

Day 4 - Santa's Watching

Scenario

Task 9 ○ [Day 4] Web Exploitation Santa's watching



[Watch DarkStar's video on solving this task!](#)

Deploy

Introduction & Story:



We're going to be taking a look at some of the fundamental tools used in web application testing. You're going to learn how to use Gobuster to enumerate a web server for hidden files and folders to aid in the recovery of Elf's forums. Later on, you're going to be introduced to an important technique that is fuzzing, where you will have the opportunity to put theory into practice.

Our malicious, despicable, vile, cruel, contemptuous, evil hacker has defaced Elf's forums and completely removed the login page! However, we may still have access to the API. The sysadmin also told us that the API creates logs using dates with a format of YYYYMMDD.

Challenge

Deploy both the instance attached to this task (the green deploy button) and the AttackBox by pressing the blue "Start AttackBox" button at the top of the page. After allowing 5 minutes, navigate to the website (MACHINE_IP) in your AttackBox browser.

It is up to you to decide if you wish to create the wordlist yourself or use a larger wordlist located in `/opt/AoC-2020/Day-4/wordlist` on the AttackBox. The wordlist is also [available for download](#) if you are using your own machine.

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!

How to approach the challenge

Since we know there's theoretically an API directory we can use gobuster to enumerate the website and see if we can find anything. Then assuming we do find something, we should investigate it for interesting files. Let's say we then find what seems to hold the logs, we know we're searching by date, so we can infer that there's a good chance that we'll be using the date parameter to interact with the API. We also know that the API takes a date in the form of YYYYMMDD. A wordlist in that format can be found in the hint for this task, although if you want an extra challenge, you can try and build a wordlist in that format yourself.

Finally, API's may not return data if the proper parameters aren't passed, so with that knowledge, we can use the options in wfuzz to filter out parameters that don't return anything.

With all that in mind, we should be able to get a flag.

wordlist = available for download (tryhackme.com)

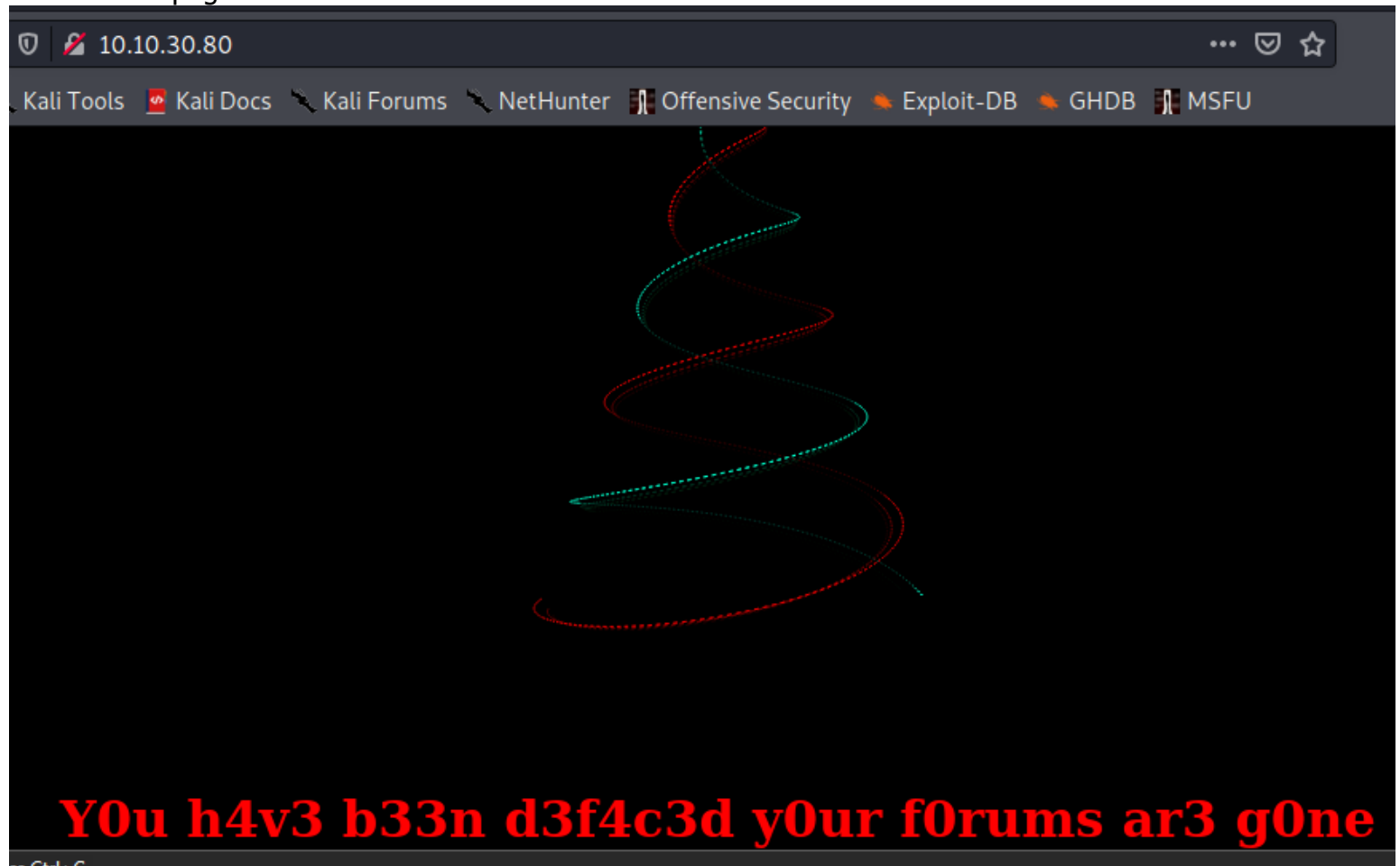
Question: Given the URL "http://shibes.xyz/api.php", what would the entire wfuzz command look like to query the "breed" parameter using the wordlist "big.txt" (assume that "big.txt" is in your current directory)

wfuzz cheat sheet

Options	Description
-c	Shows the output in color
-d	Specify the parameters you want to fuzz with, where the data is encoded for a HTML form
-z	Specifies what will replace FUZZ in the request. For example <code>-z file,big.txt</code> . We're telling wfuzz to look for files by replacing "FUZZ" with the words within "big.txt"
-hc	Don't show certain http response codes. I.e. Don't show 404 responses that indicate the file <i>doesn't</i> exist, or 200 to indicate the file <i>does</i> exist
-hl	Don't show for a certain amount of lines in the response
-hh	Don't show for a certain amount of characters

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

the root webpage



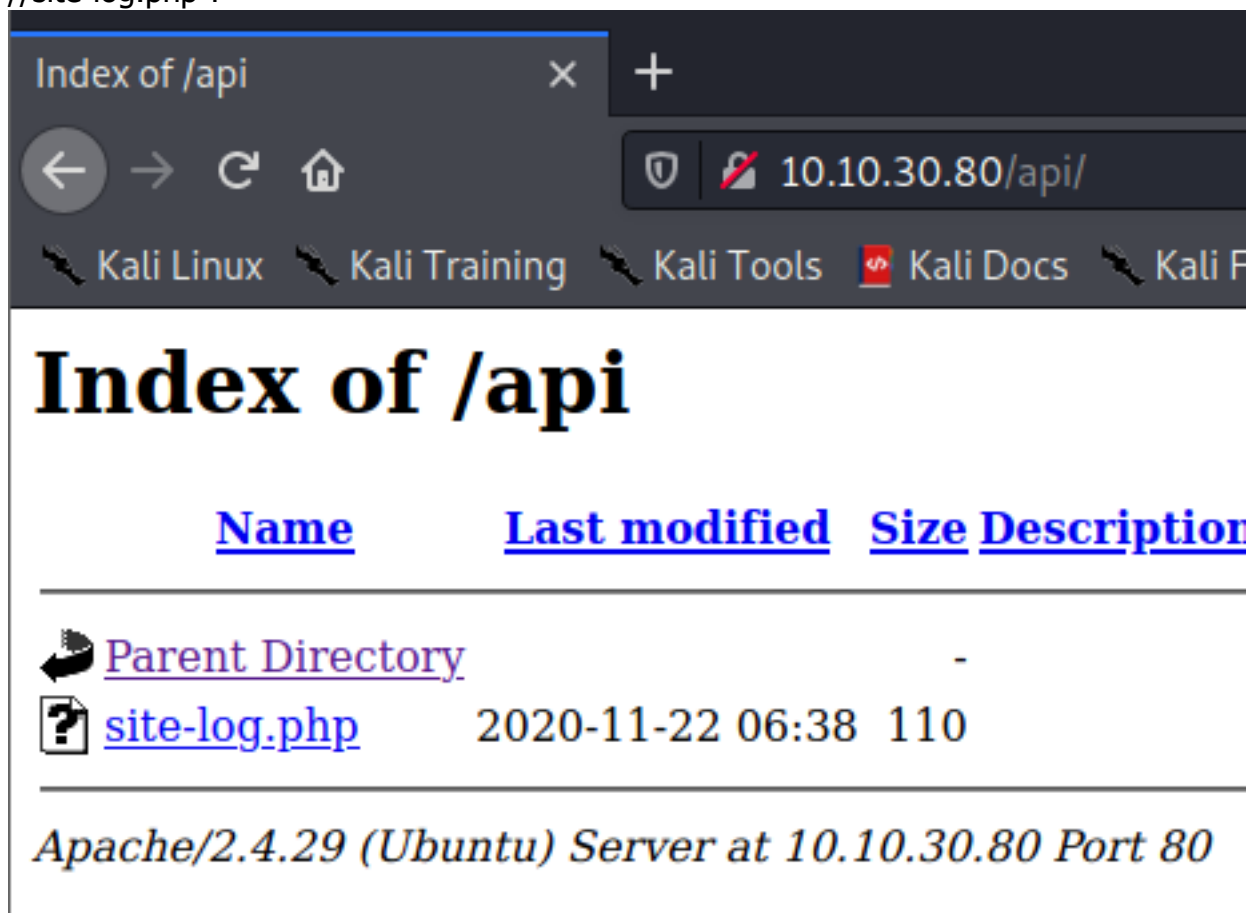
perform api directory searching using gobuster

```
$ gobuster dir -u http://10.10.30.80 -w /usr/share/wordlists/dirb/common.txt -x txt,php,html
```

found the /api directory

```
/.htpasswd.html (Status: 404)  
/api (Status: 301)  
Progress: 551 / 4615 (11.9%)
```

/api
//site-log.php ?



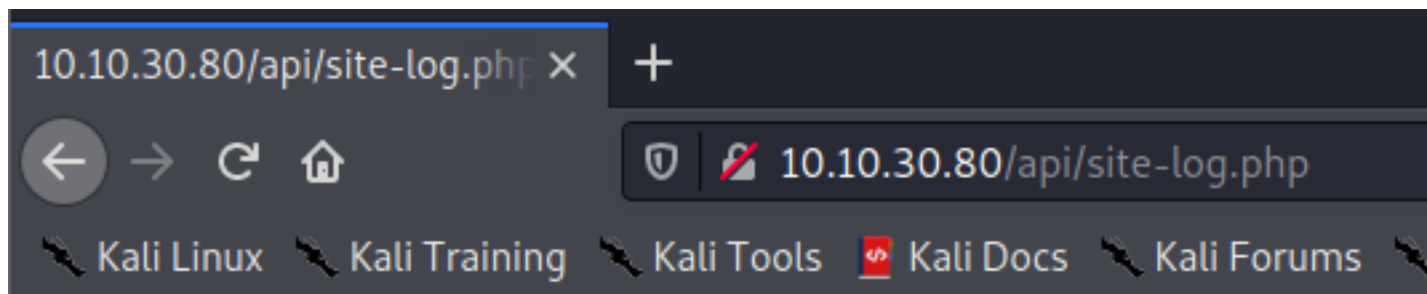
The screenshot shows a web browser window with the title "Index of /api". The address bar displays "10.10.30.80/api/". The browser's navigation bar includes buttons for back, forward, refresh, and home, along with a search bar and a "Kali Linux" logo. The main content area displays the "Index of /api" directory listing. The listing has columns for "Name", "Last modified", "Size", and "Description". It shows two entries: "Parent Directory" with a size of "-" and "site-log.php" with a size of "110". The "site-log.php" entry is highlighted. Below the listing, the text "Apache/2.4.29 (Ubuntu) Server at 10.10.30.80 Port 80" is displayed.

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

Apache/2.4.29 (Ubuntu) Server at 10.10.30.80 Port 80

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

it's empty here



perform fuzzing on date GET parameter using the wordlist downloaded from the challenge room
//found 20201125 value return 13 chars

```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/adventOfCyber2/day4]
$ wfuzz -c -z file,wordlist --hh 0 http://10.10.30.80/api/site-log.php?date=FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compi
Wfuzz's documentation for more information.
*****
* Wfuzz 3.0.1 - The Web Fuzzer *
*****

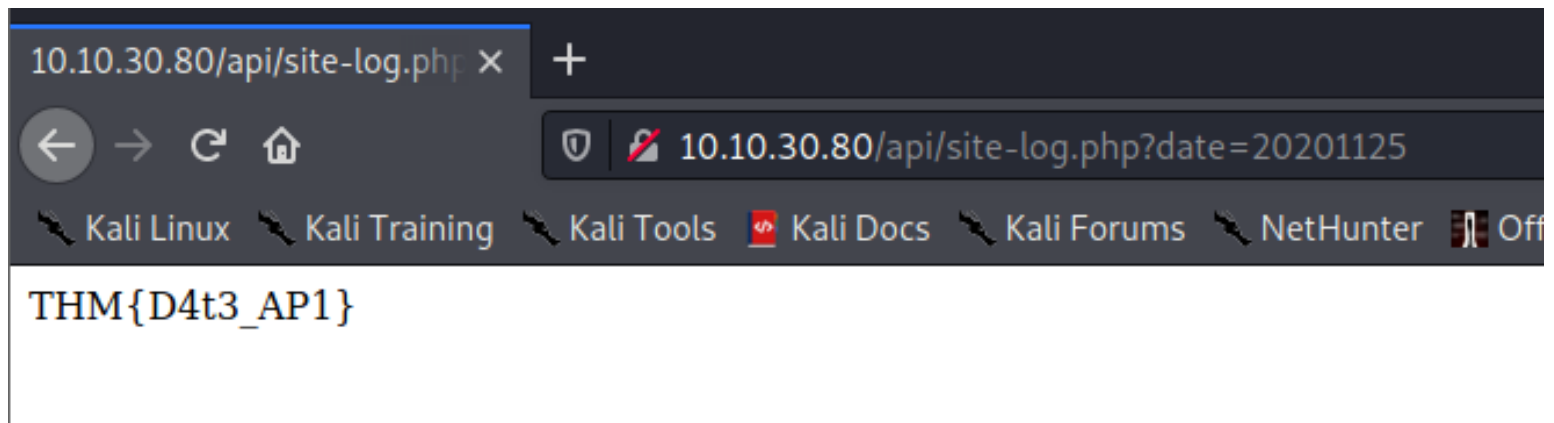
Target: http://10.10.30.80/api/site-log.php?date=FUZZ
Total requests: 63

=====
ID           Response  Lines  Word  Chars  Payload
=====
000000026:  200        0 L    1 W    13 Ch  "20201125"

Total time: 0
Processed Requests: 63
Filtered Requests: 62
Requests/sec.: 0

(nobodyatall@0xDEADBEEF)-[~/tryhackme/adventOfCyber2/day4]
```

& there's our flag!



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

