Filtering Results

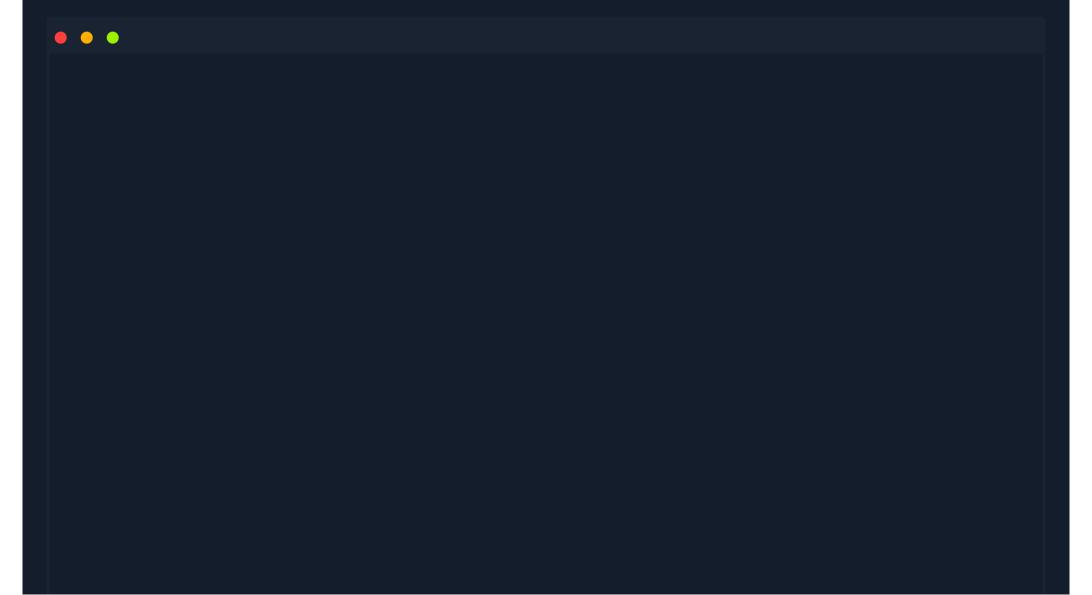
So far, we have not been using any filtering to our ffuf, and the results are automatically filtered by default by their HTTP code, which filters out code 404 NOT FOUND, and keeps the rest. However, as we saw in our previous run of ffuf, we can get many responses with code 200. So, in this case, we will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

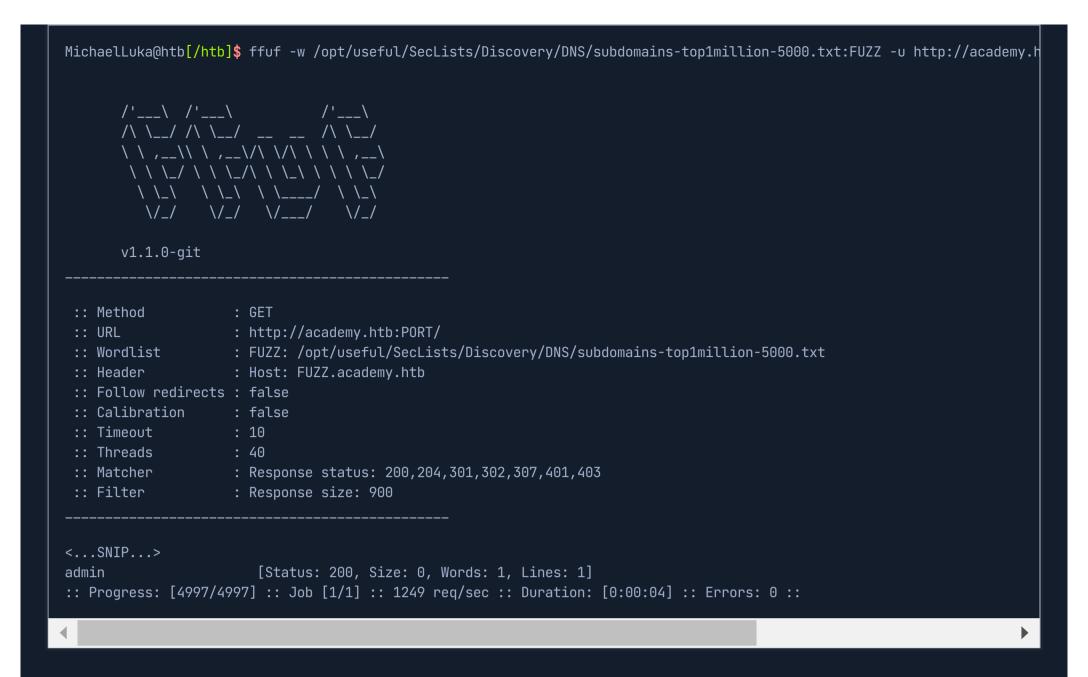
Filtering

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:

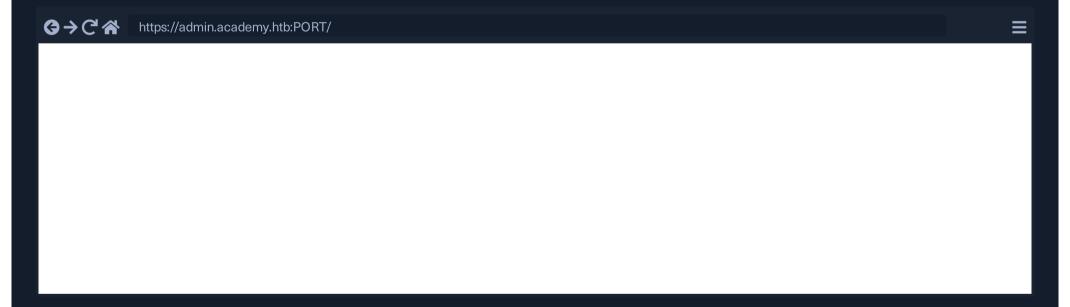
```
MichaelLuka@htb[/htb]$ ffuf -h
...SNIP...
MATCHER OPTIONS:
                   Match HTTP status codes, or "all" for everything. (default: 200,204,301,302,307,401,403)
                   Match amount of lines in response
  -ml
                   Match regexp
  -mr
                   Match HTTP response size
  -ms
                   Match amount of words in response
  -mw
FILTER OPTIONS:
                   Filter HTTP status codes from response. Comma separated list of codes and ranges
  -fc
  -fl
                   Filter by amount of lines in response. Comma separated list of line counts and ranges
  -fr
                   Filter regexp
                   Filter HTTP response size. Comma separated list of sizes and ranges
  -fs
                   Filter by amount of words in response. Comma separated list of word counts and ranges
  -fw
<....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:





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.

