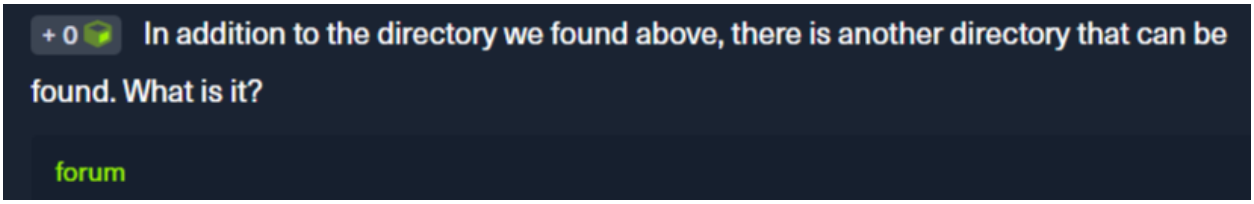
NAME: BOAZ OCHIENG

ADM NO: CS7-SA05-23004

ASSIGNMENT: ATTACKING THE WEB APPLICATIONS WITH FFUF

Fuzzing is a testing technique where several kinds of user input are sent to an interface in order to see how it will respond. The module covers the following topics: parameter fuzzing, Vhost fuzzing, domain fuzzing, directory fuzzing, page fuzzing, and recursive fuzzing. The following questions are tested in the module:

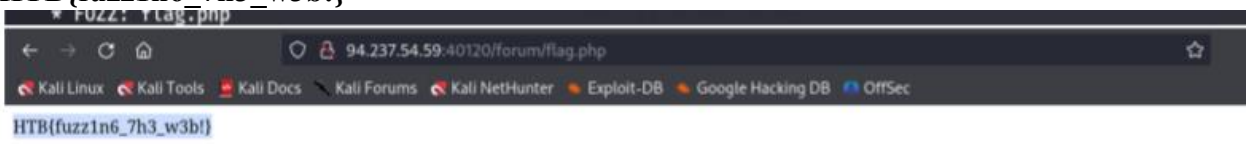
1. In addition to the directory we found above, there is another directory that can be found. What is it?
   forum




```
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 292ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 297ms]
# directory-list-2.3-small.txt [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 298ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 288ms]
#                       [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 798ms]
forum                   [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 206ms]
#                       [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3861ms]
#                       [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4870ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4873ms]
# Copyright 2007 James Fisher [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4886ms]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4876ms]
blog                    [Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 4840ms]
                        [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4880ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4884ms]
```

2. 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?
   HTB{bru73_f0r_c0mm0n_p455w0rd5}

3. 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?
   HTB{fuzz1n6_7h3_w3b!}



4. Try running a sub-domain fuzzing test on 'inlanefreight.com' to find a customer sub-domain portal. What is the full domain of it?

customer.inlanefreight.com

```
 :: Method           : GET
 :: URL              : https://FUZZ.inlanefreight.com
 :: Wordlist         : FUZZ: /home/tough/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

www                     [Status: 200, Size: 22266, Words: 2903, Lines: 316, Duration: 248ms]
support                 [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 237ms]
ns3                     [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 304ms]
blog                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 227ms]
my                      [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 233ms]
customer                [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 228ms]
```

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

   test.academy.htb

```
admin                   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 3419ms]
test                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4443ms]
:: Progress: [4989/4989] :: Job [1/1] :: 178 req/sec :: Duration: [0:00:26] :: Errors: 0 ::
```

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

   User

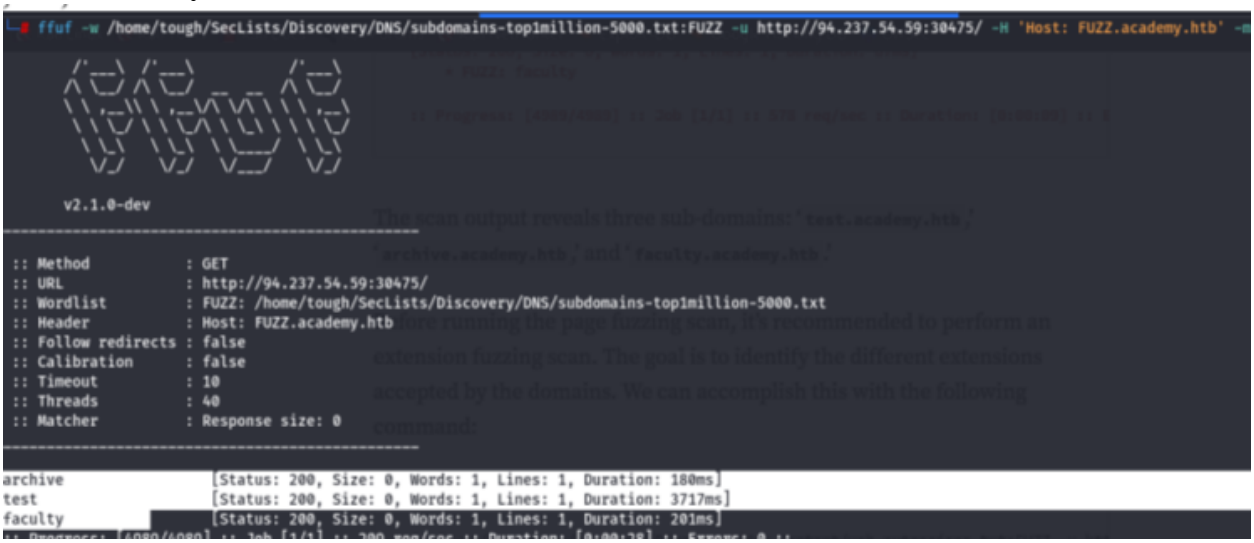
```
 :: Method           : GET
 :: URL              : http://admin.academy.htb:52289/admin/admin.php?FUZZ=key
 :: Wordlist         : FUZZ: /home/tough/SecLists/Discovery/Web-Content/burp-parameter-names.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response words: 227
________________________________________________

user                    [Status: 200, Size: 783, Words: 221, Lines: 54, Duration: 191ms]
:: Progress: [6453/6453] :: Job [1/1] :: 215 req/sec :: Duration: [0:00:33] :: Errors: 0 ::
```

7. 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?

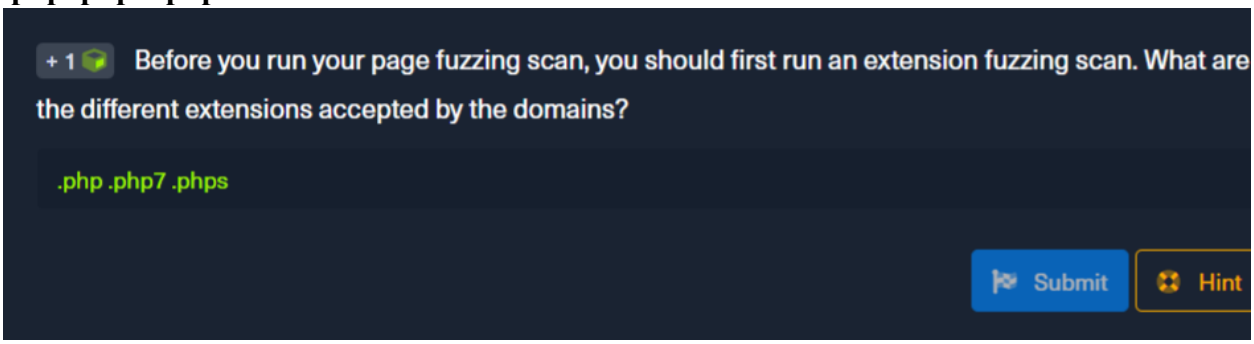
   HTB{p4r4m373r_fuzz1n6_15_k3y!}

```
________________________________________________

3                       [Status: 200, Size: 787, Words: 218, Lines: 54, Duration: 282ms]
: Progress: [1000/1000] :: Job [1/1] :: 49 req/sec :: Duration: [0:00:15] :: Errors: 0 ::

┌──(root㉿kali)-[/home/tough]
└─# curl http://admin.academy.htb:52289/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;
    }
```

8. 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)
archive faculty test



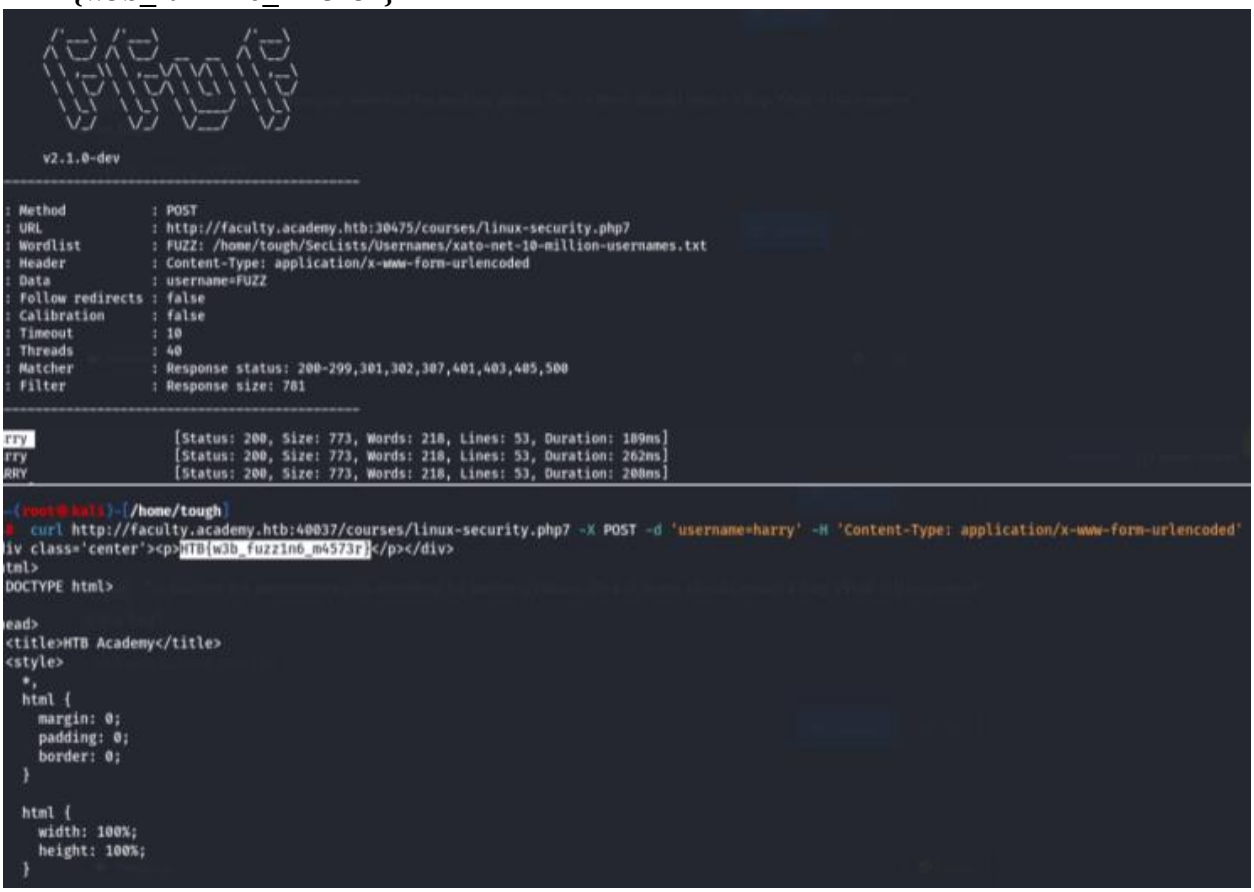
9. Before you run your page fuzzing scan, you should first run an extension fuzzing scan. What are the different extensions accepted by the domains?
.php .php7 .phps



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

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

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



To sum up, completing the Attacking Web Applications with Ffuf module was challenging but instructive. I comprehend how to enumerate web applications for hidden pages, directories, parameters, and fuzzing parameter. I had trouble accessing certain wordlists and their respective folders, but after doing some research and taking the writeups, I have been able to locate the correct directories and complete the module.

Sharable Link: https://academy.hackthebox.com/achievement/976551/54