

ATTACKING WEB APPLICATIONS WITH FFUF

ASSIGNMENT REPORT



**Peter Kinyumu,
cs-sa07-24067,
June 23rd, 2024.**

1. INTRODUCTION

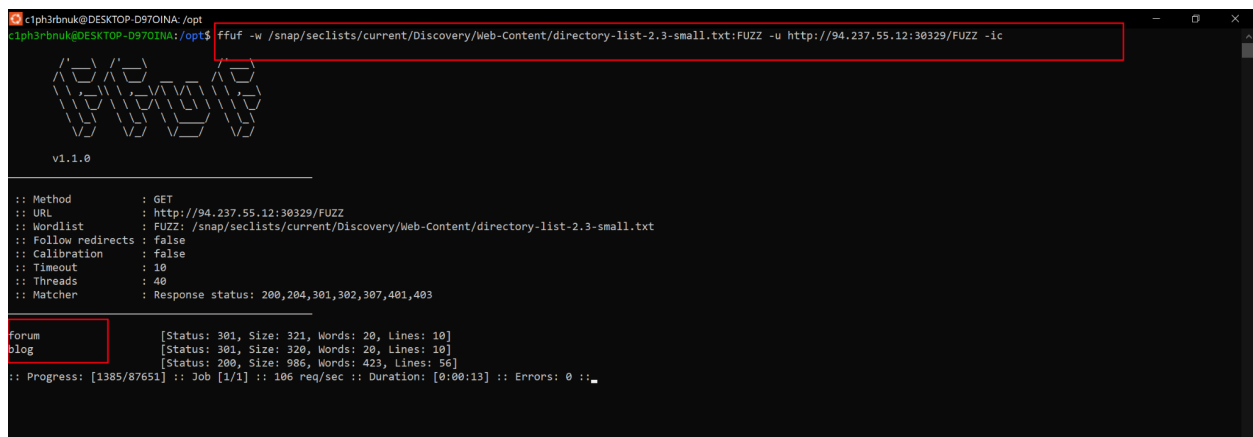
This module covers an important technique in web enumeration known as fuzzing. It teaches how to automate this process of locating hidden pages, directories, parameters and their values in web applications using a tool known as FFuF.

2. ANSWERS TO QUESTIONS

Directory Fuzzing

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

- forum



```
c1ph3rbnuk@DESKTOP-D97OINA: /opt
c1ph3rbnuk@DESKTOP-D97OINA: /opt$ ffuf -w /snap/seclists/current/Discovery/Web-Content/directory-list-2.3-small.txt -u http://94.237.55.12:30329/FUZZ -ic

v1.1.0

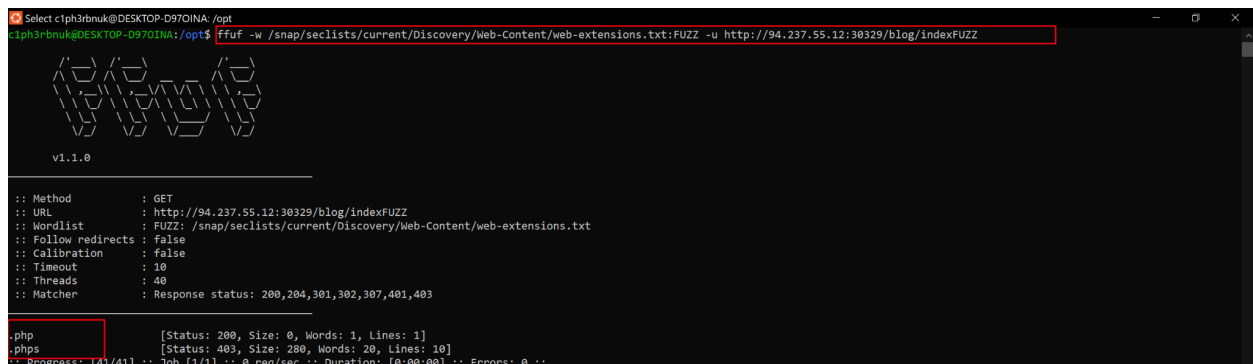
:: Method      : GET
:: URL         : http://94.237.55.12:30329/FUZZ
:: Wordlist     : FUZZ: /snap/seclists/current/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403

forum [Status: 301, Size: 321, Words: 20, Lines: 10]
blog  [Status: 301, Size: 320, Words: 20, Lines: 10]
      [Status: 200, Size: 986, Words: 423, Lines: 56]
:: Progress: [1385/87651] :: Job [1/1] :: 100 req/sec :: Duration: [0:00:13] :: Errors: 0 ::
```

Page Fuzzing

- a. 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?

- Start with identifying the type of extension the web application uses with extension fuzzing.



```
Select c1ph3rbnuk@DESKTOP-D97OINA: /opt
c1ph3rbnuk@DESKTOP-D97OINA: /opt$ ffuf -w /snap/seclists/current/Discovery/Web-Content/web-extensions.txt -u http://94.237.55.12:30329/blog/indexFUZZ

v1.1.0

:: Method      : GET
:: URL         : http://94.237.55.12:30329/blog/indexFUZZ
:: Wordlist     : FUZZ: /snap/seclists/current/Discovery/Web-Content/web-extensions.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403

.php [Status: 200, Size: 0, Words: 1, Lines: 1]
.phps [Status: 403, Size: 280, Words: 20, Lines: 10]
:: Progress: [41/41] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

- Perform **page fuzzing** with the extensions you've identified.

```

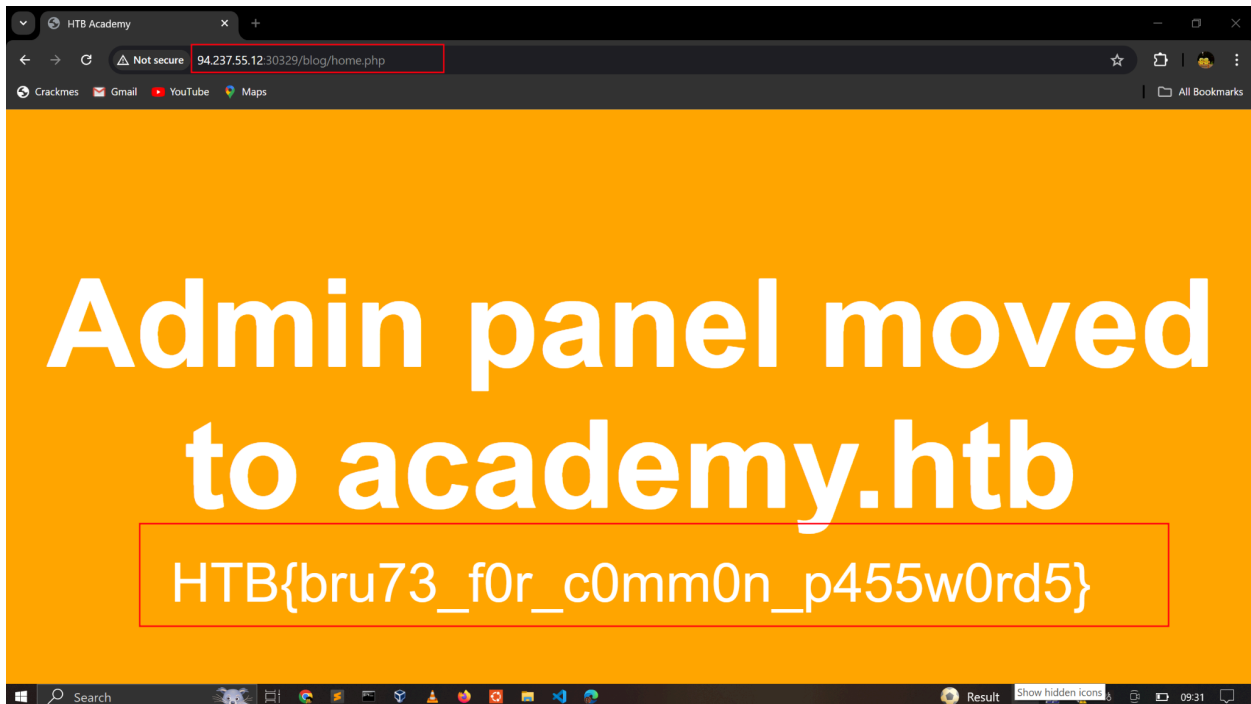
c:\ph3rbnuk@DESKTOP-0970INA:opt$ ffuf -w /snap/seclists/current/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://94.237.55.12:30329/blog/FUZZ.php -ic

v1.1.0

:: Method      : GET
:: URL         : http://94.237.55.12:30329/blog/FUZZ.php
:: Wordlist    : FUZZ: /snap/seclists/current/Discovery/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

home [Status: 200, Size: 1046, Words: 430, Lines: 50]
index [Status: 403, Size: 280, Words: 20, Lines: 10]
[Status: 200, Size: 0, Words: 1, Lines: 1]
[Status: 403, Size: 280, Words: 20, Lines: 10]
:: Progress: [87651/87651] :: Job [1/1] :: 216 req/sec :: Duration: [0:06:45] :: Errors: 0 ::
c:\ph3rbnuk@DESKTOP-0970INA:opt$

```



Recursive Fuzzing

- 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?
 - `ffuf -w /snap/seclists/current/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://94.237.55.12:30329/FUZZ -recursion -recursion-depth 1 -e .php -v -ic`
 - The command above allows us to perform a recursive fuzz from the root directory of the web application.

```
ciph3rbnuk@DESKTOP-D970INA: /opt
[Status: 200, Size: 986, Words: 423, Lines: 56]
| URL | http://94.237.55.12:30329/
+ FUZZ:

[Status: 403, Size: 280, Words: 20, Lines: 10]
| URL | http://94.237.55.12:30329/.php
+ FUZZ: .php

[Status: 200, Size: 0, Words: 1, Lines: 1]
| URL | http://94.237.55.12:30329/blog/
+ FUZZ:

[Status: 200, Size: 0, Words: 1, Lines: 1]
| URL | http://94.237.55.12:30329/blog/index.php
+ FUZZ: index.php

[Status: 403, Size: 280, Words: 20, Lines: 10]
| URL | http://94.237.55.12:30329/blog/.php
+ FUZZ: .php

[Status: 200, Size: 1046, Words: 438, Lines: 58]
| URL | http://94.237.55.12:30329/blog/home.php
+ FUZZ: home.php

[Status: 200, Size: 0, Words: 1, Lines: 1]
| URL | http://94.237.55.12:30329/blog/
+ FUZZ:

[Status: 403, Size: 280, Words: 20, Lines: 10]
| URL | http://94.237.55.12:30329/blog/.php
+ FUZZ: .php

[Status: 403, Size: 280, Words: 20, Lines: 10]
| URL | http://94.237.55.12:30329/forum/.php
+ FUZZ: .php

[Status: 200, Size: 0, Words: 1, Lines: 1]
| URL | http://94.237.55.12:30329/forum/
+ FUZZ:

[Status: 200, Size: 0, Words: 1, Lines: 1]
| URL | http://94.237.55.12:30329/forum/index.php
+ FUZZ: index.php

[Status: 200, Size: 21, Words: 1, Lines: 1]
| URL | http://94.237.55.12:30329/forum/flag.php
+ FUZZ: flag.php

[WARN] Caught keyboard interrupt (Ctrl-C)
ciph3rbnuk@DESKTOP-D970INA: /opt$
```



Sub-domain fuzzing

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

- customer.inlaneftreight.com

```
ciph3rbnuk@DESKTOP-D970INA: /opt
ciph3rbnuk@DESKTOP-D970INA: /opt$ ffuf -w /snap/seclists/current/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u https://FUZZ.inlaneftreight.com/

v1.1.0

:: Method      : GET
:: URL         : https://FUZZ.inlaneftreight.com/
:: Wordlist     : FUZZ: /snap/seclists/current/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

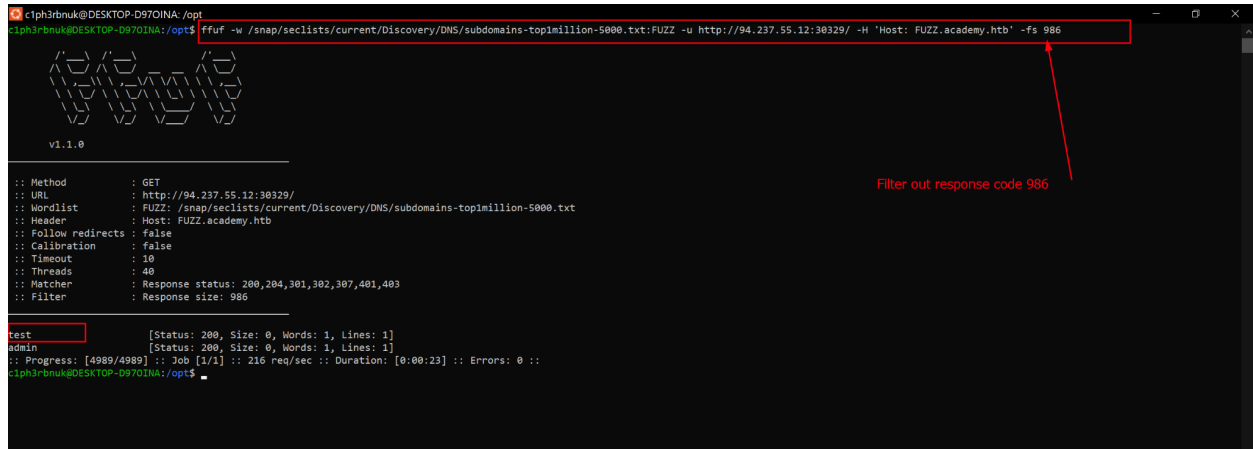
www      [Status: 200, Size: 22262, Words: 2903, Lines: 316]
support  [Status: 301, Size: 0, Words: 1, Lines: 1]
ms       [Status: 301, Size: 0, Words: 1, Lines: 1]
blog     [Status: 301, Size: 0, Words: 1, Lines: 1]
my       [Status: 301, Size: 0, Words: 1, Lines: 1]
customer [Status: 301, Size: 0, Words: 1, Lines: 1]
:: Progress: [1256/4989] :: Job [1/1] :: 14 req/sec :: Duration: [0:01:25] :: Errors: 1210 ::

customer.inlaneftreight.com
```

Vhost Fuzzing

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

- Vhost fuzzing requires fuzzing the HTTP Host header and filtering out for the incorrect response size.
- Answer = test



```
ctph3rbnuk@DESKTOP-D970INA: /opt
ctph3rbnuk@DESKTOP-D970INA: /opt$ ffuf -w /snap/seclists/current/Discovery/DNS/subdomains-topmillion-5000.txt:FUZZ -u http://94.237.55.12:30329/ -H 'Host: FUZZ.academy.htb' -fs 986

v1.1.0

:: Method      : GET
:: URL         : http://94.237.55.12:30329/
:: Wordlist    : FUZZ: /snap/seclists/current/Discovery/DNS/subdomains-topmillion-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
:: Filter     : Response size: 986

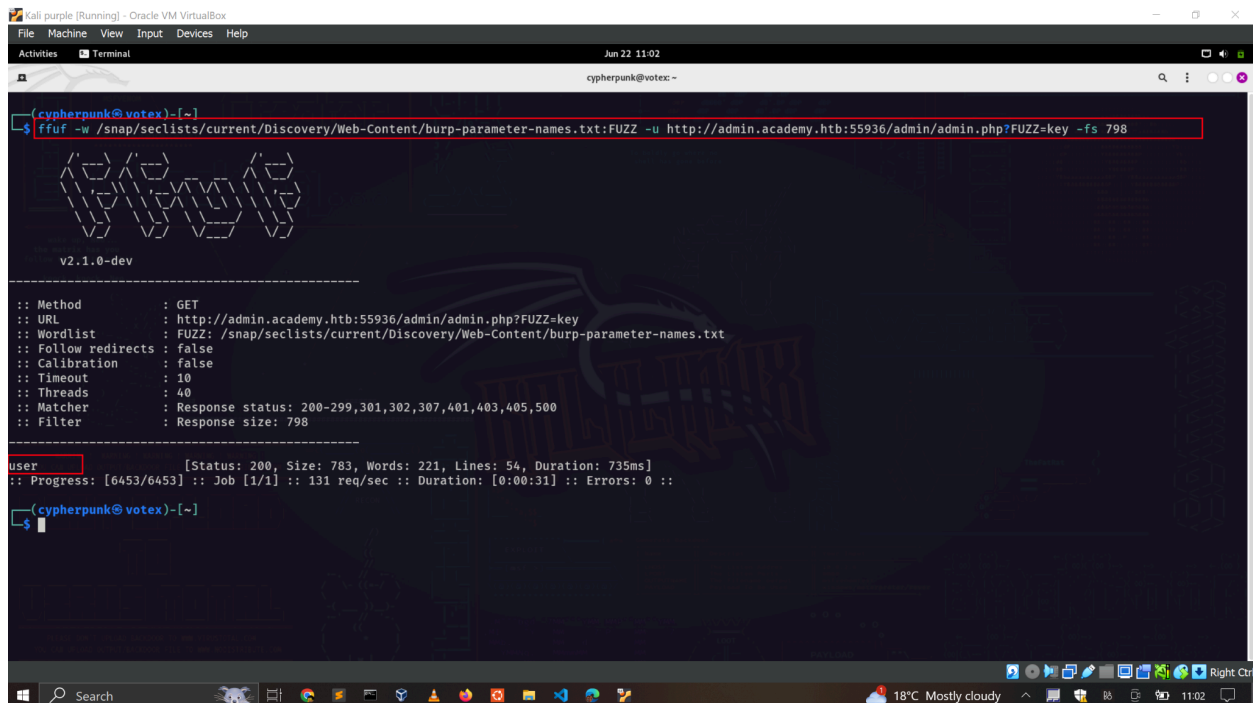
test [Status: 200, Size: 0, Words: 1, Lines: 1]
admin [Status: 200, Size: 0, Words: 1, Lines: 1]
:: Progress: [4889/4889] :: Job [1/1] :: 216 req/sec :: Duration: [0:00:23] :: Errors: 0 ::
ctph3rbnuk@DESKTOP-D970INA: /opt$
```

Filter out response code 986

Parameter Fuzzing - GET

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

- The webpage accepts user parameter



```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 22 11:02
cypherpunk@votex:~

(cypherpunk@votex)~$ ffuf -w /snap/seclists/current/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://admin.academy.htb:55936/admin/admin.php?FUZZ=key -fs 798

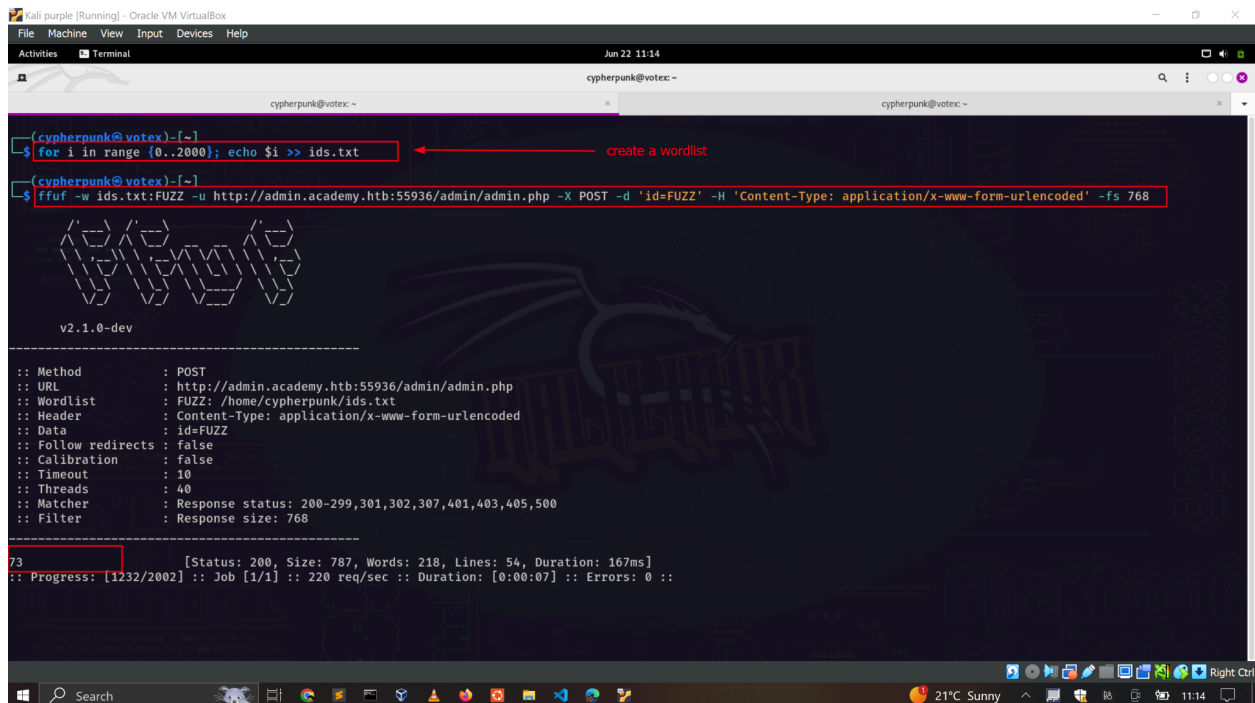
v2.1.0-dev

:: Method      : GET
:: URL         : http://admin.academy.htb:55936/admin/admin.php?FUZZ=key
:: Wordlist    : FUZZ: /snap/seclists/current/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: 735ms]
:: Progress: [6453/6453] :: Job [1/1] :: 131 req/sec :: Duration: [0:00:31] :: Errors: 0 ::
(cypherpunk@votex)~$
```

Parameter value Fuzzing

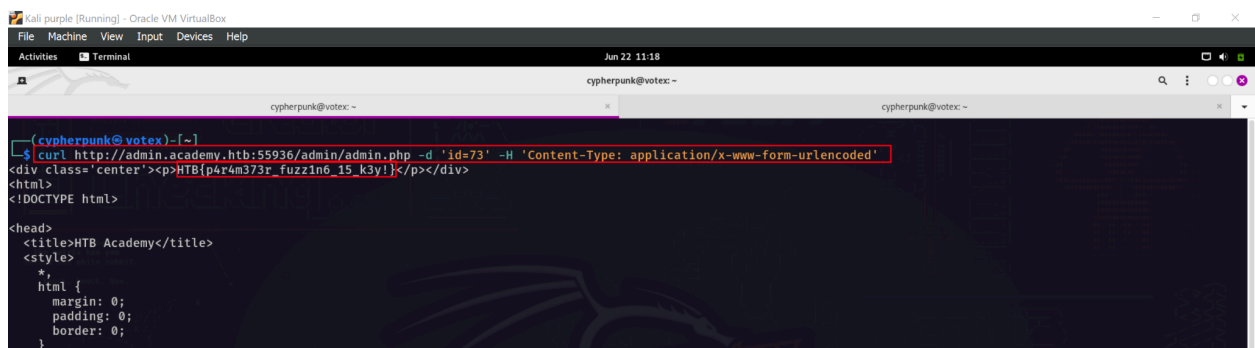
- a. Try to create the 'ids.txt' wordlist, identify the accepted value with a fuzzing scan, and then use it in a 'POST' request with 'curl' to collect the flag. What is the content of the flag?
 - Create a custom ids.txt wordlist.
 - Use it to fuzz the id POST parameter
 - Once you identify a correct value, use it to retrieve the flag.



```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 22 11:14
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~

(cypherpunk@votex)~[~]
$ for i in range {0..2000}; echo $i >> ids.txt
$ ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:55936/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:55936/admin/admin.php
:: Wordlist     : FUZZ: /home/cypherpunk/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: 167ms]
:: Progress: [1232/2002] :: Job [1/1] :: 220 req/sec :: Duration: [0:00:07] :: Errors: 0 ::
```



```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 22 11:18
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~

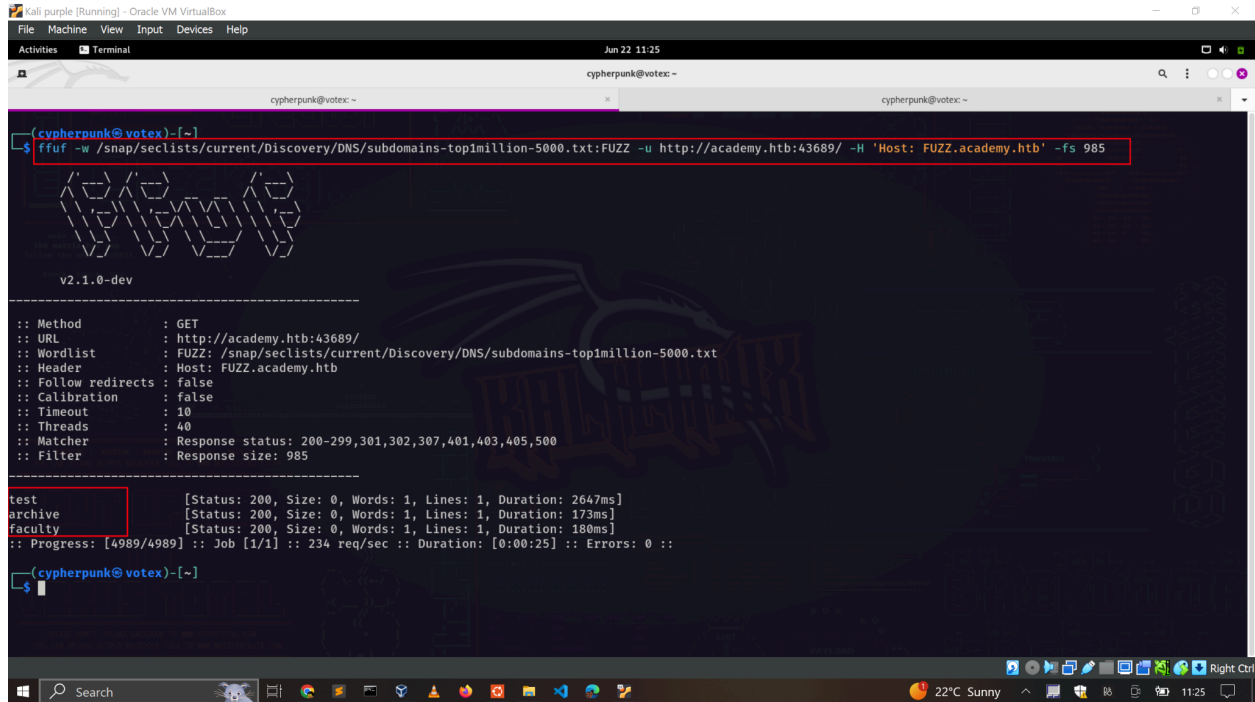
(cypherpunk@votex)~[~]
$ curl http://admin.academy.htb:55936/admin/admin.php -d 'id=73' -H 'Content-Type: application/x-www-form-urlencoded'
<div class='center'><p>HTB{p4r4m373r_fuzzin6_15_k3y!}</p></div>
<html>
<!DOCTYPE html>

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

Skills Assessment - Web Fuzzing

- a. 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)

- test, archive, faculty



```
(cypherpunk@votex)-[~]
$ ffuf -w /snap/seclists/current/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://academy.htb:43689/ -H 'Host: FUZZ.academy.htb' -fs 985

v2.1.0-dev

:: Method      : GET
:: URL         : http://academy.htb:43689/
:: Wordlist    : FUZZ: /snap/seclists/current/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

test      [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 2647ms]
archive   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 173ms]
faculty   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 180ms]
:: Progress: [4989/4989] :: Job [1/1] :: 234 req/sec :: Duration: [0:00:25] :: Errors: 0 ::

(cypherpunk@votex)-[~]
$
```

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

- Running extension fuzzing on all the subdomains unveils three different extensions: php, php7, php5.


```
c:\ph3rbrnuk@DESKTOP-D970INA: ~
c:\ph3rbrnuk@DESKTOP-D970INA:~$ curl http://faculty.academy.htb:51842/courses/linux-security.php7
<div class='center'><p>You don't have access!</p></div>
<html>
<!DOCTYPE html>

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

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

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

- The page accepts the **user** and **username** POST request parameters.

```
c:\ph3rbrnuk@DESKTOP-D970INA:~$
c:\ph3rbrnuk@DESKTOP-D970INA:~$ ffuf -w /snap/seclists/current/Discovery/Web-Content/burp-parameter-names.txt FUZZ -u http://faculty.academy.htb:31548/courses/linux-security.php7 -X POST -d 'FUZZ=key' -H 'Content-Type: application/x-www-form-urlencoded' -fs 774

v1.1.0

:: Method      : POST
:: URL         : http://faculty.academy.htb:31548/courses/linux-security.php7
:: Wordlist    : FUZZ: /snap/seclists/current/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: 200,204,301,302,307,401,403
:: Filter     : Response size: 774

user      [Status: 200, Size: 780, Words: 223, Lines: 53]
username  [Status: 200, Size: 781, Words: 223, Lines: 53]
:: Progress: [6453/6453] :: Job [1/1] :: 195 req/sec :: Duration: [0:00:33] :: Errors: 0 ::
c:\ph3rbrnuk@DESKTOP-D970INA:~$
```

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

- Fuzz the username parameter for values.
- You'll discover multiple acceptable usernames, as shown below.

```
c:\ph3rbrnuk@DESKTOP-D970INA: ~
c:\ph3rbrnuk@DESKTOP-D970INA:~$ ffuf -w /snap/seclists/current/Usernames/xato-net-10-million-usernames.txt FUZZ -u http://faculty.academy.htb:51842/courses/linux-security.php7 -X POST -d 'username=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 781

v1.1.0

:: Method      : POST
:: URL         : http://faculty.academy.htb:51842/courses/linux-security.php7
:: Wordlist    : FUZZ: /snap/seclists/current/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: 200,204,301,302,307,401,403
:: Filter     : Response size: 781

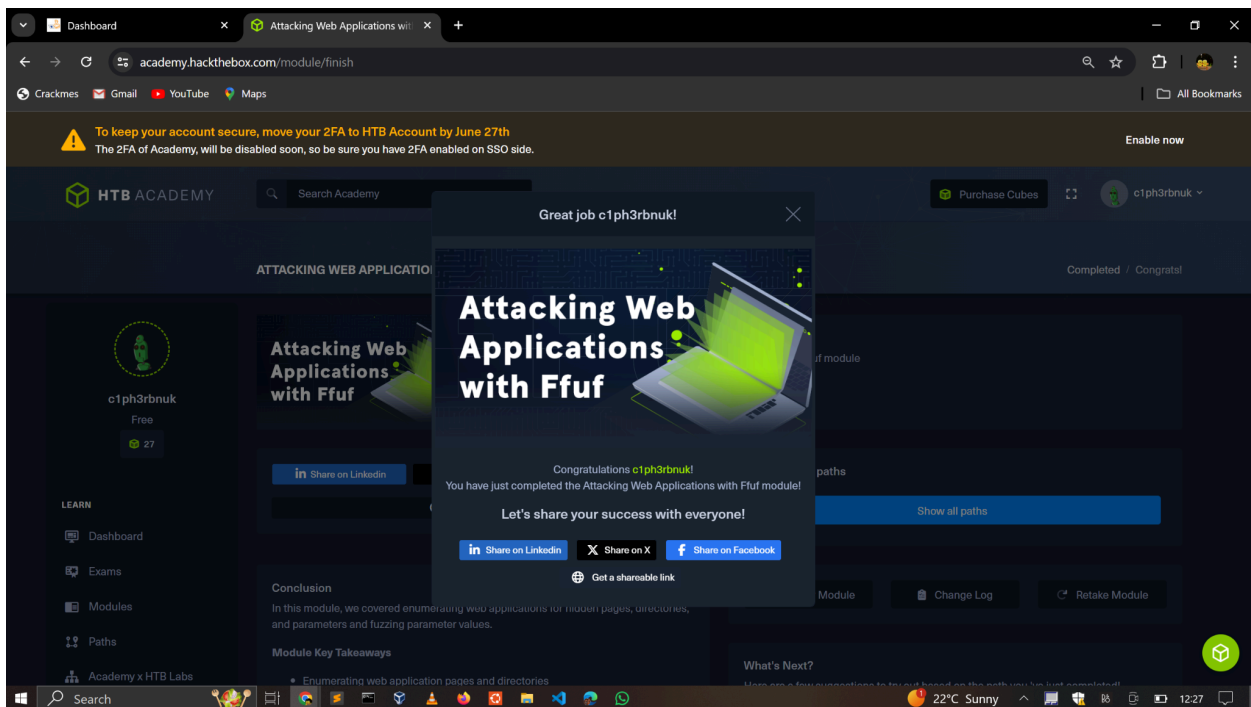
harry     [Status: 200, Size: 773, Words: 218, Lines: 53]
Harry     [Status: 200, Size: 773, Words: 218, Lines: 53]
HARRY     [Status: 200, Size: 773, Words: 218, Lines: 53]
:: Progress: [47058/8295455] :: Job [1/1] :: 231 req/sec :: Duration: [0:03:23] :: Errors: 0 ::
```

- Trying to send a POST request to each one of them reveals that “**harry**” is our correct username to retrieve the flag.

```
c1ph3rbnuk@DESKTOP-D970INA: ~  
c1ph3rbnuk@DESKTOP-D970INA:~$ curl http://faculty.academy.htb:51842/courses/linux-security.php7 -X POST -d 'username=harry' -H 'Content-Type: application/x-www-form-urlencoded'  
<div class='center'><p>HTB(w3b_fuzzin6_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: #151028;  
}
```

3. MODULE COMPLETION

<https://academy.hackthebox.com/achievement/144829/54>



4. CONCLUSION

This assignment has taught me how to automate web fuzzing using the Ffuf tool. I have learned how to fuzz directories, extensions, pages, GET and POST parameters and also the values of these parameters. It's truly empowering to have this tool in my arsenal as a security analyst.