

PSP0201

Week 2

Writeup

Group Name: ikun no 1

Members

ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

DAY 4: Web Exploitation Santa's watching

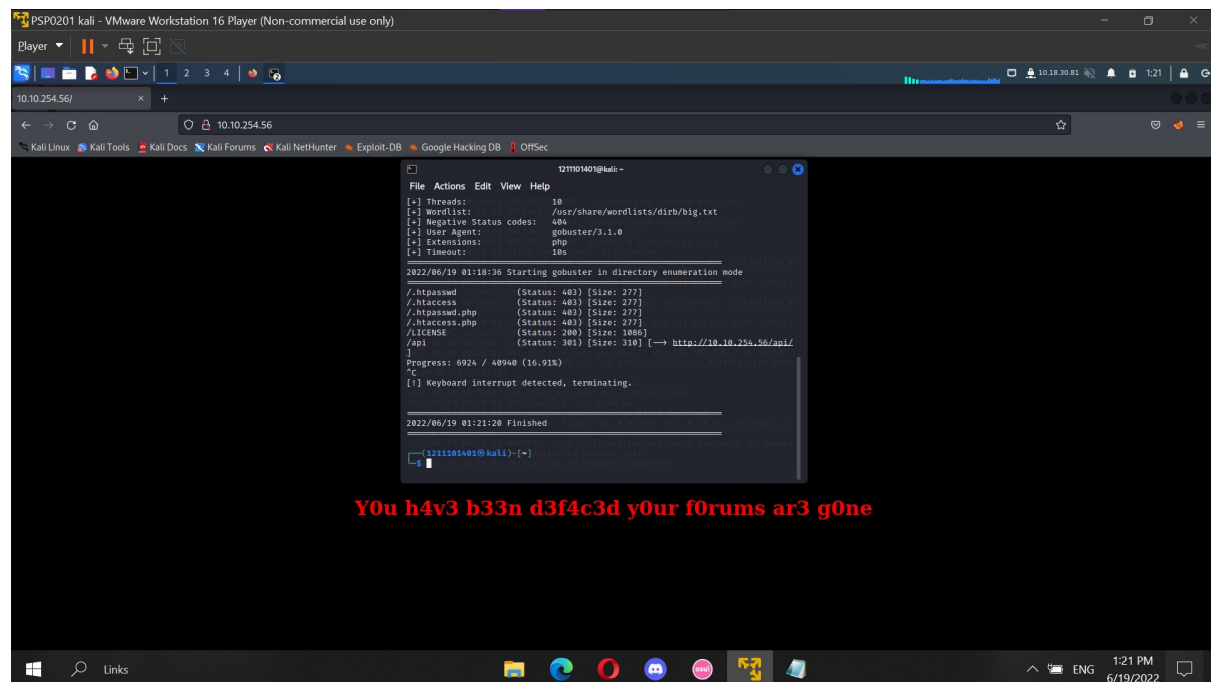
Tool used: kali Linux, Firefox, Gobuster

Solution/Walkthrough:

Q1

The format of the wfuzz is wfuzz <flag>,<wordlist> <url>?<parameter>=FUZZ'. Fill in the options into the format and the answer can be get.

Q2

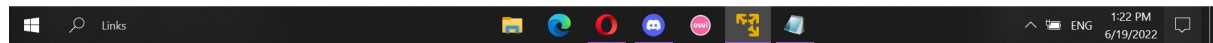
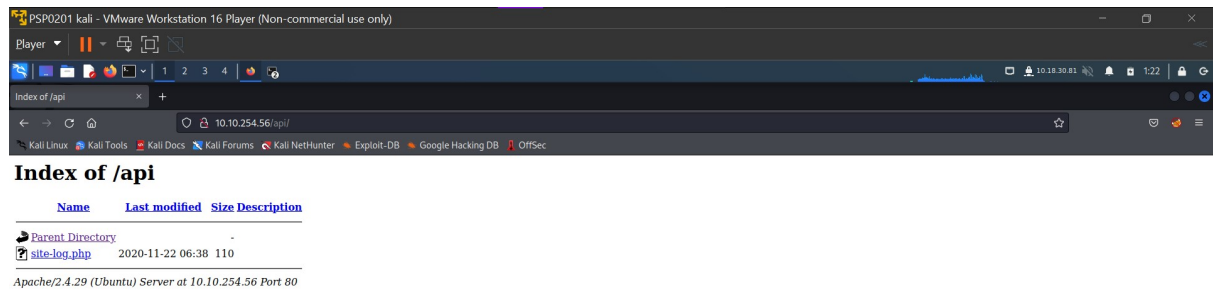


```
121101401@kali:~$ gobuster -u http://10.10.254.56/ -w /usr/share/wordlists/dirb/big.txt -x .php
2022/06/19 01:18:36 Starting gobuster in directory enumeration mode
./htpasswd      (Status: 403) [Size: 277]
./htaccess      (Status: 403) [Size: 277]
./htpasswd.php  (Status: 403) [Size: 277]
./htaccess.php  (Status: 403) [Size: 277]
./LICENSE       (Status: 200) [Size: 1806]
/api            (Status: 303) [Size: 310] [→ http://10.10.254.56/api/]
Progress: 6924 / 40940 (16.91%)
^C
[!] Keyboard interrupt detected, terminating.

2022/06/19 01:21:20 Finished
121101401@kali:~$
```

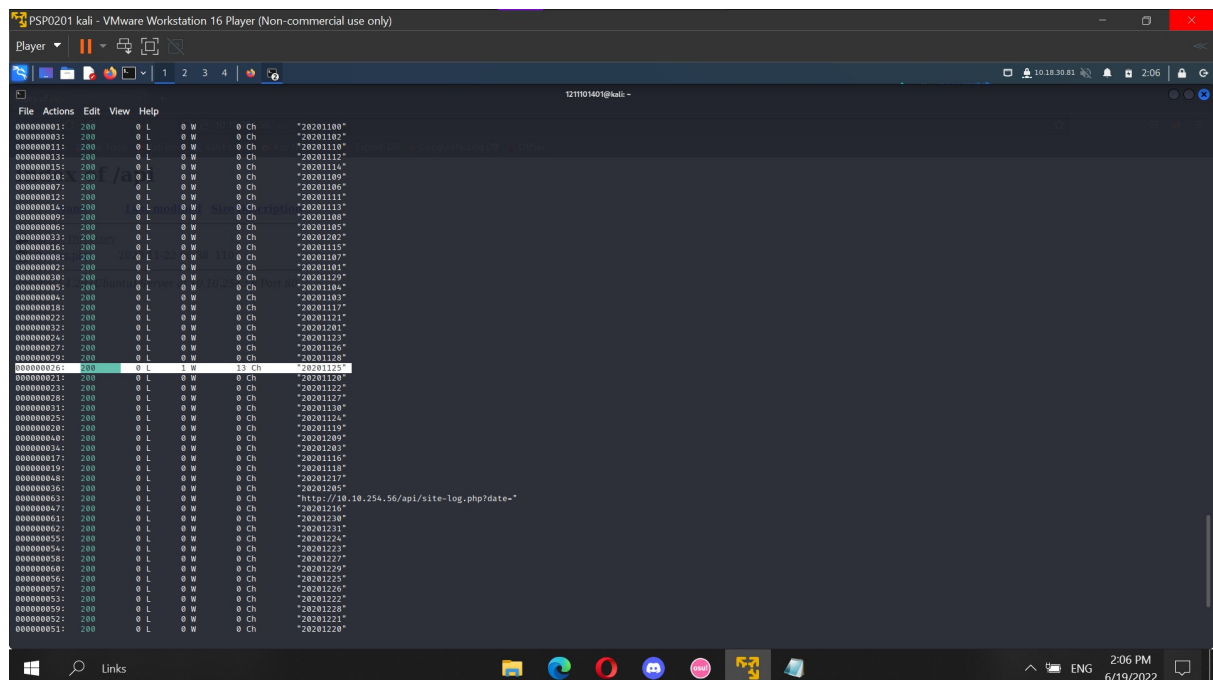
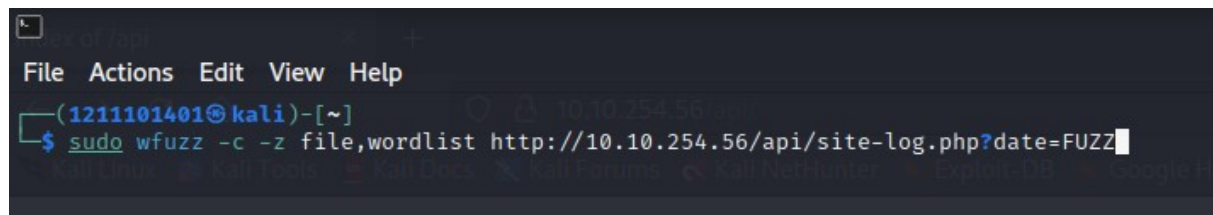
YOU h4v3 b33n d3f4c3d y0ur f0rums ar3 g0ne

Use the gobuster command which is `sudo gobuster dir -u <ip> -w <directory> -x <file type>` to find the directory like in the image above. Copy the url at the /api section and paste it into the browser.

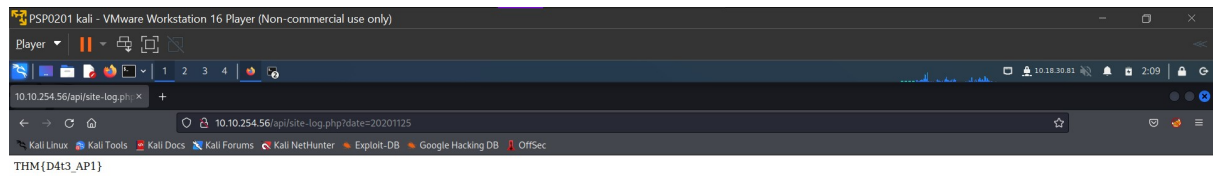


The website will now be accessible and the index of /api will then be shown on the screen. A file called site-log.php will appear at the site.

Q3



Use the wfuzz command to find out the differences. The responsive page will then be shown.



Paste the date into the site-log.php script and run it. The flag will now be shown and can be obtained. Catch the flag.

Q3

`-v` verbose information.

`-f filename,printer`

Store results in the output file using the specified printer (raw printer if omitted).

Can be found in the link <https://manpages.debian.org/buster/wfuzz/wfuzz.1.en.html> which is provided by THM.