

List of tools used: Firefox, Gobuster, Wfuzz

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)

```
kali@kali:~$ cat /dev/null > file_bf.txt http://shibes.xyz/api.php?breed-fuzz
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
wfuzz 3.1.0 - The web fuzzer
*****
Target: http://shibes.xyz/api.php?breed-fuzz
Total requests: 28476

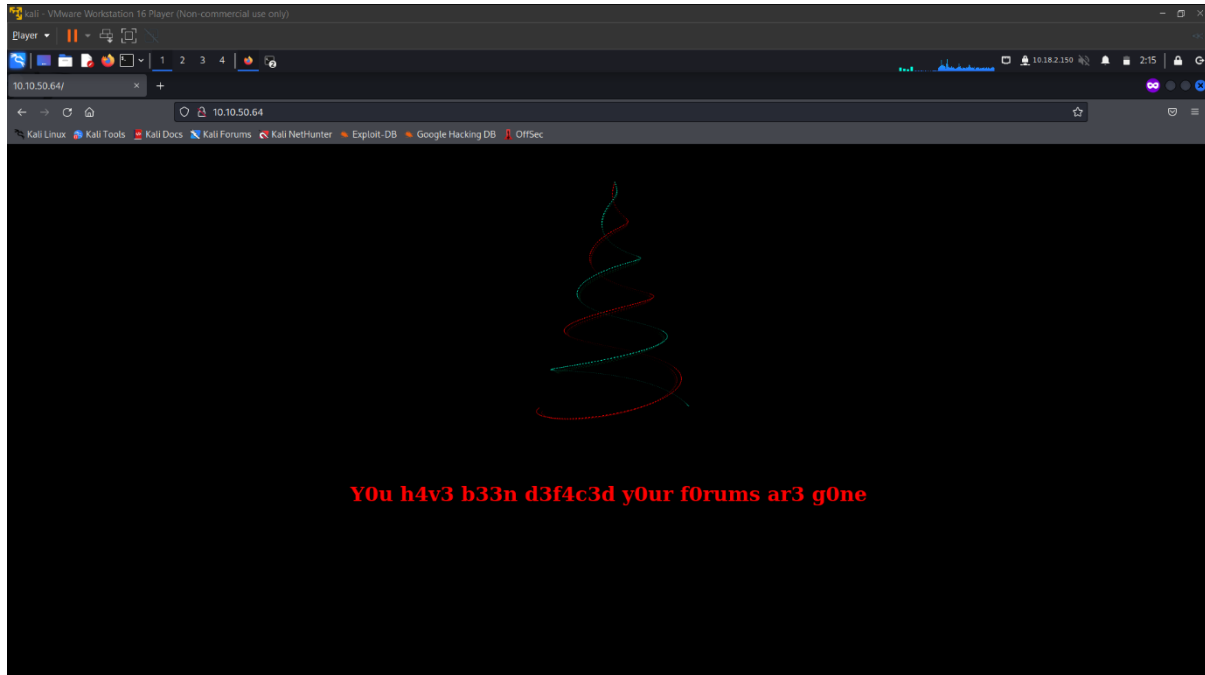
ID      Response    Lines    Word      Chars      Payload
-----
000000006: 301      7 L      12 W      178 Ch     "lree"
000000003: 301      7 L      12 W      178 Ch     "l_images"
000000005: 301      7 L      12 W      178 Ch     "l_image"
000000002: 301      7 L      12 W      178 Ch     "l_archives"
000000009: 301      7 L      12 W      178 Ch     ".bash_history"
000000031: 301      7 L      12 W      178 Ch     ".cvs"
000000007: 301      7 L      12 W      178 Ch     "ltextove_diskuse"
000000008: 301      7 L      12 W      178 Ch     "lut"
000000004: 301      7 L      12 W      178 Ch     "lbackup"
000000001: 301      7 L      12 W      178 Ch     "l"
000000014: 301      7 L      12 W      178 Ch     ".git"
000000051: 301      7 L      12 W      178 Ch     ".history"
000000012: 301      7 L      12 W      178 Ch     ".cvsignore"
000000016: 301      7 L      12 W      178 Ch     ".htaccess"
000000013: 301      7 L      12 W      178 Ch     ".forward"
000000010: 301      7 L      12 W      178 Ch     ".bashrc"
000000022: 301      7 L      12 W      178 Ch     ".rhosts"
000000020: 301      7 L      12 W      178 Ch     ".perf"
000000021: 301      7 L      12 W      178 Ch     ".profile"
000000018: 301      7 L      12 W      178 Ch     ".listing"
000000017: 301      7 L      12 W      178 Ch     ".htpasswd"
000000019: 301      7 L      12 W      178 Ch     ".passwd"
000000023: 301      7 L      12 W      178 Ch     ".ssh"
000000025: 301      7 L      12 W      178 Ch     ".svn"
000000032: 301      7 L      12 W      178 Ch     "00-backup"
000000029: 301      7 L      12 W      178 Ch     "0-12"
000000028: 301      7 L      12 W      178 Ch     "0-0-1"
000000027: 301      7 L      12 W      178 Ch     "0"
000000031: 301      7 L      12 W      178 Ch     "00"
000000030: 301      7 L      12 W      178 Ch     "0-monitors"
000000024: 301      7 L      12 W      178 Ch     ".subversion"
000000026: 301      7 L      12 W      178 Ch     ".web"
000000033: 301      7 L      12 W      178 Ch     "00-cache"
000000035: 301      7 L      12 W      178 Ch     "00-inc"
000000039: 301      7 L      12 W      178 Ch     "0000"
000000040: 301      7 L      12 W      178 Ch     "000000"
000000038: 301      7 L      12 W      178 Ch     "000"
000000041: 301      7 L      12 W      178 Ch     "00000000"
000000042: 301      7 L      12 W      178 Ch     "0001"
000000037: 301      7 L      12 W      178 Ch     "00-ps"
000000036: 301      7 L      12 W      178 Ch     "00-imp"
000000036: 301      7 L      12 W      178 Ch     "00-mp"
```

Answer: wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ

Question 2

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

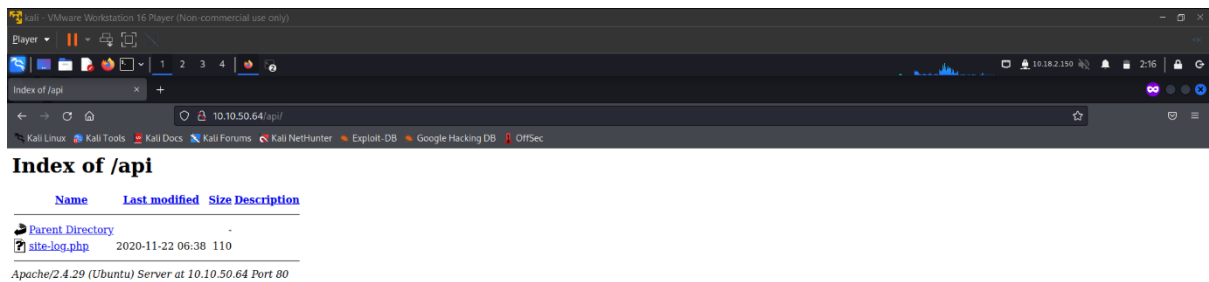
Methodology: We use Firefox to load the IP address given.



Then, we open terminal and used Gobuster and big.txt to brute-force URIs (directories and files) in website. Then, we inspect the output and see the path to API directory which is "/api".

```
kali - VMware Workstation 16 Player (Non-commercial use only)
Player
File Actions Edit View Help
[kali@kali]~$ gobuster dir -u http://10.10.50.64/ -w big.txt -x .php
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@BFirefart)
[+] Url: http://10.10.50.64/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: big.txt
[+] Negative Status codes: 405
[+] User Agent: gobuster/3.2.0-dev
[+] Extensions:
[+] Timeout: 10s
2022/10/14 02:11:03 Starting gobuster in directory enumeration mode
./htaccess (Status: 403) [Size: 276]
./htaccess. (Status: 403) [Size: 276]
./htpasswd. (Status: 403) [Size: 276]
./htpasswd (Status: 403) [Size: 276]
./LICENSE (Status: 200) [Size: 1086]
/api (Status: 301) [Size: 308] [→ http://10.10.50.64/api/]
/Server-status (Status: 403) [Size: 276]
Progress: 40952 / 40954 (100.00%)
2022/10/14 02:20:32 finished
[kali@kali]~$
```

We get back Firefox and add “/api” after the original address. Then, we get to a directory with a php file named site-log.php.



Answer: site-log.php

Question 3

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

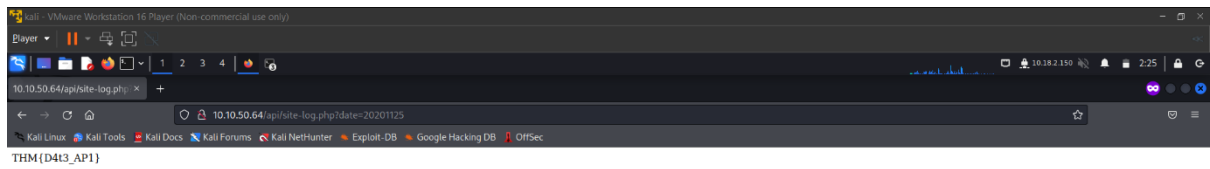
Methodology: We target the site-log.php and use wfuzz to fuzz the file a date parameter with a wordlist. We see the result and Date “20201125” have a response with 13 characters.

```
kali@kali:~$ python3 wfuzz.py -u http://10.10.10.56/api/site-log.php?date=FUZZ
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
.....
Wfuzz 3.1.0 - The Web Fuzzer
.....

Target: http://10.10.10.56/api/site-log.php?date=FUZZ
Total requests: 63

ID      Response      Lines  Word      Chars      Payload
-----
000000001: 200      0 L      0 W      0 Ch      "20201108"
000000003: 200      0 L      0 W      0 Ch      "20201102"
000000015: 200      0 L      0 W      0 Ch      "20201114"
000000016: 200      0 L      0 W      0 Ch      "20201115"
000000087: 200      0 L      0 W      0 Ch      "20201106"
000000088: 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"
000000010: 200      0 L      0 W      0 Ch      "20201109"
000000004: 200      0 L      0 W      0 Ch      "20201103"
000000005: 200      0 L      0 W      0 Ch      "20201105"
000000006: 200      0 L      0 W      0 Ch      "20201109"
000000008: 200      0 L      0 W      0 Ch      "20201107"
000000002: 200      0 L      0 W      0 Ch      "20201101"
000000011: 200      0 L      0 W      0 Ch      "20201110"
000000009: 200      0 L      0 W      0 Ch      "20201108"
000000007: 200      0 L      0 W      0 Ch      "20201216"
000000025: 200      0 L      0 W      0 Ch      "20201124"
000000001: 200      0 L      0 W      0 Ch      "20201212"
000000045: 200      0 L      0 W      0 Ch      "20201214"
000000046: 200      0 L      0 W      0 Ch      "20201215"
000000033: 200      0 L      0 W      0 Ch      "20201203"
000000019: 200      0 L      0 W      0 Ch      "20201118"
000000021: 200      0 L      0 W      0 Ch      "20201120"
000000031: 200      0 L      0 W      0 Ch      "20201112"
000000043: 200      0 L      0 W      0 Ch      "20201217"
000000037: 200      0 L      0 W      0 Ch      "20201206"
000000042: 200      0 L      0 W      0 Ch      "20201211"
000000039: 200      0 L      0 W      0 Ch      "20201208"
000000040: 200      0 L      0 W      0 Ch      "20201209"
000000036: 200      0 L      0 W      0 Ch      "20201205"
000000041: 200      0 L      0 W      0 Ch      "20201210"
000000035: 200      0 L      0 W      0 Ch      "20201207"
000000035: 200      0 L      0 W      0 Ch      "20201206"
000000012: 200      0 L      0 W      0 Ch      "20201111"
000000026: 200      0 L      1 W      13 Ch      "20201125"
000000032: 200      0 L      0 W      0 Ch      "20201201"
000000027: 200      0 L      0 W      0 Ch      "20201126"
000000034: 200      0 L      0 W      0 Ch      "20201203"
000000029: 200      0 L      0 W      0 Ch      "20201128"
000000031: 200      0 L      0 W      0 Ch      "20201129"
000000024: 200      0 L      0 W      0 Ch      "20201123"
```

We go back site-log.php and add “?date=20201125” and find the 13 characters which is the flag.

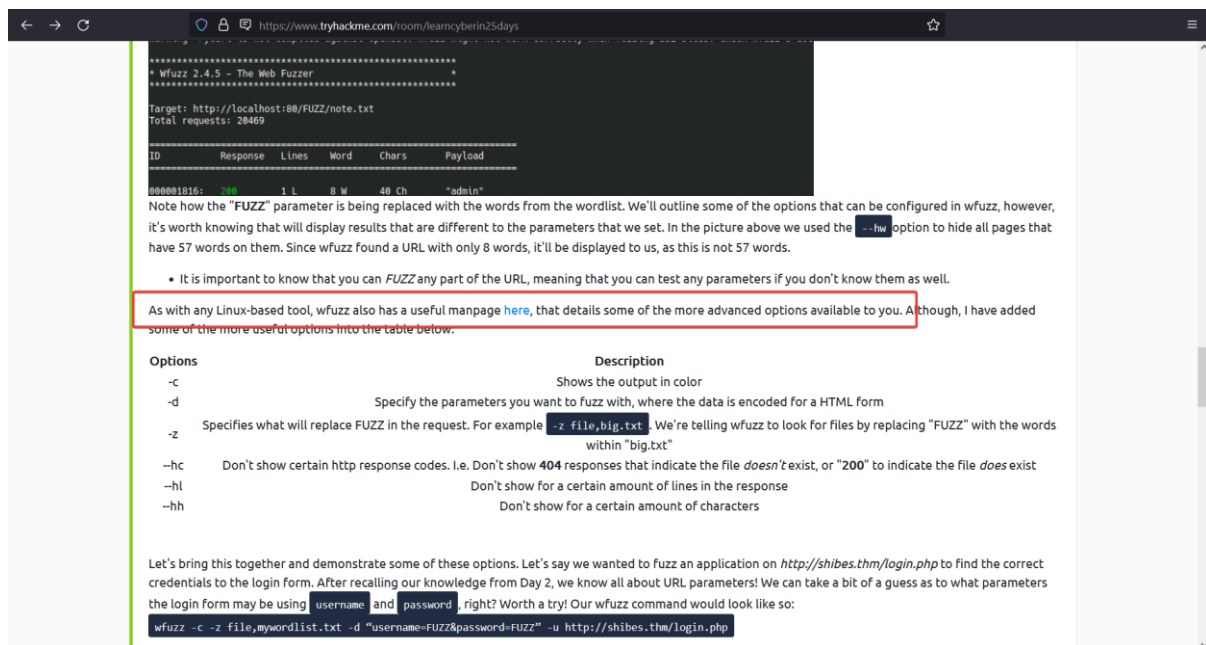


Answer: THM{D4t3_AP1}

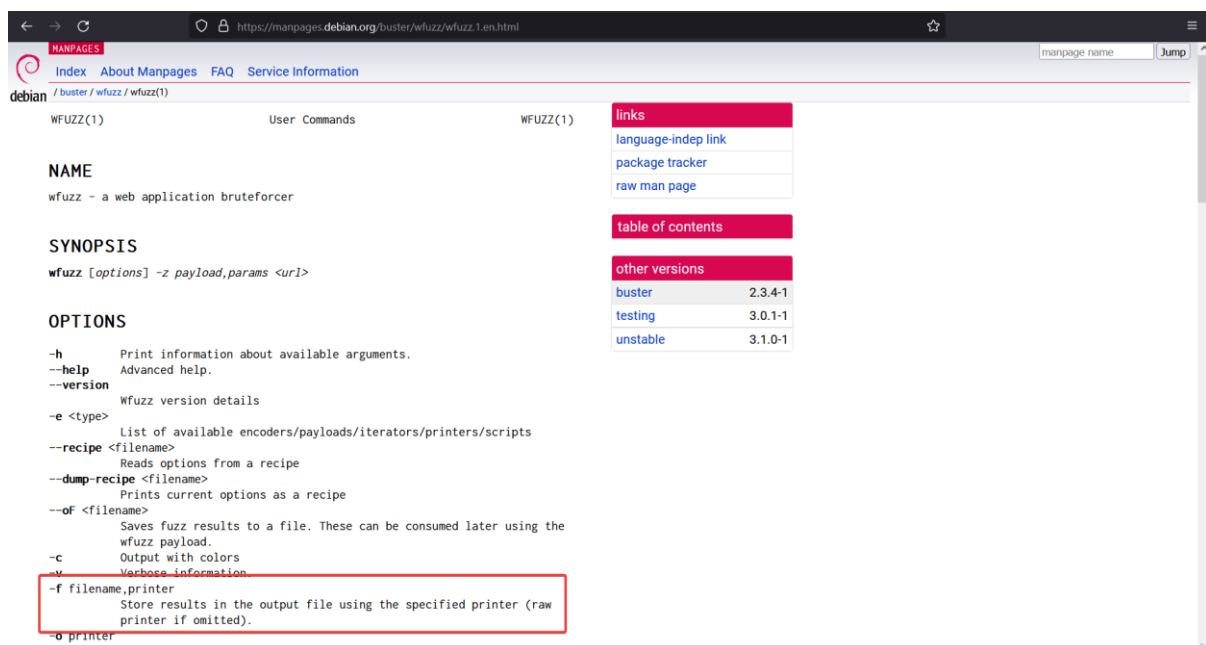
Question 4

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

Methodology: We find the wfuzz's help file link.



Then, we find -f need 2 parameters which is filename and printer.



Answer: filename, printer