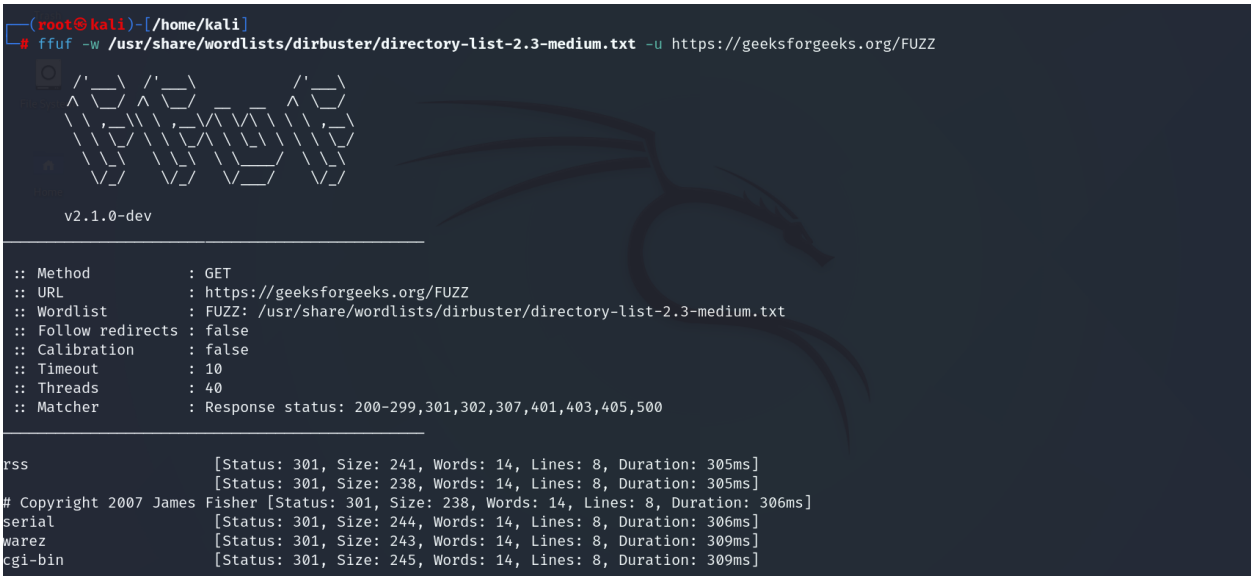
ffuf

Fuzzing is the automatic process of giving random input to an application to look for any errors or any unexpected behavior. But finding any hidden directories and files on any web server can also be categorized under fuzzing. If we try to perform this process manually then it can take dozens of months to find the directories on the server. So the automation approach is the best for performing fuzzing. FFUF is the automated tool developed in the Golang language which is the fastest fuzzer tool in today's date. It has various key features of manipulation the method from GET to POST and vice versa. We can use various wordlists for fuzzing the vhost as well. FFUF tool is an open-source and free-to-use tool.

FFUF, which stands for "Fuzz Faster U Fool," is a versatile and high-performance web fuzzer tool used for discovering web application vulnerabilities. It's primarily designed for fuzzing, a technique where you send random or specially crafted data to the inputs of a web application to identify points of weakness.

Examples: -

1. Here we are fuzzing the directories using wordlist.



```
┌──(root㉿kali)-[/home/kali]
└─# ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u https://geeksforgeeks.org/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://geeksforgeeks.org/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

rss                     [Status: 301, Size: 241, Words: 14, Lines: 8, Duration: 305ms]
                        [Status: 301, Size: 238, Words: 14, Lines: 8, Duration: 305ms]
# Copyright 2007 James Fisher [Status: 301, Size: 238, Words: 14, Lines: 8, Duration: 306ms]
serial                  [Status: 301, Size: 244, Words: 14, Lines: 8, Duration: 306ms]
warez                   [Status: 301, Size: 243, Words: 14, Lines: 8, Duration: 309ms]
cgi-bin                 [Status: 301, Size: 245, Words: 14, Lines: 8, Duration: 309ms]
```

2. Here we are discovering the virtual host using -H & -fs flags.

```
┌──(root㉿kali)-[/home/kali]
└─# ffuf -w /usr/share/wordlists/vhost.txt -u https://geeksforgeeks.org -H “Host: FUZZ” -fs 4242
Keyword FUZZ defined, but not found in headers, method, URL or POST data.

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

  :: Method           : GET
  :: URL              : https://geeksforgeeks.org
  :: Header           : “Host:
  :: Follow redirects : false
  :: Calibration      : false
  :: Timeout          : 10
  :: Threads          : 40
  :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

 :: Progress: [1/1] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 1 ::
```