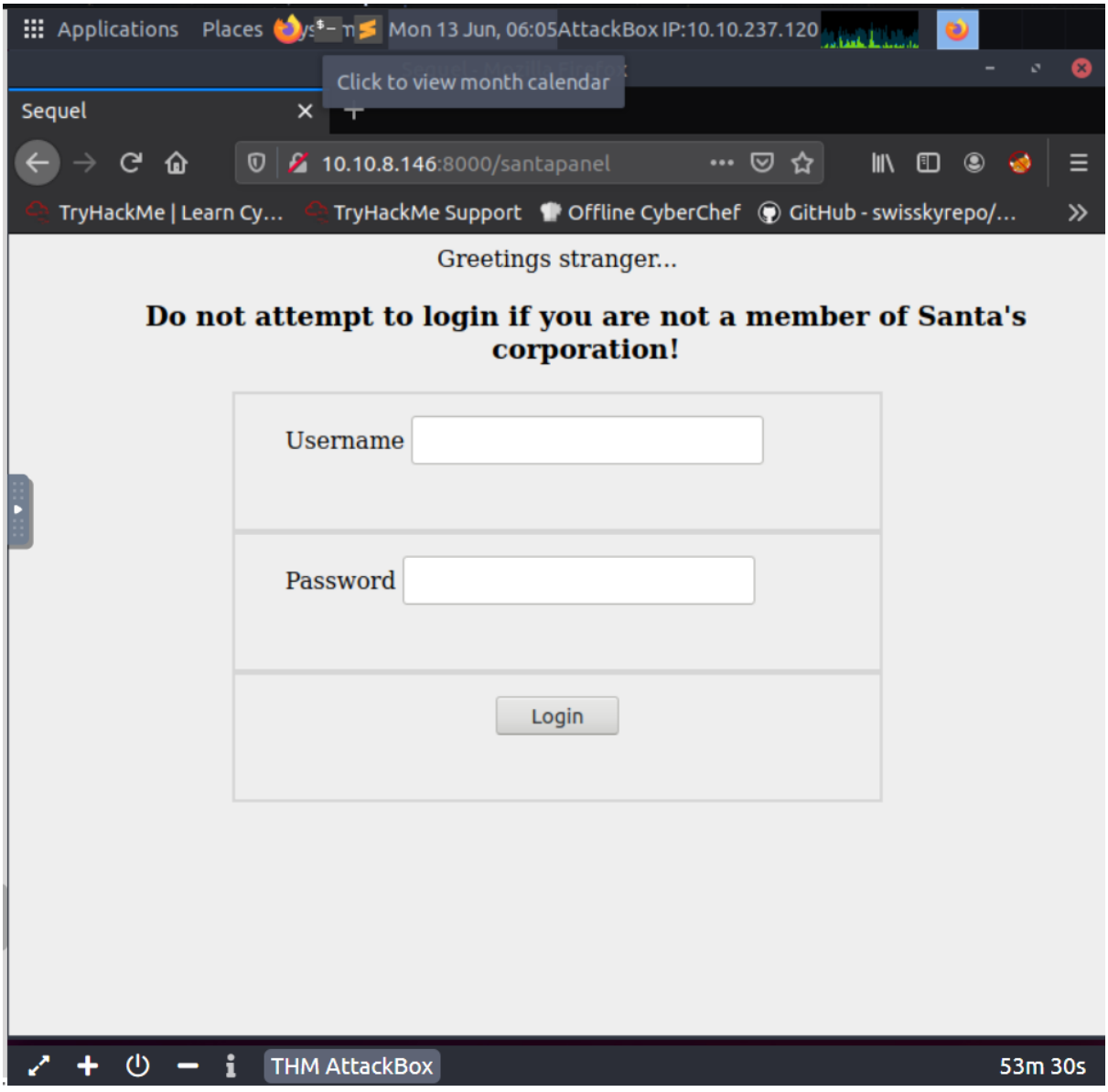
This topic describes how to configure an instance of the SQL Server Database Engine to listen on a specific fixed port by using the SQL Server Configuration Manager. If enabled, the default instance of the SQL Server Database Engine listens on TCP port 1433. Named instances of the Database Engine and 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.

Because port 1433 is the known standard for SQL Server, some organizations specify that the SQL Server port number should be changed to enhance security. This might be helpful in some environments. However, the TCP/IP architecture permits a port scanner to query for open ports, so changing the port number is not considered a robust security measure.

Question 2

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

Santa's secret login panel can be accessed by adding in /santapanel after the website's IP Address in the search bar. (IP Address:8000/santapanel)



Question 3

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

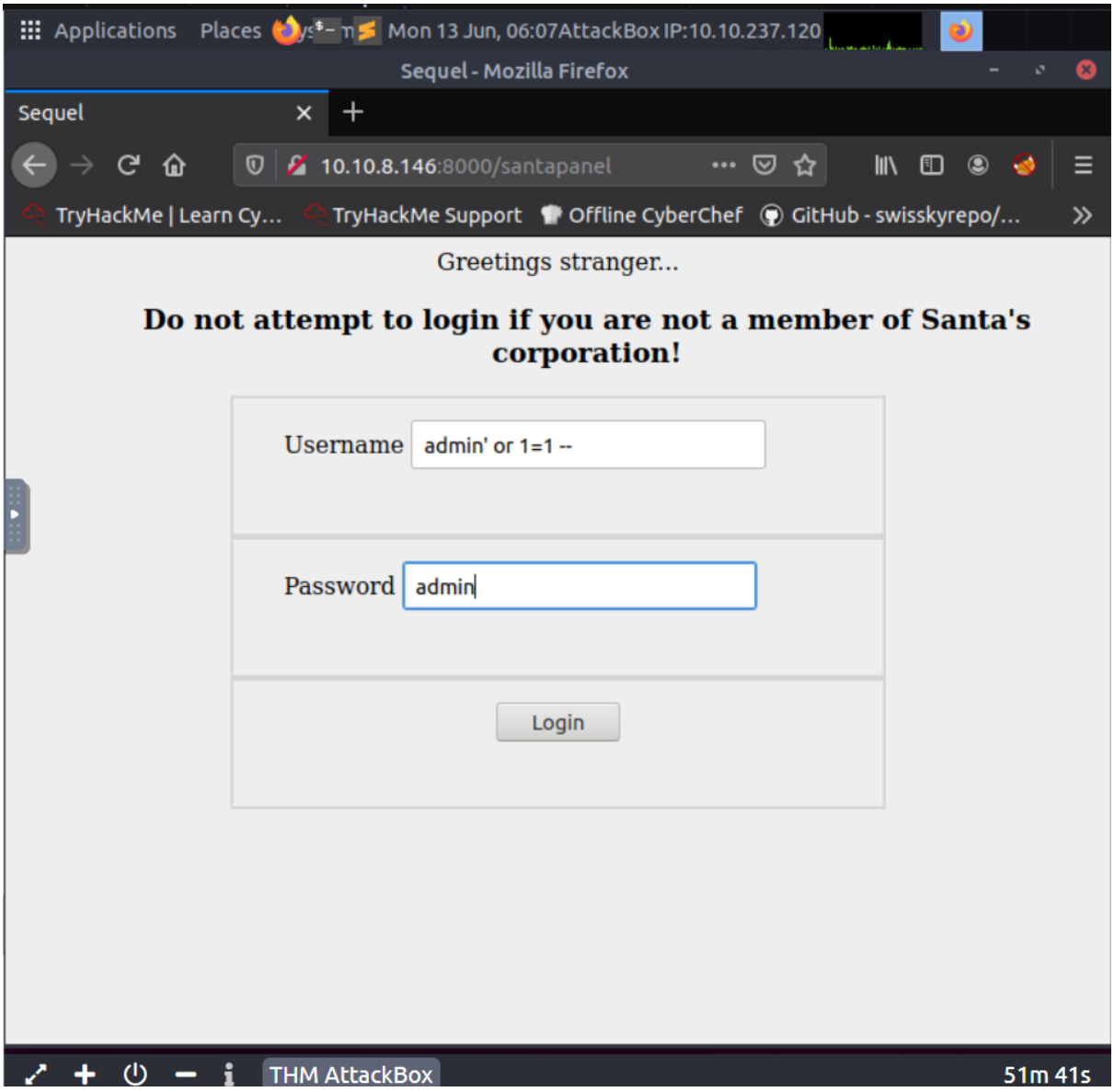
The database used is written on THM website as shown below (highlighted for viewing purposes).

Challenge

Visit the vulnerable application in Firefox, find Santa's secret login panel and bypass the login. Use some of the commands and tools covered throughout today's task to answer Questions #3 to #6.

Santa reads some documentation that he wrote when setting up the application, it reads:

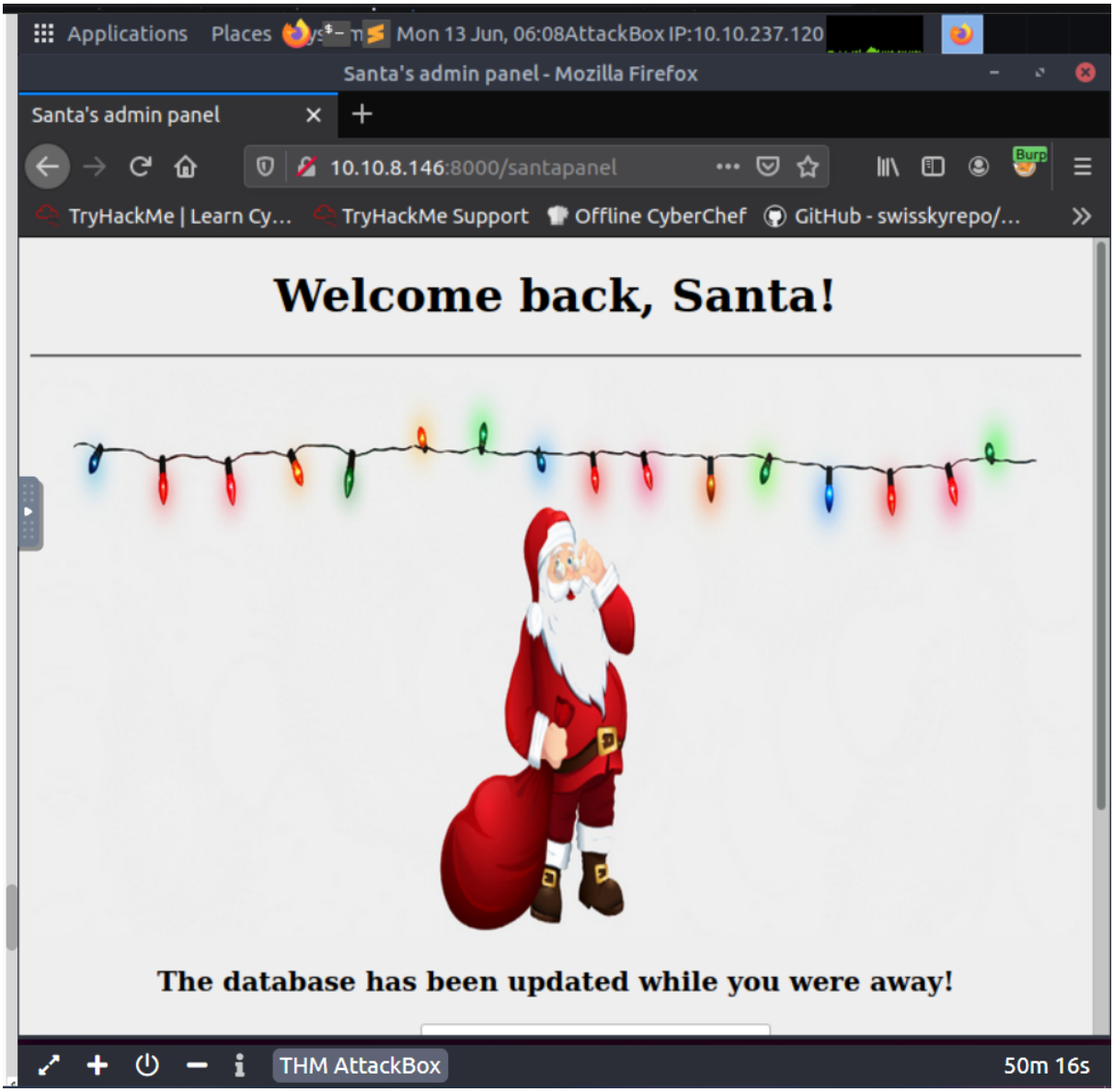
Santa's TODO: Look at alternative database systems that are better than sqlite. Also, don't forget that you installed a Web Application Firewall (WAF) after last year's attack. In case you've forgotten the command, you can tell SQLMap to try and bypass the WAF by using `--tamper=space2comment`



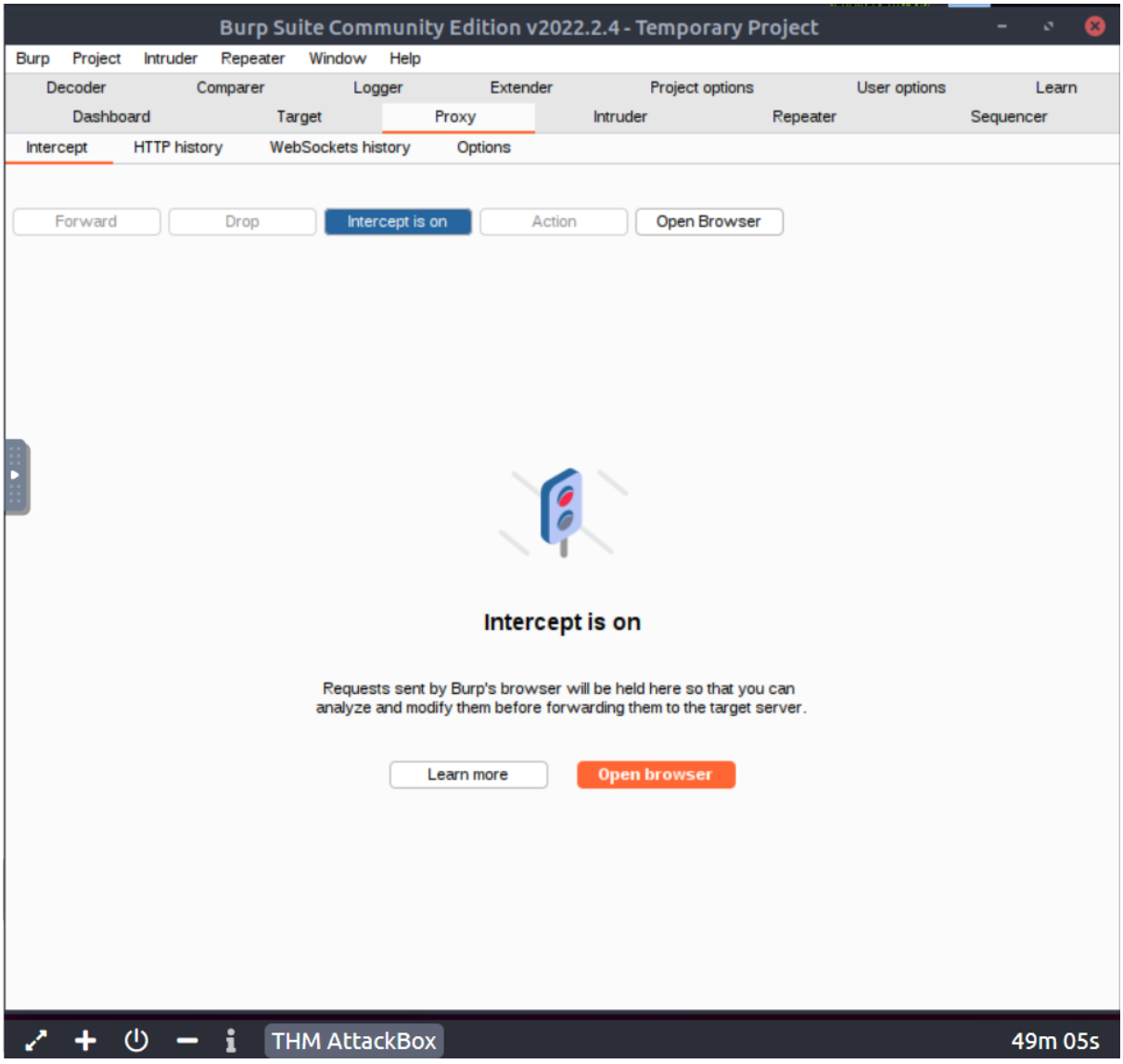
Question 4

How many entries are there in the gift database?

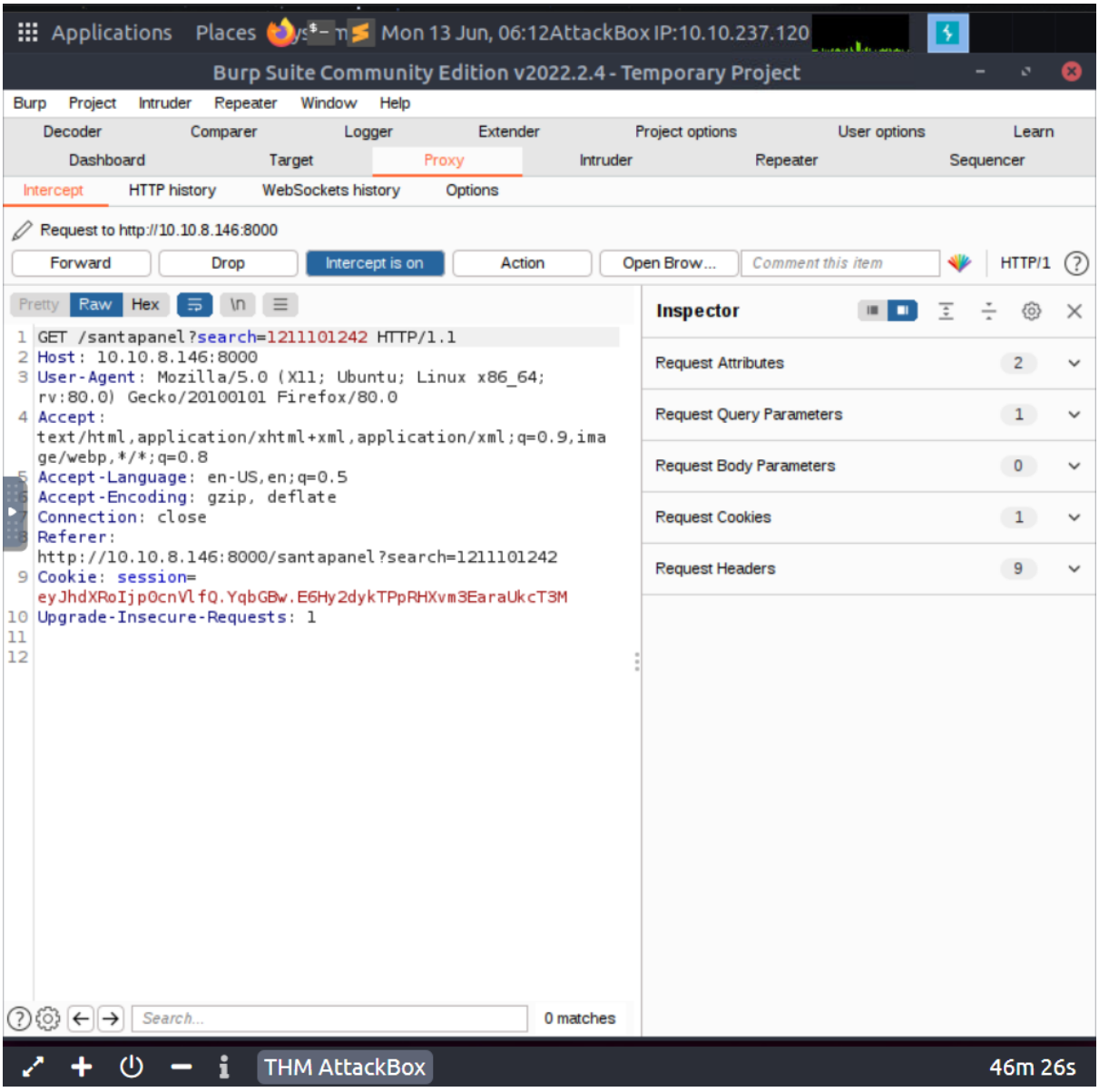
To access the gift's database, Burp must be enabled on the top right corner of the website as shown in the image below.



After doing so, proceed to turn on the intercept on Burp.

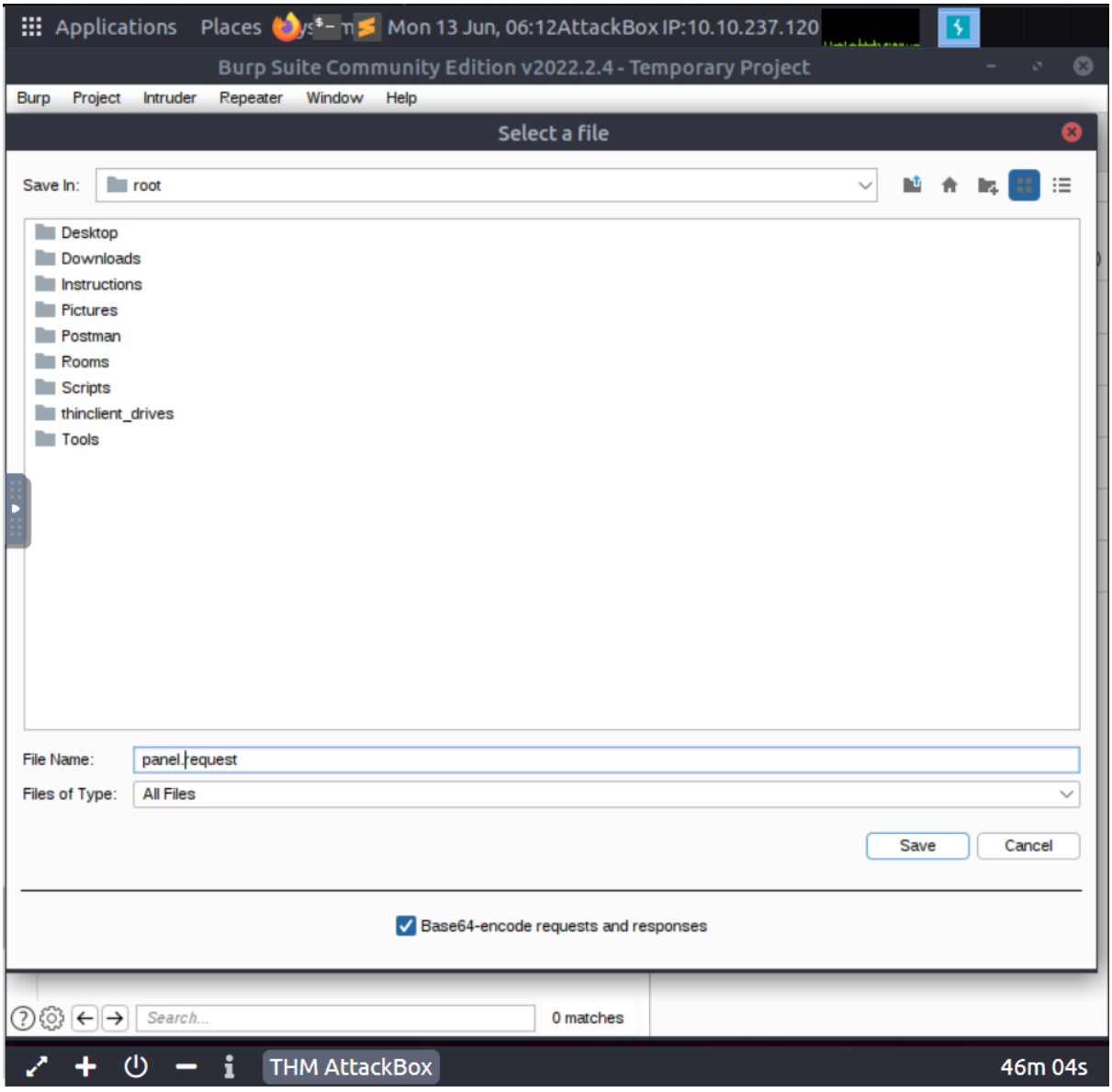


The Raw proxy for website should be the same as shown below in the image.

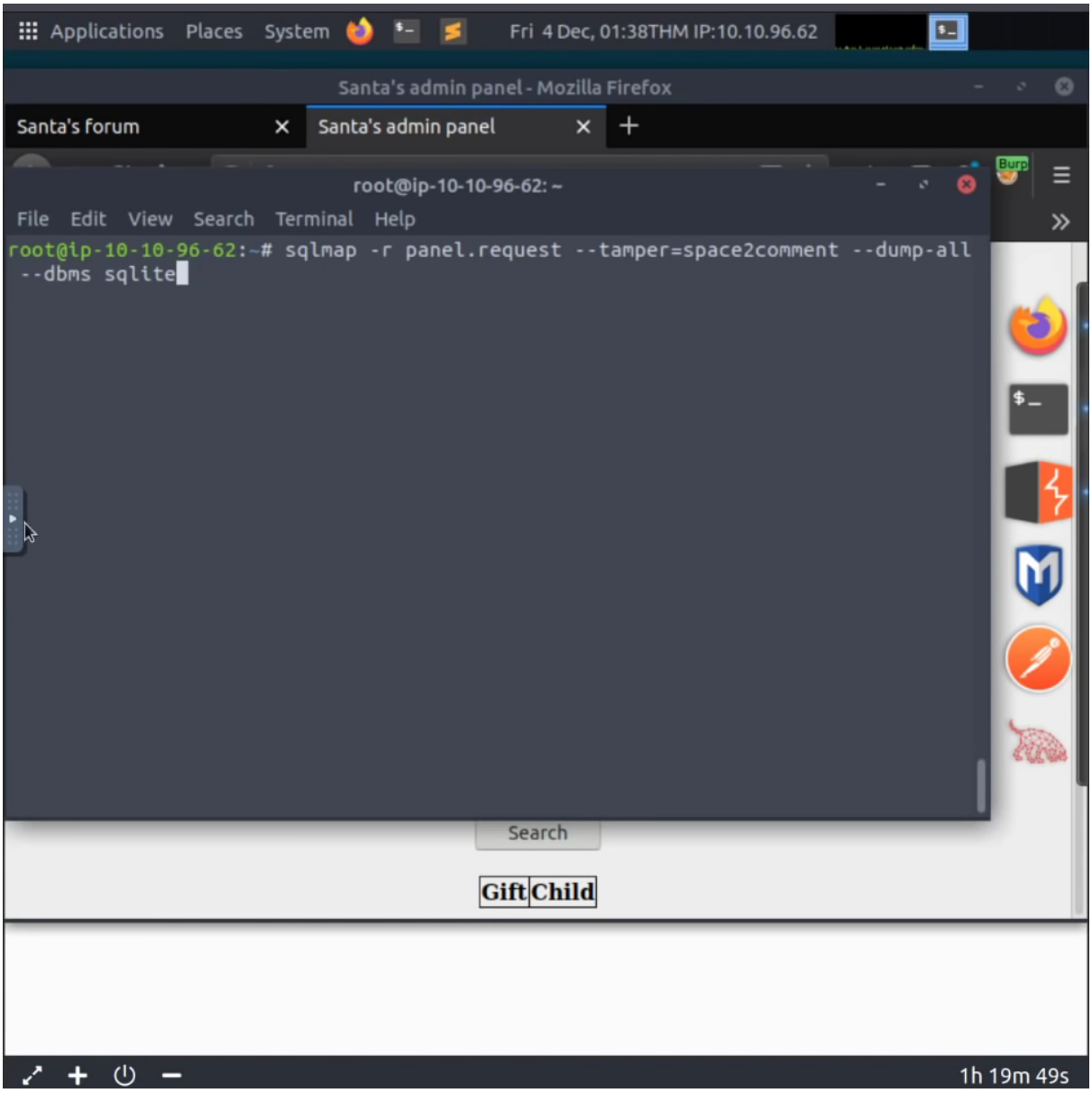


Right-click the Raw proxy and click the ‘Save Item’ option to save it as panel.request (or any other names one prefers)

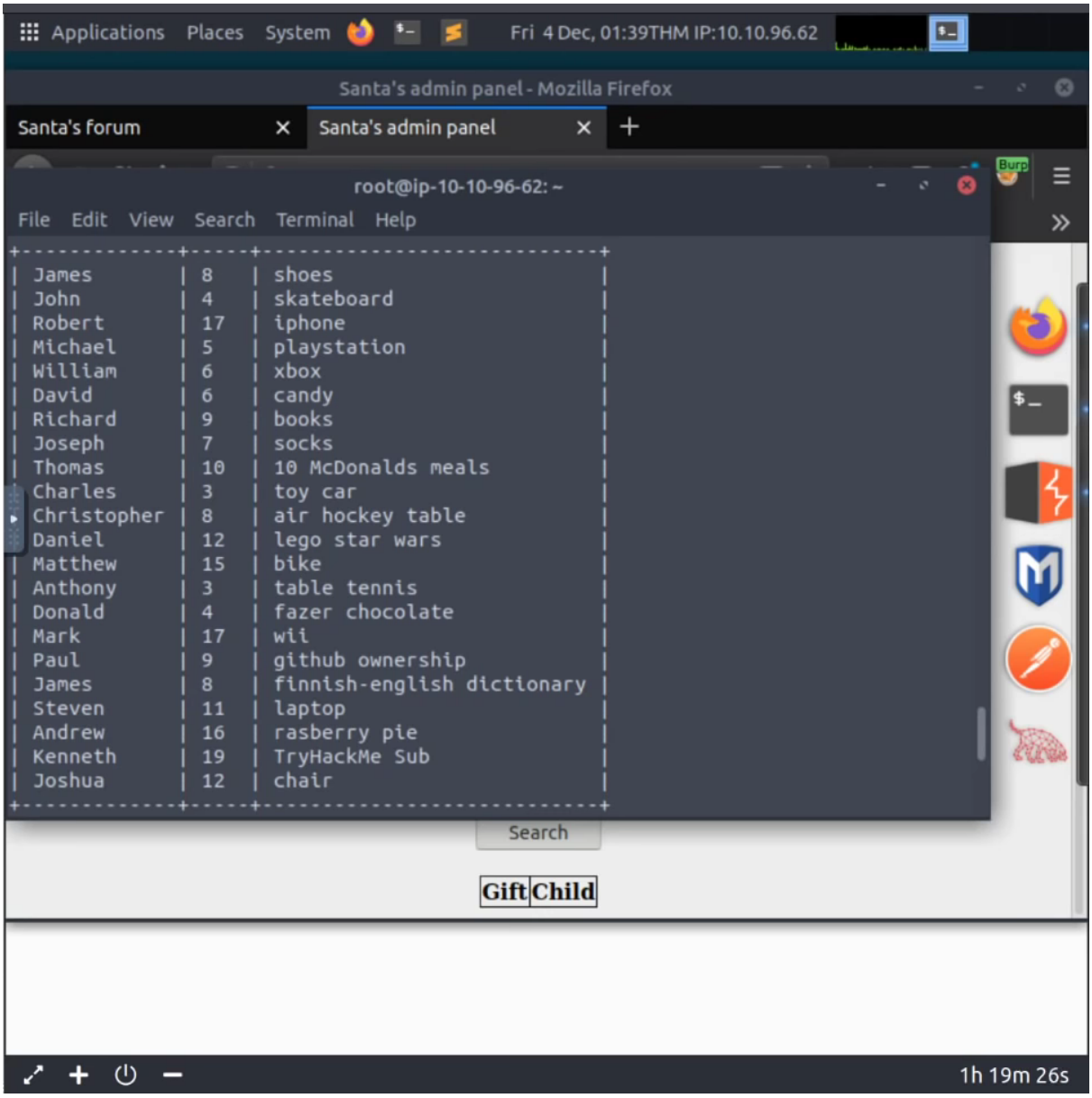
Note that the saved file’s name is important to remember as it is going to be used later in the tasks.



Open up the terminal and type in the command as shown in the image below.



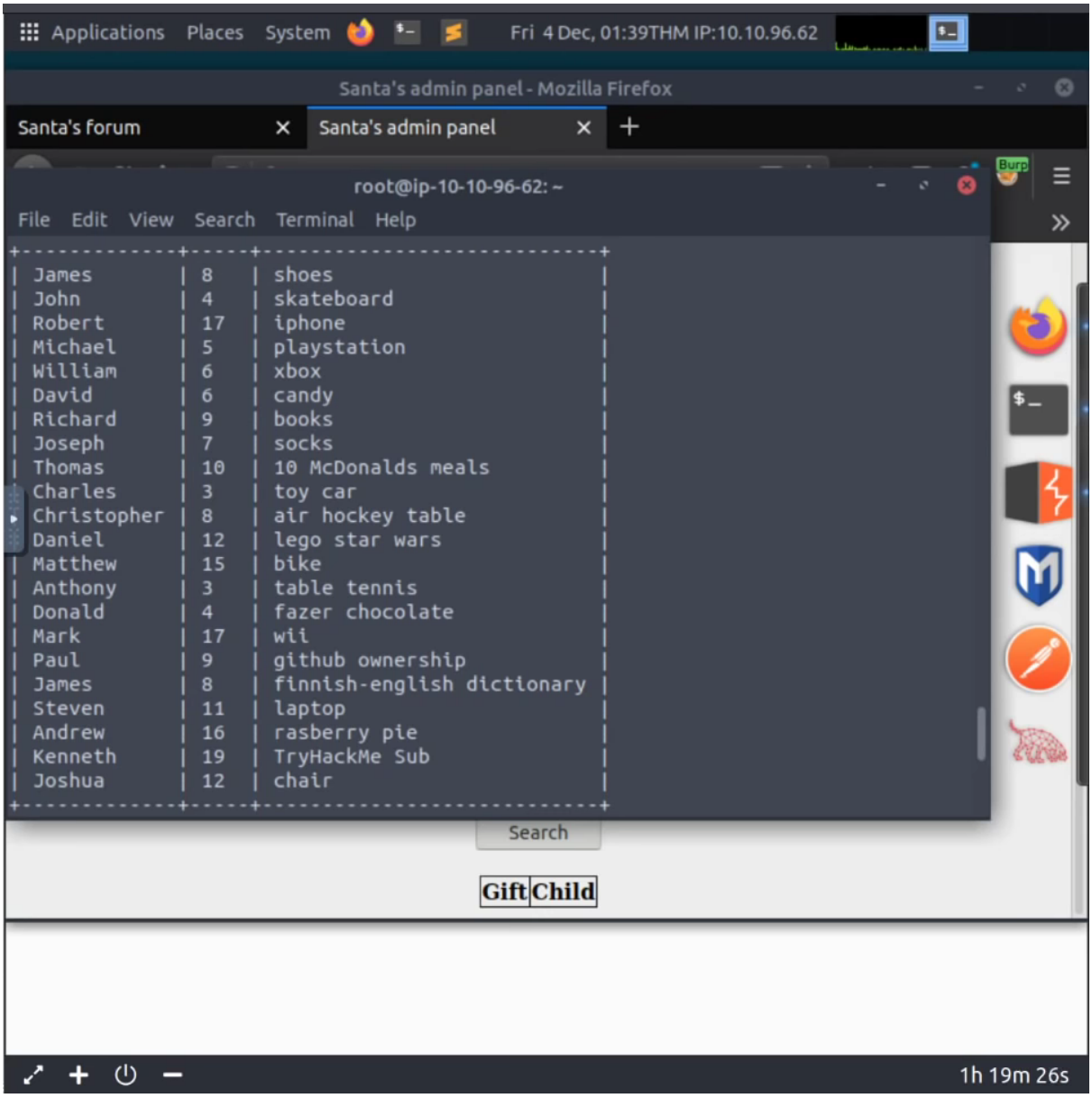
Press enter after typing in the command and scroll down until you see the gift's database count how many entries are there in the database. It should be 22.



Question 5

What is James's age?

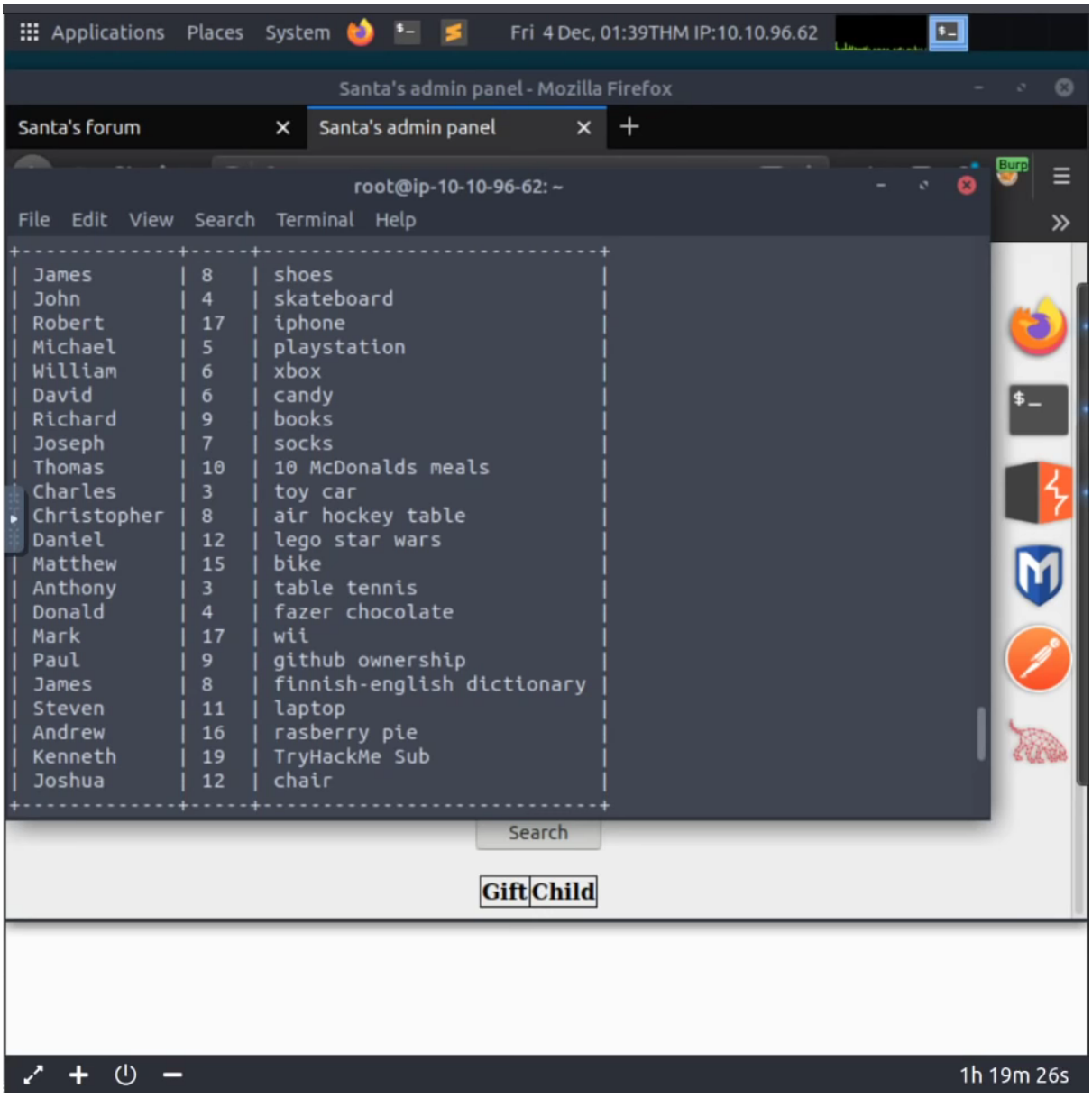
James's age can be found in the database as shown in the image below. It should be 8.



Question 6

What did Paul asked for?

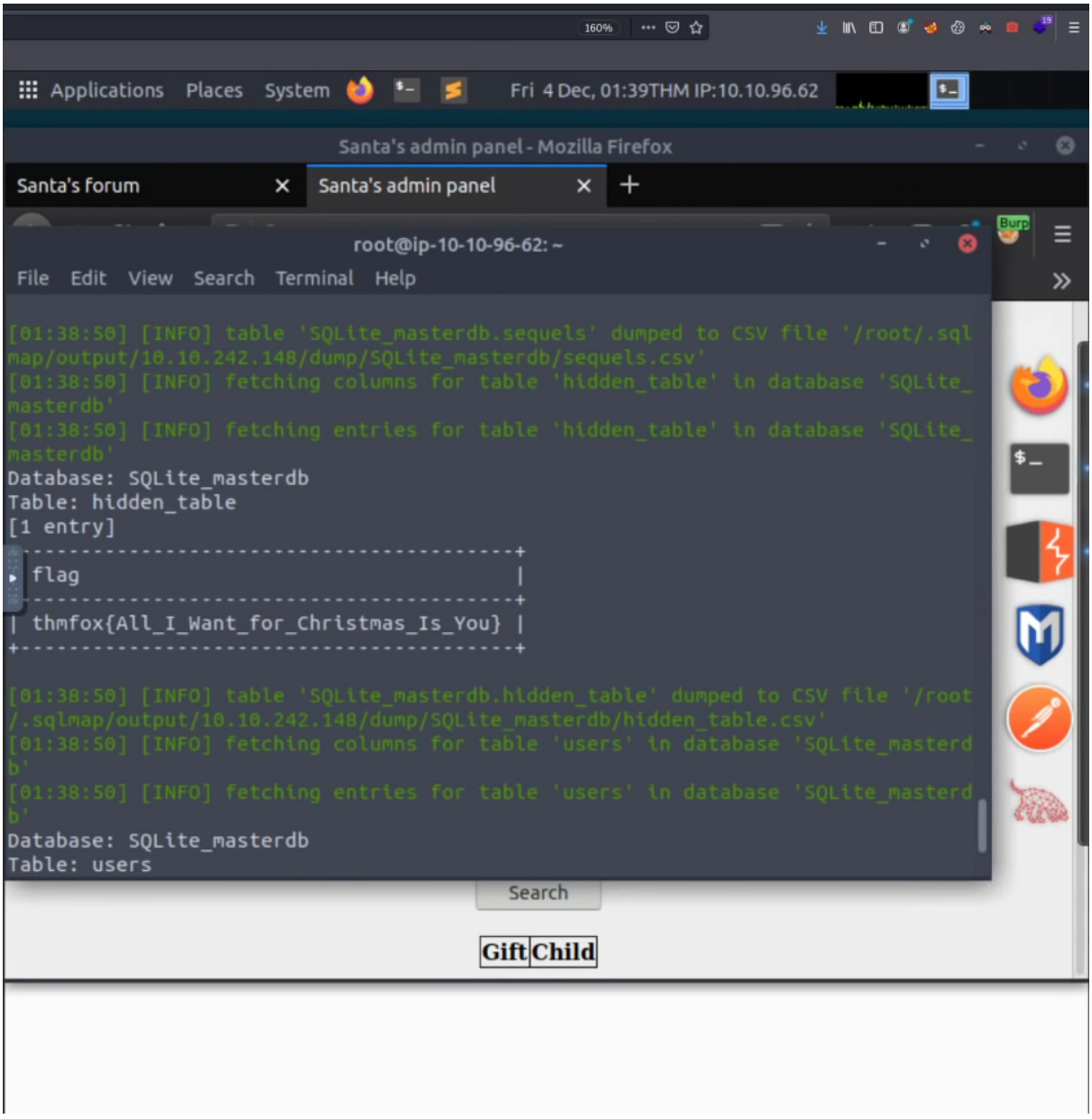
Paul's wishlist can also be found in the database as shown in the image below.



Question 7

What is the flag?

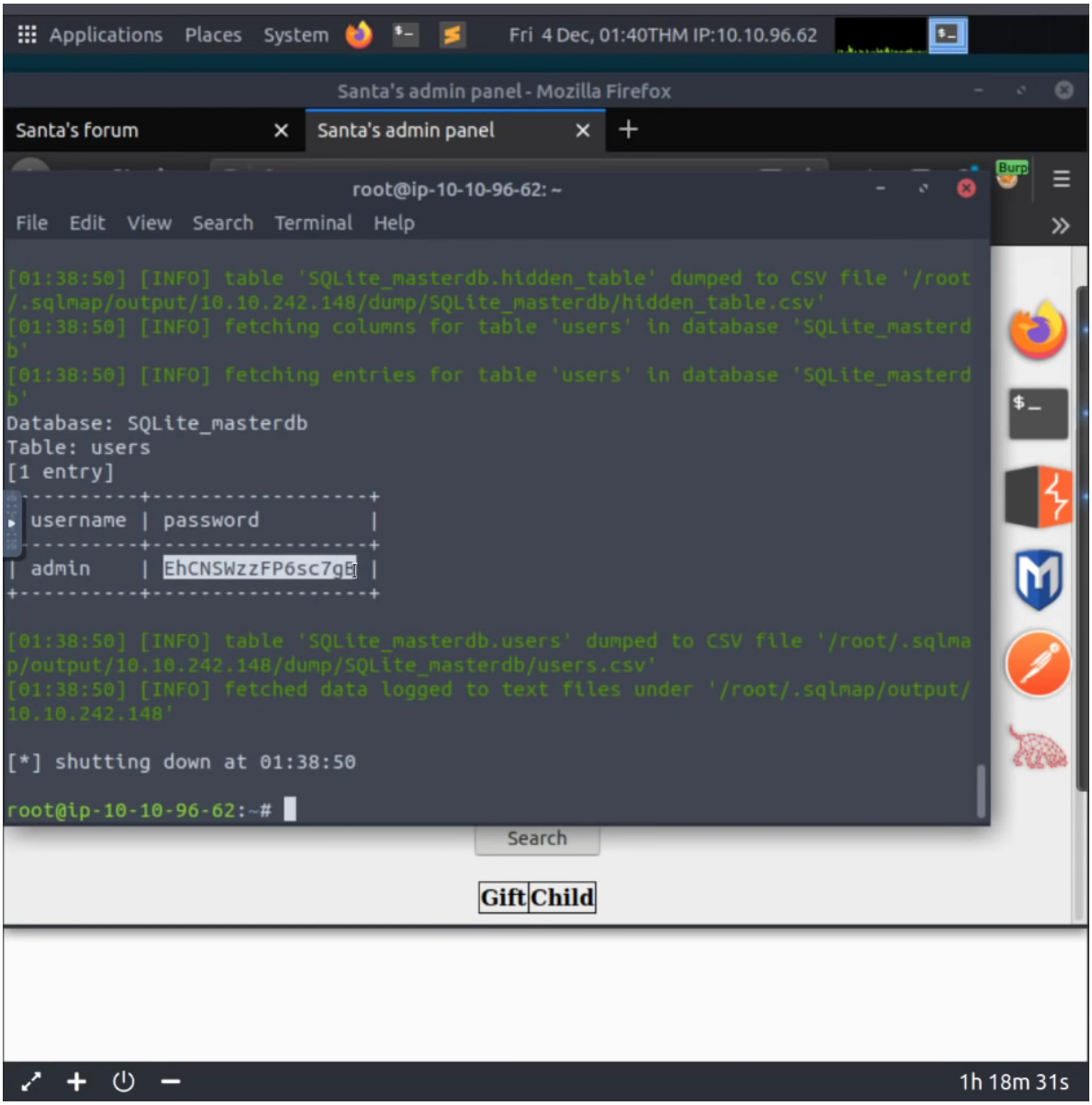
In the database, scroll down the terminal to see the flag for the website as shown in the image below.



Question 8

What is the admin's password?

In the database, scroll down the terminal again to gain access to the admin's password (highlighted for viewing purposes).



Thought Process/Methodology:

The default port number for SQL server running on TCP can be found on Microsoft's documentation through Google searches which is 1433. Having accessed to the target machine, we are exposed to the Santa's forum by typing in the IP address(IP Address:8000) given in the TryHackMe website. In order to access Santa's secret panel, we are required to add /santapanel in the search bar (IP Address:8000/santapanel). In order to gain full access to the website's database, we are required to enable Burp Suite(located at the top right corner of the website) and turn on intercept in the Burp Suite Community Edition to save the website's item under the name panel.request (or any name one prefers, the saved name must be remembered as it is crucial in completing the task later on). After saving the website's item, we need to open up terminal and type in the following command: sqlmap -r panel.request –tamper.space2comment –dump-all –dbms sqlite to gain the website's

database. After doing so, scroll down to gain answers for James’s age, Paul’s wishlist and admin’s password.