

DAY 4: Web Exploitation Santa's watching

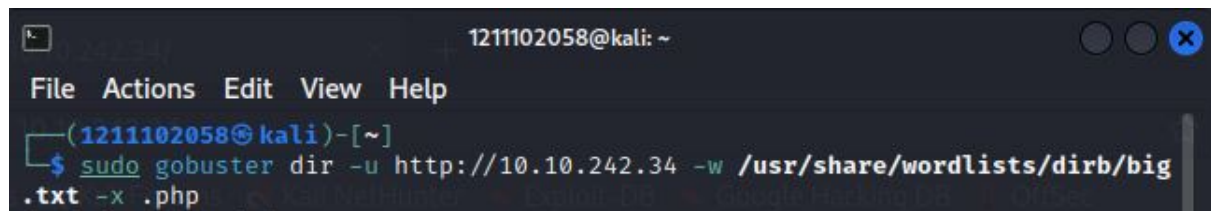
Tool used: kali Linux, Firefox, Gobuster

Solution/Walkthrough:

Q1

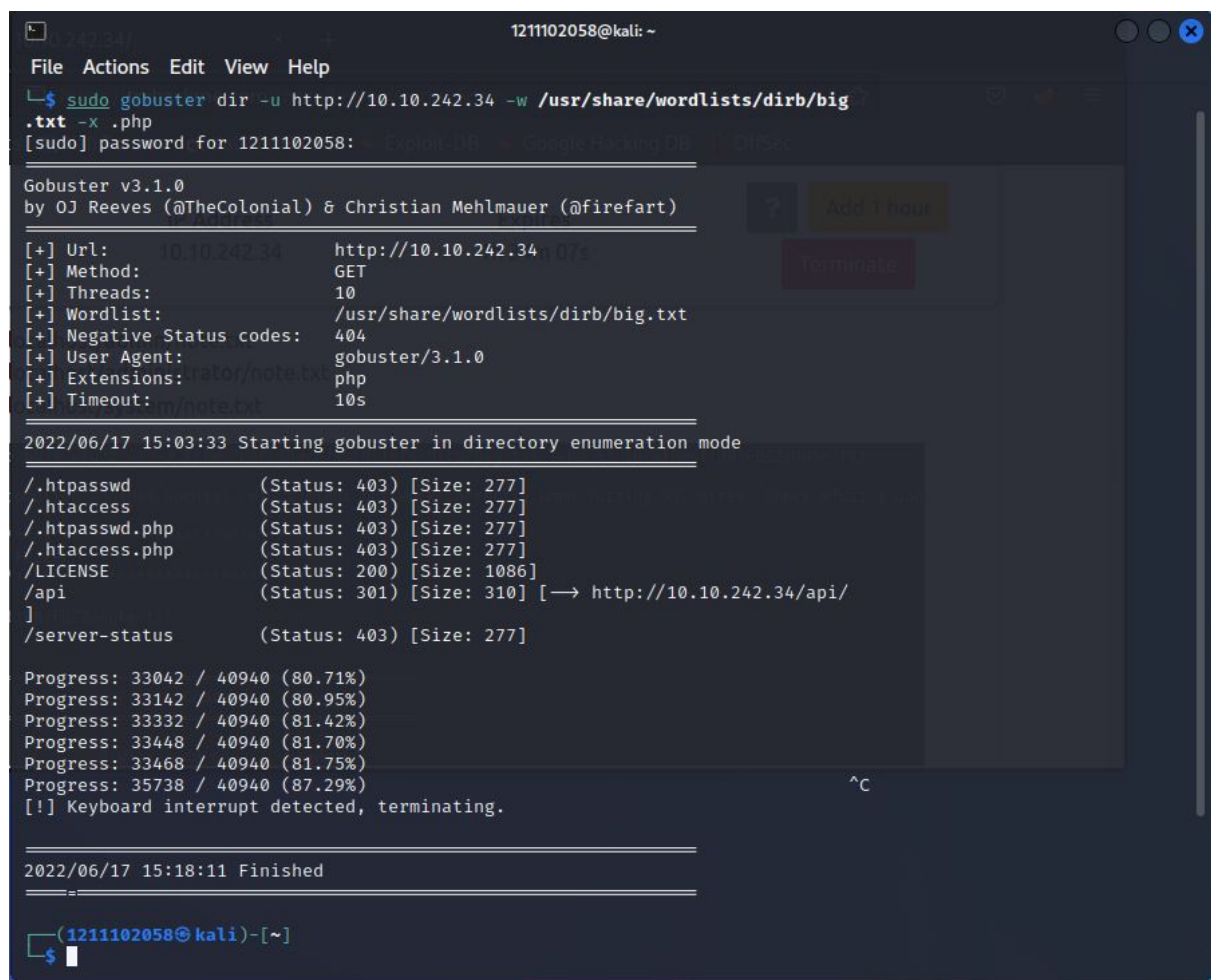
The format of the command is 'wfuzz <flag>, <wordlist> <url>?<parameter>=FUZZ'. Therefore, substitute all given info into the places and the arrangement is found.

Q2



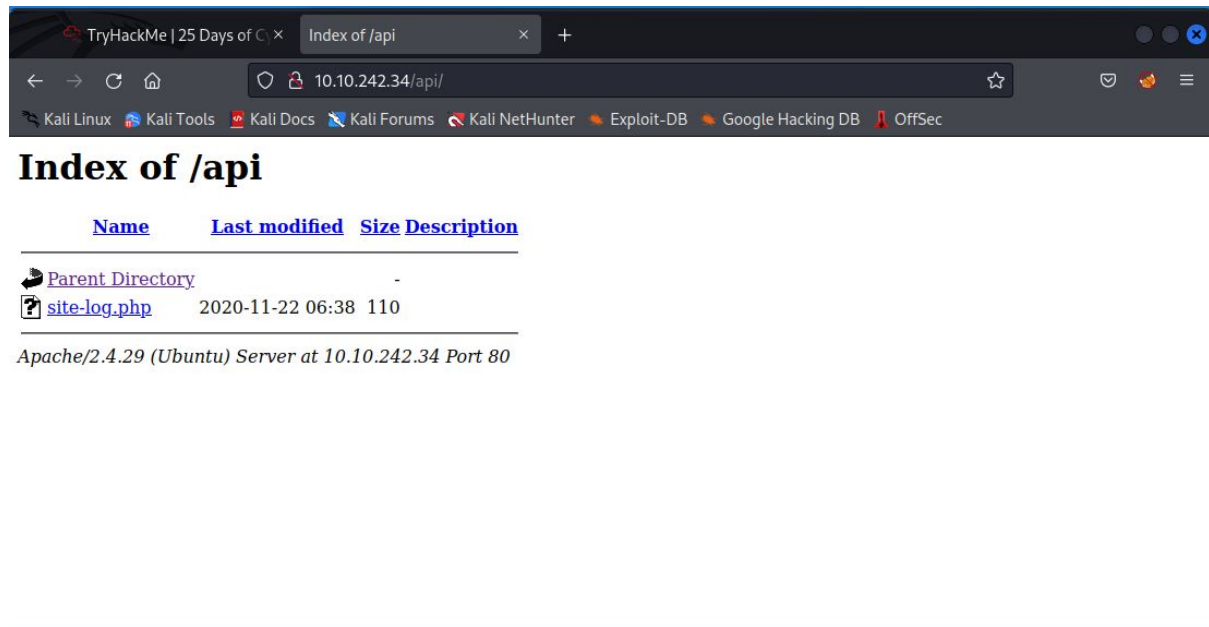
```
1211102058@kali: ~  
File Actions Edit View Help  
(1211102058@kali)-[~]  
$ sudo gobuster dir -u http://10.10.242.34 -w /usr/share/wordlists/dirb/big.txt -x .php
```

Open panel. Then use Gobuster toward the given IP address by typing the command shown. This initiates it.



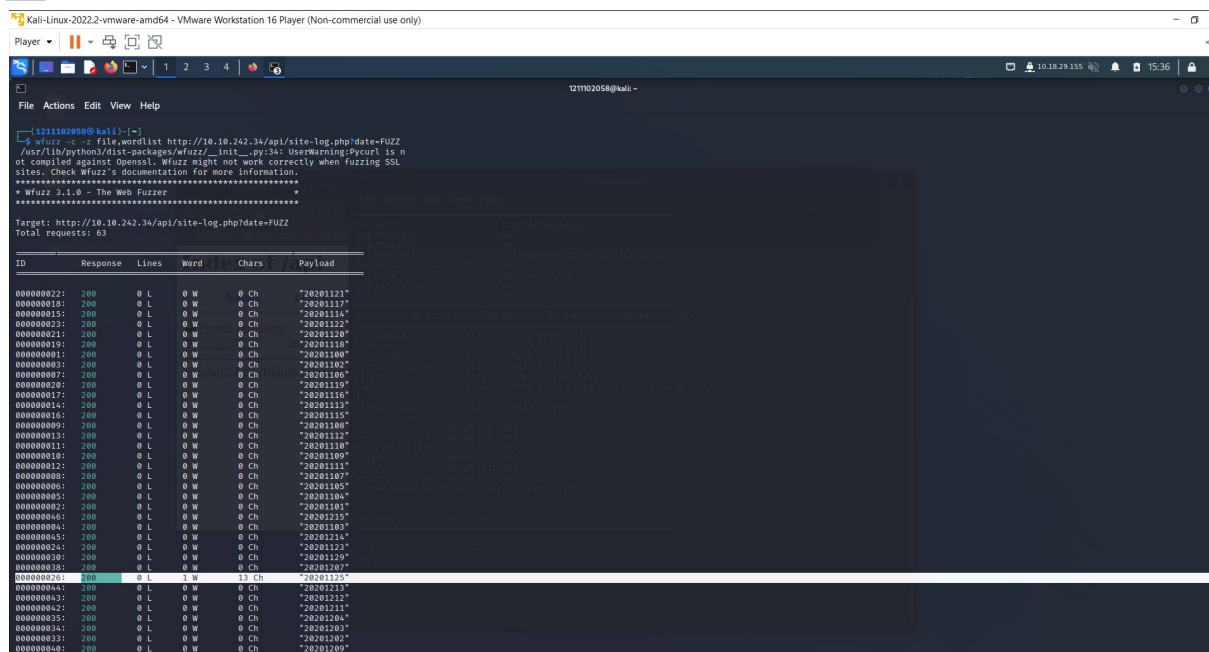
```
1211102058@kali: ~  
File Actions Edit View Help  
$ sudo gobuster dir -u http://10.10.242.34 -w /usr/share/wordlists/dirb/big.txt -x .php  
[sudo] password for 1211102058:  
Gobuster v3.1.0  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
[+] Url: 10.10.242.34 http://10.10.242.34/07s  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/wordlists/dirb/big.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.1.0  
[+] Extensions: rator/note.txt php  
[+] Timeout: rator/note.txt 10s  
2022/06/17 15:03:33 Starting gobuster in directory enumeration mode  
/.htpasswd (Status: 403) [Size: 277]  
/.htaccess (Status: 403) [Size: 277]  
/.htpasswd.php (Status: 403) [Size: 277]  
/.htaccess.php (Status: 403) [Size: 277]  
/LICENSE (Status: 200) [Size: 1086]  
/api (Status: 301) [Size: 310] [→ http://10.10.242.34/api/  
]  
/server-status (Status: 403) [Size: 277]  
Progress: 33042 / 40940 (80.71%)  
Progress: 33142 / 40940 (80.95%)  
Progress: 33332 / 40940 (81.42%)  
Progress: 33448 / 40940 (81.70%)  
Progress: 33468 / 40940 (81.75%)  
Progress: 35738 / 40940 (87.29%)  
[!] Keyboard interrupt detected, terminating.  
2022/06/17 15:18:11 Finished  
(1211102058@kali)-[~]  
$
```

After some time, we found the API directory. Copy the url and paste it on the search bar.

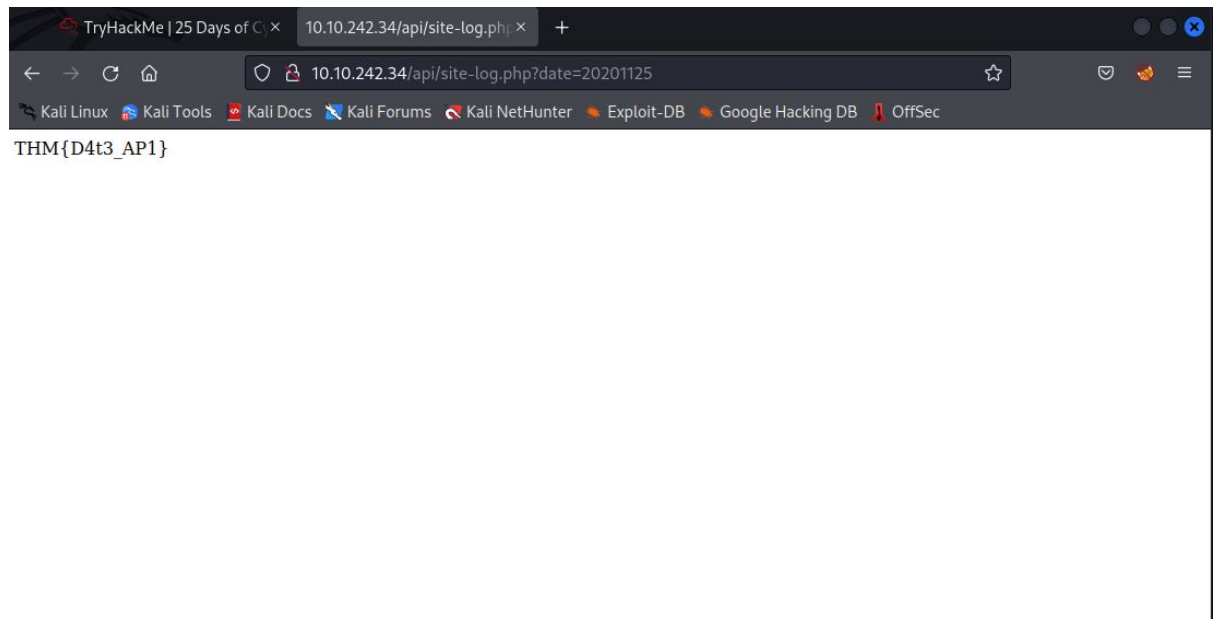


In the site, there is a file named 'site-log.php'.

Q3

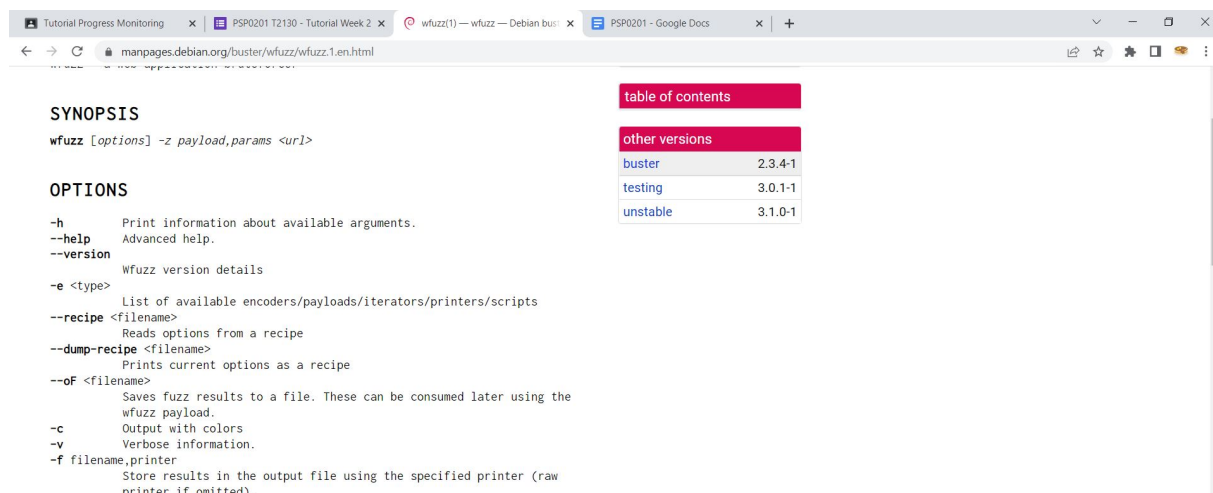


Use `wfuzz`. Examine the output and find a line that is different from others.



Return to the site and modify the url with the specific date found. Capture the flag.

Q4



Research and study from here.