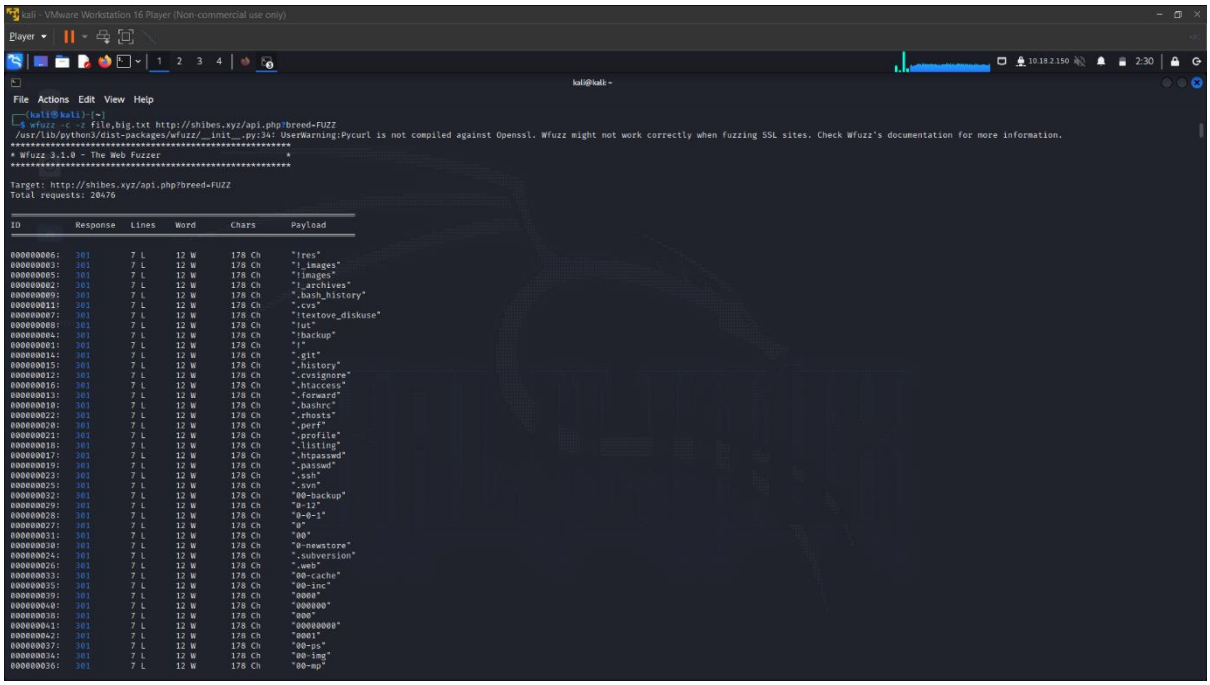
Day 4: Web Exploitation – Santa's watching

List of tools used: Firefox, Gobuster, Wfuzz

Question 1

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)

Methodology: We see that a wfuzz command is wfuzz -c -z file,filename website address then add keyword "FUZZ" to where to want to fuzz the data. We try the following command in the terminal and it runs with no error.

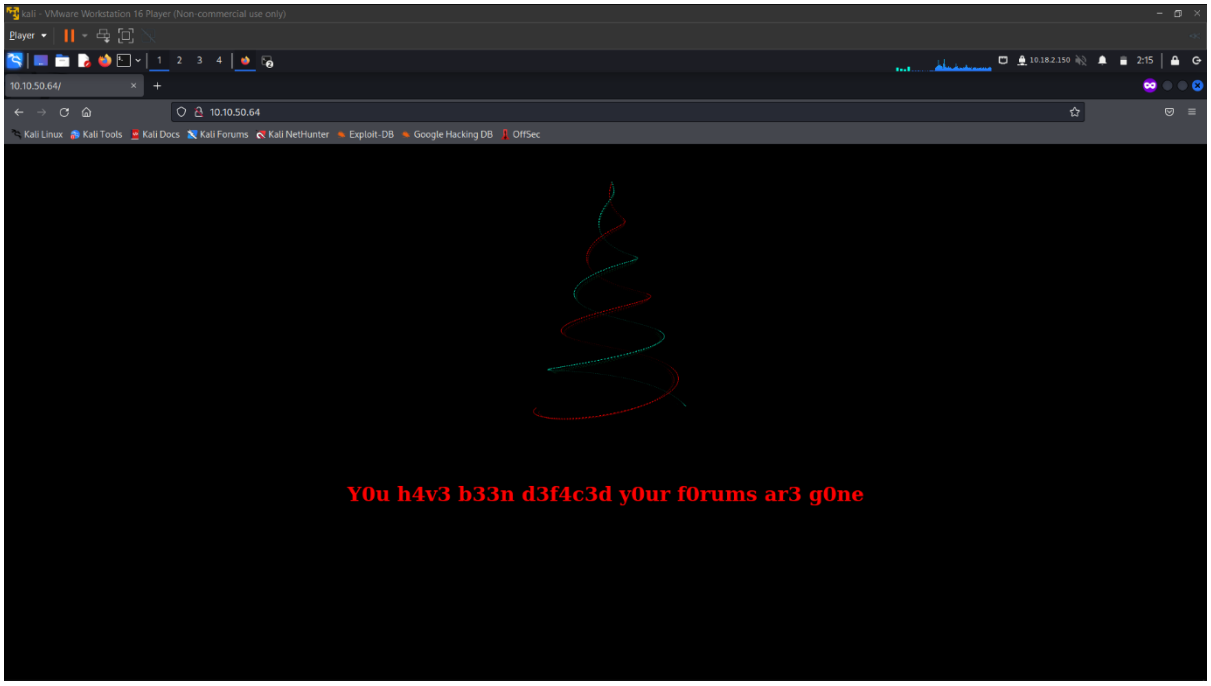


Answer: wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ

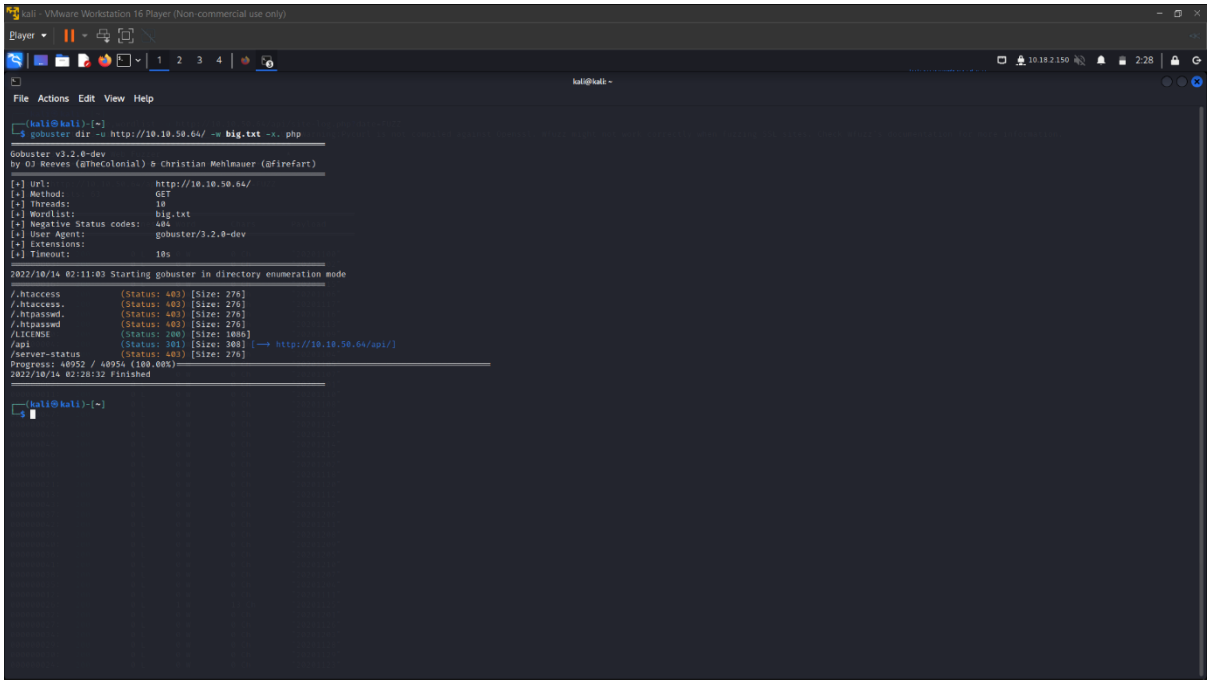
Question 2

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

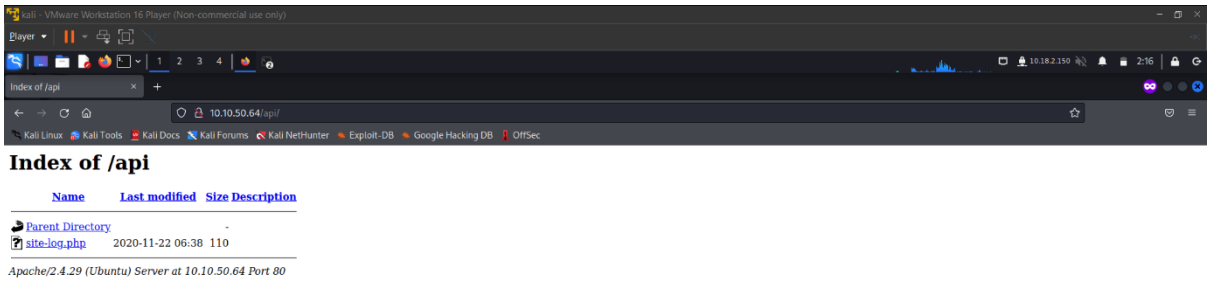
Methodology: We use Firefox to load the IP address given.



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”.



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.

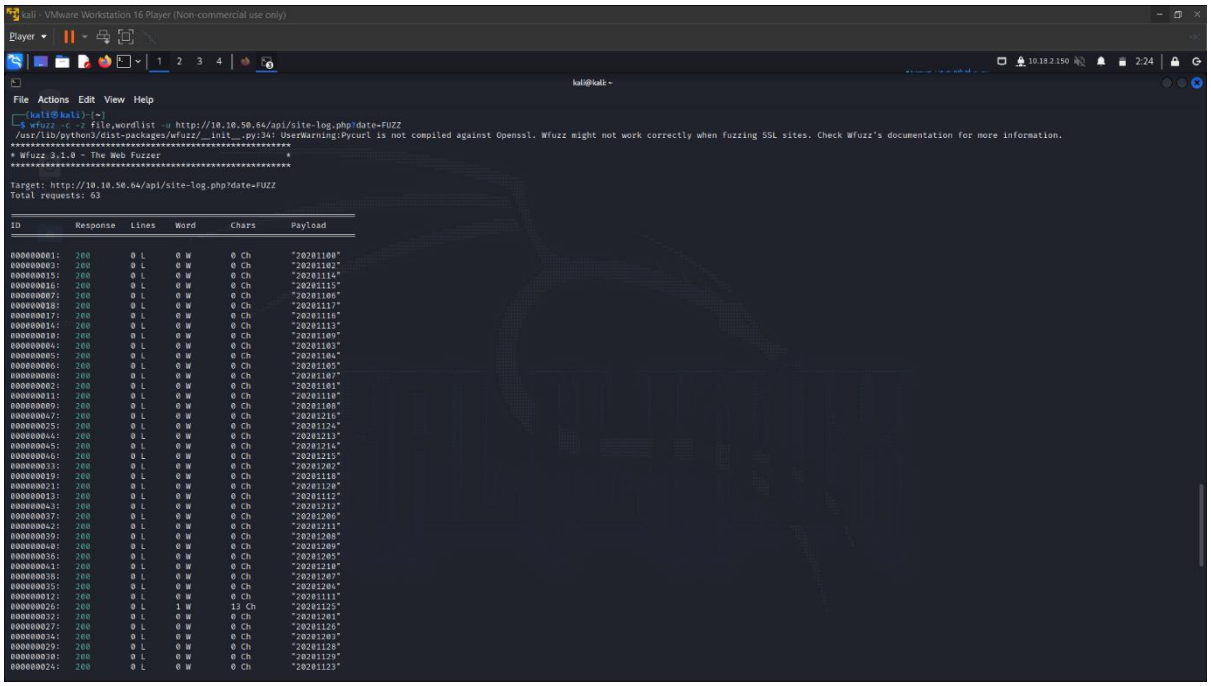


Answer: site-log.php

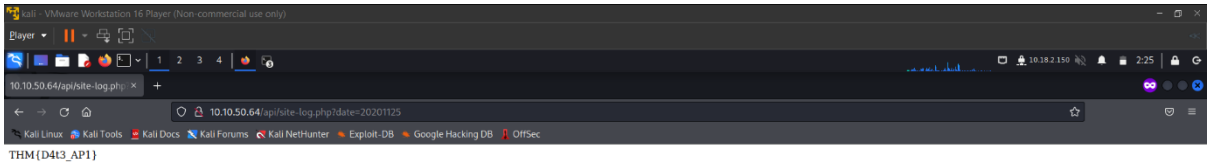
Question 3

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.



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

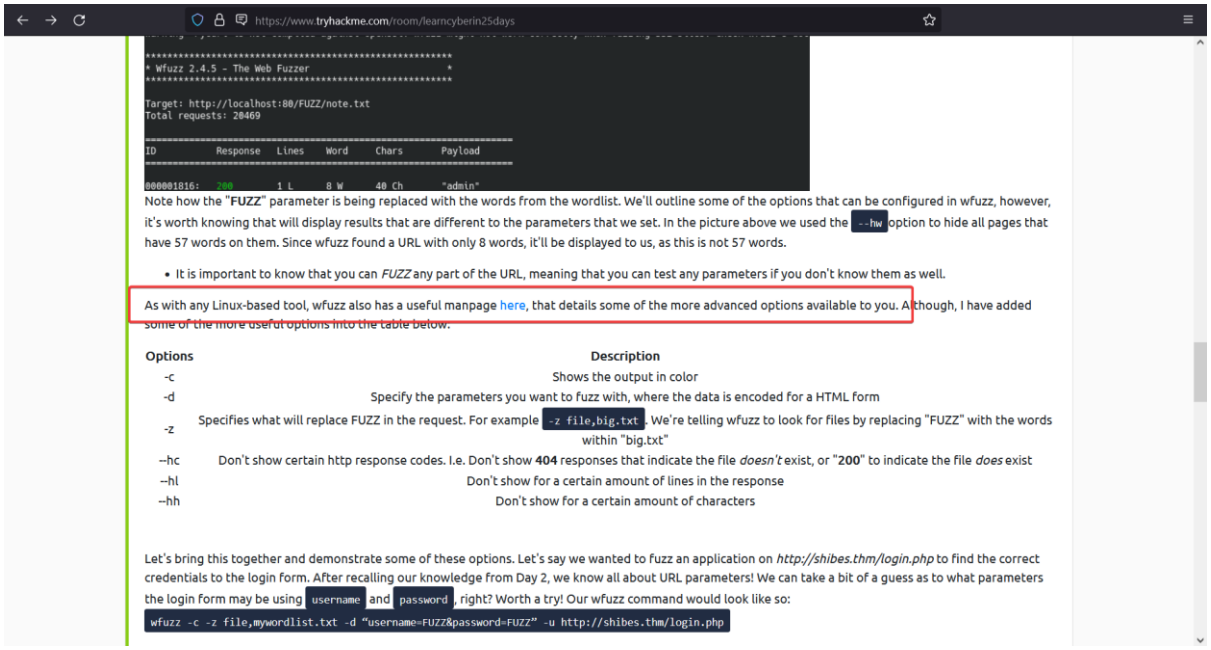


Answer: THM{D4t3_AP1}

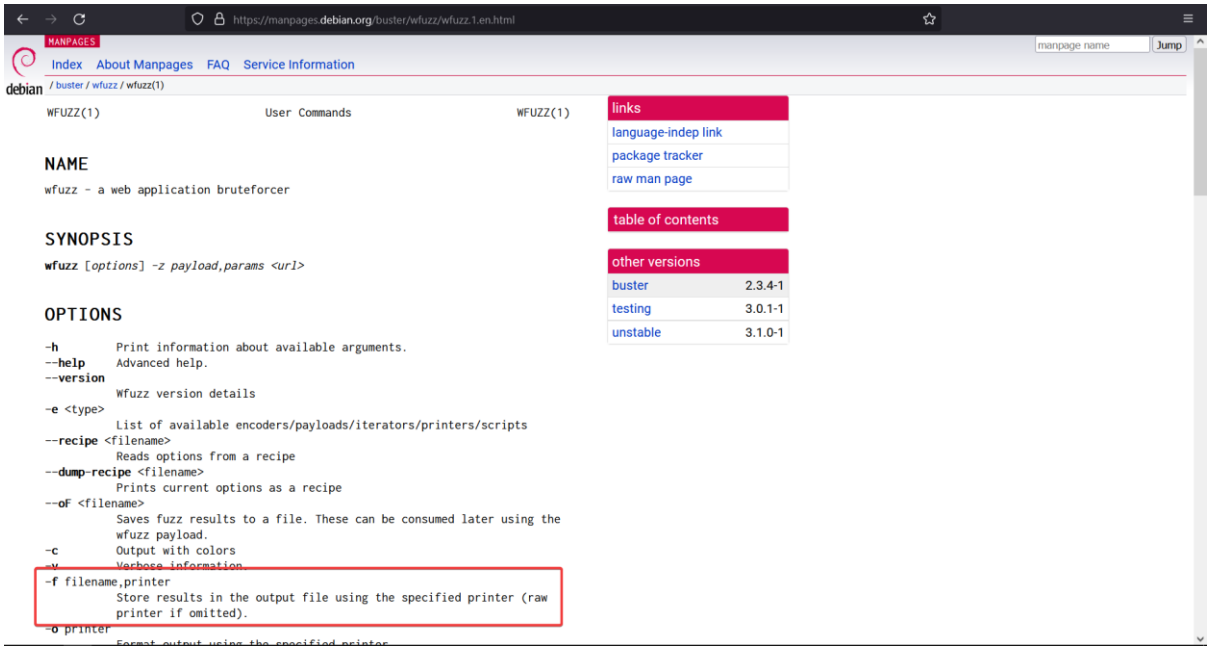
Question 4

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