PSP0201

Week 2

Writeup

Group Name: Undecided

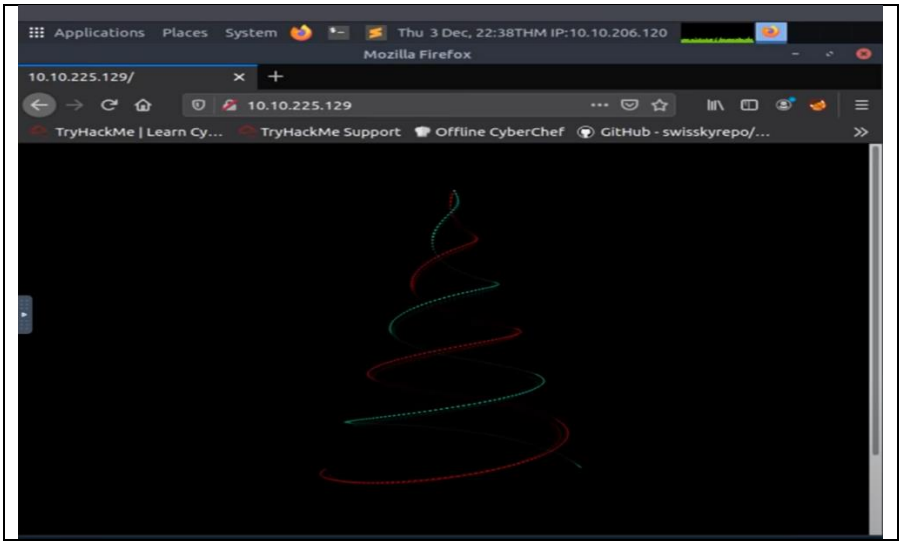
Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha Binti Muhd Firdaus	Member

Day 4: Web Exploitation – Santa's Watching

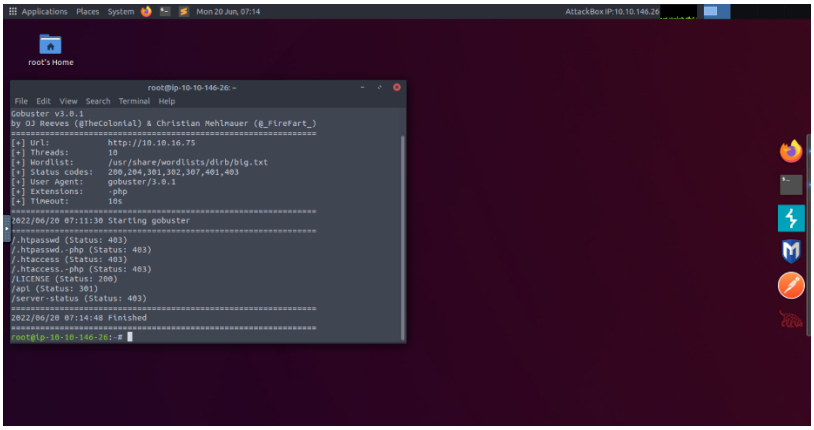
Tool used: Kali Linux, Firefox and terminal

Here we can see hackers destroyed our login page, so we need to retrieve it.



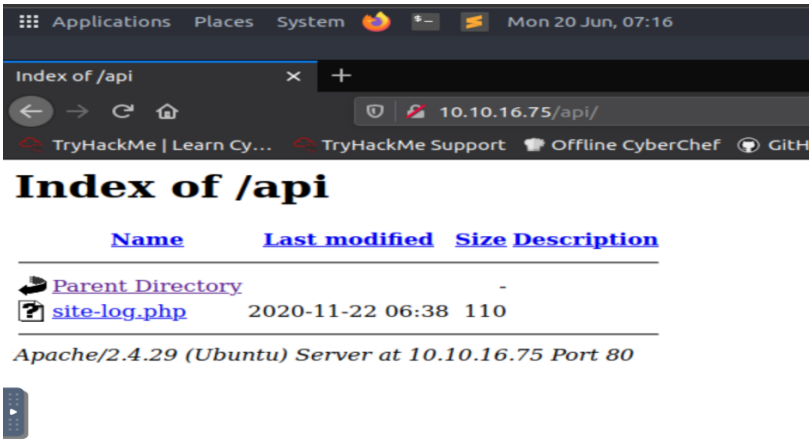
Question 1

Finding if api channel is still open, Code used- gobuster dir -u http://MachineIP -w /usr/share/wordlists/dirb/big.txt -x .php



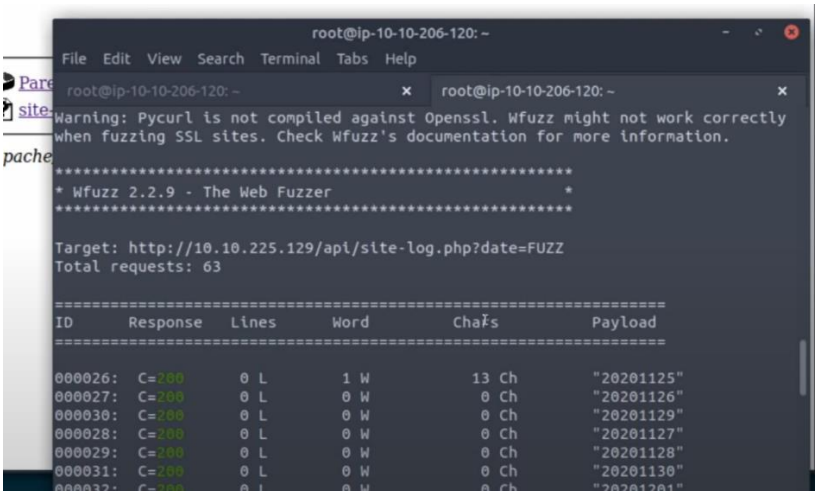
Question 2

After seeing api channel open, we checked on browser. When we added the path in the URL, it showed the directory and the log file as added in the photo above.

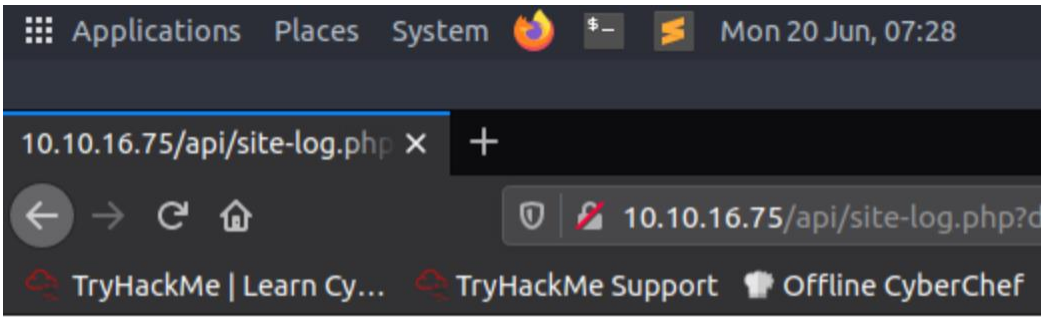


Question 3

We fuzzed the parameter on the file that we found in the API directory. Then, we enter the date parameter with the first value that we found from the payload obtained from the fuzz.



With the new URL, we were led to a page where our flag was displayed.



THM{D4t3_AP1}

Question 4

With the command 'man wfuzz', we understood that the -f parameter store results to printer.

Thought Process/Methodology:

After getting hacked, Santa's login page was removed. However, admin informed that we might still have the access to API, thus first we tried to find if the API is still working in the backhand. Hence,in the terminal using gobuster, which is a tool to find directories if they exist, we found out that the server /api status is available using the 'gobuster dir -u http://MachineIP -w /usr/share/wordlists/dirb/big.txt -x .php' command. We decided to fuzz with the command 'wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ'. With a value that we obtained from the fuzz, we enter a new parameter into the URL. We use the payload '20201125' because it has different value of chars than the others. Once the page loaded, we obtained our flag.