PSP0201  
Week 2 write up

Group name: Supreme Chickens

|  |  |  |
| --- | --- | --- |
| ID | NAME | ROLE |
| 1211103024 | Yap Jack | Leader |
| 1211102425 | Ang Hui Yee | MEMBER |
| 1211101198 | Fam YI Qi | MEMBER |
| 1211103978 | Yong Dick Shen | MEMBER |

Day1 [Web Exploitation]-A Christmas Crisis

Solutions/Walkthrough

Tools used: Kali Linux

Q1 Inspect the website. What is the title of the website?

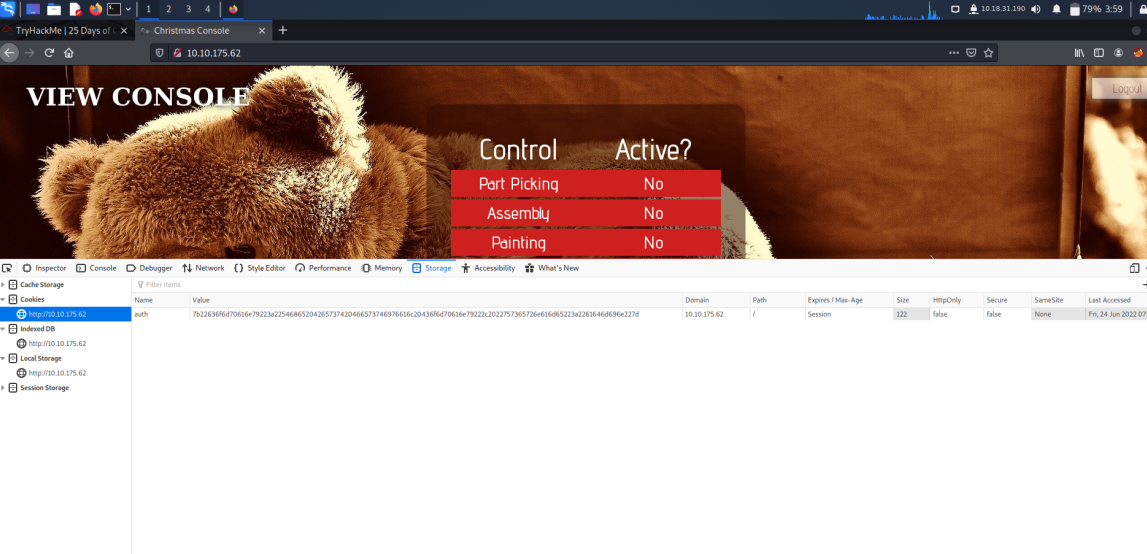
SOLUTION:

Register a account and login , after that I inspected the web and found the title of the website



Q2 What is the cookie used for authentication

SOLUTIONS: After I found the web name I also have found the cookie name



Q3 In what formed is value of the cookies encoded

Q4 Having decoded the cookie, what format is the cookie stored in

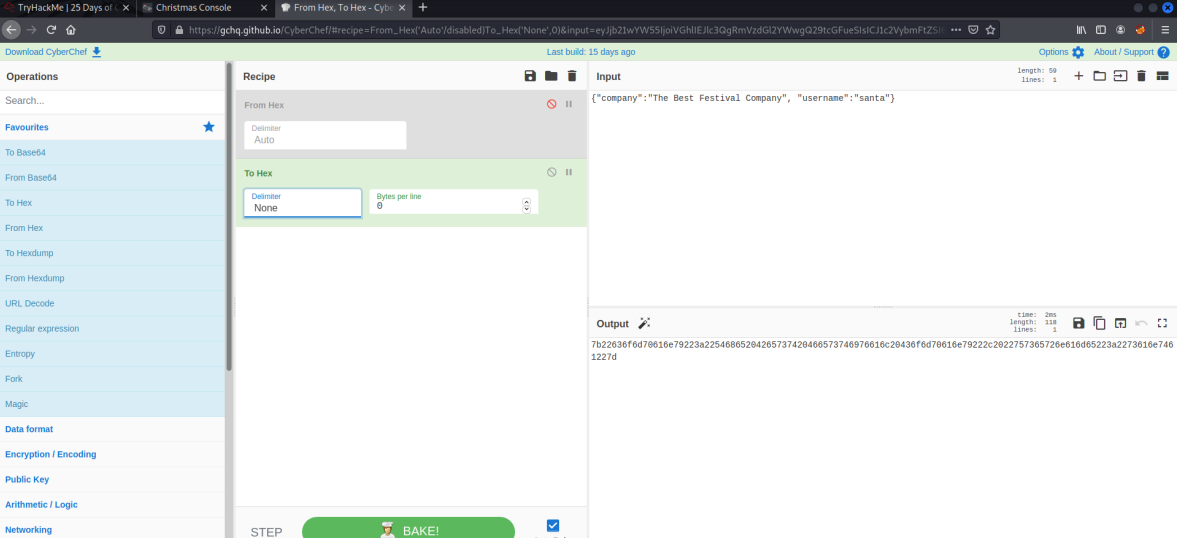
Q5 What is the value in the company field in the cookies

Q6 What is the other value found in the cookies

Q7 What is the value of the santa?

SOLUTION:

Based on the cookie we could know that it’s a hex based. After I decoded it we can see the output is using JSON format and I have also changed the username from the output given to santa since santa’s account name is santa so that I am able to get santa’s cookie value. The value in the company field is The Best Festival Company and we can see that the other value is “username”.



Q8 What is the flag you are given when the line is fully active

SOLUTION:

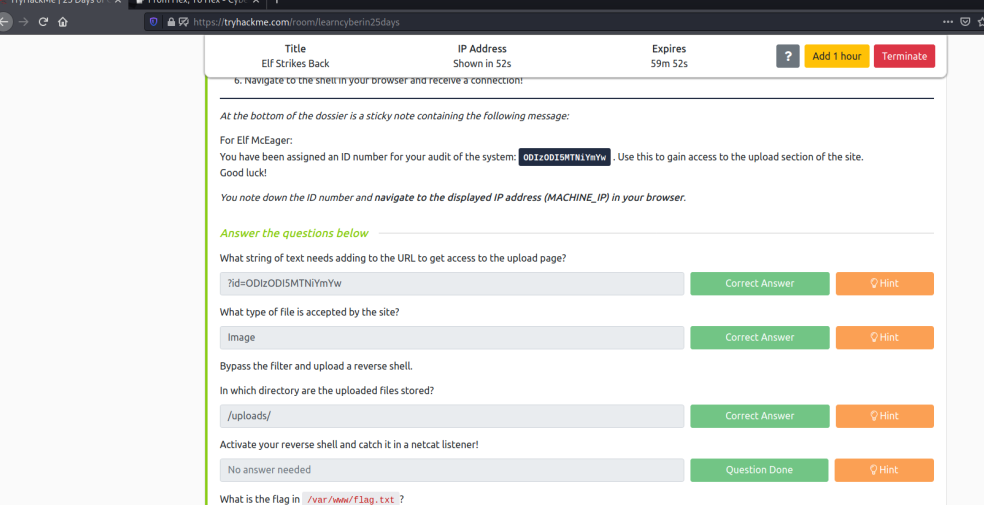
After getting santa’s cookie, I replace the org cookies’ value to the santa’s one.



DAY2- [WEB EXPLOITATION] THE ELF STRIKE BACK

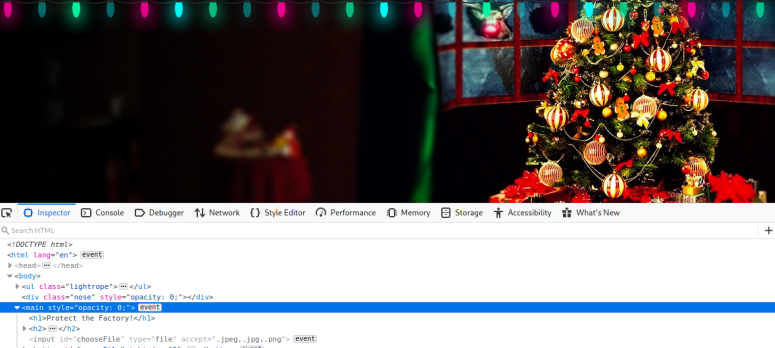
Q1 What string of the text needs adding to the URL to get access to the upload page

SOLUTION: From THM has given the hint to get us to the upload page



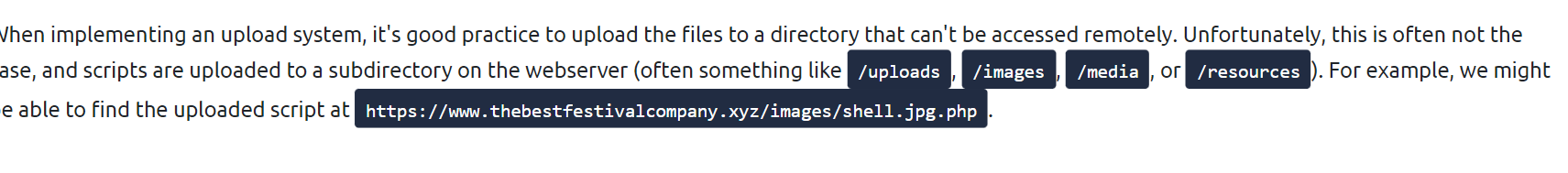
Q2 What type of file is accepted by the site

SOLUTION: After inspecting the web, I know that the web is only accepting image



Q3 In which directory are the uploaded files stored at

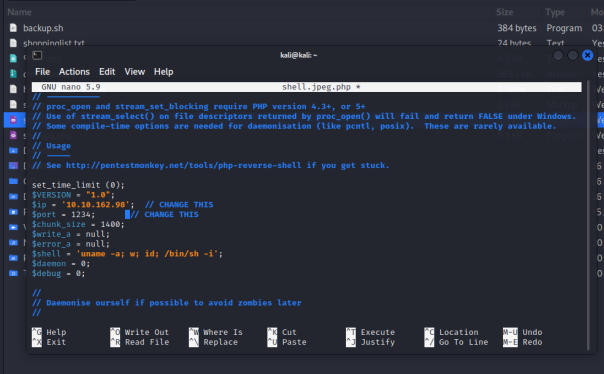
SOLUTION: Based on the information given by THM I was able to reach the upload page by guessing each of them



Q4 Read up on the netcat’s parameter explanations. Match the parameter with the explanation below

Q5 What is the flag in /var/www/flag.txt

SOLUTION: I have match the parameter with the information given in this website (<https://www.varonis.com/blog/netcat-commands>) and I was able to retrieved the flag after activated netcat.

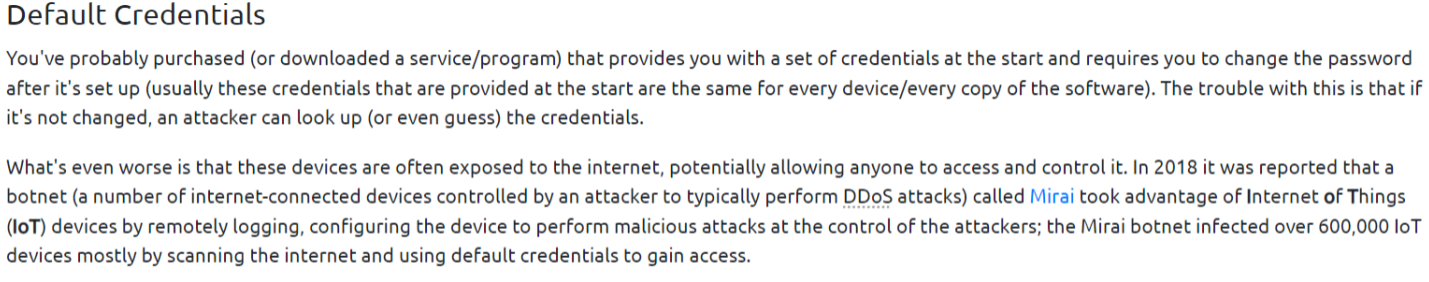


DAY3 – [WEB EXPLOITATION] Christmas Chaos

TOOLS USED: Burpsuite, foxyproxy

Q1  What is the name of the botnet mentioned in the text that was reported in 2018?

SOLUTION:



Q2 How much did Starbucks pay in USD for reporting default credentials according to the text?

SOLUTION:

250 dollars

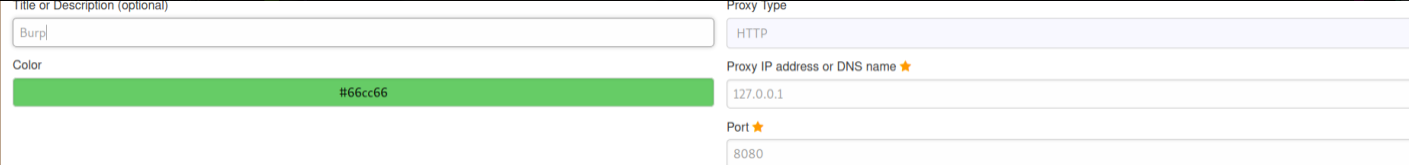
Q3: Read the report from Hackerone ID:804548 - who was the agent assigned from the Dept of Défense that disclosed the report on Jun 25th?



Q4: Examine the options on FoxyProxy on Burp. What is the port number for Burp?

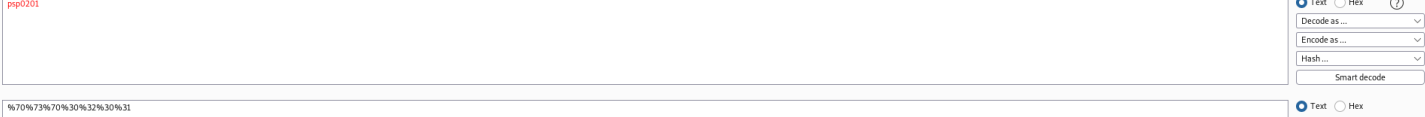
Q5: Examine the options on FoxyProxy on Burp. What is the proxy type?

SOLUTION: Its HTTP and port 8080



Q6: Experiment with decoder on Burp. What is the URL encoding for "PSP0201"?

SOLUTION:

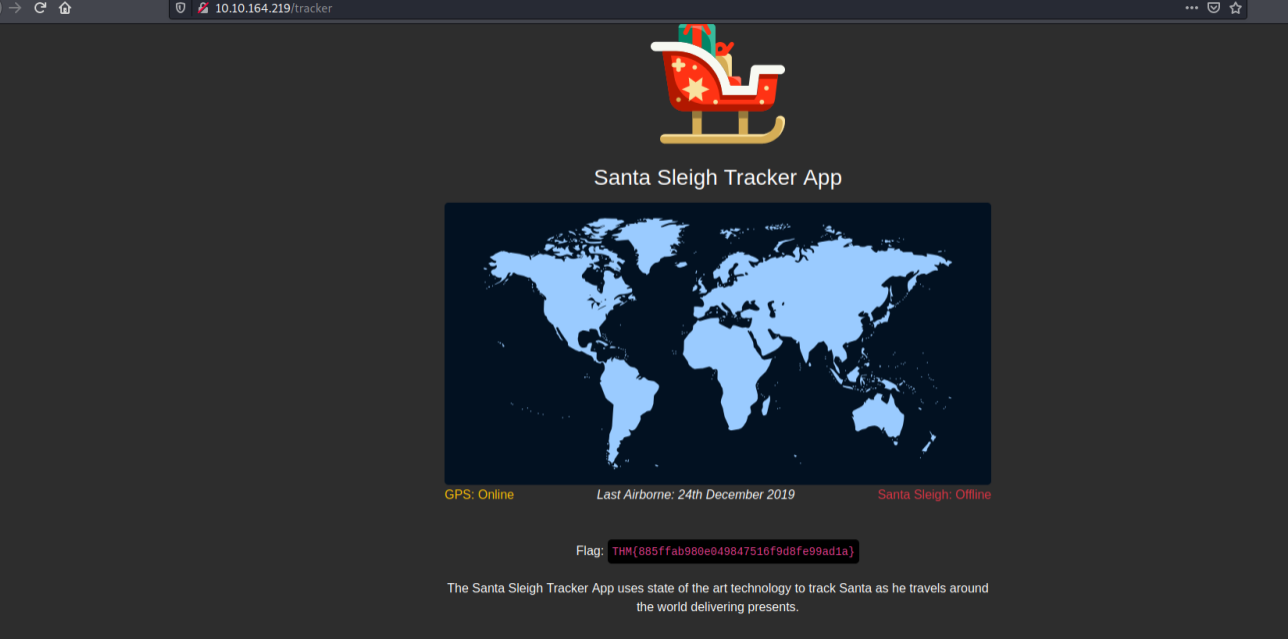


Q7 Look at the list of attack type options on intruder. Which of the following options matches the one in the description?

SOLUTION: Cluster bomb uses multiple payload sets. Different payload for each defined position up to maximum 20.

Q8 What is the flag?

SOLUTION: Found the flag after brute force login the website



DAY4 – [WEB EXPLOITATION] Santa’s watching

TOOLS USED: Kali Linux, gobuster, wfuzz

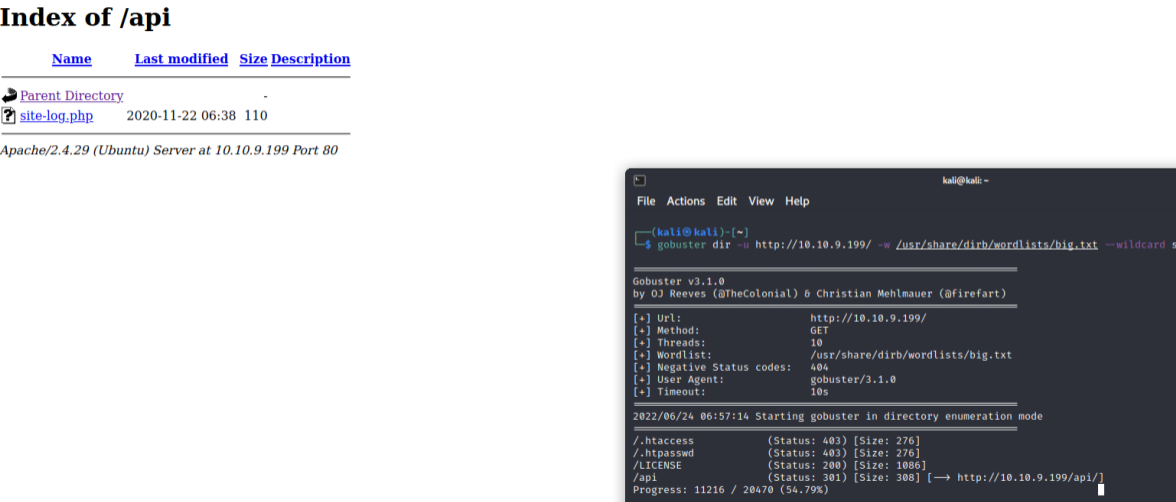
Q1 Given the URL "<http://shibes.xyz/api.php>", what would the entire wfuzz command look like to query the "breed" parameter using the wordlist "big.txt" (assume that "big.txt" is in your current directory)

SOLUTION:



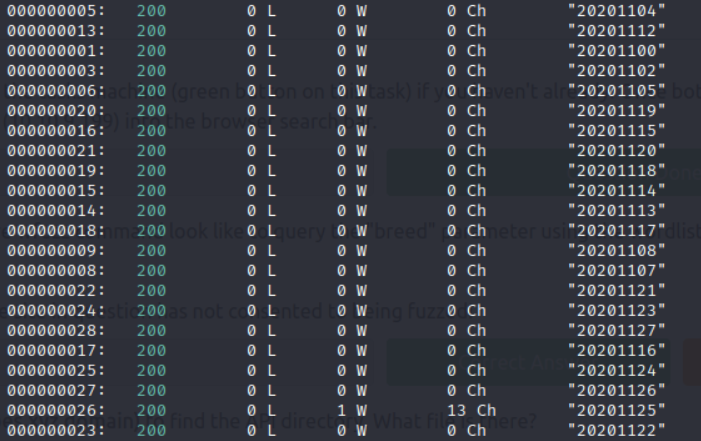
Q2 Use GoBuster (against the target you deployed -- not the [shibes.xyz](http://shibes.xyz/) domain) to find the API directory. What file is there?

SOLUTION: Found a site-log.php



Q3: Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?

SOLUTION: After fuzzing we got the date parameter and got the flag.





Q4: Look at wfuzz's help file. What does the -f parameter store results to?

SOLUTION: Printer and filename.

DAY5 – [WEB EXPLOITATION] Someone stole Santa’s gift list!

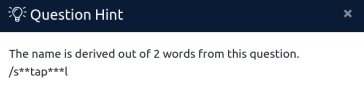
TOOLS USED: Kali Linux, Sql, Burpsuite

Q1: What is the default port number for SQL Server running on TCP?

SOLUTION: According to google, its TCP 1433

Q2: Without using directory brute forcing, what's Santa's secret login panel?

SOLUTION: From the hint given we can guess it is /santapanel



Q3: What is the database used from the hint in Santa's TODO list?

Q4: How many entries are there in the gift database?

Q5: What is James' age?

Q7: What is the flag?

Q8: What is admin's password?

SOLUTION: After saved the file from burpsuite repeater, I use “sqlmap -r filename” to request in SQLMap with “—tamper=space2comment” to bypass the WAF and “—dbms” to tell SQLMap the type of the database running with “—dump-all” to dump the entire database and finally we reached the answers.

