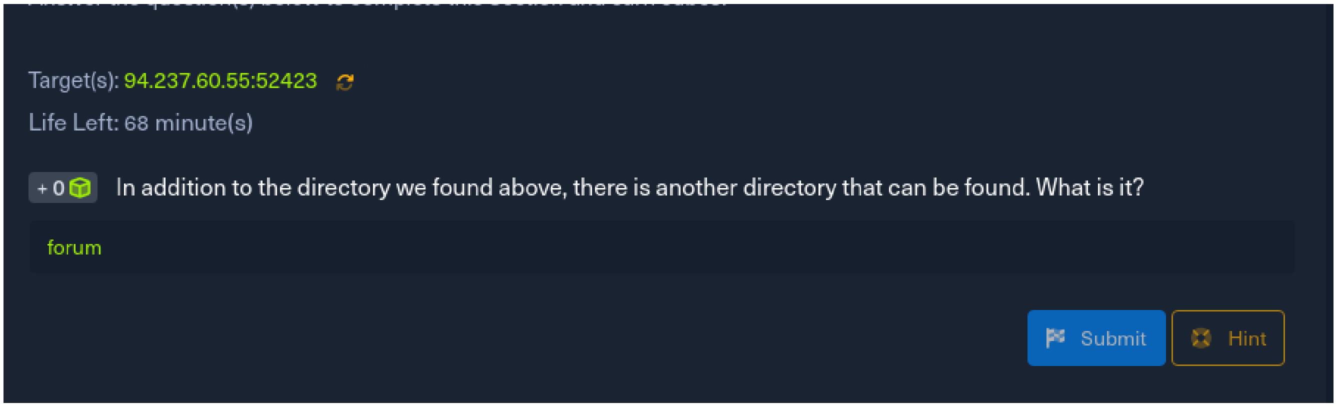
ISSACK WAITHAKA
cs-sa07-24085

Introduction
- We are going to learn about the ffuf tool for web fuzzing.
- Fuzzing is testing technique that sends various inputs to an interface to see how it reacts
- We use wordlists which contains commonly used words for web directories

ffuf
- It has only two options, The -w for wordlists and -u for the url

Questions
1.

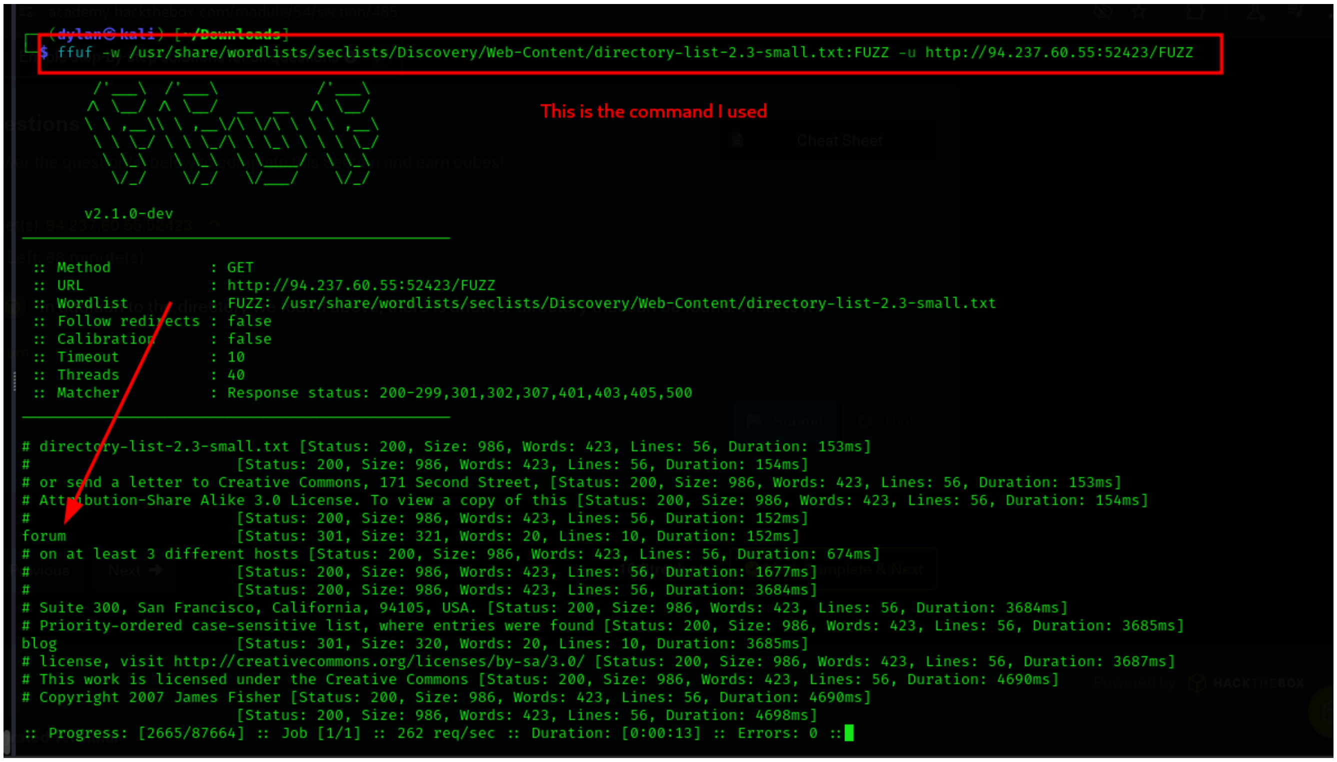


Target(s): 94.237.60.55:52423

Life Left: 68 minute(s)

+0 In addition to the directory we found above, there is another directory that can be found. What is it?

forum



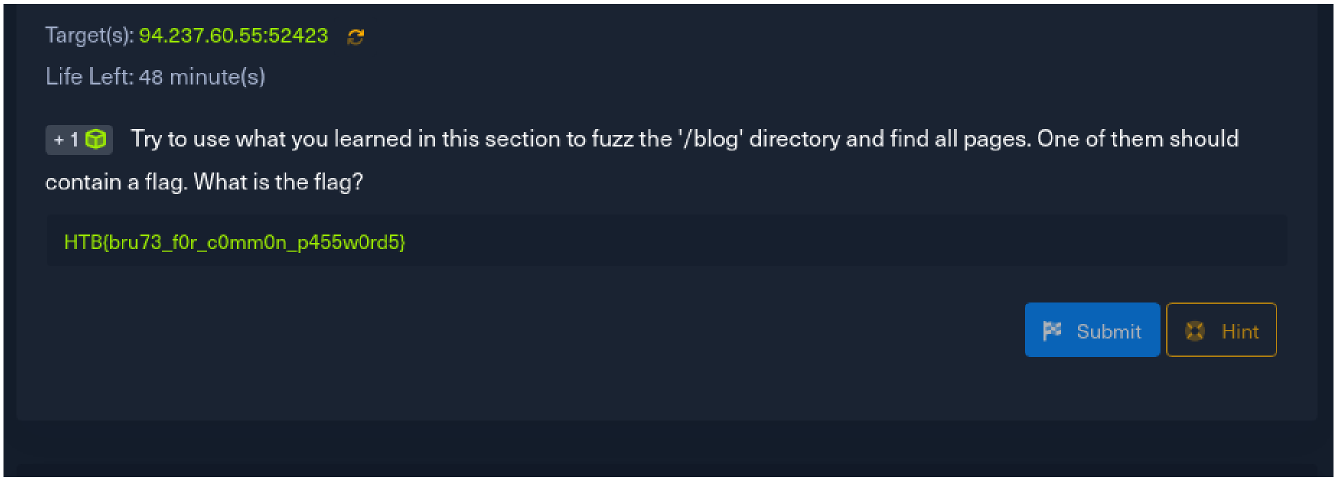
```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://94.237.60.55:52423/FUZZ

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://94.237.60.55:52423/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

# directory-list-2.3-small.txt [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 153ms]
#                       [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 154ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 153ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 154ms]
#                       [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 152ms]
forum                   [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 152ms]
# on at least 3 different hosts [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 674ms]
#                       [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 1677ms]
#                       [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3684ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3684ms]
# Priority-ordered case-sensitive list, where entries were found [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3685ms]
blog                    [Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 3685ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3687ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4690ms]
# Copyright 2007 James Fisher [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4690ms]
                        [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4698ms]
:: Progress: [2665/87664] :: Job [1/1] :: 262 req/sec :: Duration: [0:00:13] :: Errors: 0 ::
```

This is the command I used

Page fuzzing

Questions

1.

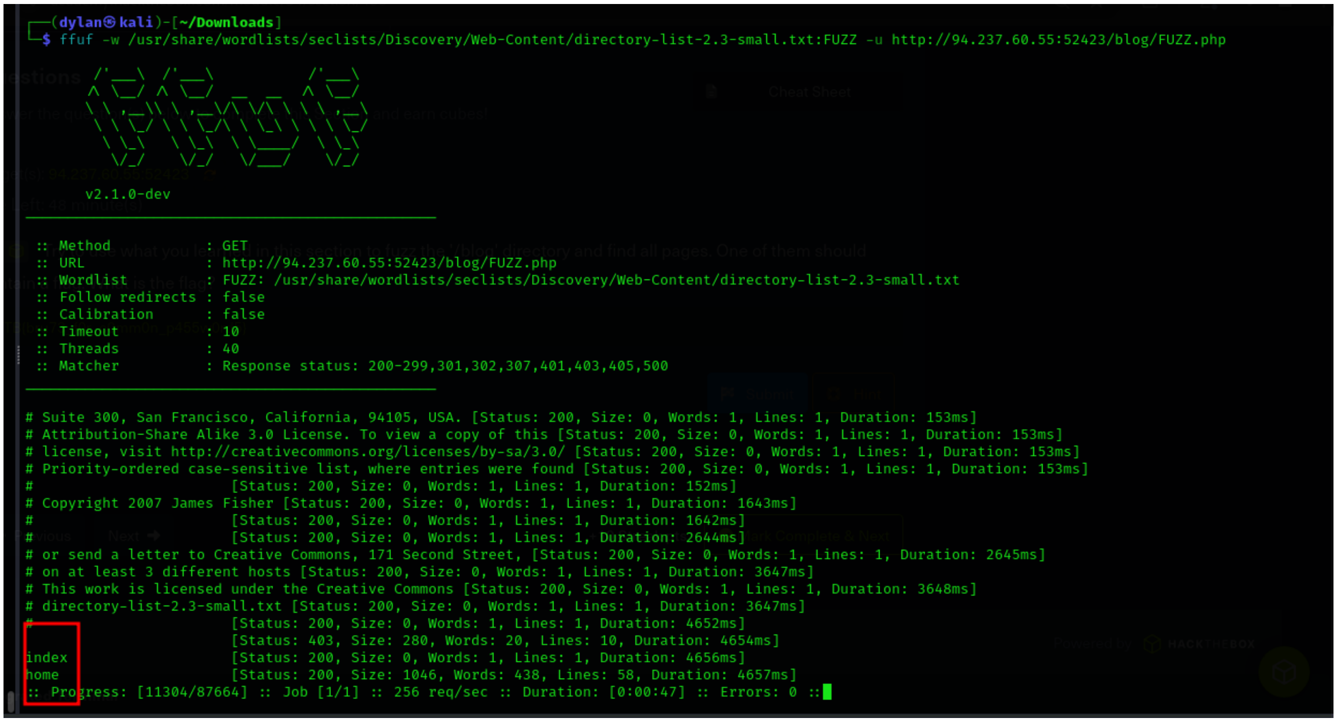


Target(s): 94.237.60.55:52423

Life Left: 48 minute(s)

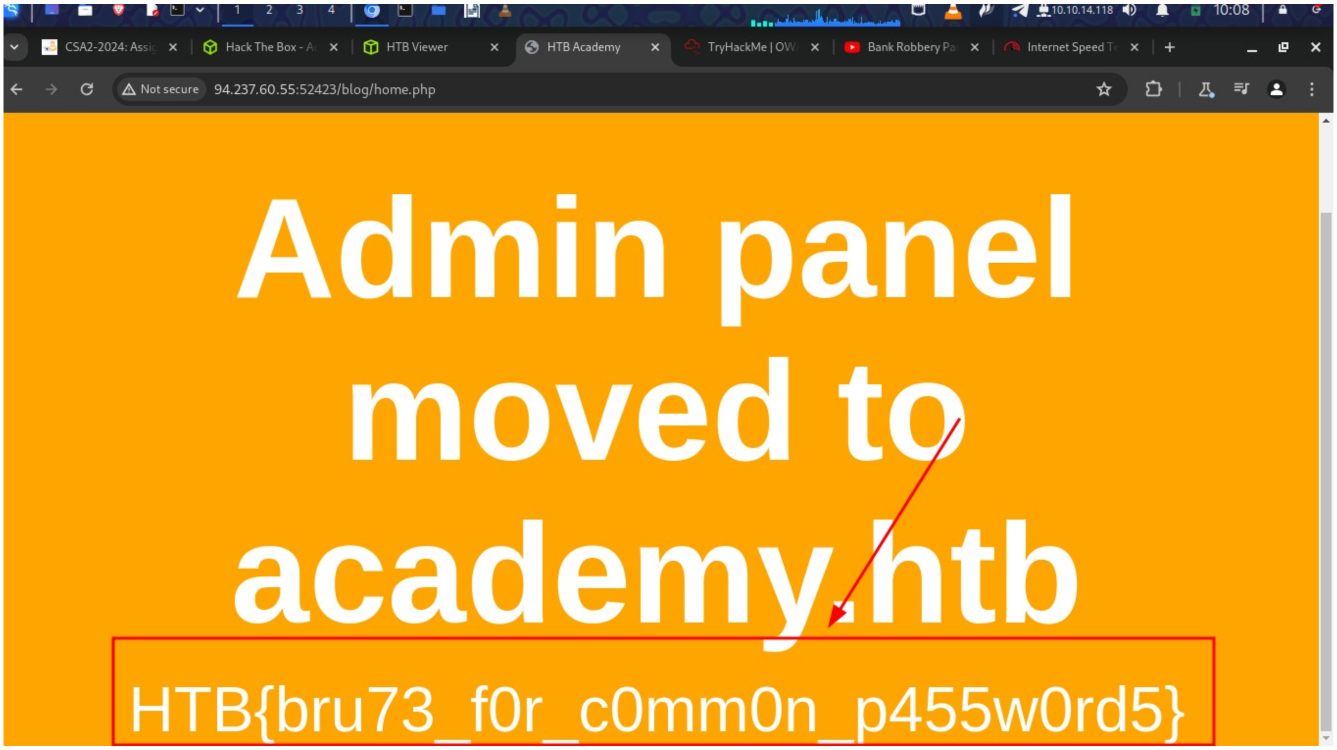
+1 Try to use what you learned in this section to fuzz the '/blog' directory and find all pages. One of them should contain a flag. What is the flag?

HTB{bru73_f0r_c0mm0n_p455w0rd5}



```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://94.237.60.55:52423/blog/FUZZ.php

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://94.237.60.55:52423/blog/FUZZ.php
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 153ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 153ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 153ms]
# Priority-ordered case-sensitive list, where entries were found [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 153ms]
#                       [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 152ms]
# Copyright 2007 James Fisher [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 1643ms]
#                       [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 1642ms]
#                       [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 2644ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 2645ms]
# on at least 3 different hosts [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 3647ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 3648ms]
# directory-list-2.3-small.txt [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 3647ms]
#                       [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4652ms]
                        [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 4654ms]
index                   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4656ms]
home                    [Status: 200, Size: 1046, Words: 438, Lines: 58, Duration: 4657ms]
:: Progress: [11304/87664] :: Job [1/1] :: 256 req/sec :: Duration: [0:00:47] :: Errors: 0 ::
```

- **I** was able to get the two, Index.php was blank and I decided to use home.php where I was able to get the flag.



Admin panel moved to academy.htb

HTB{bru73_f0r_c0mm0n_p455w0rd5}

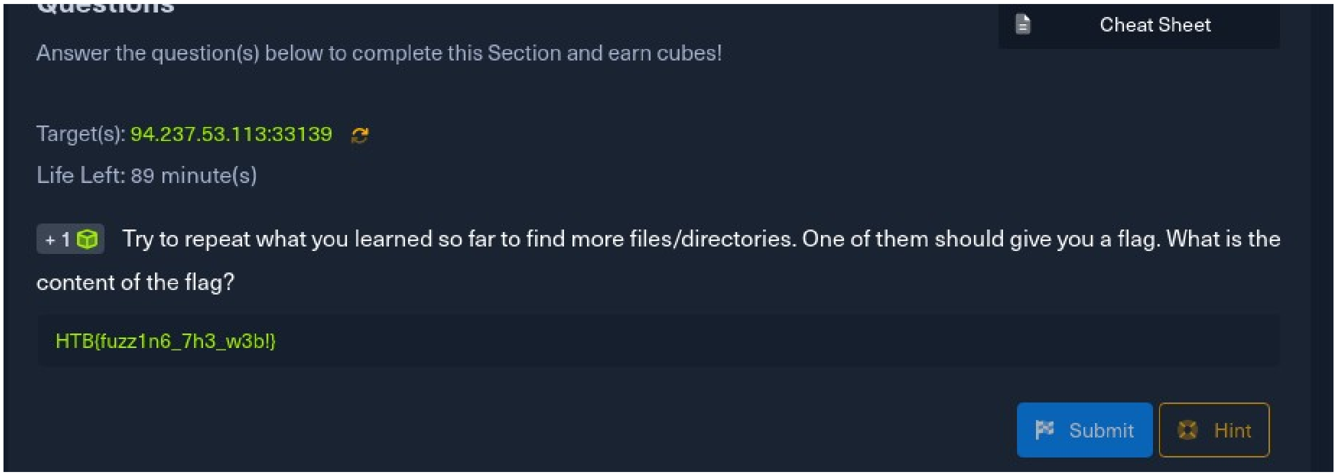
-

Recursive Fuzzing

- This helps us when we are dealing with dozens of subdirectories with each having files
- If We specify the recursion-depth it will only ffuf the directory and their sub-directories

Questions

1\.



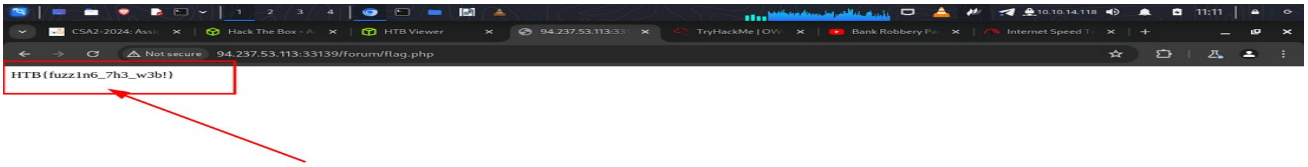
Answer the question(s) below to complete this Section and earn cubes!

Target(s): 94.237.53.113:33139

Life Left: 89 minute(s)

+ 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?

HTB{fuzz1n6_7h3_w3b!}



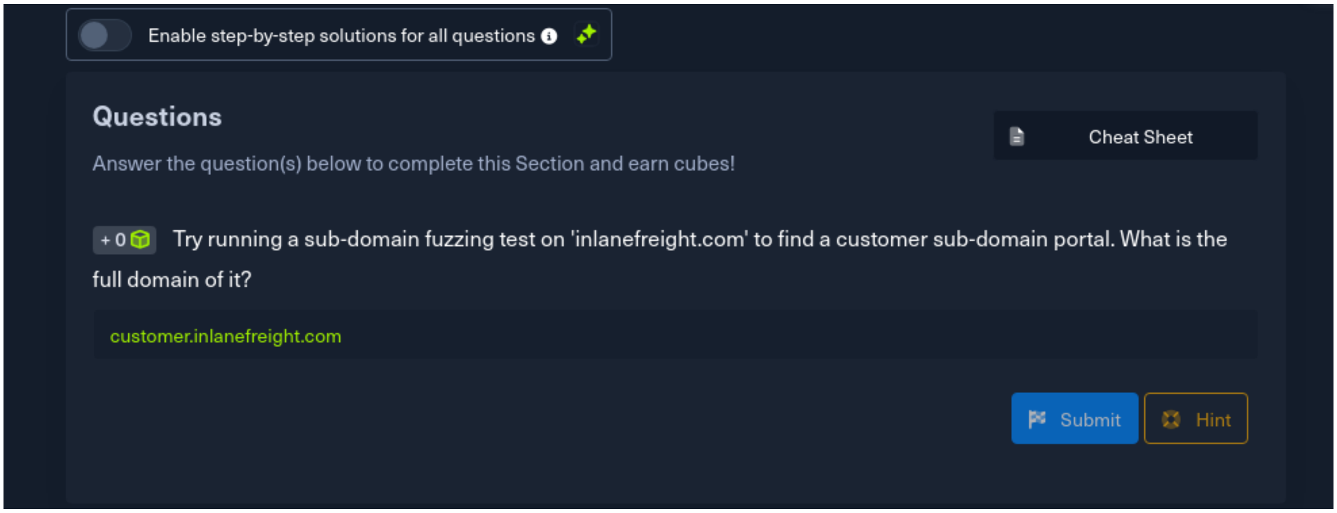
HTB{fuzz1n6_7h3_w3b!}

Sub-domain fuzzing

- A sub-domain is a website underlying another domain

Questions

1.



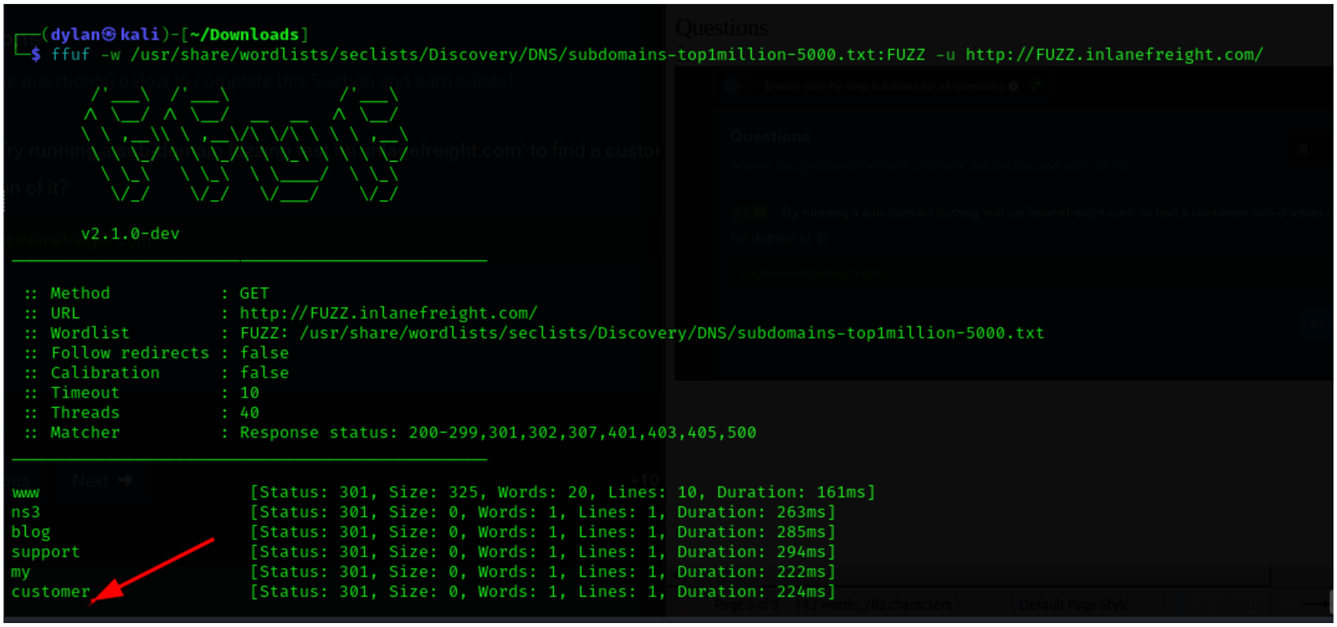
Enable step-by-step solutions for all questions

Questions

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

+0 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

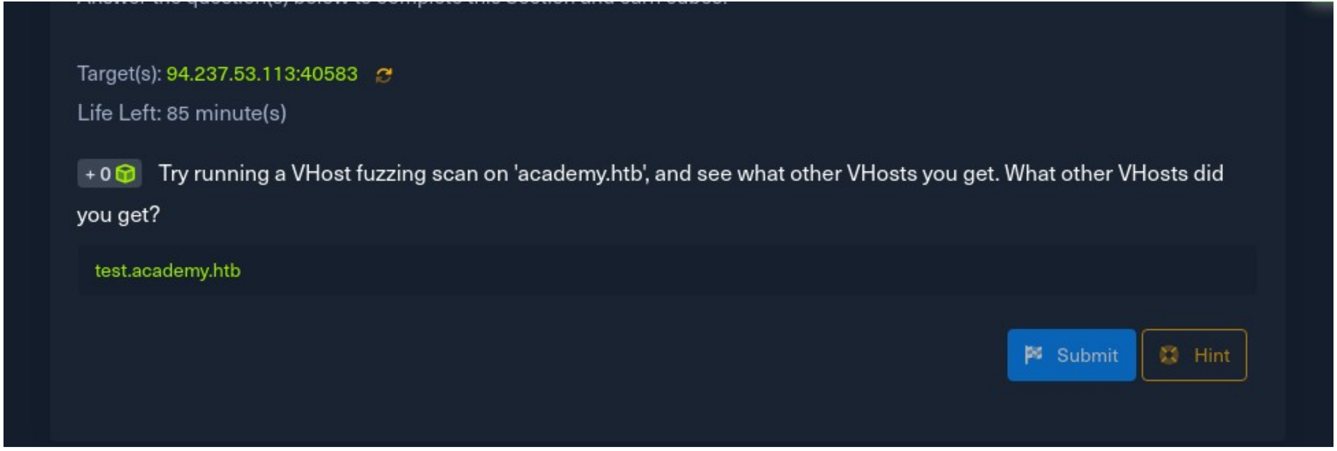


```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://FUZZ.inlanefreight.com/

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://FUZZ.inlanefreight.com/
 :: Wordlist         : FUZZ: /usr/share/wordlists/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: 301, Size: 325, Words: 20, Lines: 10, Duration: 161ms]
ns3                     [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 263ms]
blog                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 285ms]
support                 [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 294ms]
my                      [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 222ms]
customer                [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 224ms]
```

Vhost fuzzing

- Vhost is a sub-domain served from the same server and has the same IP such as a single IP could be serving.
- Vhost fuzzing will identify both public and non-public subdomains and Vhosts

Questions



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

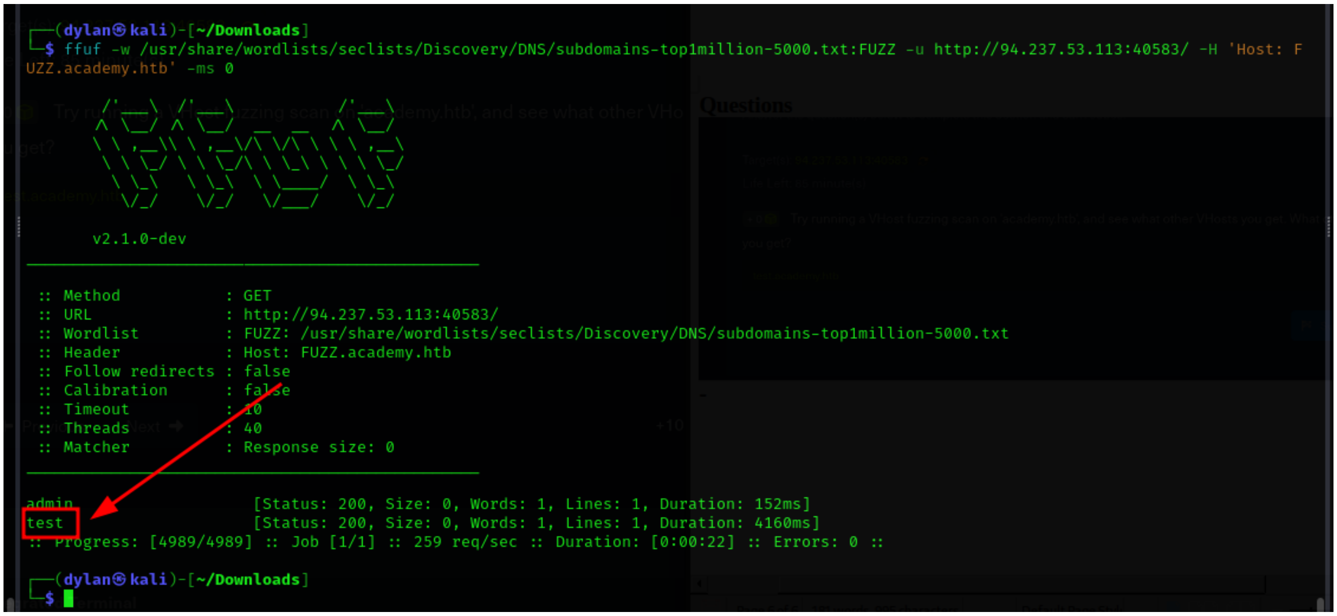
Target(s): 94.237.53.113:40583

Life Left: 85 minute(s)

+0 Try running a VHost fuzzing scan on 'academy.htb', and see what other VHosts you get. What other VHosts did you get?

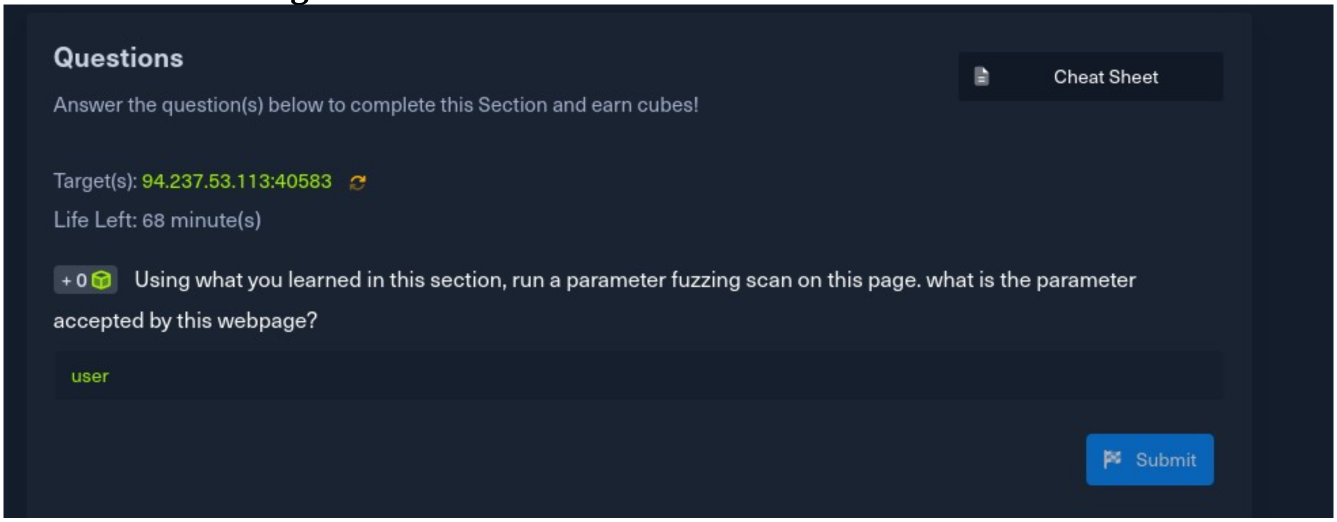
test.academy.htb

-



```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://94.237.53.113:40583/ -H 'Host: F
UZZ.academy.htb' -ms 0

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://94.237.53.113:40583/
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.academy.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response size: 0
________________________________________________

admin                   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 152ms]
test                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4160ms]
:: Progress: [4989/4989] :: Job [1/1] :: 259 req/sec :: Duration: [0:00:22] :: Errors: 0 ::

┌──(dylan㉿kali)-[~/Downloads]
└─$
```

Parameter Fuzzing – Get



Questions

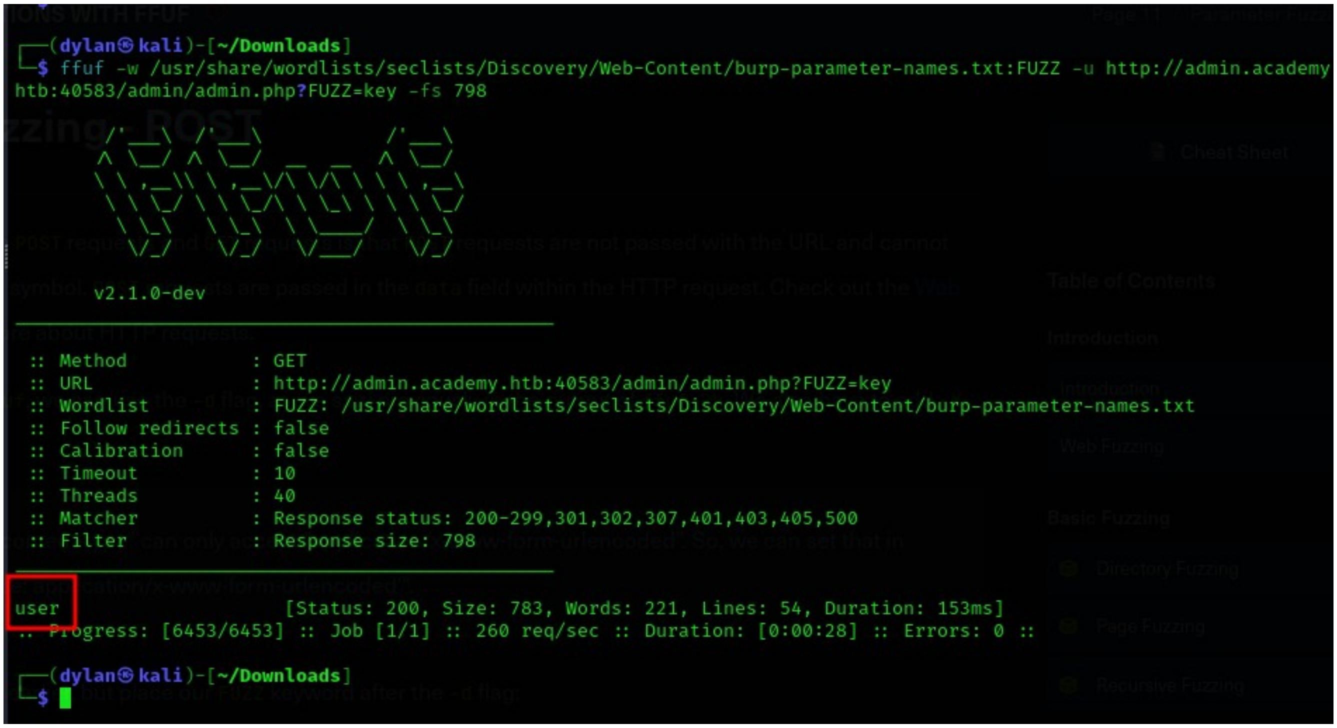
Answer the question(s) below to complete this Section and earn cubes!

Target(s): 94.237.53.113:40583

Life Left: 68 minute(s)

+0 Using what you learned in this section, run a parameter fuzzing scan on this page. what is the parameter accepted by this webpage?

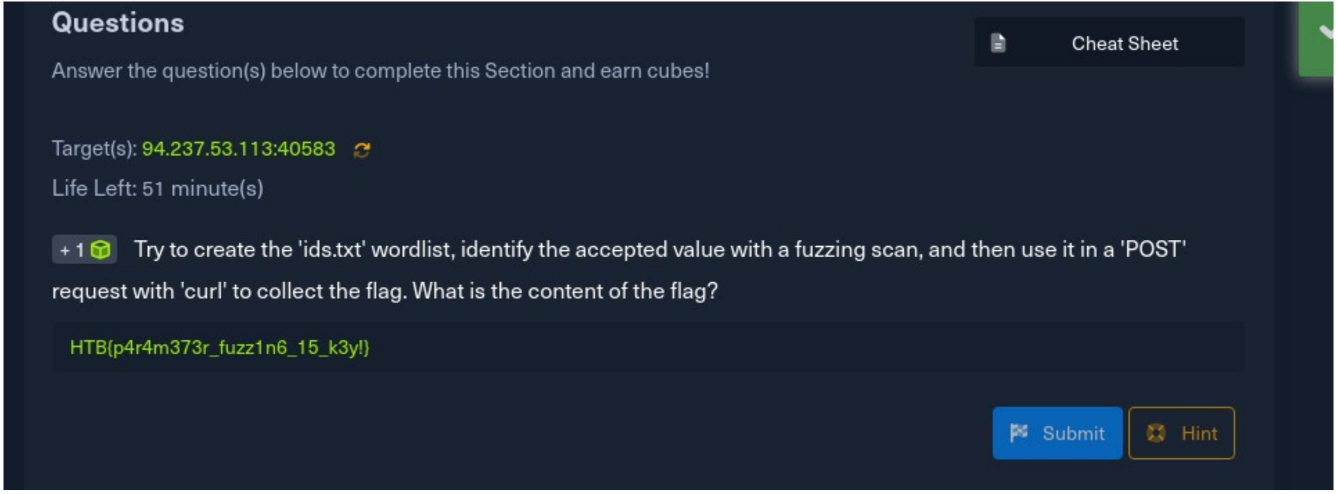
user



```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://admin.academy.
htb:40583/admin/admin.php?FUZZ=key -fs 798

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://admin.academy.htb:40583/admin/admin.php?FUZZ=key
 :: Wordlist         : FUZZ: /usr/share/wordlists/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 size: 798
________________________________________________

user                    [Status: 200, Size: 783, Words: 221, Lines: 54, Duration: 153ms]
:: Progress: [6453/6453] :: Job [1/1] :: 260 req/sec :: Duration: [0:00:28] :: Errors: 0 ::

┌──(dylan㉿kali)-[~/Downloads]
└─$ 
```

Value Fuzzing

Questions



Questions

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

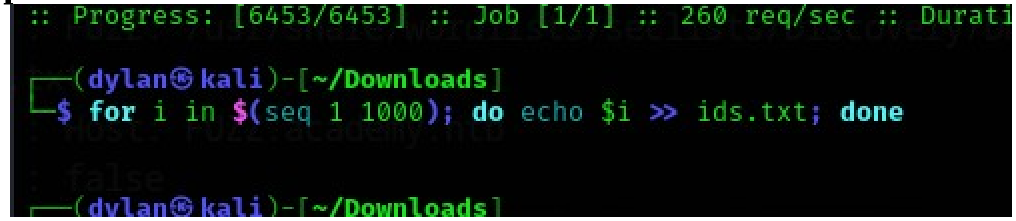
Target(s): 94.237.53.113:40583

Life Left: 51 minute(s)

+1 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!}

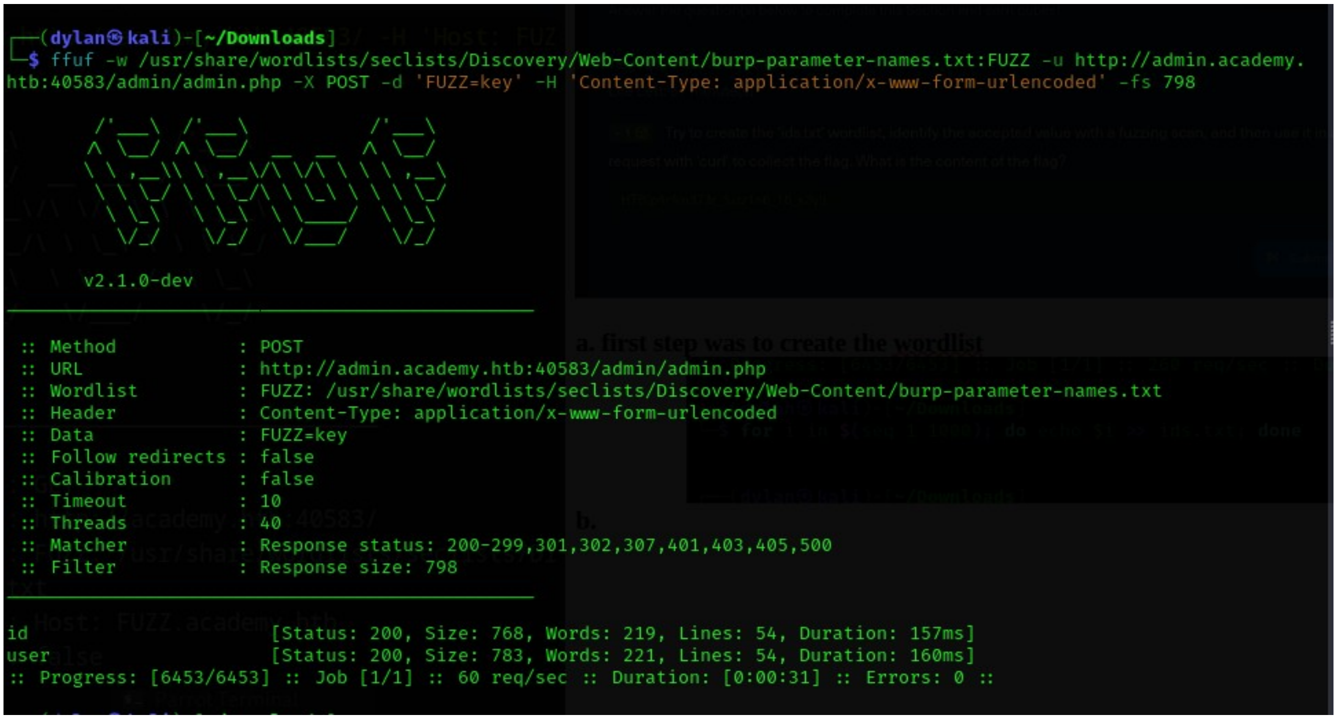
a. first step was to create the wordlists



```
 :: Progress: [6453/6453] :: Job [1/1] :: 260 req/sec :: Durati

┌──(dylan㉿kali)-[~/Downloads]
└─$ for i in $(seq 1 1000); do echo $i >> ids.txt; done

┌──(dylan㉿kali)-[~/Downloads]
```

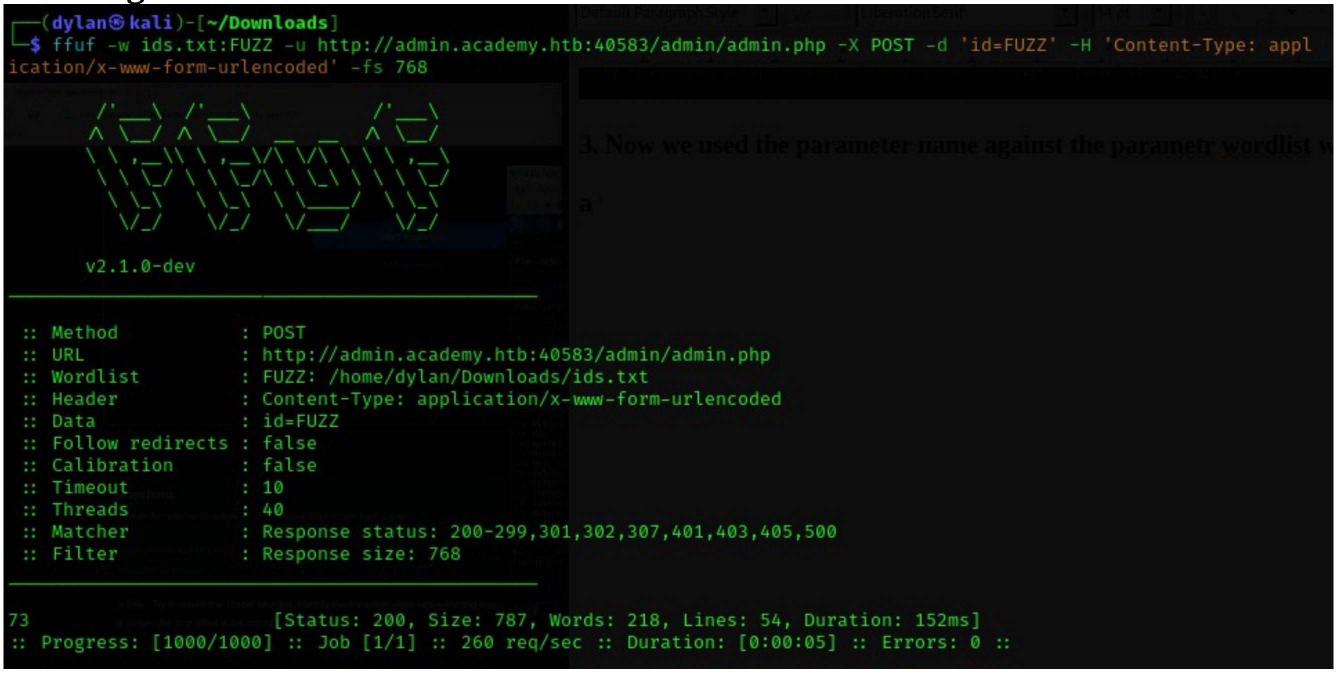
b.

We then run ffuf to identify the parameter name



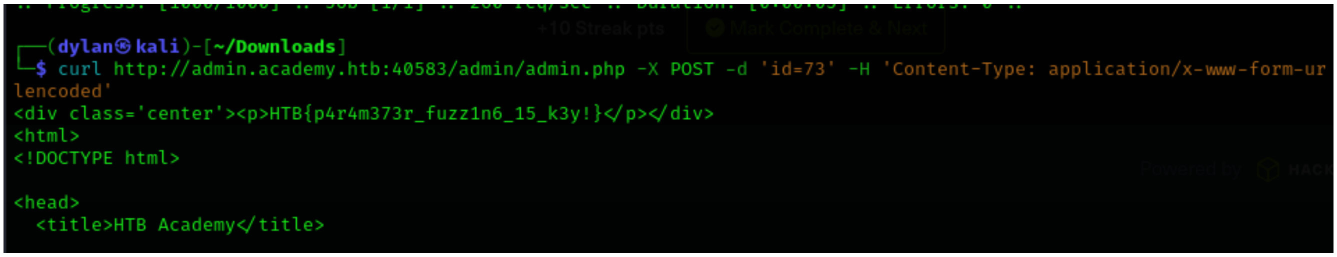
```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://admin.academy.htb:40583/admin/admin.php -X POST -d 'FUZZ=key' -H 'Content-Type: application/x-www-form-urlencoded' -fs 798

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

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://admin.academy.htb:40583/admin/admin.php
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/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: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 798
________________________________________________

id                      [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 157ms]
user                    [Status: 200, Size: 783, Words: 221, Lines: 54, Duration: 160ms]
:: Progress: [6453/6453] :: Job [1/1] :: 60 req/sec :: Duration: [0:00:31] :: Errors: 0 ::
```

c. Now we used the parameter name against the parameter wordlists we created and we got id number as 73



```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:40583/admin/admin.php -X POST -d 'id=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 768

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

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://admin.academy.htb:40583/admin/admin.php
 :: Wordlist         : FUZZ: /home/dylan/Downloads/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: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 768
________________________________________________

73                      [Status: 200, Size: 787, Words: 218, Lines: 54, Duration: 152ms]
:: Progress: [1000/1000] :: Job [1/1] :: 260 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

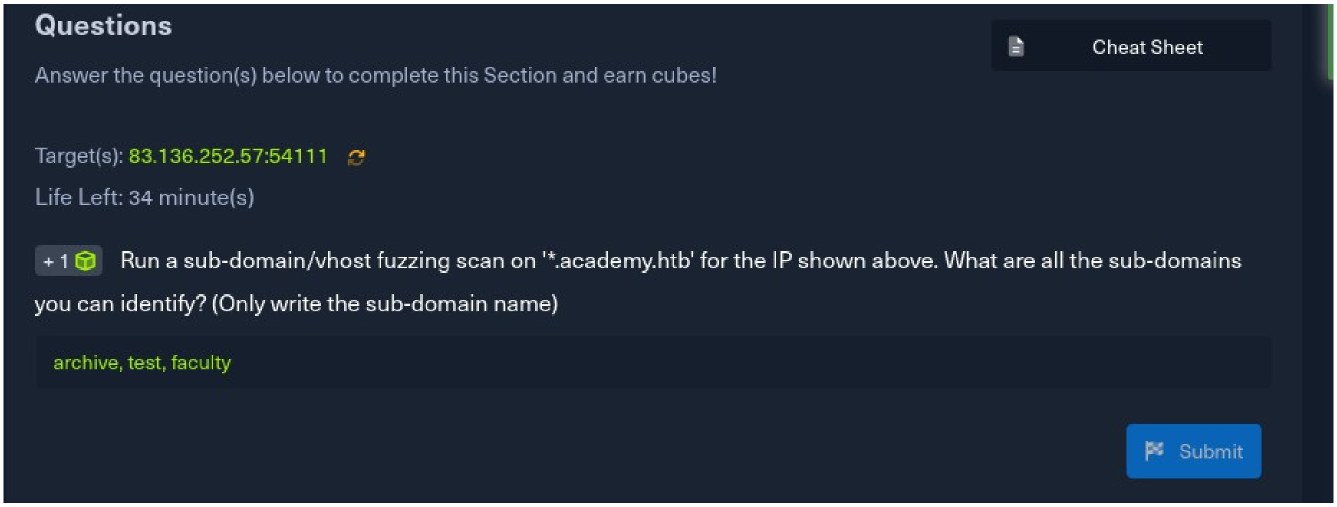
d.
We used curl to get the flag



```
┌──(dylan㉿kali)-[~/Downloads]
└─$ curl http://admin.academy.htb:40583/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>
```

Skill Assessment – Web Fuzzing

1.



Questions

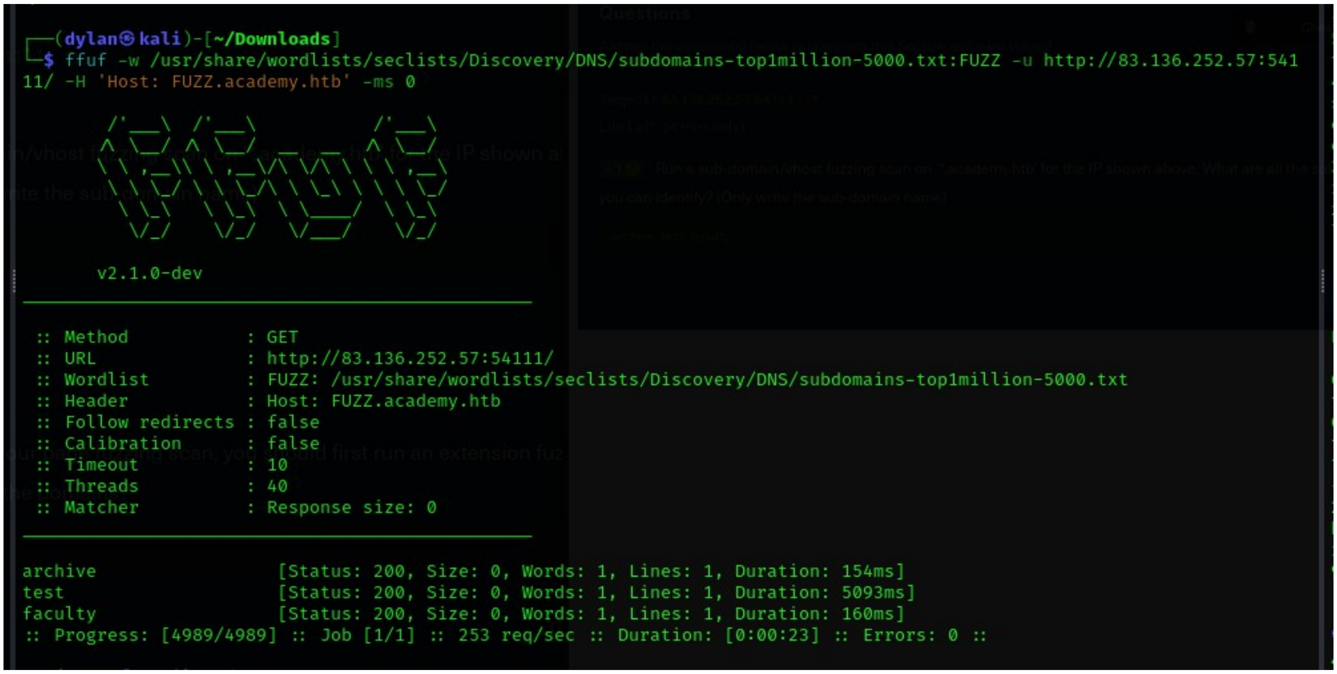
Answer the question(s) below to complete this Section and earn cubes!

Target(s): 83.136.252.57:54111

Life Left: 34 minute(s)

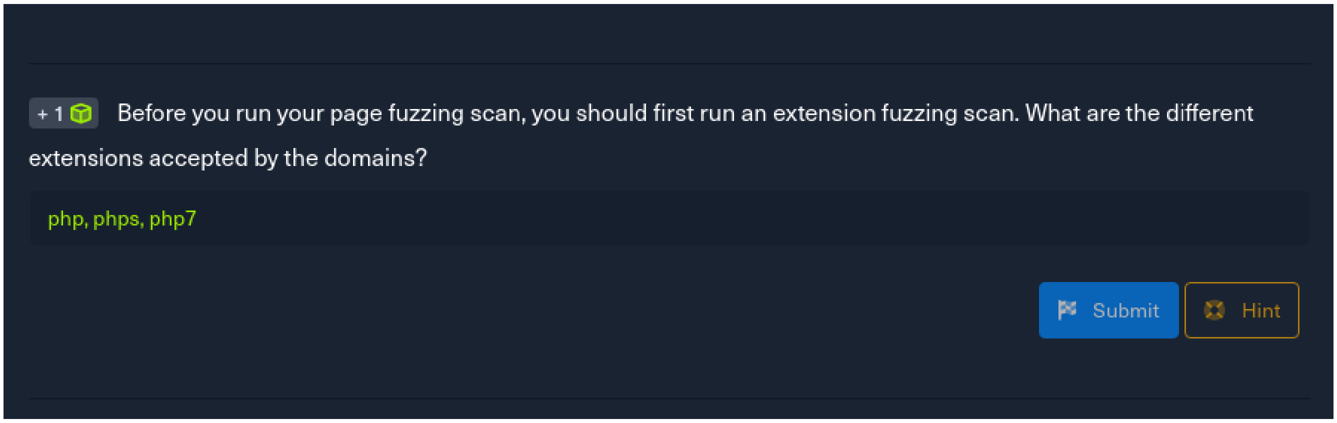
+ 1 Run a sub-domain/vhost fuzzing scan on '*.academy.htb' for the IP shown above. What are all the sub-domains you can identify? (Only write the sub-domain name)

archive, test, faculty



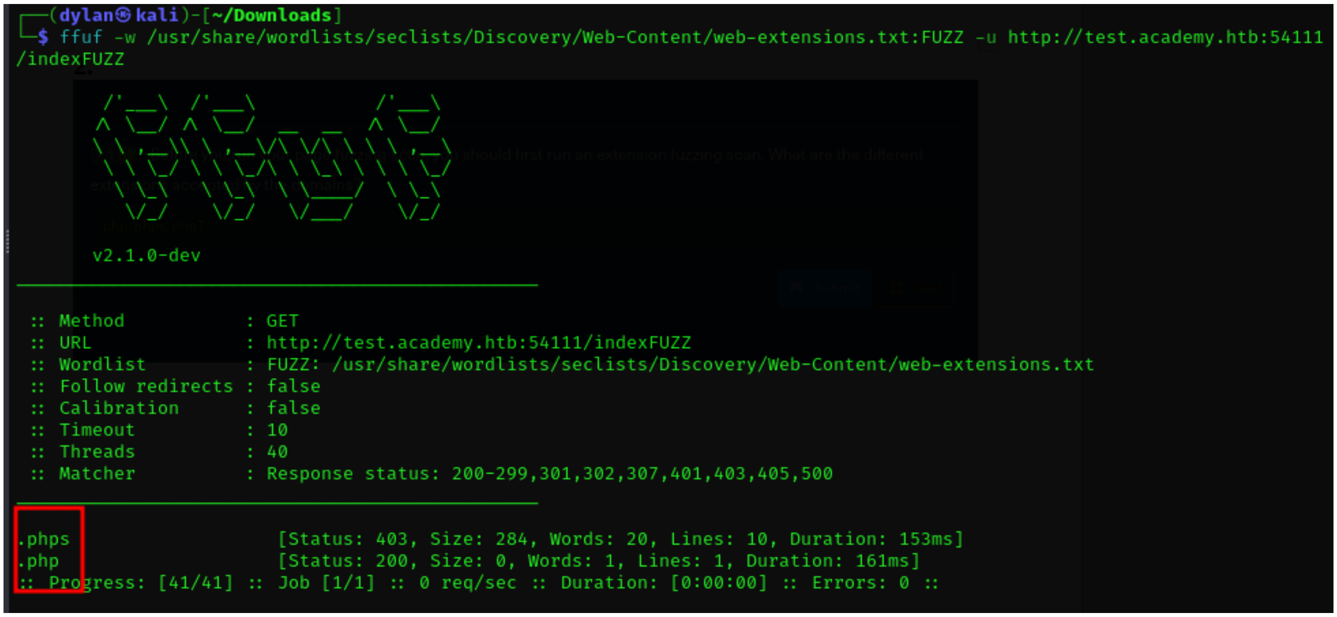
```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://83.136.252.57:54111/ -H 'Host: FUZZ.academy.htb' -ms 0

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://83.136.252.57:54111/
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.academy.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response size: 0
________________________________________________

archive                 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 154ms]
test                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 5093ms]
faculty                 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 160ms]
:: Progress: [4989/4989] :: Job [1/1] :: 253 req/sec :: Duration: [0:00:23] :: Errors: 0 ::
```

2.

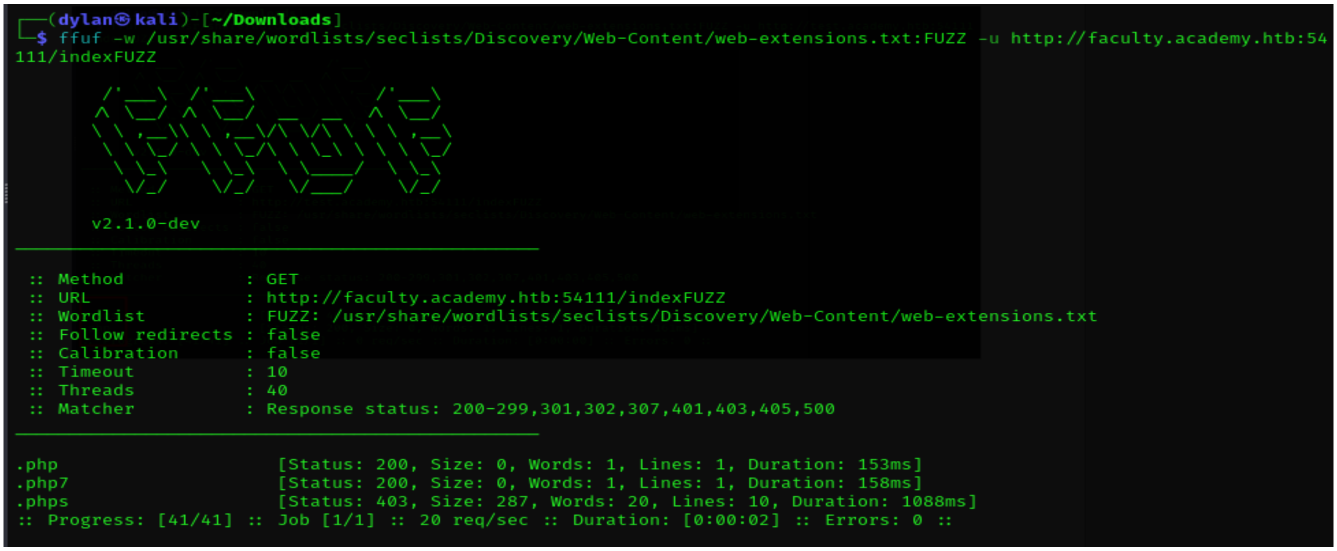


+1 Before you run your page fuzzing scan, you should first run an extension fuzzing scan. What are the different extensions accepted by the domains?

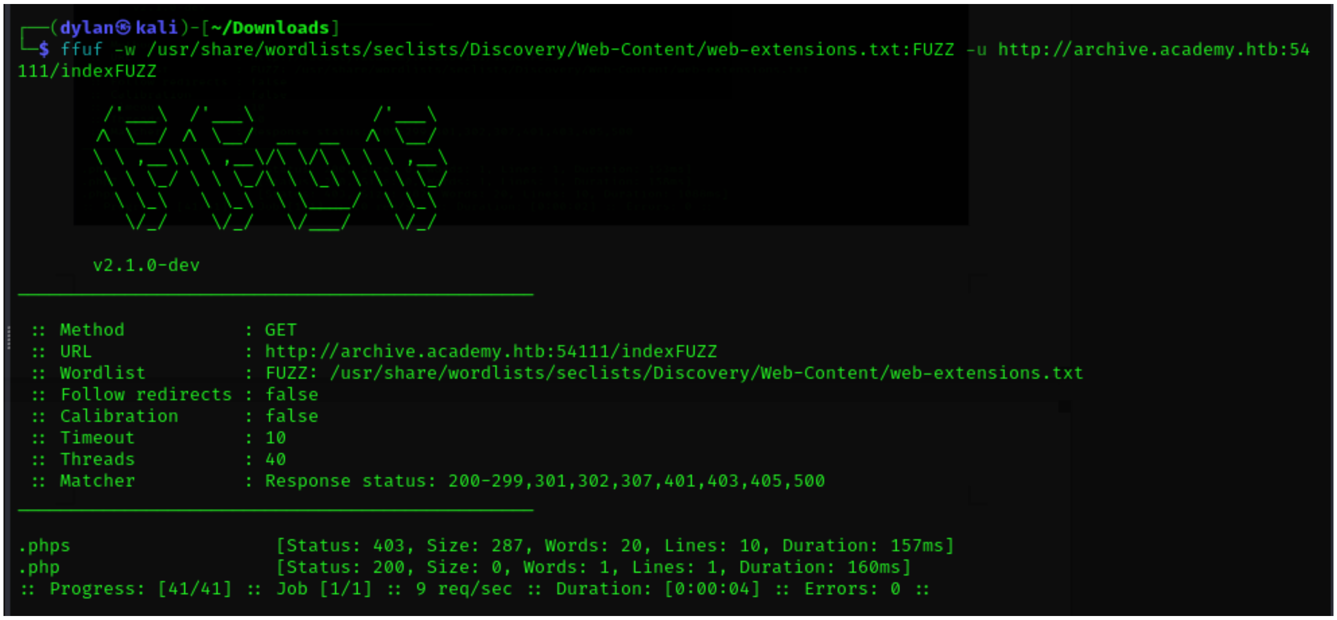
php, phps, php7



```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/web-extensions.txt:FUZZ -u http://test.academy.htb:54111
/indexFUZZ

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://test.academy.htb:54111/indexFUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/web-extensions.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.phps                   [Status: 403, Size: 284, Words: 20, Lines: 10, Duration: 153ms]
.php                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 161ms]
:: Progress: [41/41] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

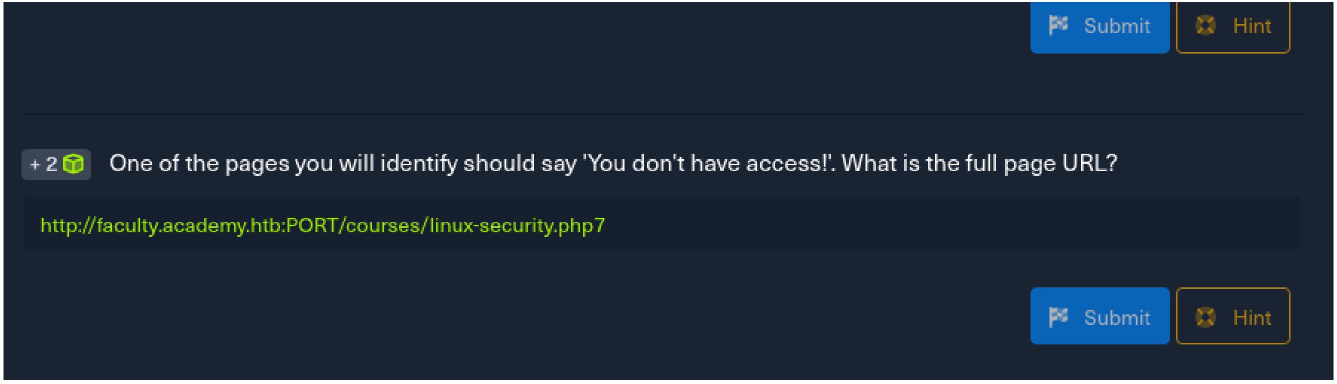


```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/web-extensions.txt:FUZZ -u http://faculty.academy.htb:54
111/indexFUZZ

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://faculty.academy.htb:54111/indexFUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/web-extensions.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.php                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 153ms]
.php7                   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 158ms]
.phps                   [Status: 403, Size: 287, Words: 20, Lines: 10, Duration: 1088ms]
:: Progress: [41/41] :: Job [1/1] :: 20 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
```



```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/web-extensions.txt:FUZZ -u http://archive.academy.htb:54
111/indexFUZZ

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://archive.academy.htb:54111/indexFUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/web-extensions.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.phps                   [Status: 403, Size: 287, Words: 20, Lines: 10, Duration: 157ms]
.php                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 160ms]
:: Progress: [41/41] :: Job [1/1] :: 9 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

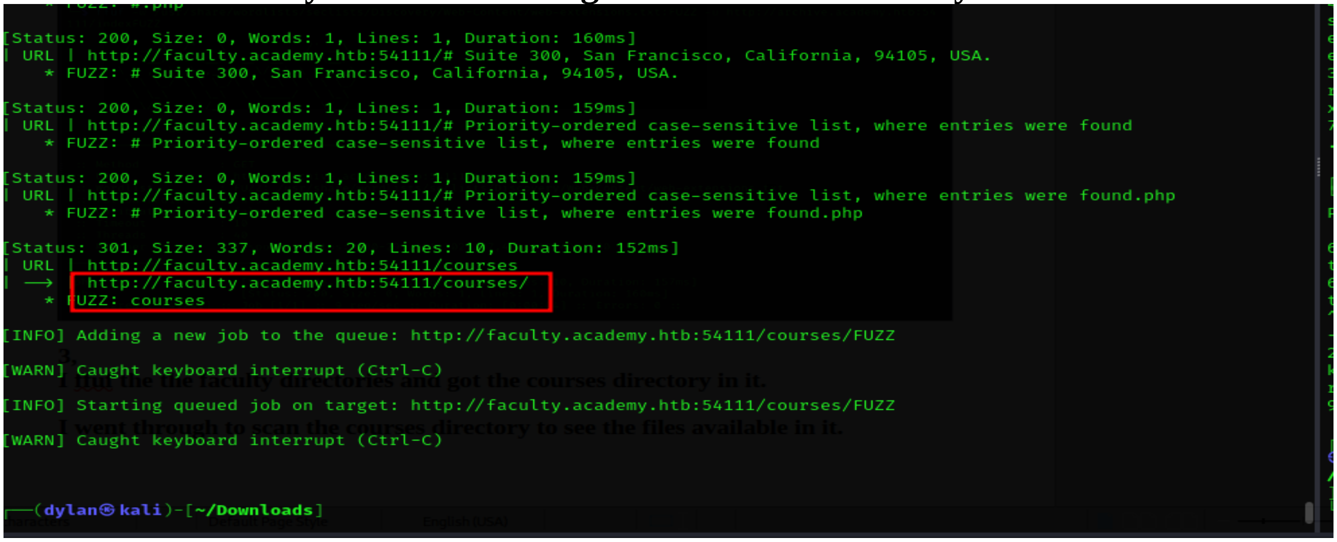
3,



+2 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

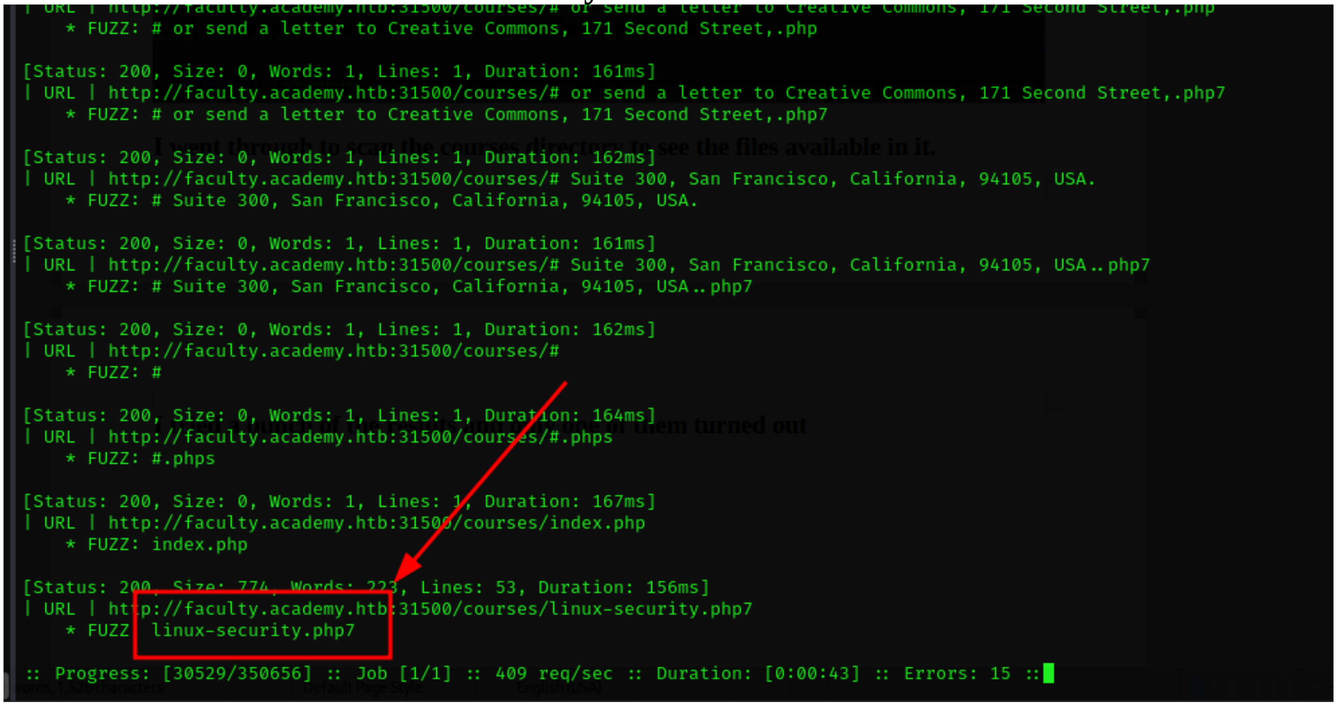
I ffuf the the faculty directories and got the courses directory in it.



```
    * FUZZ: #.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 160ms]
| URL | http://faculty.academy.htb:54111/# Suite 300, San Francisco, California, 94105, USA.
    * FUZZ: # Suite 300, San Francisco, California, 94105, USA.

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 159ms]
| URL | http://faculty.academy.htb:54111/# Priority-ordered case-sensitive list, where entries were found
    * FUZZ: # Priority-ordered case-sensitive list, where entries were found

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 159ms]
| URL | http://faculty.academy.htb:54111/# Priority-ordered case-sensitive list, where entries were found.php
    * FUZZ: # Priority-ordered case-sensitive list, where entries were found.php

[Status: 301, Size: 337, Words: 20, Lines: 10, Duration: 152ms]
| URL | http://faculty.academy.htb:54111/courses
| --> | http://faculty.academy.htb:54111/courses/
    * FUZZ: courses

[INFO] Adding a new job to the queue: http://faculty.academy.htb:54111/courses/FUZZ

[WARN] Caught keyboard interrupt (Ctrl-C)

[INFO] Starting queued job on target: http://faculty.academy.htb:54111/courses/FUZZ

[WARN] Caught keyboard interrupt (Ctrl-C)


┌──(dylan㉿kali)-[~/Downloads]
```

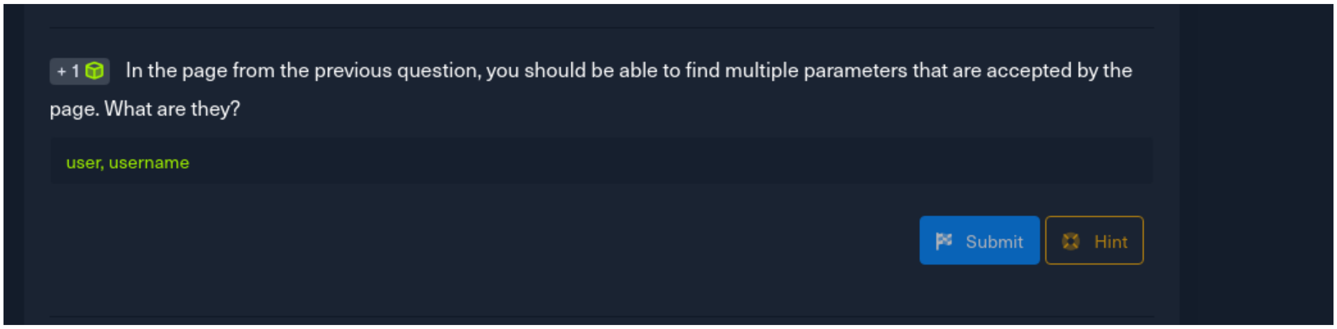
I went through to scan the courses directory to see the files available in it.

I tried a bunch of the results and only one of them turned out



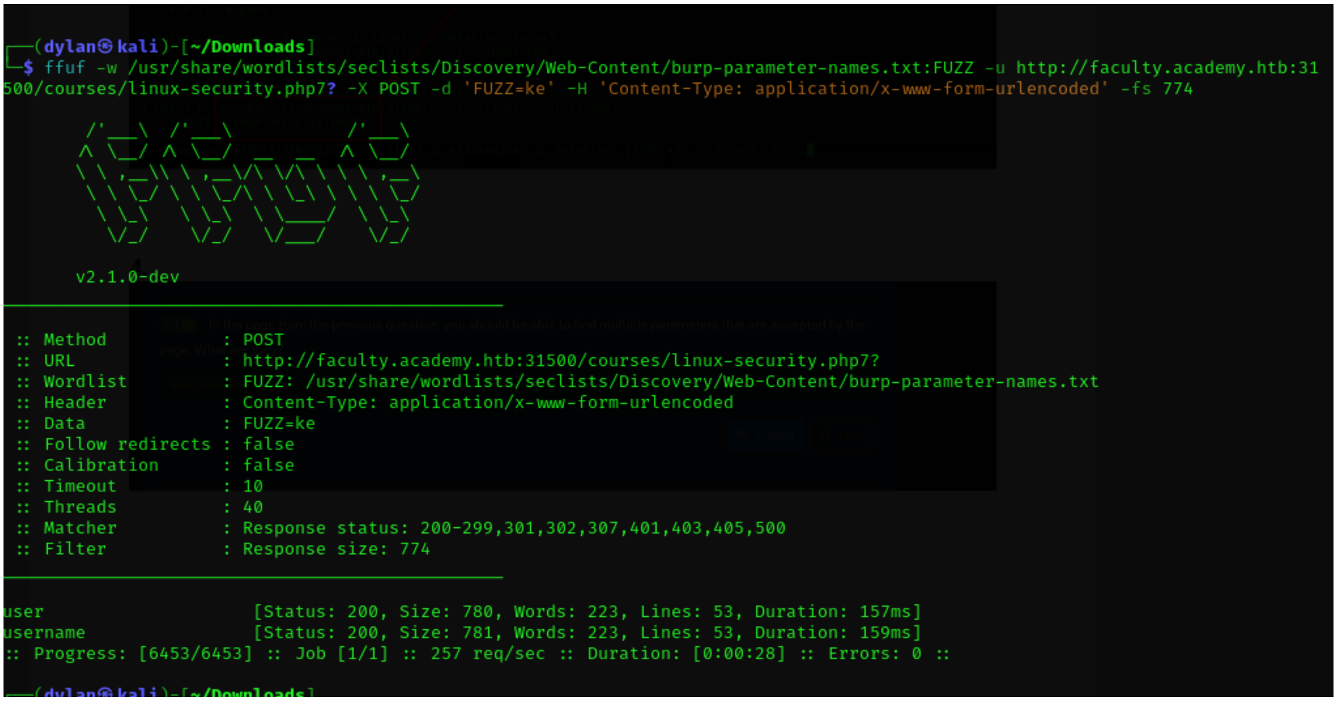
```
| URL | http://faculty.academy.htb:31500/courses/# or send a letter to Creative Commons, 171 Second Street,.php
    * FUZZ: # or send a letter to Creative Commons, 171 Second Street,.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 161ms]
| URL | http://faculty.academy.htb:31500/courses/# or send a letter to Creative Commons, 171 Second Street,.php7
    * FUZZ: # or send a letter to Creative Commons, 171 Second Street,.php7

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 162ms]
| URL | http://faculty.academy.htb:31500/courses/# Suite 300, San Francisco, California, 94105, USA.
    * FUZZ: # Suite 300, San Francisco, California, 94105, USA.

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 161ms]
| URL | http://faculty.academy.htb:31500/courses/# Suite 300, San Francisco, California, 94105, USA..php7
    * FUZZ: # Suite 300, San Francisco, California, 94105, USA..php7

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 162ms]
| URL | http://faculty.academy.htb:31500/courses/#
    * FUZZ: #

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 164ms]
| URL | http://faculty.academy.htb:31500/courses/#.phps
    * FUZZ: #.phps

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 167ms]
| URL | http://faculty.academy.htb:31500/courses/index.php
    * FUZZ: index.php

[Status: 200, Size: 774, Words: 223, Lines: 53, Duration: 156ms]
| URL | http://faculty.academy.htb:31500/courses/linux-security.php7
    * FUZZ: linux-security.php7

:: Progress: [30529/350656] :: Job [1/1] :: 409 req/sec :: Duration: [0:00:43] :: Errors: 15 ::
```

4.



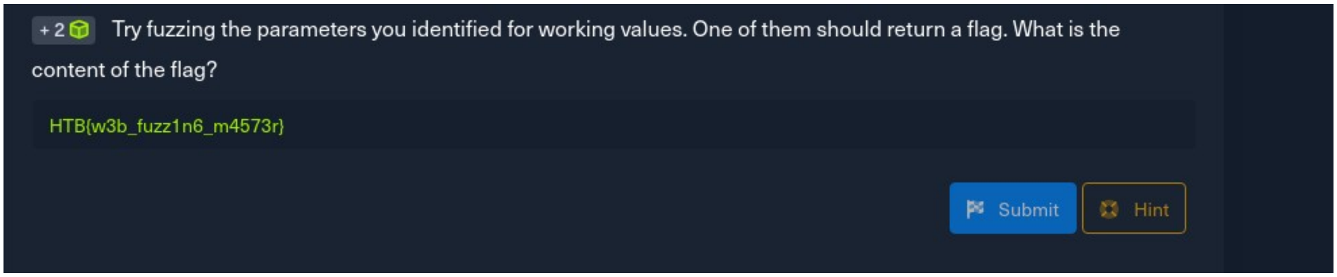
+1 In the page from the previous question, you should be able to find multiple parameters that are accepted by the page. What are they?

user, username



```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://faculty.academy.htb:31
500/courses/linux-security.php7? -X POST -d 'FUZZ=ke' -H 'Content-Type: application/x-www-form-urlencoded' -fs 774

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

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://faculty.academy.htb:31500/courses/linux-security.php7?
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/burp-parameter-names.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : FUZZ=ke
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 774
________________________________________________

user                    [Status: 200, Size: 780, Words: 223, Lines: 53, Duration: 157ms]
username                [Status: 200, Size: 781, Words: 223, Lines: 53, Duration: 159ms]
:: Progress: [6453/6453] :: Job [1/1] :: 257 req/sec :: Duration: [0:00:28] :: Errors: 0 ::

┌──(dylan㉿kali)-[~/Downloads]
```

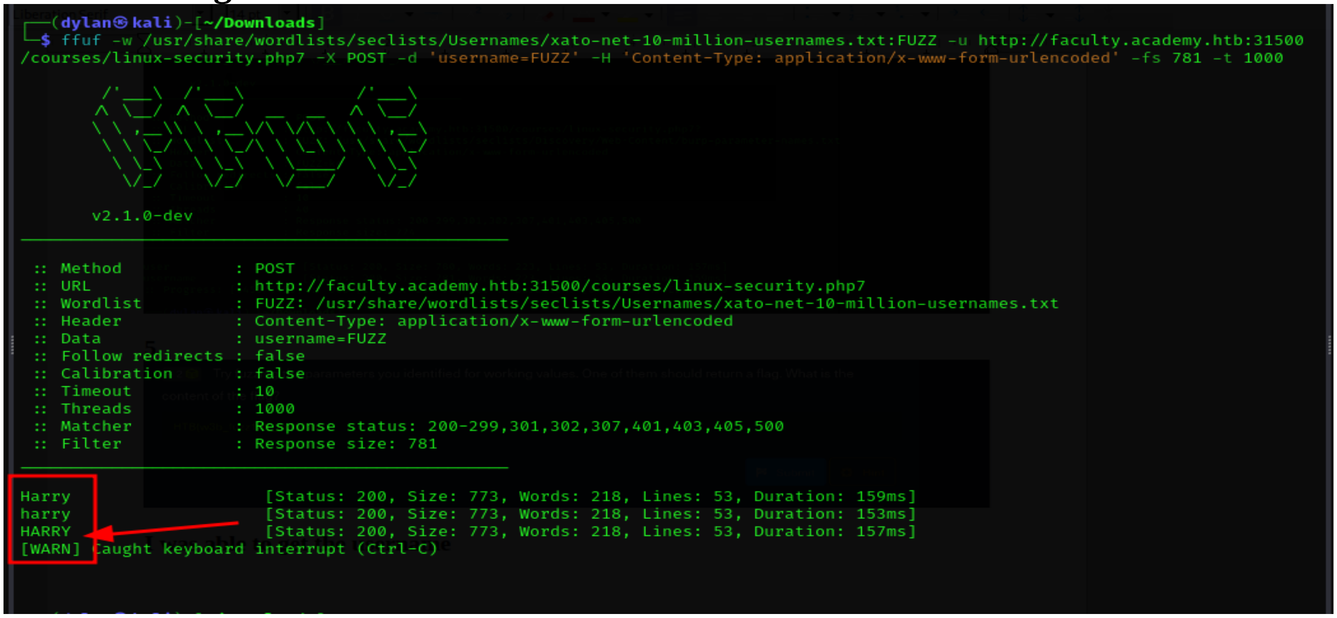
5.



+2 Try fuzzing the parameters you identified for working values. One of them should return a flag. What is the content of the flag?

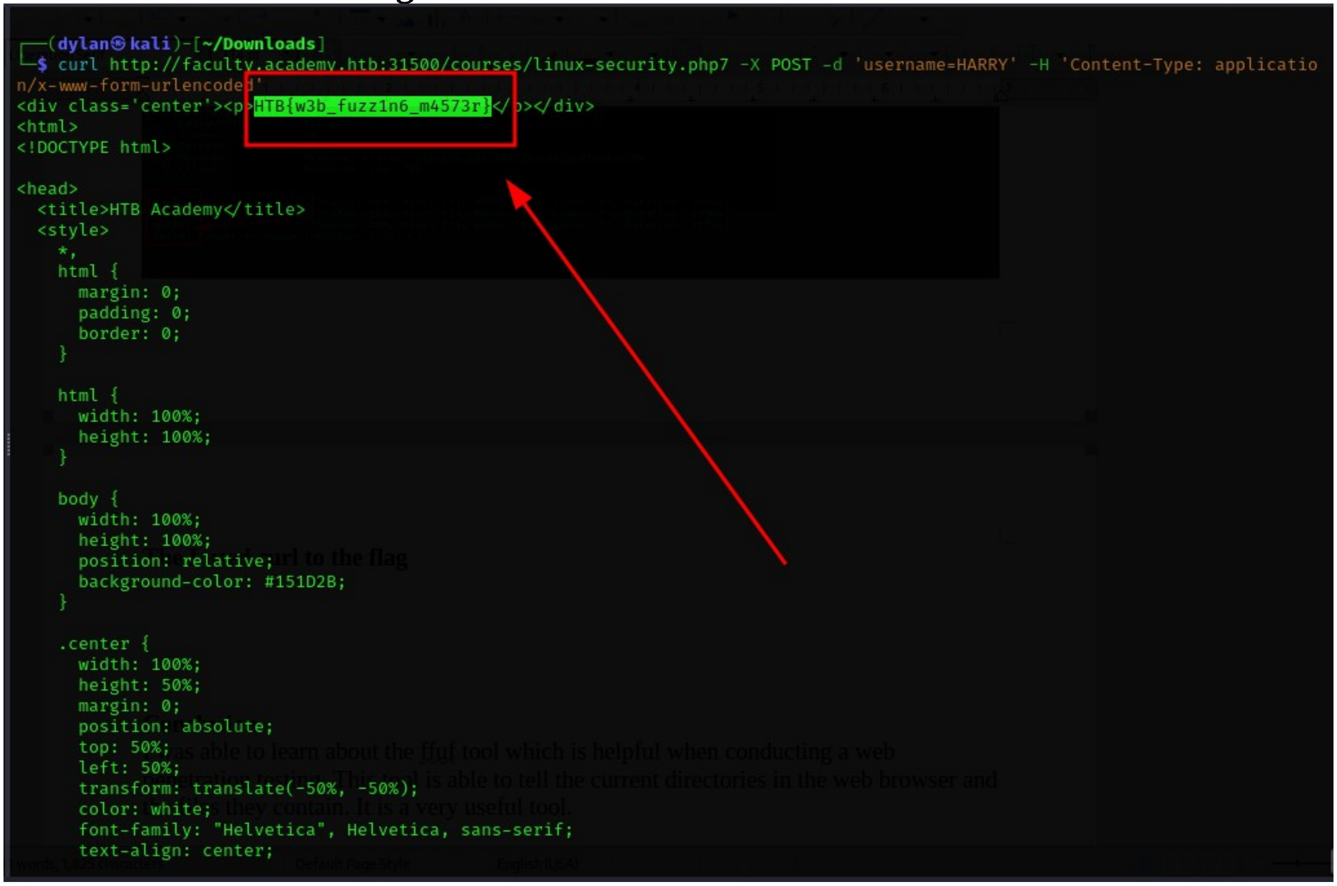
HTB{w3b_fuzz1n6_m4573r}

I was able to get the username

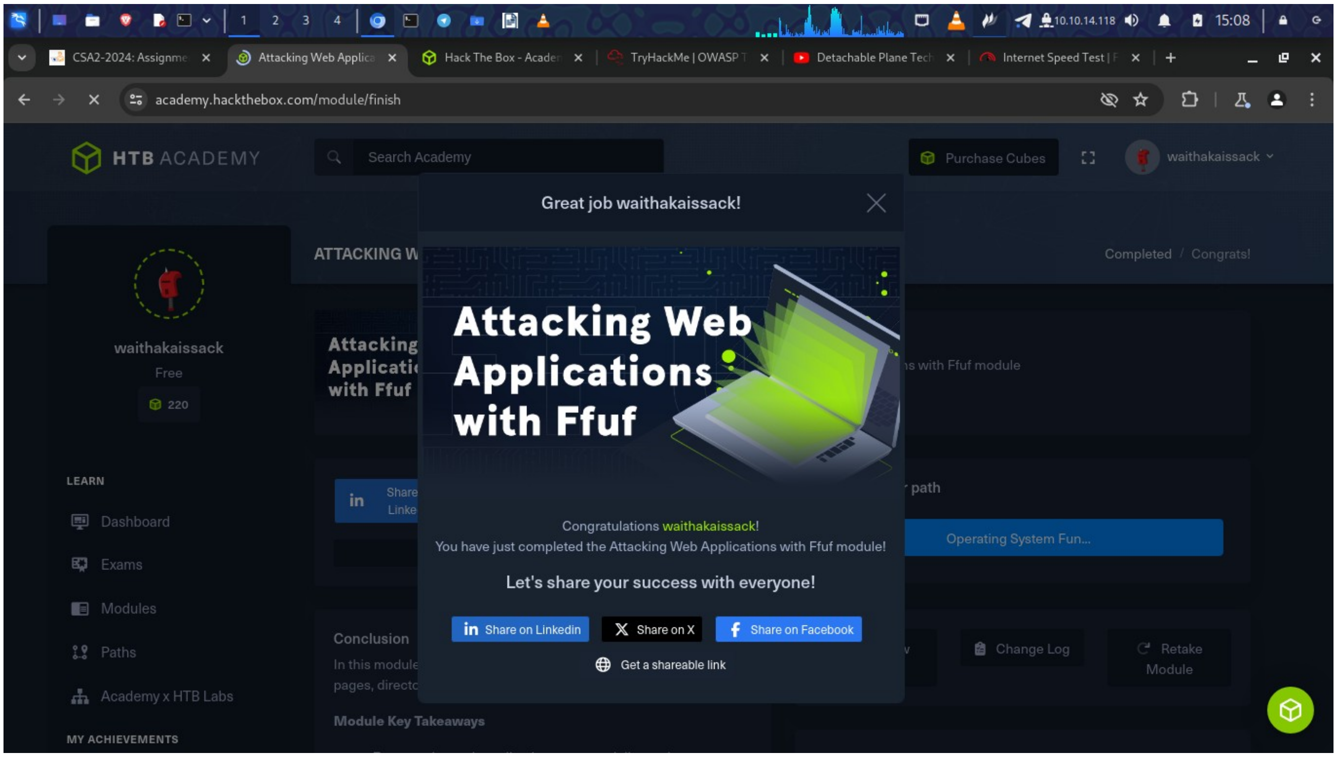


```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ffuf -w /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt:FUZZ -u http://faculty.academy.htb:31500
/courses/linux-security.php7 -X POST -d 'username=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 781 -t 1000

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

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://faculty.academy.htb:31500/courses/linux-security.php7
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : username=FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 1000
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 781
________________________________________________

Harry                   [Status: 200, Size: 773, Words: 218, Lines: 53, Duration: 159ms]
harry                   [Status: 200, Size: 773, Words: 218, Lines: 53, Duration: 153ms]
HARRY                   [Status: 200, Size: 773, Words: 218, Lines: 53, Duration: 157ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

The I used curl to the flag



```
┌──(dylan㉿kali)-[~/Downloads]
└─$ curl http://faculty.academy.htb:31500/courses/linux-security.php7 -X POST -d 'username=HARRY' -H 'Content-Type: applicatio
n/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;
```



Great job waithakaissack!

Congratulations waithakaissack!
You have just completed the Attacking Web Applications with Ffuf module!

Let's share your success with everyone!

https://academy.hackthebox.com/achievement/798750/54

Conclusion

I was able to learn about the ffuf tool which is helpful when conducting a web penetration testing. This tool is able to tell the current directories in the web browser and the files they contain. It is a very useful tool.