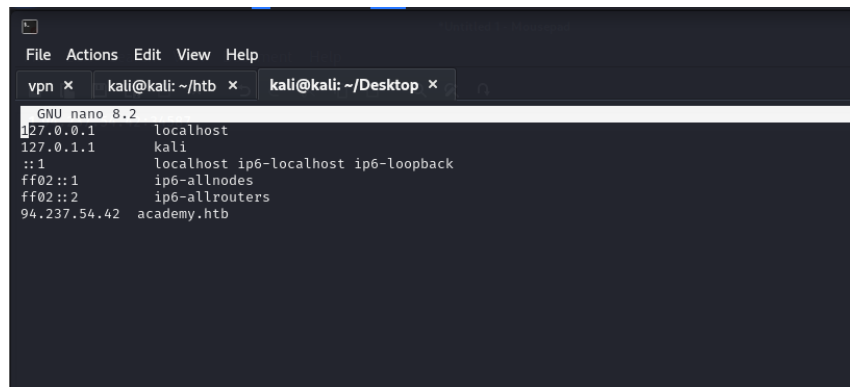


Ffuf - Skills Assessment

Target: 94.237.54.42:34587

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)

Add new IP to /etc/hosts file for the academy.htb domain



```
GNU nano 8.2
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
94.237.54.42 academy.htb
```

Running subdomain fuzzing scan on *.academy.htb

```
ffuf -u http://FUZZ.academy.htb:34587 -w /usr/share/wordlist
s/seclists/Discovery/DNS/subdomains-top1million-5000.txt
```

at the same time running vhost fuzzing using the host header on the *.academy.htb end point

```
ffuf -u http://academy.htb:34587/ -H 'Host: FUZZ.academy.htb'
-w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top
1million-5000.txt
```

```
jira      [Status: 200, Size: 985, Words: 423, Lines: 55, Duration: 90ms]
ns8       [Status: 200, Size: 985, Words: 423, Lines: 55, Duration: 92ms]
partners  [Status: 200, Size: 985, Words: 423, Lines: 55, Duration: 92ms]
ml        [Status: 200, Size: 985, Words: 423, Lines: 55, Duration: 92ms]
list      [Status: 200, Size: 985, Words: 423, Lines: 55, Duration: 91ms]
images1   [Status: 200, Size: 985, Words: 423, Lines: 55, Duration: 93ms]
business  [Status: 200, Size: 985, Words: 423, Lines: 55, Duration: 92ms]
club      [Status: 200, Size: 985, Words: 423, Lines: 55, Duration: 92ms]
update    [Status: 200, Size: 985, Words: 423, Lines: 55, Duration: 90ms]
fw        [Status: 200, Size: 985, Words: 423, Lines: 55, Duration: 90ms]
devel     [Status: 200, Size: 985, Words: 423, Lines: 55, Duration: 90ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

```
ffuf -u http://academy.htb:34587/ -H 'Host: FUZZ.academy.htb'
-w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top
1million-5000.txt -fs 985
```

```
(kali@kali)~[/htb]
$ ffuf -u http://academy.htb:34587/ -H 'Host: FUZZ.academy.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -fs 985

v2.1.0-dev

:: Method      : GET
:: URL         : http://academy.htb:34587/
:: 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

test      [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 99ms]
archive   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 91ms]
faculty   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 92ms]
:: Progress: [4989/4989] :: Job [1/1] :: 431 req/sec :: Duration: [0:00:14] :: Errors: 0 ::
```

There we find: test, archive, faculty

My subdomain scans didn't find these. I also ran the subdomain fuzzing scan with gobuster. That didn't either.

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

Add the discovered subdomains to etc/hosts

```
GNU nano 8.2
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
94.237.54.42 academy.htb test.academy.htb faculty.academy.htb archive.academy.htb
```

Fuzzing the test page for web extension types

```
ffuf -u http://test.academy.htb:34587/index.FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/web-extensions.txt
```

Doing the same for archive and faculty gave the same result: .phps, but the responses are 403 error

```
v2.1.0-dev
:: Method      : GET
:: URL         : http://faculty.academy.htb:34587/index.FUZZ
:: 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: 91ms]
:: Progress: [43/43] :: Job [1/1] :: 8 req/sec :: Duration: [0:00:05] :: Errors: 0 ::

(kali@kali)-[~/htb]
$ ffuf -u http://archive.academy.htb:34587/index.FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/web-extensions.txt

v2.1.0-dev
:: Method      : GET
:: URL         : http://archive.academy.htb:34587/index.FUZZ
:: 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: 113ms]
:: Progress: [43/43] :: Job [1/1] :: 14 req/sec :: Duration: [0:00:03] :: Errors: 0 ::

(kali@kali)-[~/htb]
$
```

Looking back after some trouble shooting I realized I appended a . to the end point in my command which was giving some problems because my word list has a . before the extension already!

```
ffuf -u http://test.academy.htb:34587/indexFUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/web-extensions.txt
```

Now we get 2 web extensions: .php and .phps (with phps still giving a 403)

```
(kali@kali)~[/htb]
$ ffuf -u http://test.academy.htb:34587/indexFUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/web-extensions.txt

v2.1.0-dev

:: Method      : GET
:: URL         : http://test.academy.htb:34587/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: 101ms]
.phps [Status: 403, Size: 284, Words: 20, Lines: 10, Duration: 3428ms]
:: Progress: [43/43] :: Job [1/1] :: 12 req/sec :: Duration: [0:00:03] :: Errors: 0 ::
```

Running the scan on the other end points faculty shows a php7 extension being allowed as well

I decreased the transparency of the terminal after seeing the bold academy in the background of that last screen shot lol

```
(kali@kali)~[/htb]
$ ffuf -u http://faculty.academy.htb:34587/indexFUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/web-extensions.txt

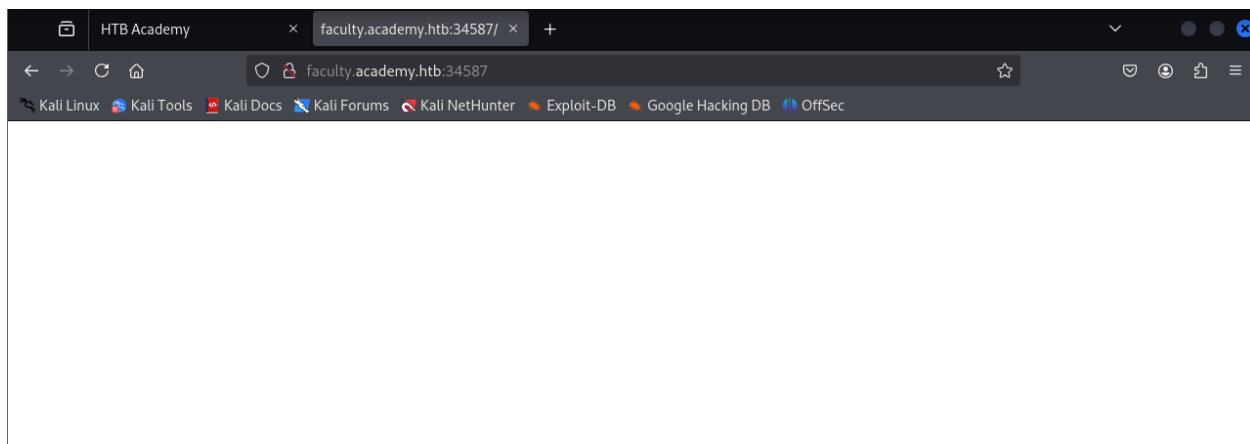
v2.1.0-dev

:: Method      : GET
:: URL         : http://faculty.academy.htb:34587/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

.php7 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 3237ms]
.phps [Status: 403, Size: 287, Words: 20, Lines: 10, Duration: 4247ms]
.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4250ms]
:: Progress: [43/43] :: Job [1/1] :: 10 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

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

Going to the end points themselves (i.e. faculty.academy.htb, test, archive) just shows a white page. So I'm assuming they now want me to perform directory fuzzing on the subdomains discovered to find pages.



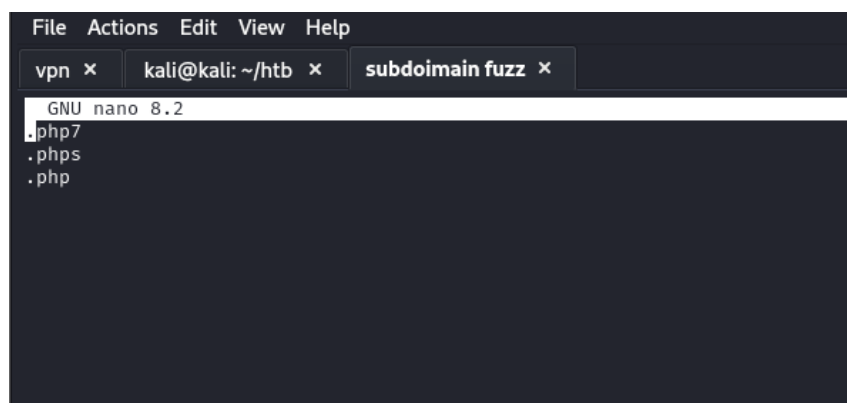
Now that I have some file extensions, fuzzing for pages

```
ffuf -u http://faculty.academy.htb:34587/FUZZ.php -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -ic -t 200
```

Running this on all 3 end points didn't find anything besides index

So at this point I took the hint, but it should've been clear to begin recursive scanning.

Make a file list of the discovered extensions



My first idea was using that list (after removing the . actually) so setup a command that would look the directory and the file extensions dynamically, but this failed because I didn't realize that in Ffuf the end of the URL needs to be the FUZZ

keyword when you are doing recursion. Technically not useful, but this is what it looked like, and the error.

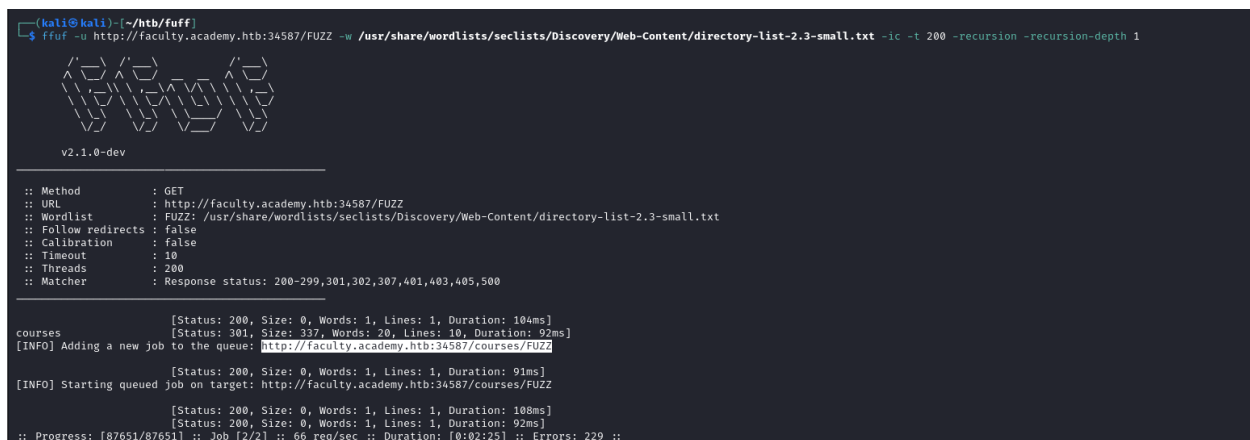
```
ffuf -u http://faculty.academy.htb:34587/list1.list2 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:list1 -ic -t 200 -w extensions.list:list2 -recursion -recursion-depth 1
```

Encountered error(s): 1 errors occurred.

* When using -recursion the URL (-u) must end with FUZZ keyword.

So my next strategy was to use recursion, and just change out the file extension manually. Starting with .php as it seemed the most common.

Running the faculty fuzz scan I find <http://faculty.academy.htb:34587/courses> and the recursive fuzzing didn't find anything past that



```
(kali@kali)~/.htb/ffuf
$ ffuf -u http://faculty.academy.htb:34587/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -ic -t 200 -recursion -recursion-depth 1

v2.1.0-dev

:: Method      : GET
:: URL         : http://faculty.academy.htb:34587/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 200
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 104ms]
courses [Status: 301, Size: 337, Words: 20, Lines: 10, Duration: 92ms]
[INFO] Adding a new job to the queue: http://faculty.academy.htb:34587/courses/FUZZ
[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 91ms]
[INFO] Starting queued job on target: http://faculty.academy.htb:34587/courses/FUZZ
[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 188ms]
[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 92ms]
:: Progress: [87651/87651] :: Job [2/2] :: 66 req/sec :: Duration: [0:02:25] :: Errors: 229 ::
```

The Archive recursive also found the courses site.

At this point I had to run some errands so, the port is updated as is the IP in my hosts file

Having found the archive.academy.htb/courses and faculty.academy.htb/courses I think fuzzing those for index.FUZZ for different file extensions could be valuable

Fuzzing the file extension types for index on archive we find php:



```

:: Method      : GET
:: URL         : http://archive.academy.htb:31177/courses/index.FUZZ
:: Wordlist     : FUZZ: /home/kali/htb/fuff/extensions.list
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

```

```
(kali㉿kali)-[~/htb/fuff]
$
```



```

:: Method      : GET
:: URL         : http://faculty.academy.htb:31177/courses/index.FUZZ
:: Wordlist     : FUZZ: /home/kali/htb/fuff/extensions.list
:: Follow redirects : false
:: Calibration  : false
:: Timeout      : 10
:: Threads      : 40
:: Matcher      : Response status: 200-299,301,302,307,401,403,405,500

```

on each of the 3 vhost

```
ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/
directory-list-2.3-small.txt -u http://test.academy.htb:3117
7/FUZZ -recursion -recursion-depth 1 -e .php,.phps,.php7 -fs
284 -ic -t 200
```

filtering for 284 here as it was the repetitive one the first time I ran this

I think repeating this step helped reframe my mind and goals after taking a step away from the lab. Eventually after much trial and error above I find:

<http://faculty.academy.htb:31177/courses/linux-security.php7>

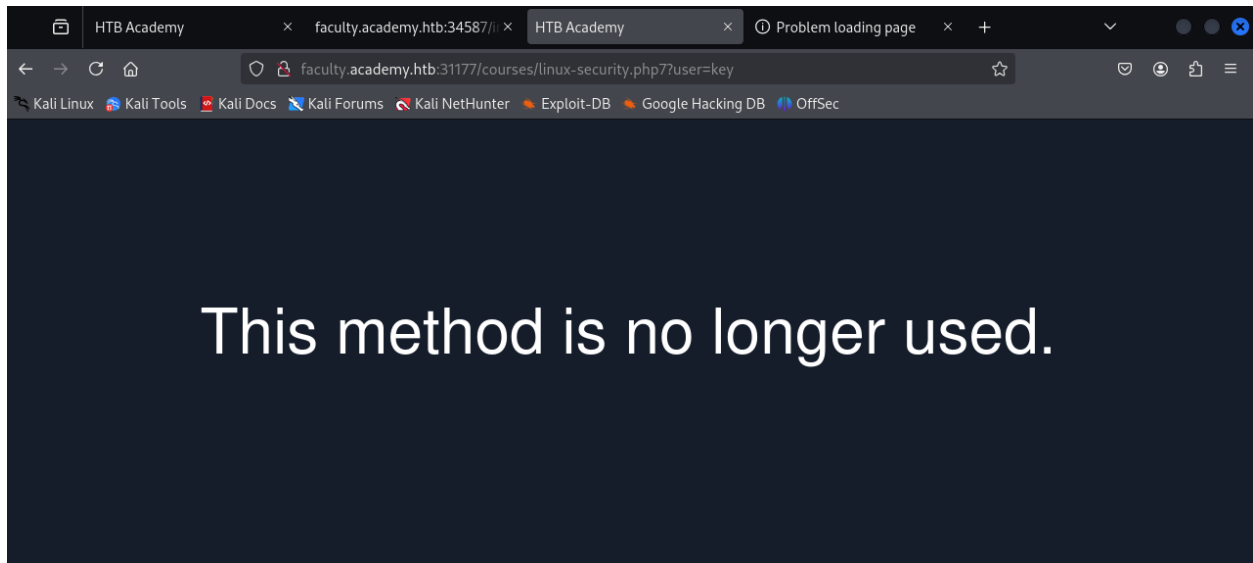
```
(kali@kali)~(/htb/ffuf)
$ ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u http://faculty.academy.htb:31177/FUZZ -recursion -recursion-depth 1 -e .php,.phps,.php7 -ic -t 200 -fs 287

v2.1.0-dev

:: Method      : GET
:: URL         : http://faculty.academy.htb:31177/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     : 200
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response size: 287

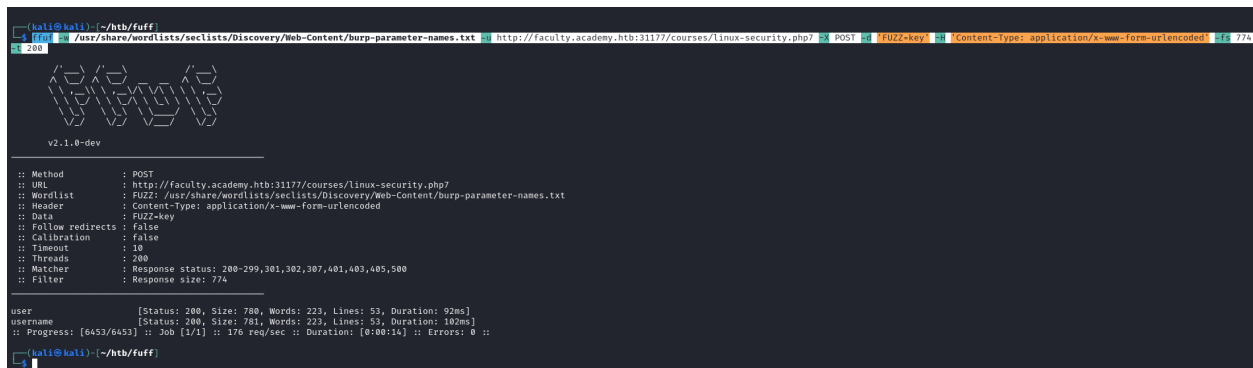
index.php      [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 9796ms]
index.php7    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 118ms]
courses      [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 133ms]
[INFO] Adding a new job to the queue: http://faculty.academy.htb:31177/courses/FUZZ
[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 92ms]
[INFO] Starting queued job on target: http://faculty.academy.htb:31177/courses/FUZZ
index.php     [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 93ms]
index.php7   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 93ms]
linux-security.php7 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 94ms]
[Status: 200, Size: 774, Words: 223, Lines: 53, Duration: 92ms]
:: Progress: [42932/350604] :: Job [2/2] :: 1529 req/sec :: Duration: [0:00:37] :: Errors: 1444 ::
```


Attempting to access the site, now I get



The question calls for multiple and fuzzing get request only found one parameter. So I fuzz post request too. Doing so I find user and username. So we have our multiple options now.

```
ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/burp-parameter-names.txt -u http://faculty.academy.htb:31177/courses/linux-security.php7 -X POST -d 'FUZZ=key' -H 'Content-Type: application/x-www-form-urlencoded' -fs 774 -t 200
```



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

content of the flag?

I initially attempted just the ids list of numbers 1-1000 and that didn't find anything, then the fact that one of the parameters was named username made me think to use a list of actual usernames.

Skimming through seclists I found one named names.txt at the following path on kali

```
/usr/share/wordlists/seclists/Usernames/Names/names.txt
```

```
ffuf -w /usr/share/wordlists/seclists/Usernames/Names/names.txt -u http://faculty.academy.htb:31177/courses/linux-security.php7 -X POST -d 'username=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 781
```



```
(kali@kali)~/.htb/ffuf
$ ffuf -w /usr/share/wordlists/seclists/Usernames/Names/names.txt -u http://faculty.academy.htb:31177/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:31177/courses/linux-security.php7
:: Wordlist     : FUZZ: /usr/share/wordlists/seclists/Usernames/Names/names.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: 92ms]
:: Progress: [10177/10177] :: Job [1/1] :: 434 req/sec :: Duration: [0:00:26] :: Errors: 0 ::
(kali@kali)~/.htb/ffuf
```

From that I found harry

Then I sent a curl post request using harry as the value in the username parameter and got the flag

```
curl http://faculty.academy.htb:31177/courses/linux-security.php7 -X POST -d 'username=harry' -H http://faculty.academy.htb:31177/courses/linux-security.php7
```