Attacking Web Applications with Ffuf

Introduction

In this module the learner will learn tools and methods to utilize for directory and parameter fuzzing/brute-forcing. In this module, the main focus is built on the ffuf tool for web fuzzing, as it is one of the most common and reliable tools available for web fuzzing.

The learner will go on to understand following topics:

- Fuzzing for directories
- Fuzzing for files and extensions
- Identifying hidden vhosts
- Fuzzing for PHP parameters
- Fuzzing for parameter values

Activities

Web Fuzzing

Fuzzing refers to a testing technique that sends various types of user input to a certain interface to study how it would react.

Wordlists

This refers to a wordlist containing commonly used words for web directories and pages, very similar to a ***Password Dictionary Attack***.

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

The learner can find the entire SecLists repo available under /opt/useful/SecLists. The specific wordlist to be utilized for pages and directory fuzzing is another commonly used wordlist called directory-list-2.3, and it is available in various forms and sizes. The learner can find the one we will be using under:

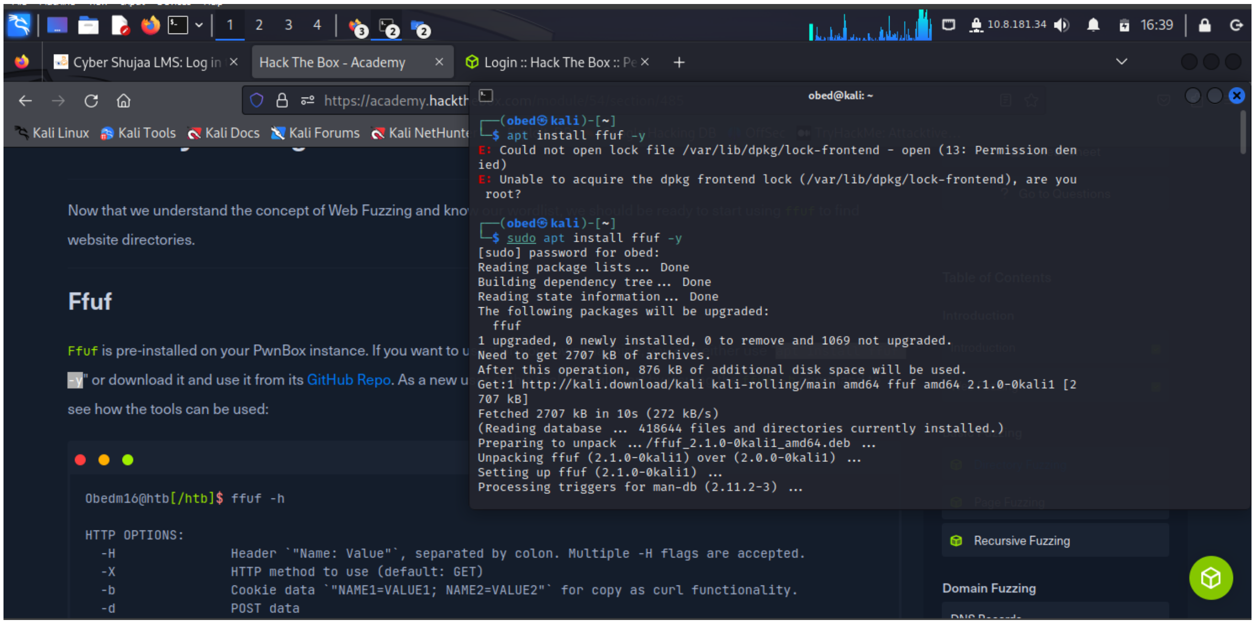
```
locate directory-list-2.3-small.txt
```

Directory Fuzzing

The learner having known a location of the wordlist to be used and the concept of Web fuzzing, they are ready to exercise this activity to find website directories.

Ffuf

Ffuf is pre-installed on the PwnBox instance. If the learner want to use it on their own machine, they can either use "**sudo apt install ffuf -y**" or download it and use it from its GitHub Repo. As a new user of this tool, we will start by issuing the **ffuf -h** command to see how the tools can be used:



```
┌──(obed㉿kali)-[~]
└─$ apt install ffuf -y
E: Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission den
ied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), are you
 root?

┌──(obed㉿kali)-[~]
└─$ sudo apt install ffuf -y
[sudo] password for obed:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be upgraded:
  ffuf
1 upgraded, 0 newly installed, 0 to remove and 1069 not upgraded.
Need to get 2707 kB of archives.
After this operation, 876 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 ffuf amd64 2.1.0-0kali1 [2
707 kB]
Fetched 2707 kB in 10s (272 kB/s)
(Reading database ... 418644 files and directories currently installed.)
Preparing to unpack .../ffuf_2.1.0-0kali1_amd64.deb ...
Unpacking ffuf (2.1.0-0kali1) over (2.0.0-0kali1) ...
Setting up ffuf (2.1.0-0kali1) ...
Processing triggers for man-db (2.11.2-3) ...
```

Now that we understand the concept of Web Fuzzing and kno

website directories.

Ffuf

Ffuf is pre-installed on your PwnBox instance. If you want to u

-y" or download it and use it from its GitHub Repo. As a new u

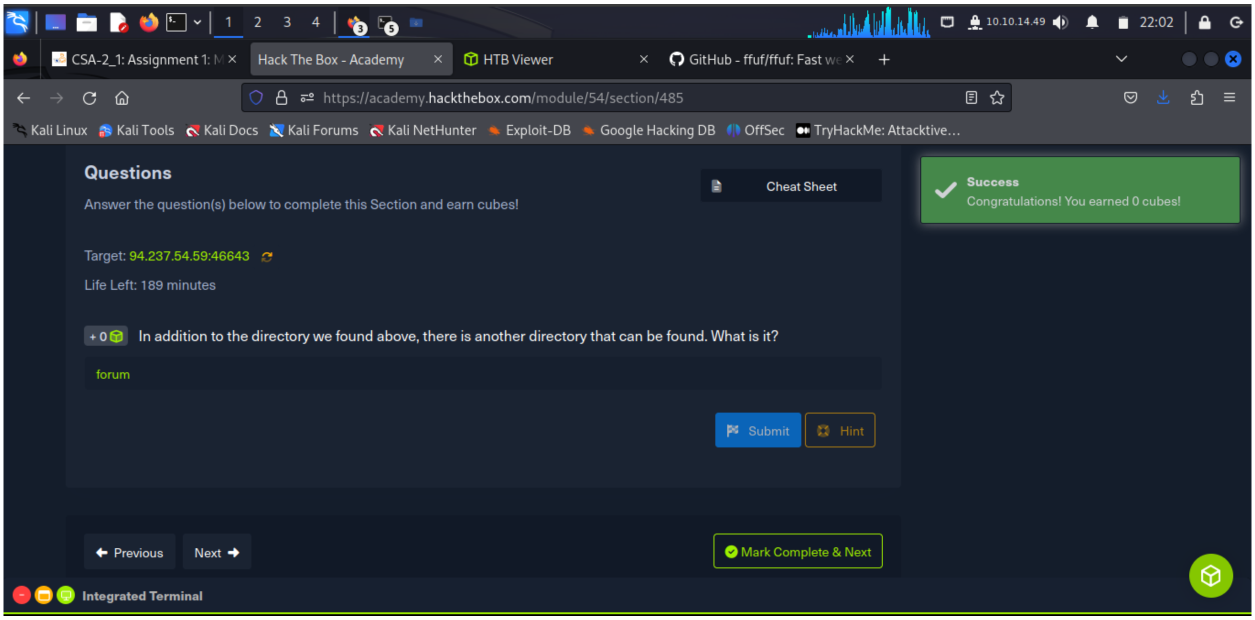
see how the tools can be used:

```
Obedm16@htb[/htb]$ ffuf -h

HTTP OPTIONS:
  -H               Header `"Name: Value"`, separated by colon. Multiple -H flags are accepted.
  -X               HTTP method to use (default: GET)
  -b               Cookie data `"NAME1=VALUE1; NAME2=VALUE2"` for copy as curl functionality.
  -d               POST data
```

Directory Fuzzing

As we can see from the example above, the main two options are **-w** for wordlists and **-u** for the URL. We can assign a keyword to a wordlist to refer to it where we want to fuzz.

Next, as we want to be fuzzing for web directories, we can place the FUZZ keyword where the directory would be within our URL, with:



Questions

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

Target: 94.237.54.59:46643

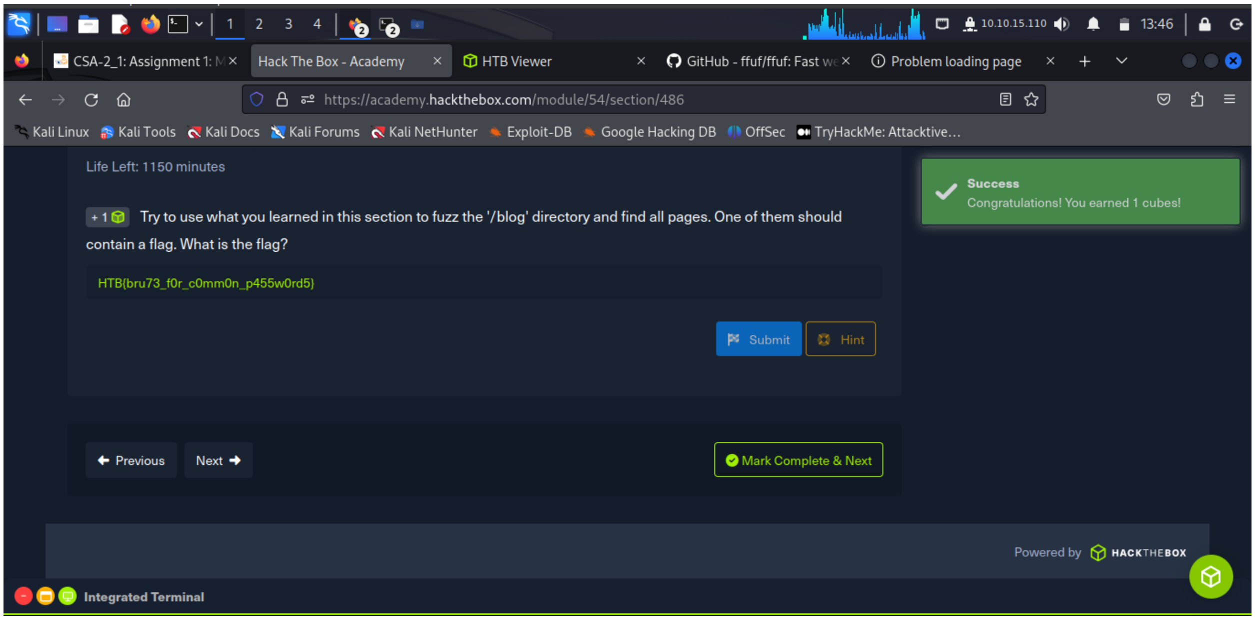
Life Left: 189 minutes

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

forum

Success
Congratulations! You earned 0 cubes!

The learner run **94.237.54.59:46643/blog/home.php**

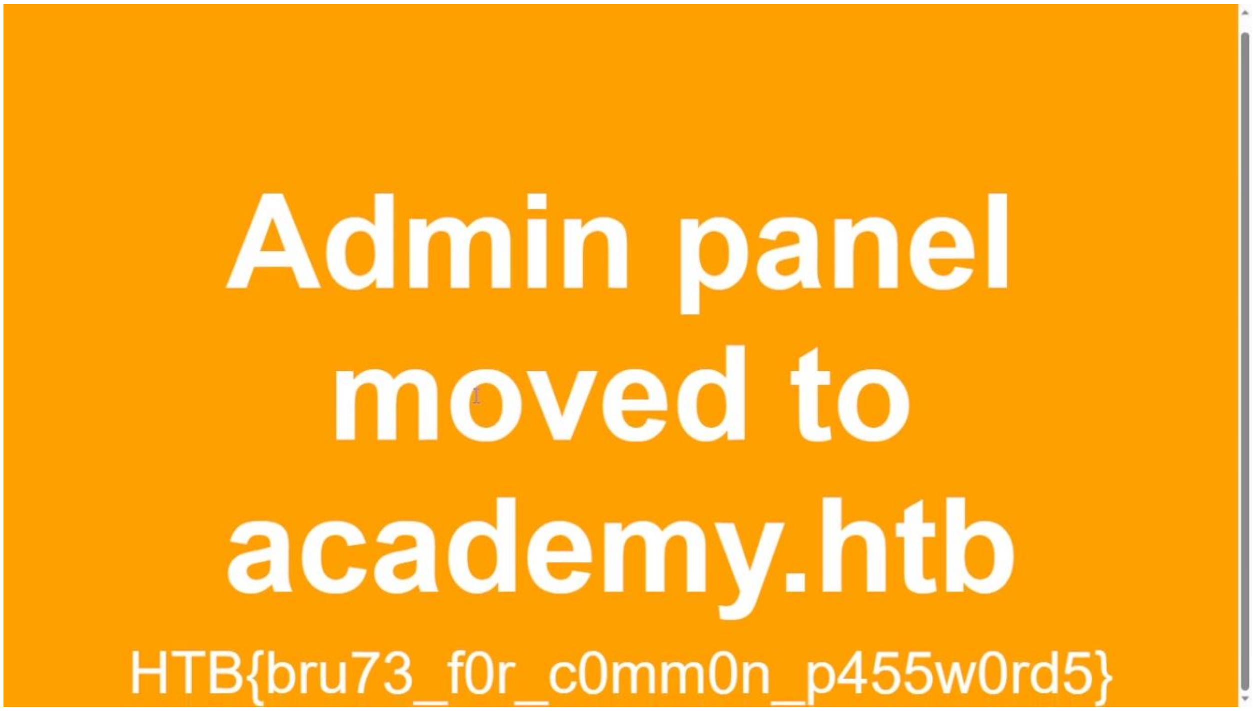


Life Left: 1150 minutes

+ 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}

Success
Congratulations! You earned 1 cubes!



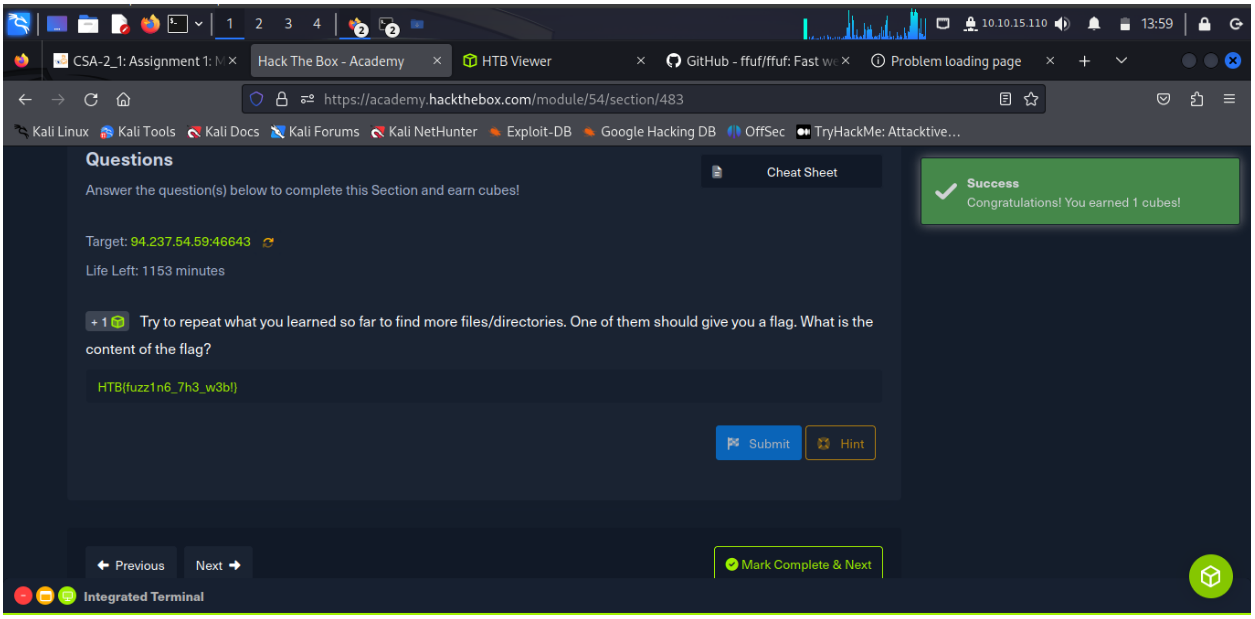
Admin panel moved to academy.htb

HTB{bru73_f0r_c0mm0n_p455w0rd5}

Recursive Fuzzing

For dozens of directories, each with their own subdirectories and files are automated through **recursive fuzzing**.

It automatically starts another scan under any newly identified directories that may have on their pages until it has fuzzed the main website and all of its subdirectories.



Questions

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

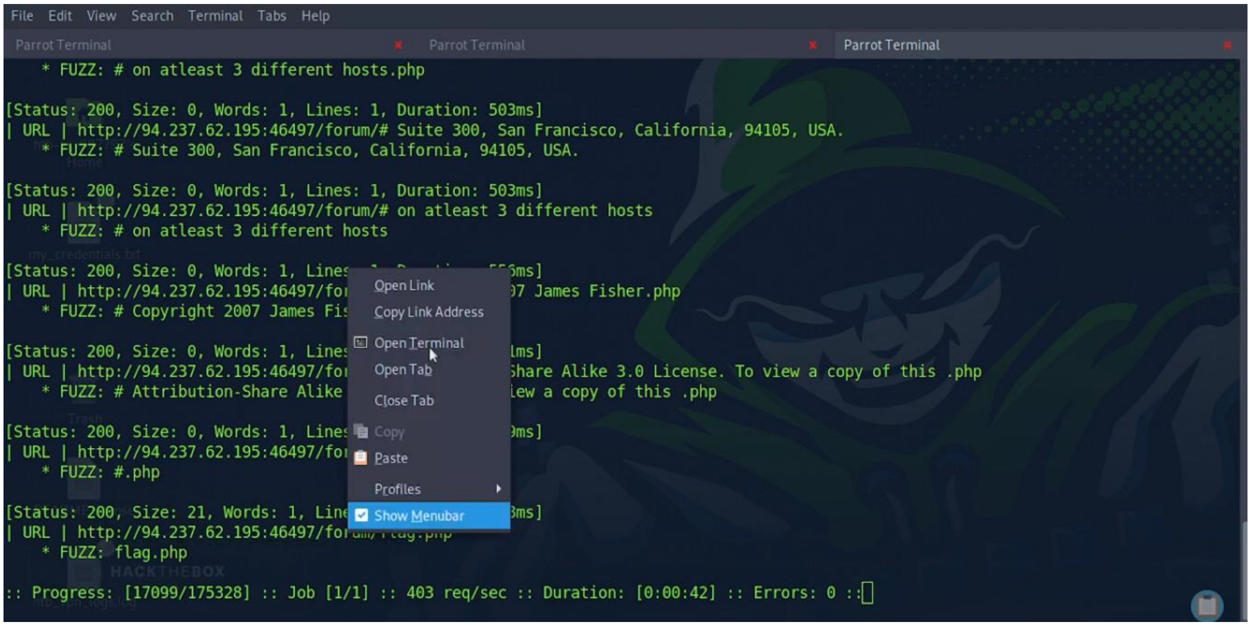
Target: 94.237.54.59:46643

Life Left: 1153 minutes

+ 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?

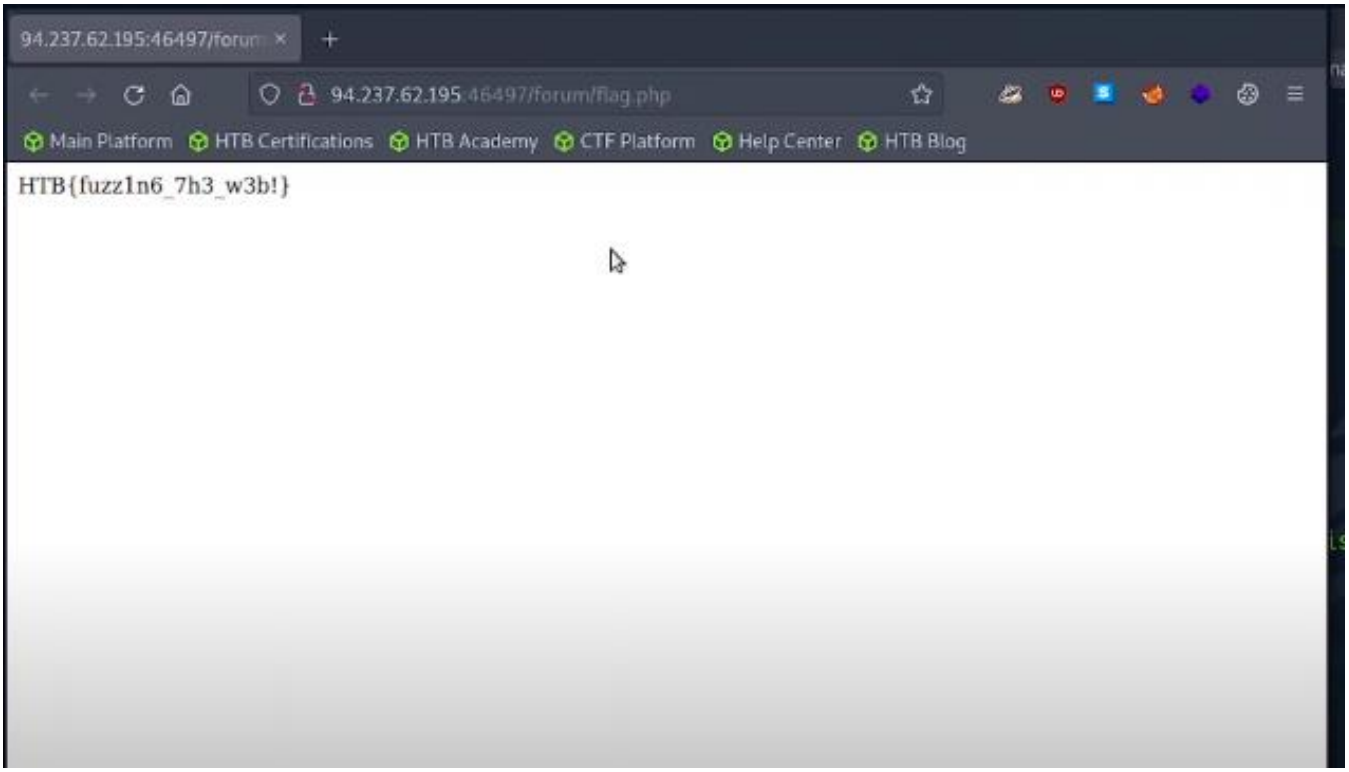
HTB{fuzz1n6_7h3_w3b!}

Success
Congratulations! You earned 1 cubes!



```
    * FUZZ: # on atleast 3 different hosts.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 503ms]
| URL | http://94.237.62.195:46497/forum/# Suite 300, San Francisco, California, 94105, USA.
    * FUZZ: # Suite 300, San Francisco, California, 94105, USA.

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 503ms]
| URL | http://94.237.62.195:46497/forum/# on atleast 3 different hosts
    * FUZZ: # on atleast 3 different hosts

[Status: 200, Size: 0, Words: 1, Lines                   56ms]
| URL | http://94.237.62.195:46497/fo                    07 James Fisher.php
    * FUZZ: # Copyright 2007 James Fis

[Status: 200, Size: 0, Words: 1, Lines                   1ms]
| URL | http://94.237.62.195:46497/fo                    Share Alike 3.0 License. To view a copy of this .php
    * FUZZ: # Attribution-Share Alike                     iew a copy of this .php

[Status: 200, Size: 0, Words: 1, Lines                   3ms]
| URL | http://94.237.62.195:46497/fo
    * FUZZ: #.php

[Status: 200, Size: 21, Words: 1, Line                   3ms]
| URL | http://94.237.62.195:46497/forum/flag.php
    * FUZZ: flag.php

:: Progress: [17099/175328] :: Job [1/1] :: 403 req/sec :: Duration: [0:00:42] :: Errors: 0 ::
```

From the above, the learner run **http:94.237.62.195:46497/forum/flag.php**



HTB{fuzz1n6_7h3_w3b!}

DNS Records

Browsers only understand how to go to IPs, and if we provide them with a URL, they try to map the URL to an IP by looking into the local /etc/hosts file and the public DNS Domain Name System. If the URL is not in either, it would not know how to connect to it.

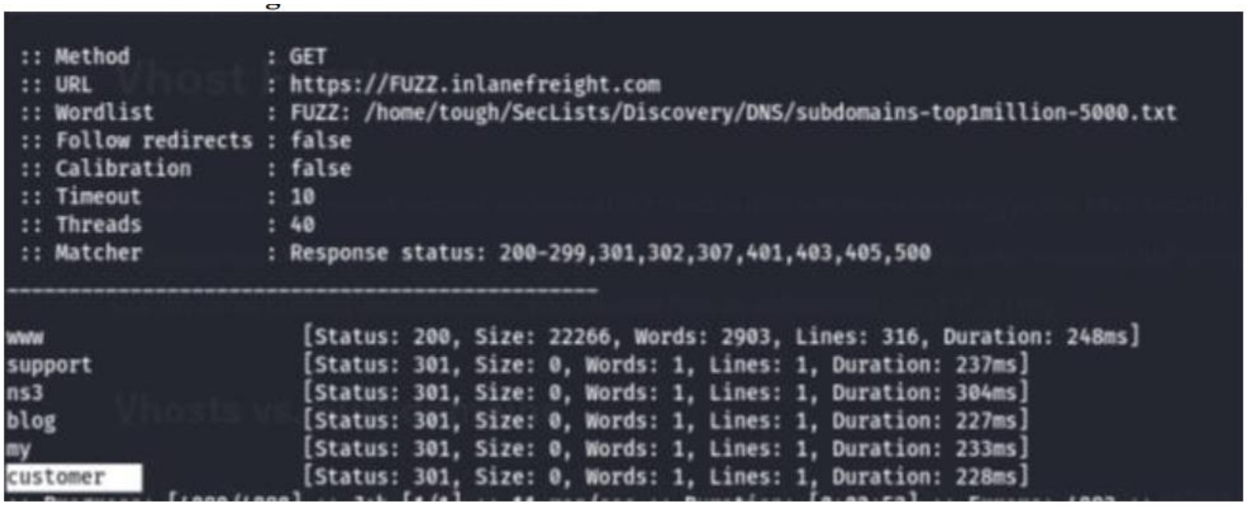
Sub-domain Fuzzing

The learner will learn how to use ffuf to identify sub-domains e.g., *.website.com for any website.

Sub-domains

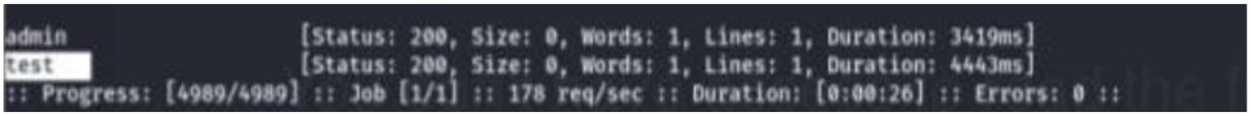
A sub-domain is any website underlying another domain. For example, ***https://photos.google.com*** is the photos sub-domain of ***google.com.***

Run the **ffuf -w /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://FUZZ. inlanefreight.com**



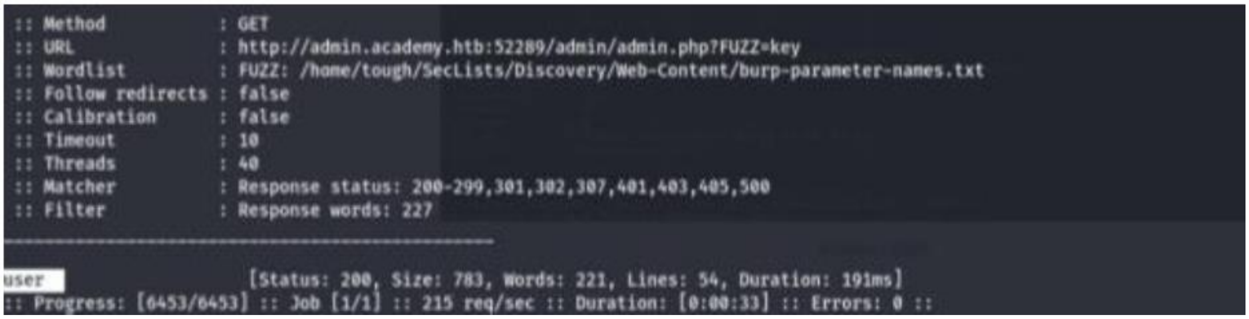
```
 :: Method           : GET
 :: URL              : https://FUZZ.inlanefreight.com
 :: Wordlist         : FUZZ: /home/tough/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : 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]
```

The full subdomain is **customer.inlanefreight.com**



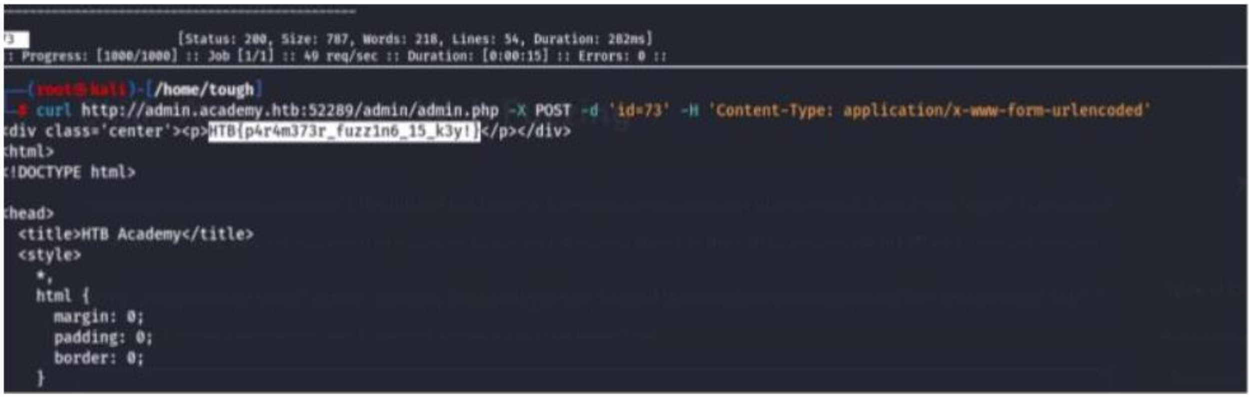
```
admin                   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 3419ms]
test                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4443ms]
:: Progress: [4989/4989] :: Job [1/1] :: 178 req/sec :: Duration: [0:00:26] :: Errors: 0 ::
```

When the learner run a VHost fuzzing scan on 'academy.htb', the other VHosts seen is: **test.academy.htb**



```
:: 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 ::
```

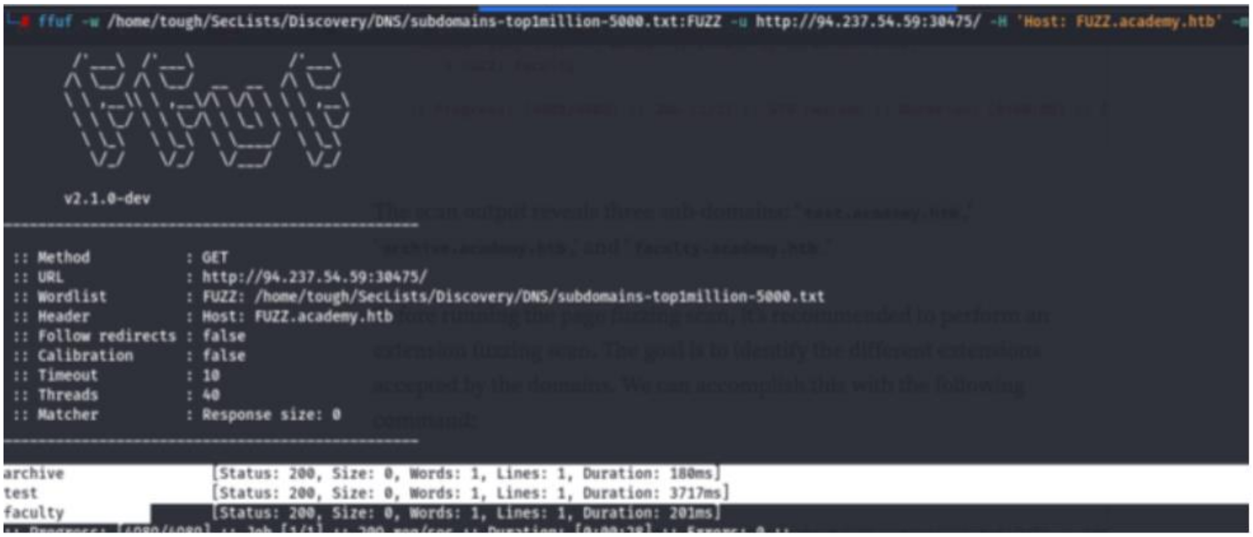
Upon running a parameter fuzzing scan on this page, the parameter accepted by this webpage is **User.**



```
________________________________________________

73                      [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;
    }
```

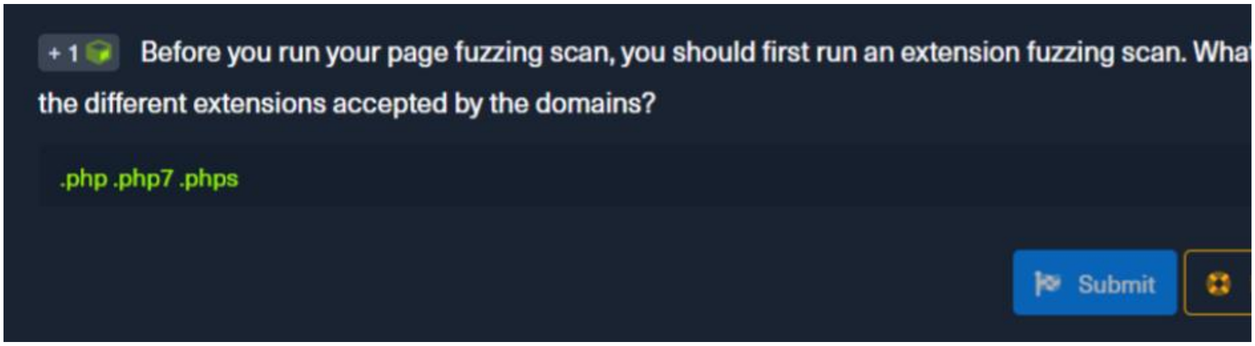
On creating the 'ids.txt' wordlist, identified and the accepted value with a fuzzing scan; and used in a 'POST' request with 'curl' in collecting the flag is:

HTB{p4r4m373r_fuzz1n6_15_k3y!}



```
└─# ffuf -w /home/tough/SecLists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://94.237.54.59:30475/ -H 'Host: FUZZ.academy.htb' -m

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

       v2.1.0-dev
________________________________________________

:: Method           : GET
:: URL              : http://94.237.54.59:30475/
:: Wordlist         : FUZZ: /home/tough/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: 180ms]
test                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 3717ms]
faculty                 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 201ms]
:: Progress: [4989/4989] :: Job [1/1] :: 200 req/sec :: Duration: [0:00:28] :: Errors: 0 ::
```

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**

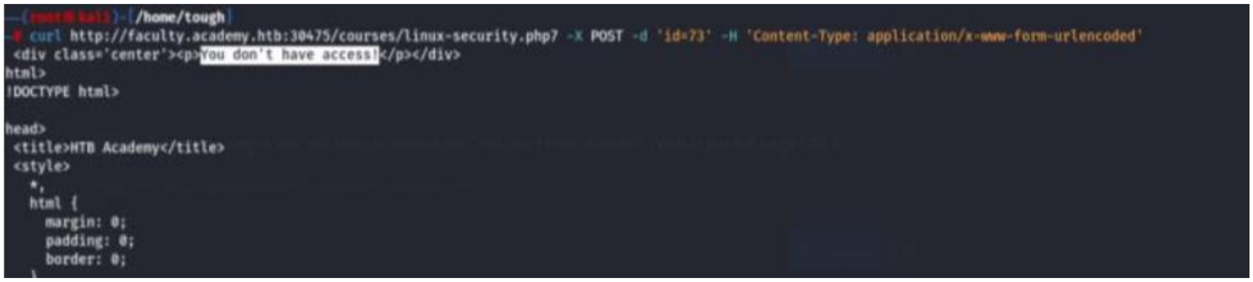


+ 1 Before you run your page fuzzing scan, you should first run an extension fuzzing scan. Wha

the different extensions accepted by the domains?

.php .php7 .phps

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**

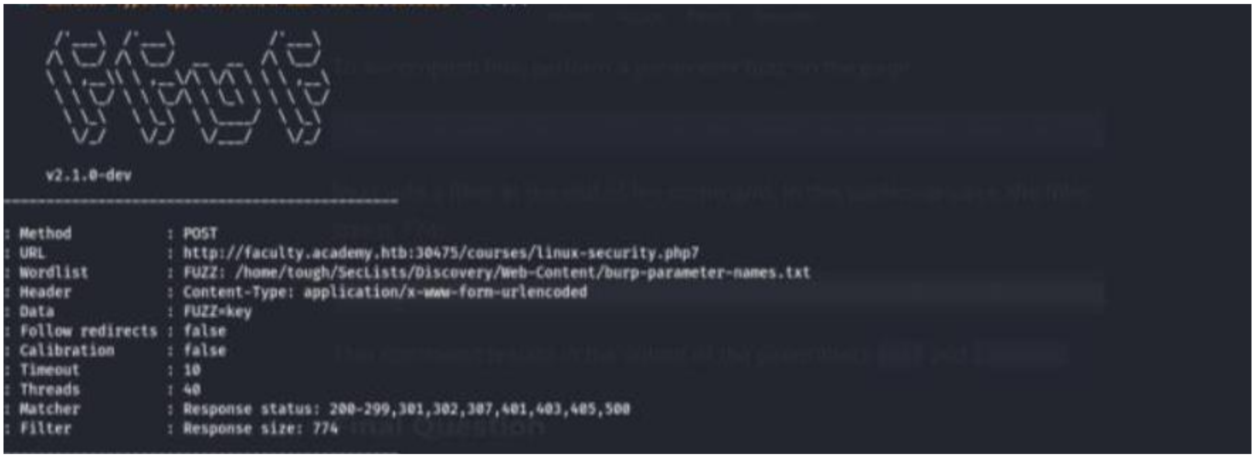


```
┌──(root㉿kali)-[/home/tough]
└─# curl http://faculty.academy.htb:30475/courses/linux-security.php7 -X POST -d 'id=73' -H 'Content-Type: application/x-www-form-urlencoded'
 <div class='center'><p>You don't have access!</p></div>
html>
!DOCTYPE html>

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

One of the pages you will identify should say 'You don't have access!'. What is the full

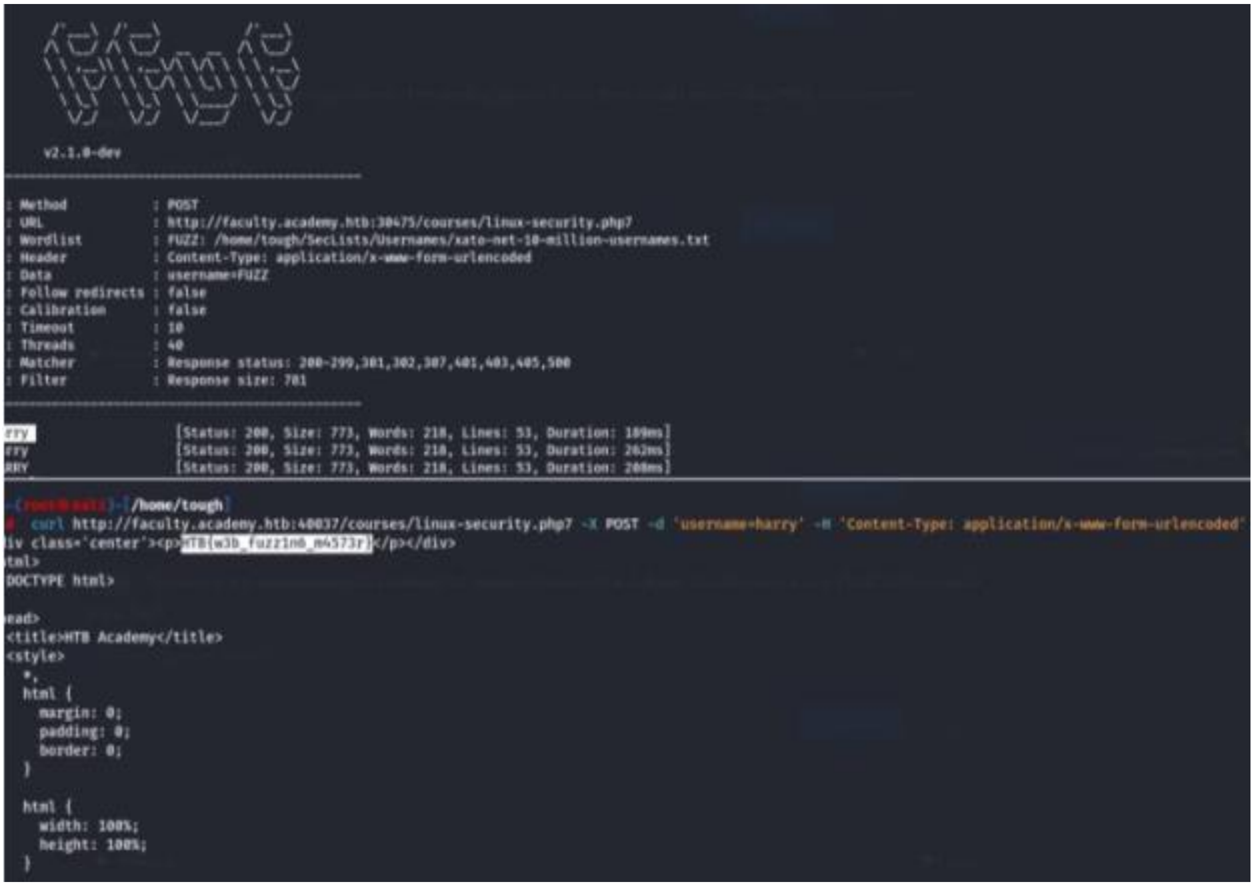
page URL? **http://faculty.academy.htb:PORT/courses/linux-security.php7**

customer.inlanefreight.com



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

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://faculty.academy.htb:30475/courses/linux-security.php7
 :: Wordlist         : FUZZ: /home/tough/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
```

In the page from the previous question, you should be able to find multiple parameters that are accepted by the page. They are: **user username**

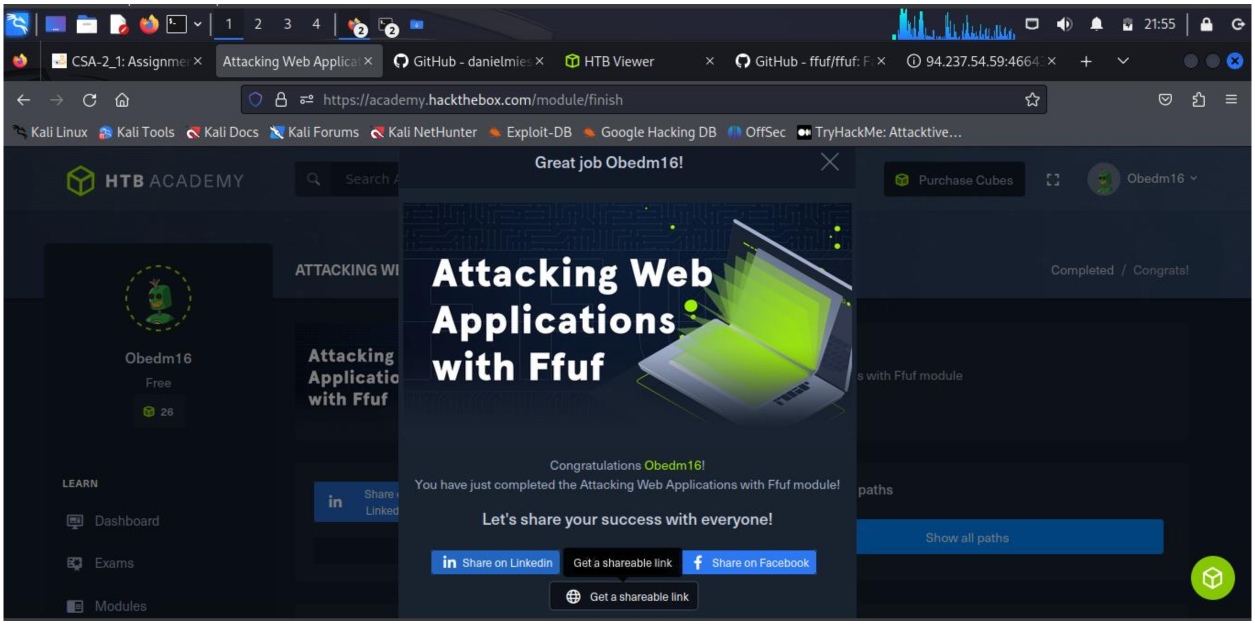


```
        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://faculty.academy.htb:30475/courses/linux-security.php7
 :: Wordlist         : FUZZ: /home/tough/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
________________________________________________

rry                     [Status: 200, Size: 773, Words: 218, Lines: 53, Duration: 189ms]
rry                     [Status: 200, Size: 773, Words: 218, Lines: 53, Duration: 262ms]
RRY                     [Status: 200, Size: 773, Words: 218, Lines: 53, Duration: 208ms]

-([illegible])-[/home/tough]
  curl http://faculty.academy.htb:40037/courses/linux-security.php7 -X POST -d 'username=harry' -H 'Content-Type: application/x-www-form-urlencoded'
iv class='center'><p>HTB{w3b_fuzz1n6_m4573r}</p></div>
tml>
DOCTYPE html>

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

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

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

Conclusion

The learning concepts of domain fuzzing and sub domain is a bit challenging, but with time the learner was able penetrate sites and achieved to Attack Web Applications with **ffuf command** and other complex tools (FUZZ)



Great job Obedm16!

Attacking Web Applications with Ffuf

Congratulations Obedm16!

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

Let's share your success with everyone!

Completion: https://academy.hackthebox.com/achievement/978332/54