

Filtering Results

So far, we have not been using any filtering to our `ffuf`, and the results are automatically filtered by default by their HTTP code, which filters out code `404 NOT FOUND`, and keeps the rest. However, as we saw in our previous run of `ffuf`, we can get many responses with code `200`. So, in this case, we will have to filter the results based on another factor, which we will learn in this section.

Filtering

`ffuf` provides the option to match or filter out a specific HTTP code, response size, or amount of words. We can see that with `ffuf -h`:

```
Filtering Results

MisaelMacias@htb[/htb]$ ffuf -h
...SNIP...
MATCHER OPTIONS:
  -mc      Match HTTP status codes, or "all" for everything. (default: 200,204,301,302,307,401,403)
  -ml      Match amount of lines in response
  -mr      Match regex
  -ms      Match HTTP response size
  -mw      Match amount of words in response

FILTER OPTIONS:
  -fc      Filter HTTP status codes from response. Comma separated list of codes and ranges
  -fl      Filter by amount of lines in response. Comma separated list of line counts and ranges
  -fr      Filter regex
  -fs      Filter HTTP response size. Comma separated list of sizes and ranges
  -fw      Filter by amount of words in response. Comma separated list of word counts and ranges
<...SNIP...>
```

In this case, we cannot use matching, as we don't know what the response size from other VHosts would be. We know the response size of the incorrect results, which, as seen from the test above, is `900`, and we can filter it out with `-fs 900`. Now, let's repeat the same previous command, add the above flag, and see what we get:

```
Filtering Results

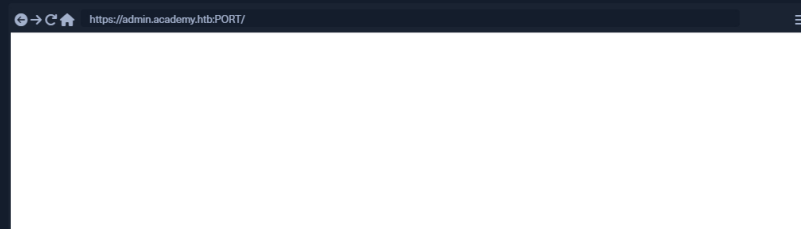
MisaelMacias@htb[/htb]$ ffuf -w /opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://acad

v1.1.0-git

:: Method      : GET
:: URL         : http://academy.htb:PORT/
:: Wordlist    : FUZZ: /opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt
:: Header      : Host: FUZZ.academy.htb
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403
:: Filter      : Response size: 900

<...SNIP...>
admin [Status: 200, Size: 0, Words: 1, Lines: 1]
:: Progress: [4997/4997] :: Job [1/1] :: 1249 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

We can verify that by visiting the page, and seeing if we can connect to it:




Note 1: Don't forget to add "admin.academy.htb" to "/etc/hosts".

Note 2: If your exercise has been restarted, ensure you still have the correct port when visiting the website.

We see that we can access the page, but we get an empty page, unlike what we got with `academy.htb`, therefore confirming this is indeed a different VHost. We can even visit `https://admin.academy.htb:PORT/blog/index.php`, and we will see that we would get a `404 PAGE NOT FOUND`, confirming that we are now indeed on a different VHost.

Try running a recursive scan on `admin.academy.htb`, and see what pages you can identify.

 **Connect to Pwnbox**
Your own web-based Parrot Linux Instance to play our labs.

[Cheat Sheet](#)[Go to Questions](#)

Table of Contents

Introduction

[Introduction](#)[Web Fuzzing](#)

Basic Fuzzing

[Directory Fuzzing](#)[Page Fuzzing](#)[Recursive Fuzzing](#)

Domain Fuzzing

[DNS Records](#)[Sub-domain Fuzzing](#)[Vhost Fuzzing](#)[Filtering Results](#)

Parameter Fuzzing

[Parameter Fuzzing - GET](#)[Parameter Fuzzing - POST](#)[Value Fuzzing](#)

Skills Assessment

[Skills Assessment - Web Fuzzing](#)

My Workstation

OFFLINE

[Start Instance](#)

00 / 1 spawns left

Pwnbox Location

UK

162ms

ⓘ Terminate Pwnbox to switch location

Start Instance

00 / 1 spawns left

Waiting to start...

☐ Enable step-by-step solutions for all questions

Questions

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



Cheat Sheet

Target(s): [Click here to spawn the target system!](#)

🔍 Try running a VHost fuzzing scan on 'academy.htb', and see what other VHosts you get. What other VHosts did you get?

testLacademy.htb

Submit

Hint

← Previous

Next →

✔ Mark Complete & Next

