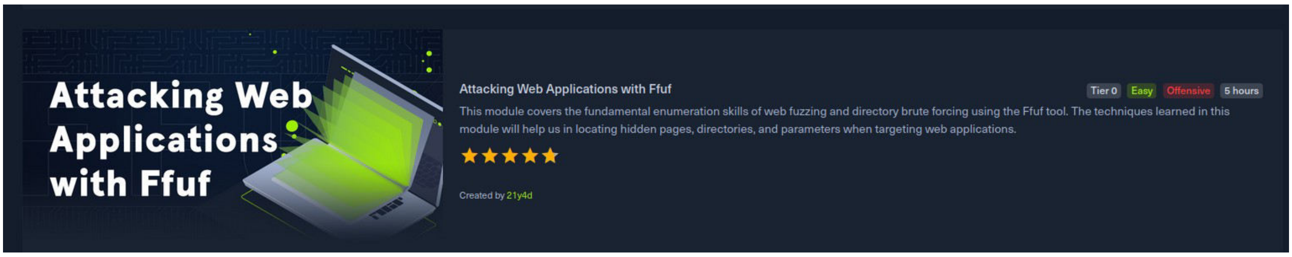
Eric Mwenda

Attacking Web Applications with Ffuf

https://academy.hackthebox.com/achievement/596337/54



Attacking Web Applications with Ffuf

Tier 0 Easy Offensive 5 hours

This module covers the fundamental enumeration skills of web fuzzing and directory brute forcing using the Ffuf tool. The techniques learned in this module will help us in locating hidden pages, directories, and parameters when targeting web applications.

★★★★★

Created by 21y4d

Tools such as ffuf provide us with a handy automated way to fuzz the web application's individual components or a web page. This means, for example, that we use a list that is used to send requests to the webserver if the page with the name from our list exists on the webserver. If we get a response code 200, then we know that this page exists on the webserver, and we can look at it manually.

Web Fuzzing

The term fuzzing refers to a testing technique that sends various types of user input to a certain interface to study how it would react. If we were fuzzing for SQL injection vulnerabilities, we would be sending random special characters and seeing how the server would react. If we were fuzzing for a buffer overflow, we would be sending long strings and incrementing their length to see if and when the binary would break.

Wordlists

Wordlist contains a combination of commonly used words for web directories and pages, very similar to a Password Dictionary Attack.

Some of the most commonly used wordlists can be found under the GitHub SecLists repository, which categorizes wordlists under various types of fuzzing, even including commonly used passwords, which we'll later utilize for Password Brute Forcing.

Directory Fuzzing

Ffuf is mostly pre-installed on kali linux machines. If you want to use it on your own machine, you can either use "apt install ffuf -y" or download it and use it from its GitHub Repo. As a new user of this tool, we will start by issuing the ffuf -h command to see how the tools can be used:

There are main two options are -w for wordlists and -u for the URL. We can assign a wordlist to a keyword to refer to it where we want to fuzz. For example, we can pick our wordlist and assign the keyword FUZZ to it by adding :FUZZ after it:

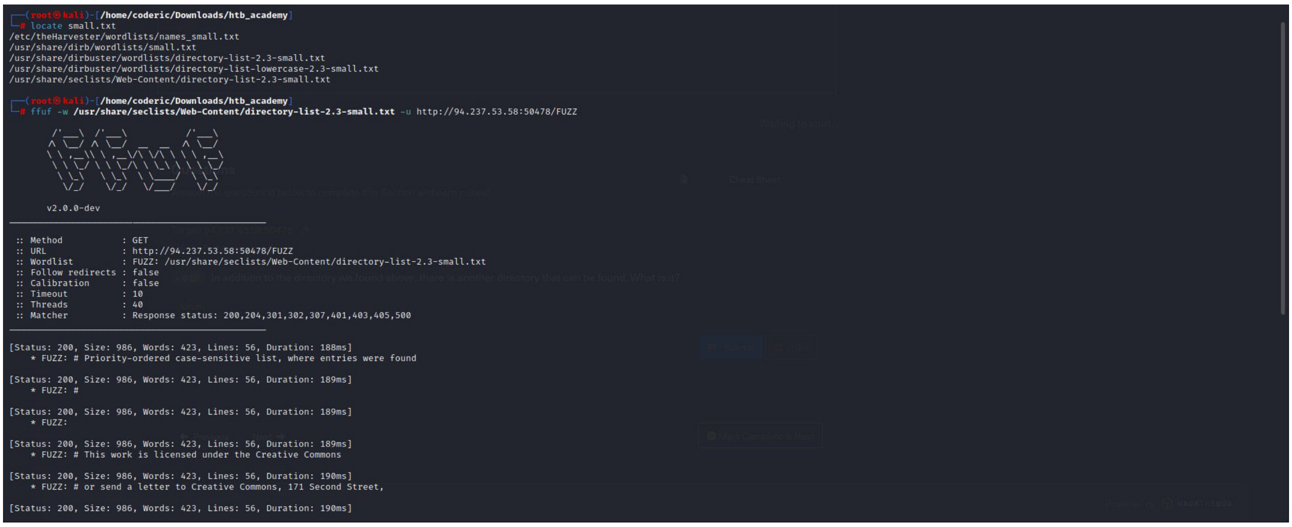
Questions

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

Target: 94.237.53.58:50478

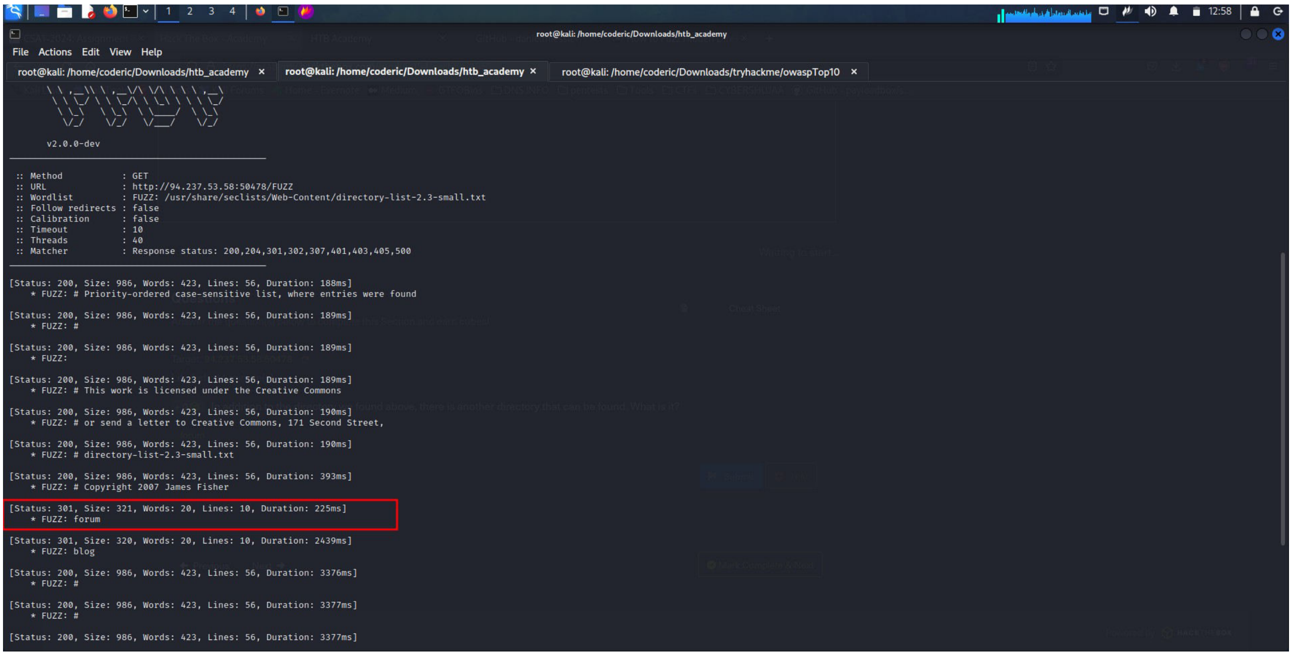
In addition to the directory we found above, there is another directory that can be found. What is it?
Ans: forum

First is to start a ffuf scanning



```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# locate small.txt
/etc/theHarvester/wordlists/names_small.txt
/usr/share/dirb/wordlists/small.txt
/usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt
/usr/share/seclists/Web-Content/directory-list-2.3-small.txt

┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# ffuf -w /usr/share/seclists/Web-Content/directory-list-2.3-small.txt -u http://94.237.53.58:50478/FUZZ

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://94.237.53.58:50478/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 188ms]
    * FUZZ: # Priority-ordered case-sensitive list, where entries were found

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 189ms]
    * FUZZ: #

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 189ms]
    * FUZZ:

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 189ms]
    * FUZZ: # This work is licensed under the Creative Commons

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 190ms]
    * FUZZ: # or send a letter to Creative Commons, 171 Second Street,

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 190ms]
```

I had a few results such as blog and forum, I tried answer blog it was not the one but forum was tha answer.



1
2
3
4
12:58
root@kali: /home/coderic/Downloads/htb_academy
File Actions Edit View Help
root@kali: /home/coderic/Downloads/htb_academy ×
root@kali: /home/coderic/Downloads/htb_academy ×
root@kali: /home/coderic/Downloads/tryhackme/owaspTop10 ×

```
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://94.237.53.58:50478/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 188ms]
    * FUZZ: # Priority-ordered case-sensitive list, where entries were found

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 189ms]
    * FUZZ: #

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 189ms]
    * FUZZ:

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 189ms]
    * FUZZ: # This work is licensed under the Creative Commons

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 190ms]
    * FUZZ: # or send a letter to Creative Commons, 171 Second Street,

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 190ms]
    * FUZZ: # directory-list-2.3-small.txt

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 393ms]
    * FUZZ: # Copyright 2007 James Fisher

[Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 225ms]
    * FUZZ: forum

[Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 2439ms]
    * FUZZ: blog

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3376ms]
    * FUZZ: #

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3377ms]
    * FUZZ: #

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3377ms]
```

Extension Fuzzing

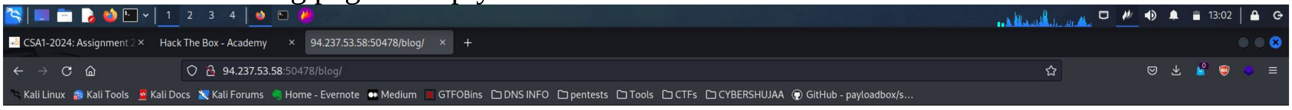
In the previous section, we found that we had access to /blog, but the directory returned an empty page, and we cannot manually locate any links or pages. So, we will once again utilize web fuzzing to see if the directory contains any hidden pages. However, before we start, we must find out what types of pages the website uses, like .html, .aspx, .php, or something else.

One common way to identify that is by finding the server type through the HTTP response headers and guessing the extension. For example, if the server is apache, then it may be .php, or if it was IIS, then it could be .asp or .aspx, and so on. This method is not very practical, though. So, we will again utilize ffuf to fuzz the extension, similar to how we fuzzed for directories. Instead of placing the FUZZ keyword where the directory name would be, we would place it where the extension would be .FUZZ, and use a wordlist for common extensions. We can utilize the following wordlist in SecLists for extensions:

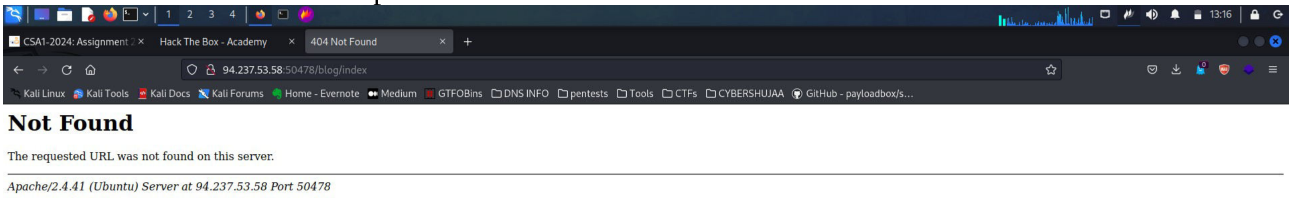
Questions

Try to use what you learned in this section to fuzz the '/blog' directory and find all pages. One of them should contain a flag. What is the flag?

As we can see the /blog page is empty



We need to find all pages.
For the server we know its Apache

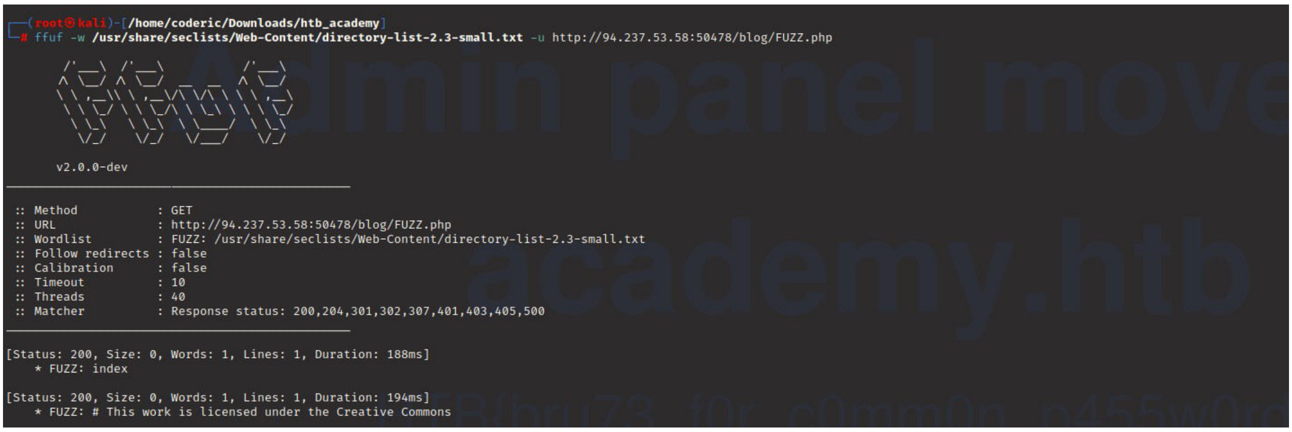


Not Found

The requested URL was not found on this server.

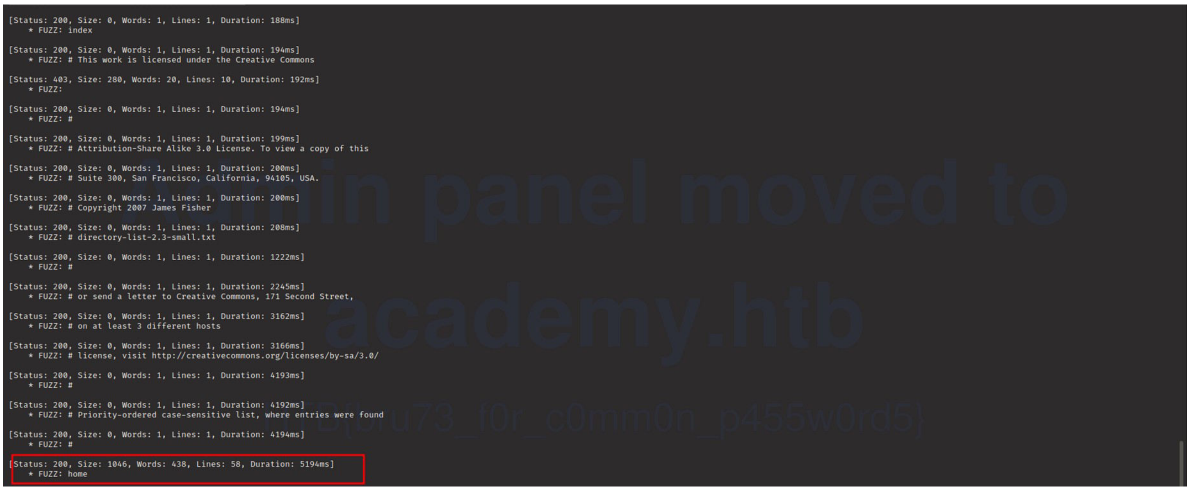
Apache/2.4.41 (Ubuntu) Server at 94.237.53.58 Port 50478

Command used:- **ffuf -w /usr/share/seclists/Web-Content/directory-list-2.3-small.txt -u http://94.237.53.58:50478/blog/FUZZ.php**



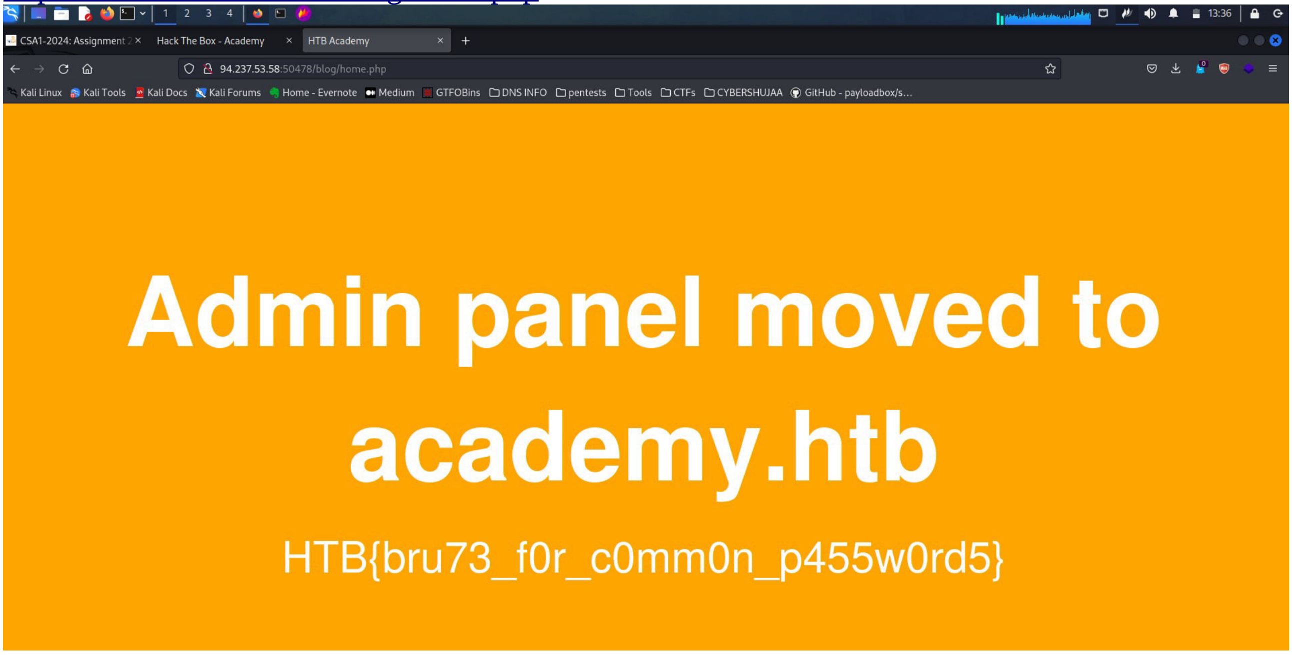
```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# ffuf -w /usr/share/seclists/Web-Content/directory-list-2.3-small.txt -u http://94.237.53.58:50478/blog/FUZZ.php

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://94.237.53.58:50478/blog/FUZZ.php
 :: Wordlist         : FUZZ: /usr/share/seclists/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 188ms]
    * FUZZ: index

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 194ms]
    * FUZZ: # This work is licensed under the Creative Commons
```

We have a php file called home, all I needed to do was to add this directory in the IP address on my browser to get a flag.



```
[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 188ms]
    * FUZZ: index

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 194ms]
    * FUZZ: # This work is licensed under the Creative Commons

[Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 192ms]
    * FUZZ:

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 194ms]
    * FUZZ: #

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 199ms]
    * FUZZ: # Attribution-Share Alike 3.0 License. To view a copy of this

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 200ms]
    * FUZZ: # Suite 300, San Francisco, California, 94105, USA.

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 200ms]
    * FUZZ: # Copyright 2007 James Fisher

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 208ms]
    * FUZZ: # directory-list-2.3-small.txt

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 1222ms]
    * FUZZ: #

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 2245ms]
    * FUZZ: # or send a letter to Creative Commons, 171 Second Street,

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 3162ms]
    * FUZZ: # on at least 3 different hosts

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 3166ms]
    * FUZZ: # license, visit http://creativecommons.org/licenses/by-sa/3.0/

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4193ms]
    * FUZZ: #

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4192ms]
    * FUZZ: # Priority-ordered case-sensitive list, where entries were found

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4194ms]
    * FUZZ: #

[Status: 200, Size: 1046, Words: 438, Lines: 58, Duration: 5194ms]
    * FUZZ: home
```

http://94.237.53.58:50478/blog/home.php



Admin panel moved to academy.htb

HTB{bru73_f0r_c0mm0n_p455w0rd5}

Recursive Fuzzing

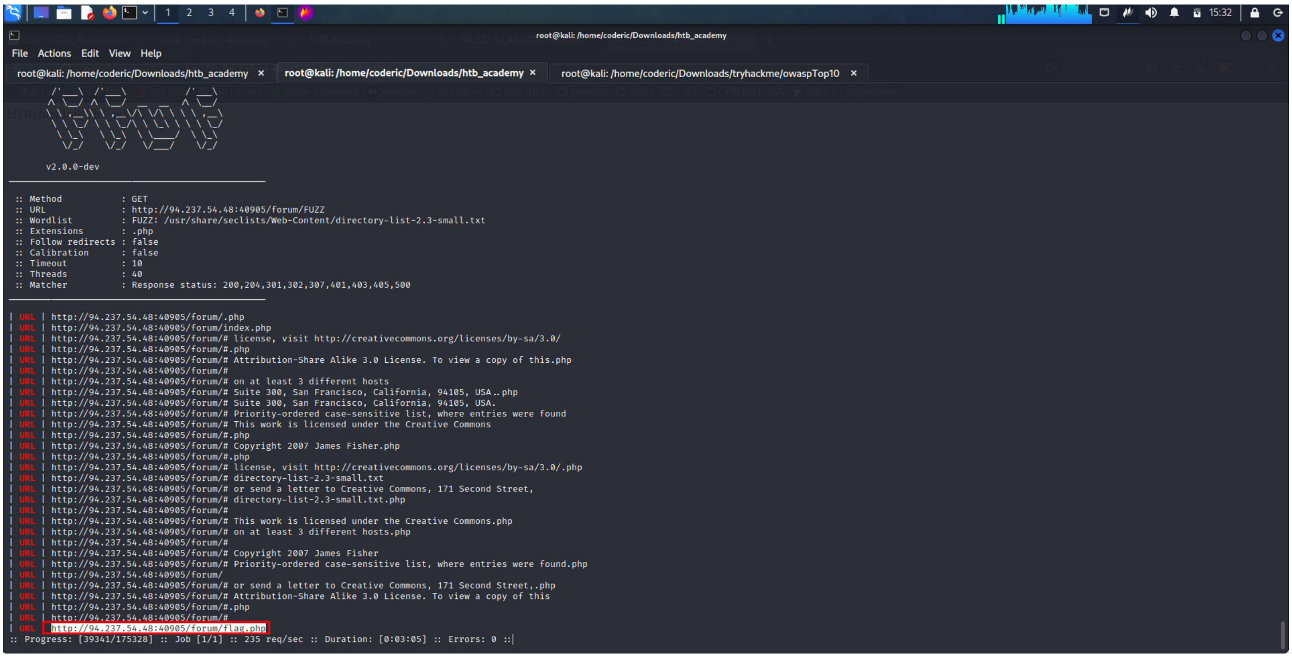
Recursive Flags

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.
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
the **flag -v** to output the full URLs. Otherwise, it may be difficult to tell which .php file lies under which directory.

Questions

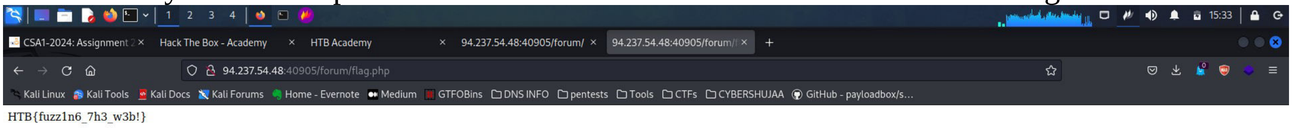
Try to repeat what you learned so far to find more files/directories. One of them should give you a flag. What is the content of the flag? **Ans: HTB{fuzz1n6_7h3_w3b!}**
From the previous scan, we were able to see another hidden directory called forum.
This time I decided to take a look at it using ffuf.

Command used:- ffuf -w /usr/share/seclists/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://94.237.54.48:40905/forum/FUZZ -recursion -recursion-depth 1 -e .php -v | grep URL


root@kali: /home/coderic/Downloads/htb_academy
File Actions Edit View Help
root@kali: /home/coderic/Downloads/htb_academy
root@kali: /home/coderic/Downloads/htb_academy
root@kali: /home/coderic/Downloads/tryhackme/owaspTop10

```
       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://94.237.54.48:40905/forum/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Web-Content/directory-list-2.3-small.txt
 :: Extensions       : .php
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

| URL | http://94.237.54.48:40905/forum/.php
| URL | http://94.237.54.48:40905/forum/index.php
| URL | http://94.237.54.48:40905/forum/# license, visit http://creativecommons.org/licenses/by-sa/3.0/
| URL | http://94.237.54.48:40905/forum/#.php
| URL | http://94.237.54.48:40905/forum/# Attribution-Share Alike 3.0 License. To view a copy of this.php
| URL | http://94.237.54.48:40905/forum/#
| URL | http://94.237.54.48:40905/forum/# on at least 3 different hosts
| URL | http://94.237.54.48:40905/forum/# Suite 300, San Francisco, California, 94105, USA..php
| URL | http://94.237.54.48:40905/forum/# Suite 300, San Francisco, California, 94105, USA.
| URL | http://94.237.54.48:40905/forum/# Priority-ordered case-sensitive list, where entries were found
| URL | http://94.237.54.48:40905/forum/# This work is licensed under the Creative Commons
| URL | http://94.237.54.48:40905/forum/#.php
| URL | http://94.237.54.48:40905/forum/# Copyright 2007 James Fisher.php
| URL | http://94.237.54.48:40905/forum/#.php
| URL | http://94.237.54.48:40905/forum/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.php
| URL | http://94.237.54.48:40905/forum/# directory-list-2.3-small.txt
| URL | http://94.237.54.48:40905/forum/# or send a letter to Creative Commons, 171 Second Street,
| URL | http://94.237.54.48:40905/forum/# directory-list-2.3-small.txt.php
| URL | http://94.237.54.48:40905/forum/#
| URL | http://94.237.54.48:40905/forum/# This work is licensed under the Creative Commons.php
| URL | http://94.237.54.48:40905/forum/# on at least 3 different hosts.php
| URL | http://94.237.54.48:40905/forum/#
| URL | http://94.237.54.48:40905/forum/# Copyright 2007 James Fisher
| URL | http://94.237.54.48:40905/forum/# Priority-ordered case-sensitive list, where entries were found.php
| URL | http://94.237.54.48:40905/forum/
| URL | http://94.237.54.48:40905/forum/# or send a letter to Creative Commons, 171 Second Street,.php
| URL | http://94.237.54.48:40905/forum/# Attribution-Share Alike 3.0 License. To view a copy of this
| URL | http://94.237.54.48:40905/forum/#.php
| URL | http://94.237.54.48:40905/forum/#
| URL | http://94.237.54.48:40905/forum/flag.php
:: Progress: [39341/175328] :: Job [1/1] :: 235 req/sec :: Duration: [0:03:05] :: Errors: 0 ::
```

One directory seemed suspicious so I took a look at it. This is how I found the flag



HTB{fuzz1n6_7h3_w3b!}

DNS Records

In this section it is explained in the case we visit the IP directly, the browser goes to that IP directly and knows how to connect to it. But in this case, we tell it to go to academy.htb, so it looks into the local /etc/hosts file and doesn't find any mention of it. It asks the public DNS about it (such as Google's DNS 8.8.8.8) and does not find any mention of it, since it is not a public website, and eventually fails to connect. So, to connect to academy.htb, we would have to add it to our /etc/hosts file.

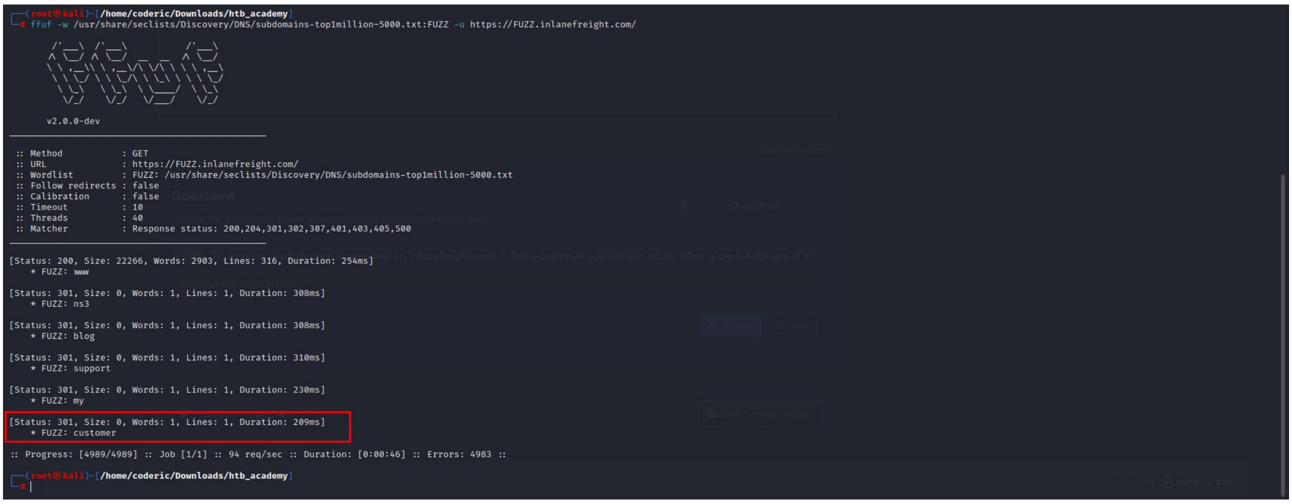
Command used to add a DNS to the /ect/hosts file is:-
sudo sh -c 'echo "SERVER_IP academy.htb" >> /etc/hosts'

Sub-domains Fuzzing

A sub-domain is any website underlying another domain. For example, https://photos.google.com photos is the sub-domain of google.com.

Questions

Answer the question(s) below to complete this Section and earn cubes!
Try running a sub-domain fuzzing test on 'inlanefreight.com' to find a customer sub-domain portal. What is the full domain of it?
Ans: customer.inlanefreight.com



```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u https://FUZZ.inlanefreight.com/

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://FUZZ.inlanefreight.com/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 22266, Words: 2903, Lines: 316, Duration: 254ms]
    * FUZZ: www

[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 308ms]
    * FUZZ: ns3

[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 308ms]
    * FUZZ: blog

[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 310ms]
    * FUZZ: support

[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 230ms]
    * FUZZ: my

[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 209ms]
    * FUZZ: customer

:: Progress: [4989/4989] :: Job [1/1] :: 94 req/sec :: Duration: [0:00:46] :: Errors: 4983 ::

┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# |
```

From my results I have a hint **customer** and since it is a sub-domain the answer has to include the domain **'inlanefreight.com** to make **customer.inlanefreight.com**

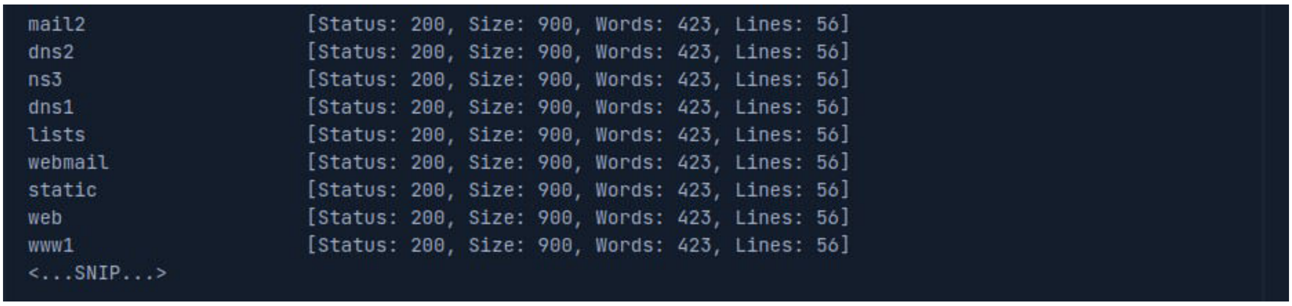
Vhost Fuzzing

Vhosts vs. Sub-domains

The key difference between VHosts and sub-domains is that a VHost is basically a 'sub-domain' served on the same server and has the same IP, such that a single IP could be serving two or more different websites.

It is possible when we use the sub-domain fuzzing, we would only be able to identify public sub-domains but will not identify any sub-domains that are not public.
To scan for VHosts, without manually adding the entire wordlist to our /etc/hosts, we will be fuzzing HTTP headers, specifically the Host: header. To do that, we can use the -H flag to specify a header.
FUZZ keyword : **ffuf -w /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://academy.htb:PORT/ -H 'Host: FUZZ.academy.htb'**

Results:



```
mail2                   [Status: 200, Size: 900, Words: 423, Lines: 56]
dns2                    [Status: 200, Size: 900, Words: 423, Lines: 56]
ns3                     [Status: 200, Size: 900, Words: 423, Lines: 56]
dns1                    [Status: 200, Size: 900, Words: 423, Lines: 56]
lists                   [Status: 200, Size: 900, Words: 423, Lines: 56]
webmail                 [Status: 200, Size: 900, Words: 423, Lines: 56]
static                  [Status: 200, Size: 900, Words: 423, Lines: 56]
web                     [Status: 200, Size: 900, Words: 423, Lines: 56]
www1                    [Status: 200, Size: 900, Words: 423, Lines: 56]
<...SNIP...>
```

Most response is 200 Ok! , this is expected when a vhost is present. we are simply changing the header while visiting http://academy.htb:PORT/. So, we know that we will always get 200 OK.

If the VHost does exist and we send a correct one in the header, we should get a different response size, as in that case, we would be getting the page from that VHosts, which is likely to show a different page.

Filtering Results

This helps us minimize the number of results gotten from a search or focus the scan on the desired area.
Ffuf provides the option to match or filter out a specific HTTP code, response size, or amount of words.
For example, we know the response size of incorrect results as 900, we use **-fs 900** to filter out this size response.

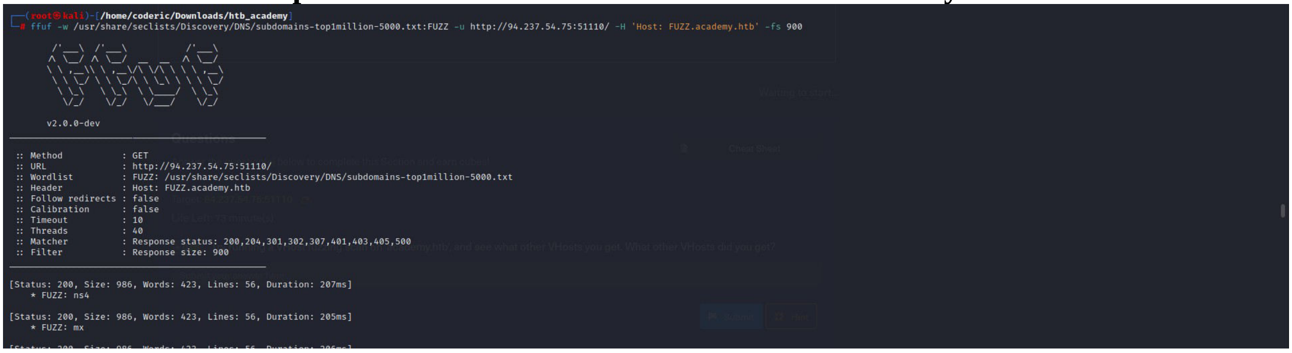
Questions

Target: 94.237.54.75:51110

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

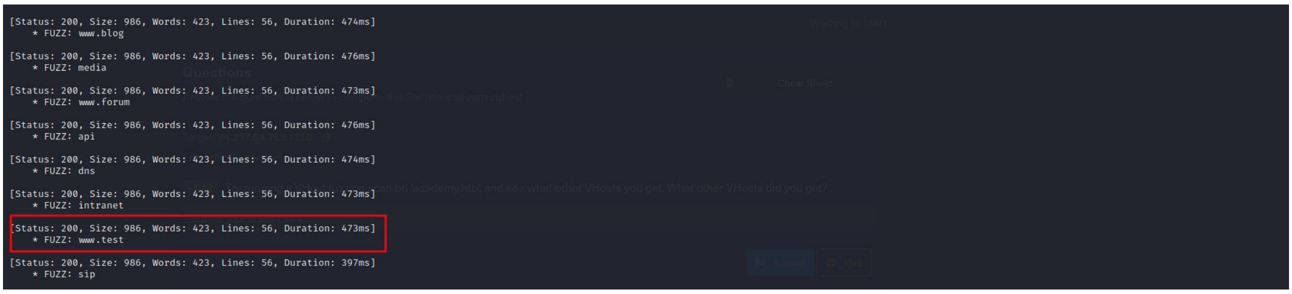
Ans: test.academy.htb

Command used:- **ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://94.237.54.75:51110/ -H 'Host: FUZZ.academy.htb' -fs 900**



```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://94.237.54.75:51110/ -H 'Host: FUZZ.academy.htb' -fs 900

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://94.237.54.75:51110/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.academy.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 900
________________________________________________

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 207ms]
    * FUZZ: ns4

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 205ms]
    * FUZZ: mx

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 206ms]
```

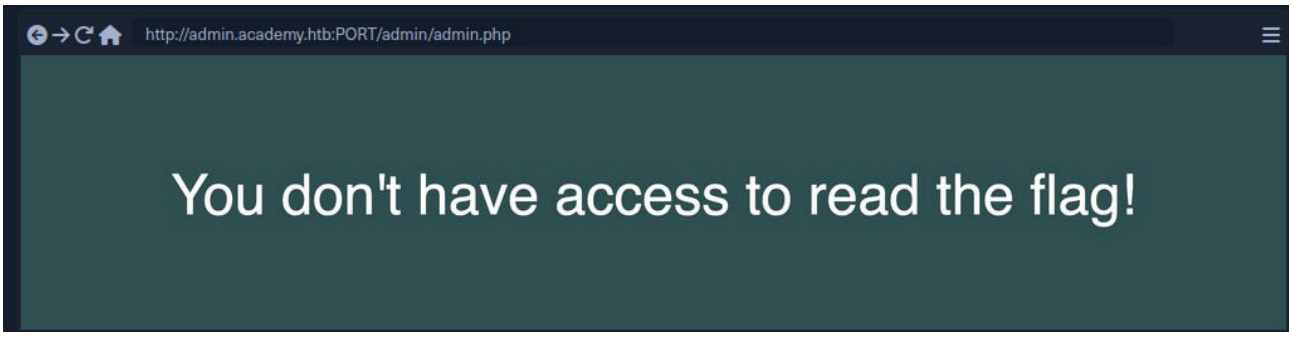
Results:



```
[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 474ms]
    * FUZZ: www.blog

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 476ms]
    * FUZZ: media

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 473ms]
    * FUZZ: www.forum

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 476ms]
    * FUZZ: api

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 474ms]
    * FUZZ: dns

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 473ms]
    * FUZZ: intranet

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 473ms]
    * FUZZ: www.test

[Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 397ms]
    * FUZZ: sip
```

Parameter Fuzzing - GET

If we run a recursive ffuf scan on admin.academy.htb, we should find http://admin.academy.htb:PORT/admin/admin.php. If we try accessing this page, we see the following:



http://admin.academy.htb:PORT/admin/admin.php

You don't have access to read the flag!

That indicates that there must be something that identifies users to verify whether they have access to read the flag. We did not login, nor do we have any cookie that can be verified at the backend. So, perhaps there is a key that we can pass to the page to read the flag. Such keys would usually be passed as a parameter, using either a GET or a POST HTTP request. This section will discuss how to fuzz for such parameters until we identify a parameter that can be accepted by the page.

GET Request Fuzzing

GET requests, which are usually passed right after the URL, with a ? symbol, like:
http://admin.academy.htb:PORT/admin/admin.php?param1=key.

What we have to do is replace param1 with FUZZ and rerun our scan
Example command used:

ffuf -w /opt/useful/SecLists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://admin.academy.htb:PORT/admin/admin.php?FUZZ=key -fs xxx

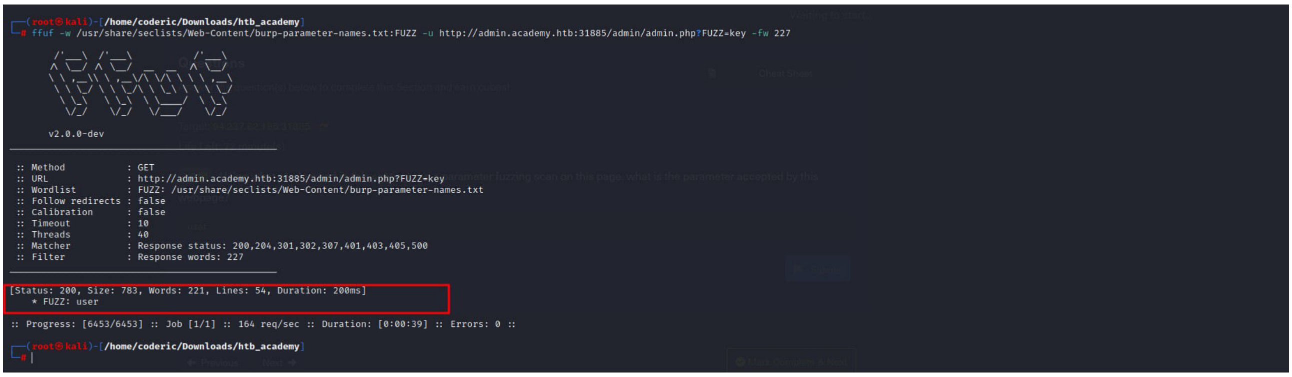
Questions

Target: 94.237.54.75:51110

Using what you learned in this section, run a parameter fuzzing scan on this page. what is the parameter accepted by this webpage?
Ans: user

Command used:- ffuf -w /usr/share/seclists/Web-Content/burp-parameter-names.txt:FUZZ -u http://admin.academy.htb:31885/admin/admin.php?FUZZ=key -fw 227

-fw is a word filter.



```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# ffuf -w /usr/share/seclists/Web-Content/burp-parameter-names.txt:FUZZ -u http://admin.academy.htb:31885/admin/admin.php?FUZZ=key -fw 227

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://admin.academy.htb:31885/admin/admin.php?FUZZ=key
 :: Wordlist         : FUZZ: /usr/share/seclists/Web-Content/burp-parameter-names.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response words: 227
________________________________________________

[Status: 200, Size: 783, Words: 221, Lines: 54, Duration: 200ms]
    * FUZZ: user

:: Progress: [6453/6453] :: Job [1/1] :: 164 req/sec :: Duration: [0:00:39] :: Errors: 0 ::

┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# |
```

Parameter Fuzzing - POST

The main difference between POST requests and GET requests is that POST requests are not passed with the URL and cannot simply be appended after a ? symbol. POST requests are passed in the data field within the HTTP request.
To fuzz the data field with ffuf, we can use the -d flag, as we saw previously in the output of ffuf -h.
We also have to add -X POST to send POST requests.

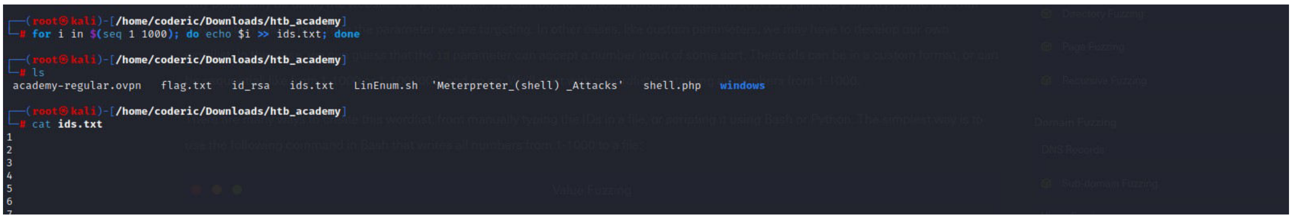
Syntax Command:-

ffuf -w /opt/useful/SecLists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'FUZZ=key' -H 'Content-Type: application/x-www-form-urlencoded' -fs xxx

Value Fuzzing

In value fussing the command should be fairly similar to the POST command we used to fuzz for parameters, but our FUZZ keyword should be put where the parameter value would be, and we will use the ids.txt wordlist we just created, as follows:

Creating **ids.tx** command**:- for i in $(seq 1 1000); do echo $i >> ids.txt; done**



```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# for i in $(seq 1 1000); do echo $i >> ids.txt; done

┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# ls
 academy-regular.ovpn   flag.txt   id_rsa   ids.txt   LinEnum.sh  'Meterpreter_(shell) _Attacks'   shell.php   windows

┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# cat ids.txt
1
2
3
4
5
6
```

Value fuzzing command:- **ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'id=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs xxx**

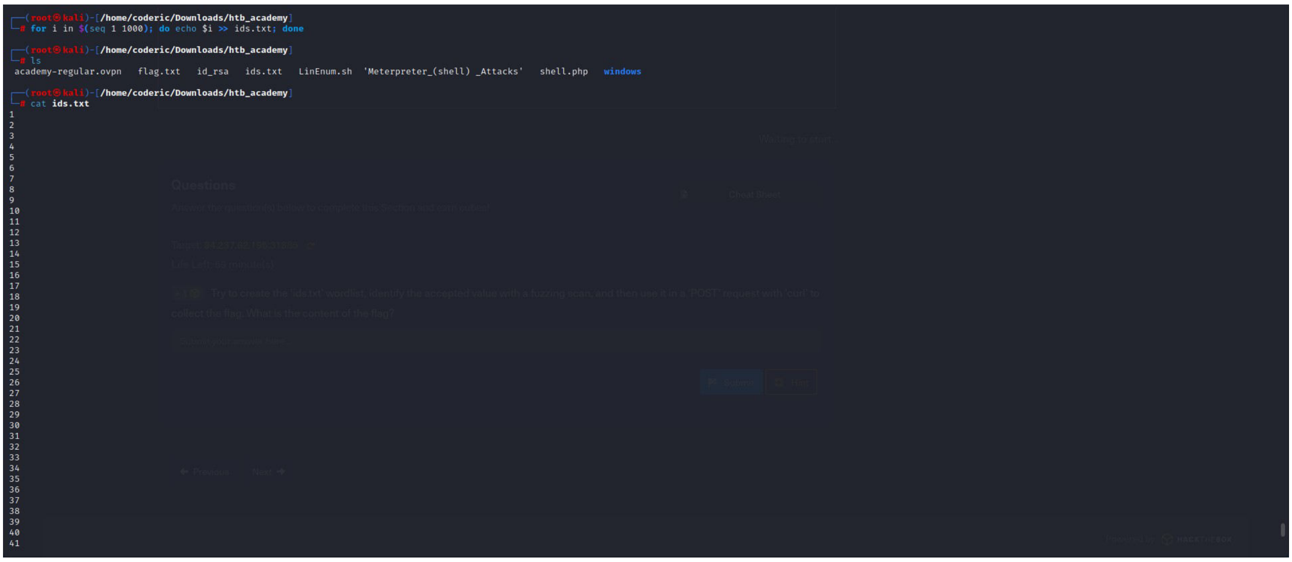
Questions

Target: 94.237.62.195:31885

Try to create the 'ids.txt' wordlist, identify the accepted value with a fuzzing scan, and then use it in a 'POST' request with 'curl' to collect the flag. What is the content of the flag?

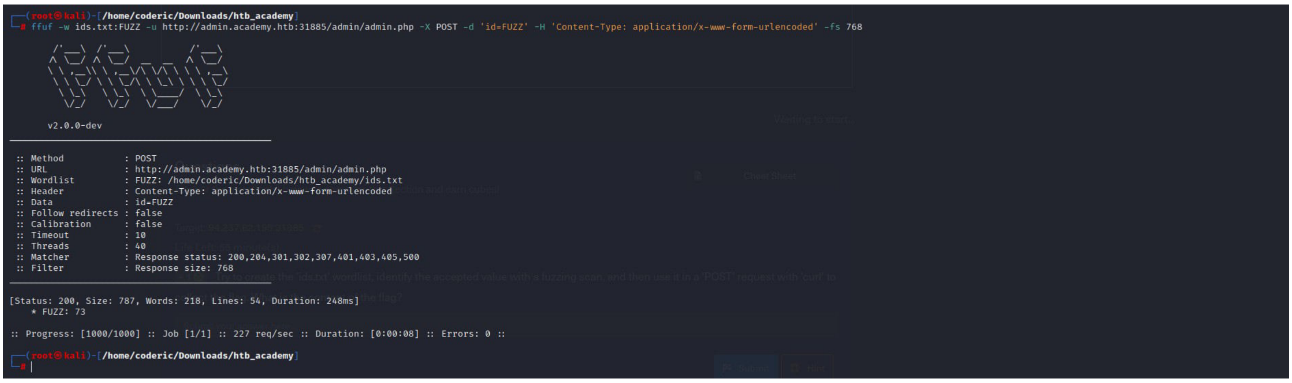
Ans: HTB{p4r4m373r_fuzz1n6_15_k3y!}

Ids.txt created:



```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# for i in $(seq 1 1000); do echo $i >> ids.txt; done

┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# ls
 academy-regular.ovpn   flag.txt   id_rsa   ids.txt   LinEnum.sh  'Meterpreter_(shell) _Attacks'   shell.php   windows

┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# cat ids.txt
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
```

Identifying the accepted value with a fuzzing scan:
Command used:-
ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:31885/admin/admin.php -X POST -d 'id=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 768

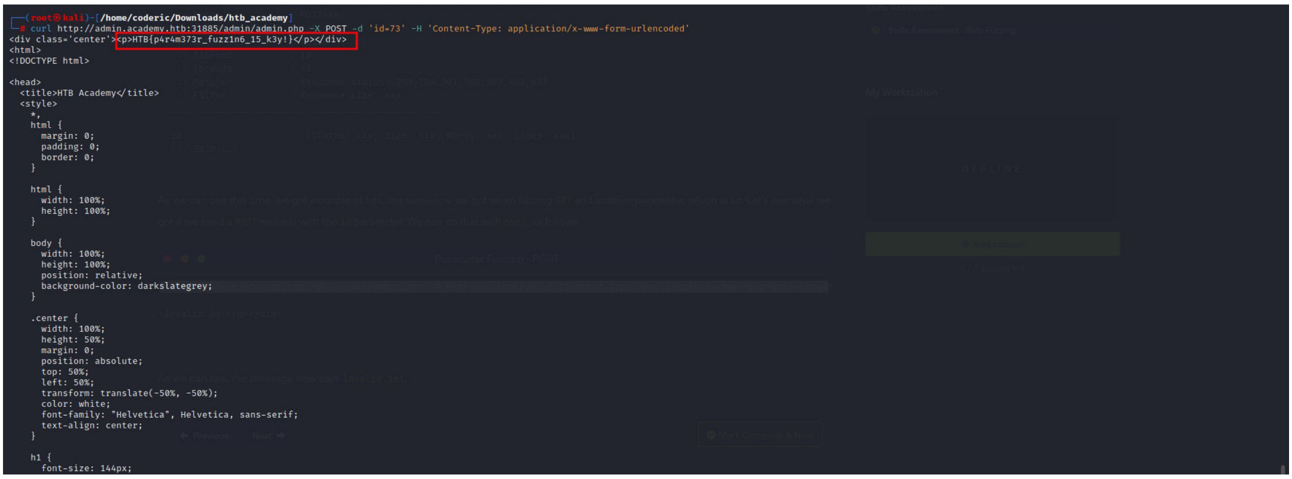


```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:31885/admin/admin.php -X POST -d 'id=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 768

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

       v2.0.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://admin.academy.htb:31885/admin/admin.php
 :: Wordlist         : FUZZ: /home/coderic/Downloads/htb_academy/ids.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : id=FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 768
________________________________________________

[Status: 200, Size: 787, Words: 218, Lines: 54, Duration: 248ms]
    * FUZZ: 73

:: Progress: [1000/1000] :: Job [1/1] :: 227 req/sec :: Duration: [0:00:08] :: Errors: 0 ::

┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# |
```

Using the value achieved in a 'POST' request with 'curl' to collect the flag.

Command Used:- **curl http://admin.academy.htb:31885/admin/admin.php -X POST -d 'id=73' -H 'Content-Type: application/x-www-form-urlencoded'**

Results:



```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# curl http://admin.academy.htb:31885/admin/admin.php -X POST -d 'id=73' -H 'Content-Type: application/x-www-form-urlencoded'
<div class='center'><p>HTB{p4r4m373r_fuzz1n6_15_k3y!}</p></div>
<html>
<!DOCTYPE html>

<head>
  <title>HTB Academy</title>
  <style>
    *,
    html {
      margin: 0;
      padding: 0;
      border: 0;
    }

    html {
      width: 100%;
      height: 100%;
    }

    body {
      width: 100%;
      height: 100%;
      position: relative;
      background-color: darkslategrey;
    }

    .center {
      width: 100%;
      height: 50%;
      margin: 0;
      position: absolute;
      top: 50%;
      left: 50%;
      transform: translate(-50%, -50%);
      color: white;
      font-family: "Helvetica", Helvetica, sans-serif;
      text-align: center;
    }

    h1 {
      font-size: 144px;
```

Flag is:- **HTB{p4r4m373r_fuzz1n6_15_k3y!}**

Skills Assessment - Web Fuzzing

You are given an online academy's IP address but have no further information about their website. As the first step of conducting a Penetration Test, you are expected to locate all pages and domains linked to their IP to enumerate the IP and domains properly.

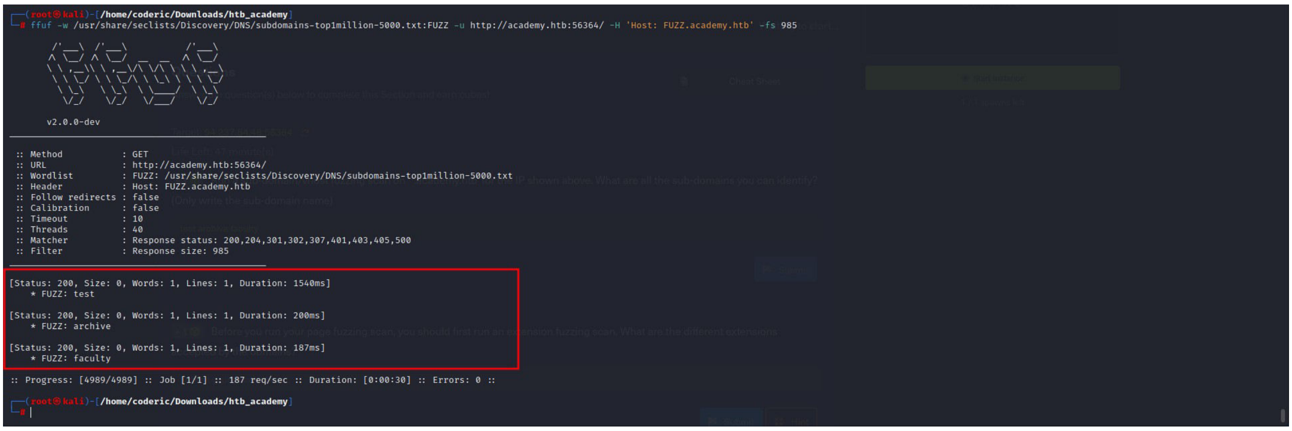
Finally, you should do some fuzzing on pages you identify to see if any of them has any parameters that can be interacted with. If you do find active parameters, see if you can retrieve any data from them.

Questions

Target: 94.237.54.48:56364

Run a sub-domain/vhost fuzzing scan on '*.academy.htb' for the IP shown above. What are all the sub-domains you can identify? (Only write the sub-domain name)
Ans: test archive faculty

Command Used:- **ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://academy.htb:56364/ -H 'Host: FUZZ.academy.htb' -fs 985**

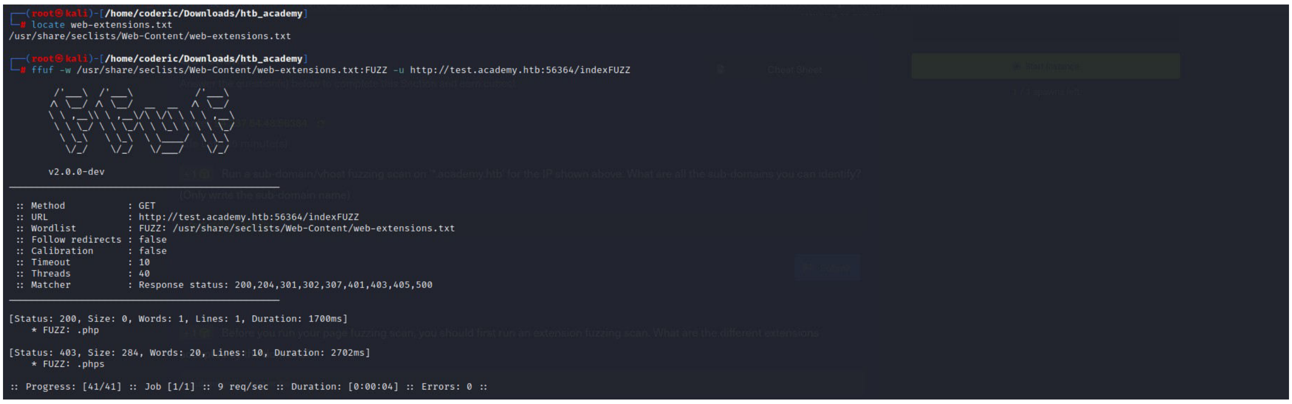


```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://academy.htb:56364/ -H 'Host: FUZZ.academy.htb' -fs 985

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://academy.htb:56364/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.academy.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 985
________________________________________________

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 1540ms]
    * FUZZ: test

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 200ms]
    * FUZZ: archive

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 187ms]
    * FUZZ: faculty

:: Progress: [4989/4989] :: Job [1/1] :: 187 req/sec :: Duration: [0:00:30] :: Errors: 0 ::

┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# |
```

Before you run your page fuzzing scan, you should first run an extension fuzzing scan. What are the different extensions accepted by the domains?
Ans: php7 php phps

Command used:- **ffuf -w /usr/share/seclists/Web-Content/web-extensions.txt:FUZZ -u http://<domain>.academy.htb:56364/indexFUZZ**

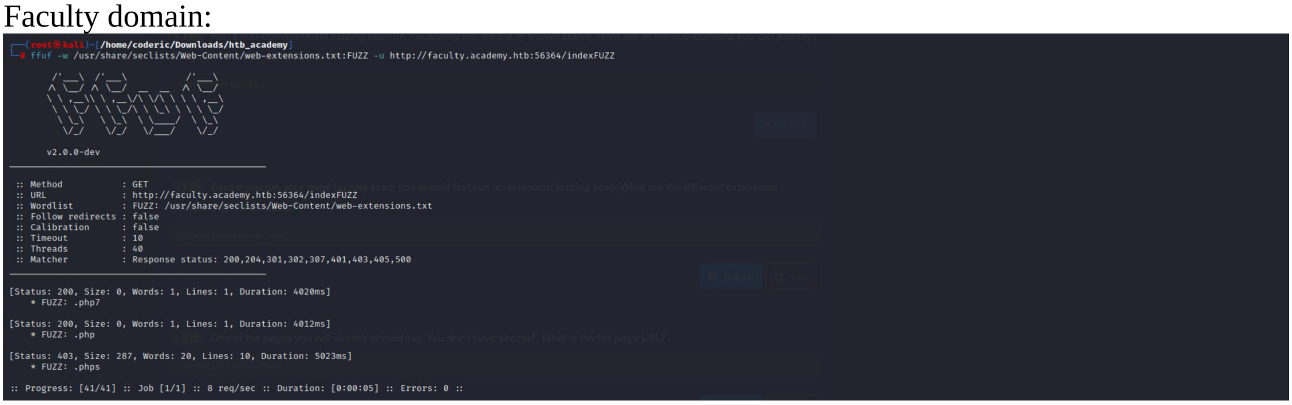
Test domain:



```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# locate web-extensions.txt
/usr/share/seclists/Web-Content/web-extensions.txt

┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# ffuf -w /usr/share/seclists/Web-Content/web-extensions.txt:FUZZ -u http://test.academy.htb:56364/indexFUZZ

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://test.academy.htb:56364/indexFUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Web-Content/web-extensions.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 1700ms]
    * FUZZ: .php

[Status: 403, Size: 284, Words: 20, Lines: 10, Duration: 2702ms]
    * FUZZ: .phps

:: Progress: [41/41] :: Job [1/1] :: 9 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

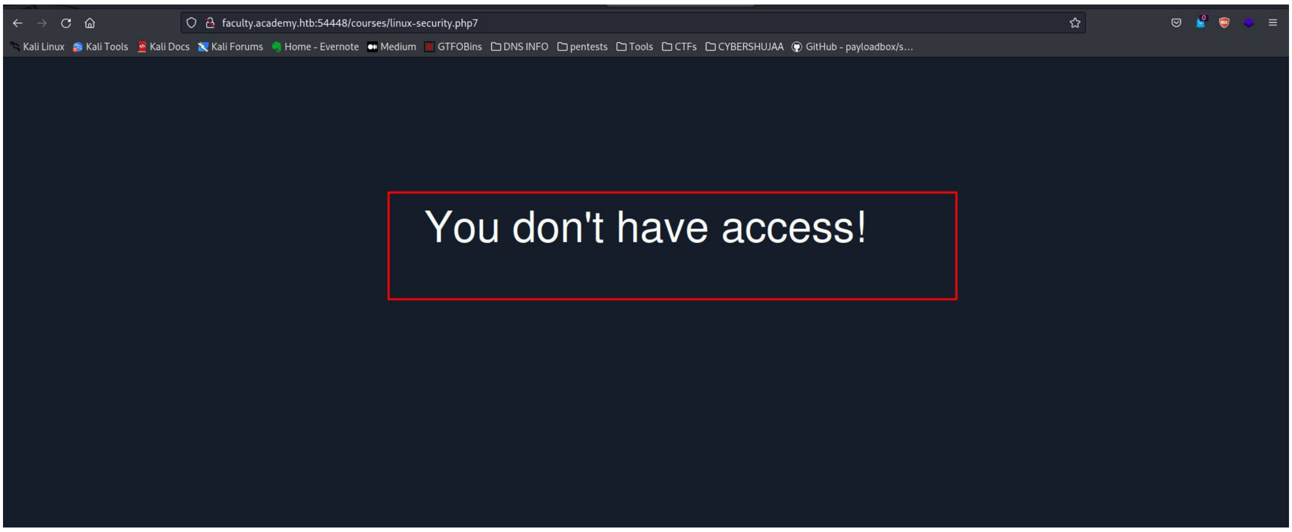
Archive domain did not give a result

Faculty domain:



```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# ffuf -w /usr/share/seclists/Web-Content/web-extensions.txt:FUZZ -u http://faculty.academy.htb:56364/indexFUZZ

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://faculty.academy.htb:56364/indexFUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Web-Content/web-extensions.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4020ms]
    * FUZZ: .php7

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4012ms]
    * FUZZ: .php

[Status: 403, Size: 287, Words: 20, Lines: 10, Duration: 5023ms]
    * FUZZ: .phps

:: Progress: [41/41] :: Job [1/1] :: 8 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

One of the pages you will identify should say 'You don't have access!'. What is the full page URL?
Ans: http://faculty.academy.htb:port/courses/linux-security.php7



faculty.academy.htb:54448/courses/linux-security.php7

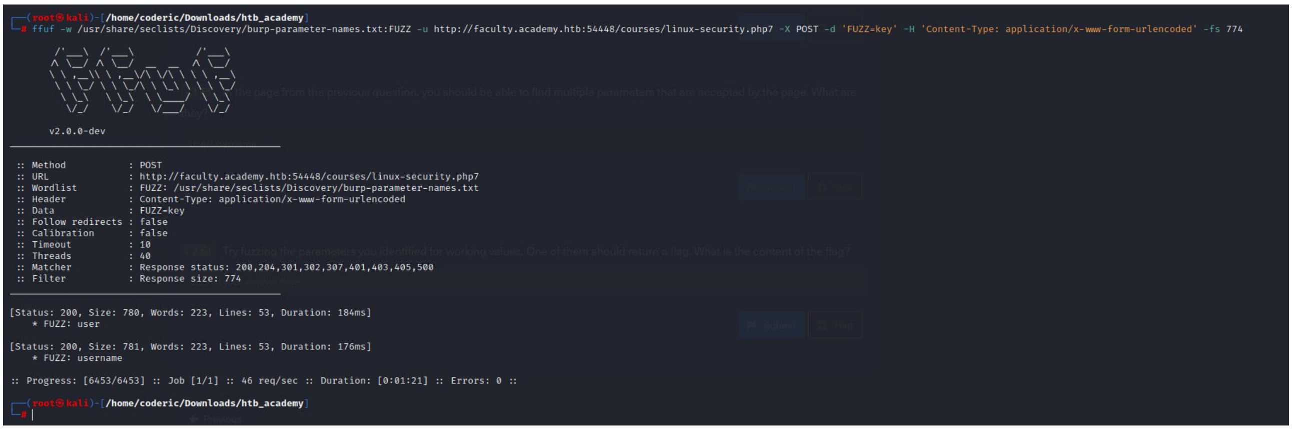
You don't have access!

In the page from the previous question, you should be able to find multiple parameters that are accepted by the page. What are they?

Ans: user, username

Command used:- **ffuf -w /usr/share/seclists/Discovery/burp-parameter-names.txt:FUZZ -u http://faculty.academy.htb:54448/courses/linux-security.php7 -X POST -d 'FUZZ=key' -H 'Content-Type: application/x-www-form-urlencoded' -fs 774**

Results:

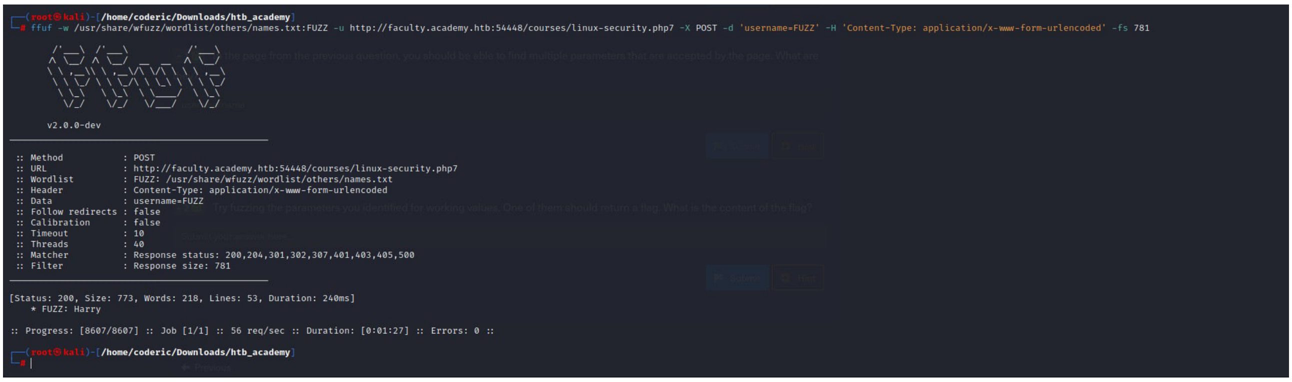


```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# ffuf -w /usr/share/seclists/Discovery/burp-parameter-names.txt:FUZZ -u http://faculty.academy.htb:54448/courses/linux-security.php7 -X POST -d 'FUZZ=key' -H 'Content-Type: application/x-www-form-urlencoded' -fs 774

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

       v2.0.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://faculty.academy.htb:54448/courses/linux-security.php7
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/burp-parameter-names.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : FUZZ=key
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 774
________________________________________________

[Status: 200, Size: 780, Words: 223, Lines: 53, Duration: 184ms]
    * FUZZ: user

[Status: 200, Size: 781, Words: 223, Lines: 53, Duration: 176ms]
    * FUZZ: username

:: Progress: [6453/6453] :: Job [1/1] :: 46 req/sec :: Duration: [0:01:21] :: Errors: 0 ::

┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# |
```

Try fuzzing the parameters you identified for working values. One of them should return a flag. What is the content of the flag? **Ans: HTB{w3b_fuzz1n6_m4573r}**

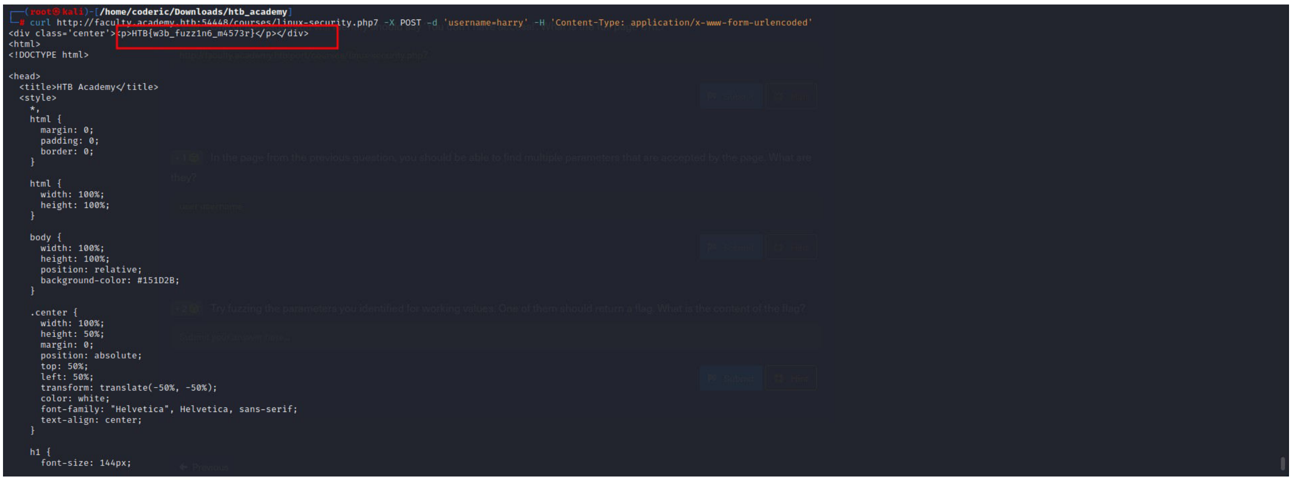
First was to identify a username: **Harry**

Command used:- **ffuf -w /usr/share/wfuzz/wordlist/others/names.txt:FUZZ -u http://faculty.academy.htb:54448/courses/linux-security.php7 -X POST -d 'username=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 78**



```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# ffuf -w /usr/share/wfuzz/wordlist/others/names.txt:FUZZ -u http://faculty.academy.htb:54448/courses/linux-security.php7 -X POST -d 'username=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 781

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

       v2.0.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://faculty.academy.htb:54448/courses/linux-security.php7
 :: Wordlist         : FUZZ: /usr/share/wfuzz/wordlist/others/names.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : username=FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 781
________________________________________________

[Status: 200, Size: 773, Words: 218, Lines: 53, Duration: 240ms]
    * FUZZ: Harry

:: Progress: [8607/8607] :: Job [1/1] :: 56 req/sec :: Duration: [0:01:27] :: Errors: 0 ::

┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# |
```

Next is to pass this username in our parameter.



```
┌──(root㉿kali)-[/home/coderic/Downloads/htb_academy]
└─# curl http://faculty.academy.htb:54448/courses/linux-security.php7 -X POST -d 'username=harry' -H 'Content-Type: application/x-www-form-urlencoded'
<div class='center'><p>HTB{w3b_fuzz1n6_m4573r}</p></div>
<html>
<!DOCTYPE html>

<head>
  <title>HTB Academy</title>
  <style>
    *,
    html {
      margin: 0;
      padding: 0;
      border: 0;
    }

    html {
      width: 100%;
      height: 100%;
    }

    body {
      width: 100%;
      height: 100%;
      position: relative;
      background-color: #151D2B;
    }

    .center {
      width: 100%;
      height: 50%;
      margin: 0;
      position: absolute;
      top: 50%;
      left: 50%;
      transform: translate(-50%, -50%);
      color: white;
      font-family: "Helvetica", Helvetica, sans-serif;
      text-align: center;
    }

    h1 {
      font-size: 144px;
```

HTB{w3b_fuzz1n6_m4573r}

Conclusion.

In my conclusion, the module on attacking web applications with FFUF in the Hack The Box Academy has provided me with valuable insights into the powerful capabilities of FFUF as a versatile web fuzzer. By exploring various techniques and strategies, I have gained a deeper understanding of how to efficiently discover hidden directories, files and potential vulnerabilities within web applications. The hands-on approach and practical exercises offered in this module has equipped me with practical skills applicable to real-world penetration testing scenarios. I can now say I am better equipped to assess and secure web applications by leveraging FFUF's robust features in their ethical hacking endeavors than I was before.

Thank You.