Recursive Fuzzing

So far, we have been fuzzing for directories, then going under these directories, and then fuzzing for files. However, if we had dozens of directories, each with their own subdirectories and files, this would take a very long time to complete. To be able to automate this, we will utilize what is known as `recursive fuzzing`.

Recursive Flags

When we scan recursively, it automatically starts another scan under any newly identified directories that may have on their pages until it has fuzzed the main website and all of its subdirectories.

Some websites may have a big tree of sub-directories, like `/login/user/content/uploads/...etc`, and this will expand the scanning tree and may take a very long time to scan them all. This is why it is always advised to specify a `depth` to our recursive scan, such that it will not scan directories that are deeper than that depth. Once we fuzz the first directories, we can then pick the most interesting directories and run another scan to direct our scan better.

In `ffuf`, we can enable recursive scanning with the `-recursion` flag, and we can specify the depth with the `-recursion-depth` flag. If we specify `-recursion-depth 1`, it will only fuzz the main directories and their direct sub-directories. If any sub-sub-directories are identified (like `/login/user`, it will not fuzz them for pages). When using recursion in `ffuf`, we can specify our extension with `-e .php`

Note: we can still use `.php` as our page extension, as these extensions are usually site-wide.

Finally, we will also add the flag `-v` to output the full URLs. Otherwise, it may be difficult to tell which `.php` file lies under which directory.

Recursive Scanning

Let us repeat the first command we used, add the recursion flags to it while specifying `.php` as our extension, and see what results we get:

```
MichaelLuka@htb[/htb]$ ffuf -w /opt/useful/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://SERV


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

       v1.1.0-git
________________________________________________

 :: Method           : GET
 :: URL              : http://SERVER_IP:PORT/FUZZ
 :: Wordlist         : FUZZ: /opt/useful/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Extensions       : .php
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

[Status: 200, Size: 986, Words: 423, Lines: 56] | URL | http://SERVER_IP:PORT/
    * FUZZ:

[INFO] Adding a new job to the queue: http://SERVER_IP:PORT/forum/FUZZ
[Status: 200, Size: 986, Words: 423, Lines: 56] | URL | http://SERVER_IP:PORT/index.php
    * FUZZ: index.php

[Status: 301, Size: 326, Words: 20, Lines: 10] | URL | http://SERVER_IP:PORT/blog | --> | http://SERVER_IP:PORT/blog/
    * FUZZ: blog

<...SNIP...>
[Status: 200, Size: 0, Words: 1, Lines: 1] | URL | http://SERVER_IP:PORT/blog/index.php
    * FUZZ: index.php

[Status: 200, Size: 0, Words: 1, Lines: 1] | URL | http://SERVER_IP:PORT/blog/
    * FUZZ:

<...SNIP...>
```

As we can see this time, the scan took much longer, sent almost six times the number of requests, and the wordlist doubled in size (once with `.php` and once without). Still, we got a large number of results, including all the results we previously identified, all with a single line of command.

Start Instance

1 / 1 spawns left

Waiting to start...

Questions

Cheat Sheet

Answer the question(s) below to complete this Section and earn cubes!

Target: Click here to spawn the target system!

+ 1 Try to repeat what you learned so far to find more files/directories. One of them should give you a flag. What is the content of the flag?

Submit your answer here...

Submit

Hint

Previous Next

Cheat Sheet

? Go to Questions

Table of Contents

Introduction

Basic Fuzzing

Domain Fuzzing

Parameter Fuzzing

Skills Assessment

Skills Assessment - Web Fuzzing

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left