

Attacking Web Applications with Ffuf | Basic Fuzzing

Attacking Web Applications with Ffuf | Basic Fuzzing Writeup

Written By: Alexander Sapo

Directory Fuzzing

Tool Used

ffuf

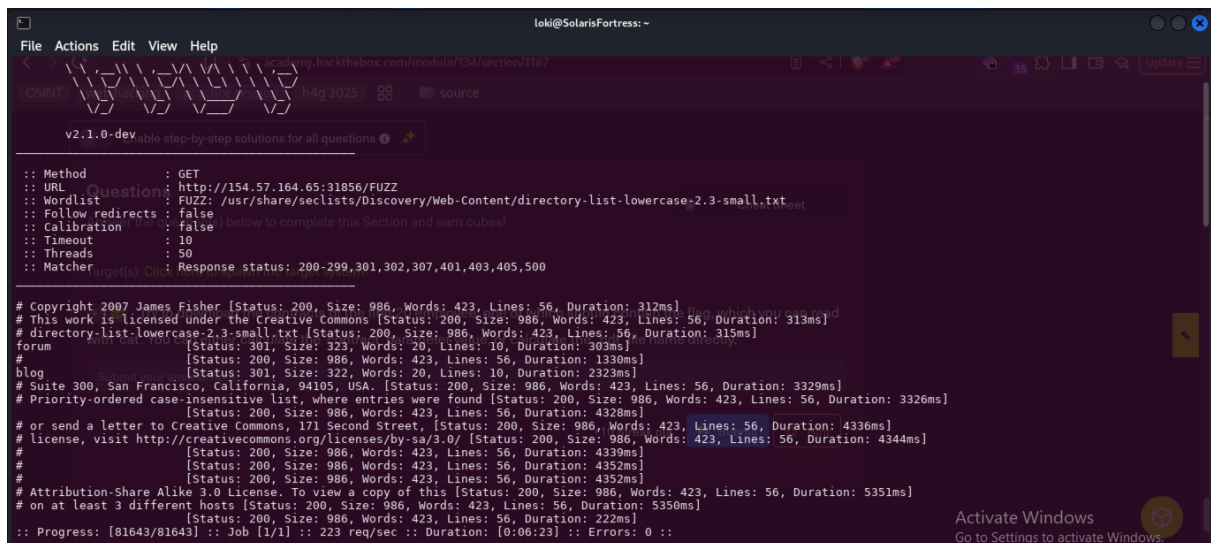
Question:

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


```
-small.txt
```

Command Execution

I pasted the target URL and executed directory fuzzing against the web root.



```
loki@SolarisFortress: ~  
File Actions Edit View Help  
academy.hackthebox.com/module/134/section/1187  
OSINT 14g 2028 55 source  
v2.1.0-devable step-by-step solutions for all questions  
Question  
:: Method : GET  
:: URL : http://154.57.164.65:31856/FUZZ  
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-small.txt  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout : 10  
:: Threads : 50  
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500  
# Copyright 2007 James Fisher [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 312ms]  
# This work is licensed under the Creative Commons [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 313ms]  
# directory-list-lowercase-2.3-small.txt [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 315ms]  
forum [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 303ms]  
# [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 1330ms]  
blog [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 2323ms]  
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3329ms]  
# Priority-ordered case-insensitive list, where entries were found [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 3326ms]  
# [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4328ms]  
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4336ms]  
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4344ms]  
# [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4339ms]  
# [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4352ms]  
# [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 4352ms]  
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 5351ms]  
# on at least 3 different hosts [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 5350ms]  
# [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 222ms]  
:: Progress: [81643/81643] :: Job [1/1] :: 223 req/sec :: Duration: [0:06:23] :: Errors: 0 ::  
Activate Windows  
Go to Settings to activate Windows.
```

Result

The following directories were discovered:

```
blog  
forum
```

Page and Extension Fuzzing

Questions

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


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?

Questions


 Cheat Sheet

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

Target(s): [Click here to spawn the target system!](#)

+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}

 Submit

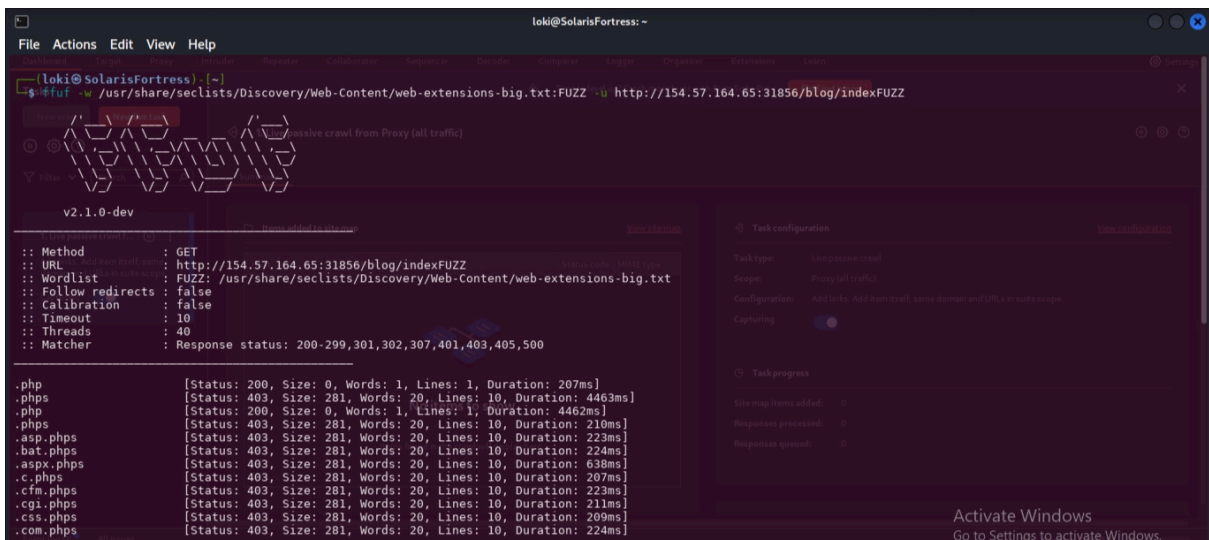
 Hint

flag: HTB{bru73_f0r_c0mm0n_p455w0rd5}

process:

Target directory: `blog`

To determine which file extension the application uses, I fuzzed possible extensions against the `index` file in the blog directory.



```
loki@SolarisFortress: ~  
File Actions Edit View Help  
[loki@SolarisFortress: ~]  
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/web-extensions-big.txt:FUZZ -u http://154.57.164.65:31856/blog/indexFUZZ  
v2.1.0-dev  
:: Method : GET  
:: URL : http://154.57.164.65:31856/blog/indexFUZZ  
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/Web-Content/web-extensions-big.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: 207ms]  
[Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 4463ms]  
[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4462ms]  
[Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 210ms]  
[Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 223ms]  
[Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 224ms]  
[Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 638ms]  
[Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 207ms]  
[Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 223ms]  
[Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 211ms]  
[Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 209ms]  
[Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 224ms]
```

Command

```
ffuf -w /opt/useful/seclists/Discovery/Web-Content/web-exte  
nsions.txt:FUZZ \
```

```
-u http://SERVER_IP:PORT/blog/indexFUZZ
```

Note

The chosen wordlist already contains the dot (.), so no additional dot is needed after `index` during fuzzing.

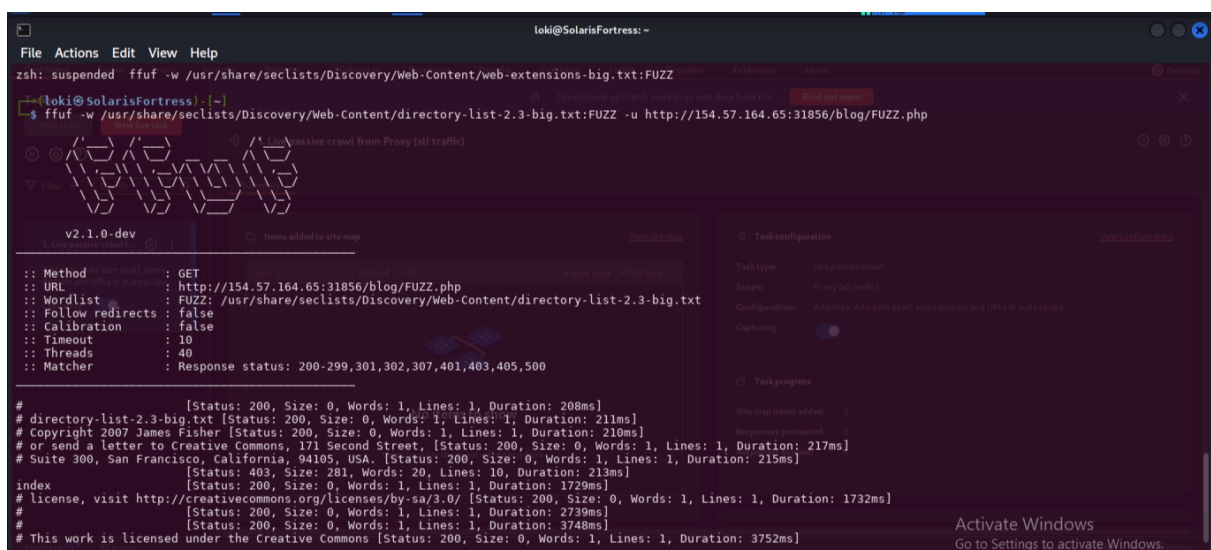
Result

The extension in use was identified as:

```
.php
```

After identifying the extension, I proceeded to fuzz for hidden pages within the `blog` directory.

Command



```
loki@SolarisFortress: ~
File Actions Edit View Help
zsh: suspended ffuf -w /usr/share/seclists/Discovery/Web-Content/web-extensions-big.txt:FUZZ
loki@SolarisFortress: ~
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt:FUZZ -u http://154.57.164.65:31856/blog/FUZZ.php

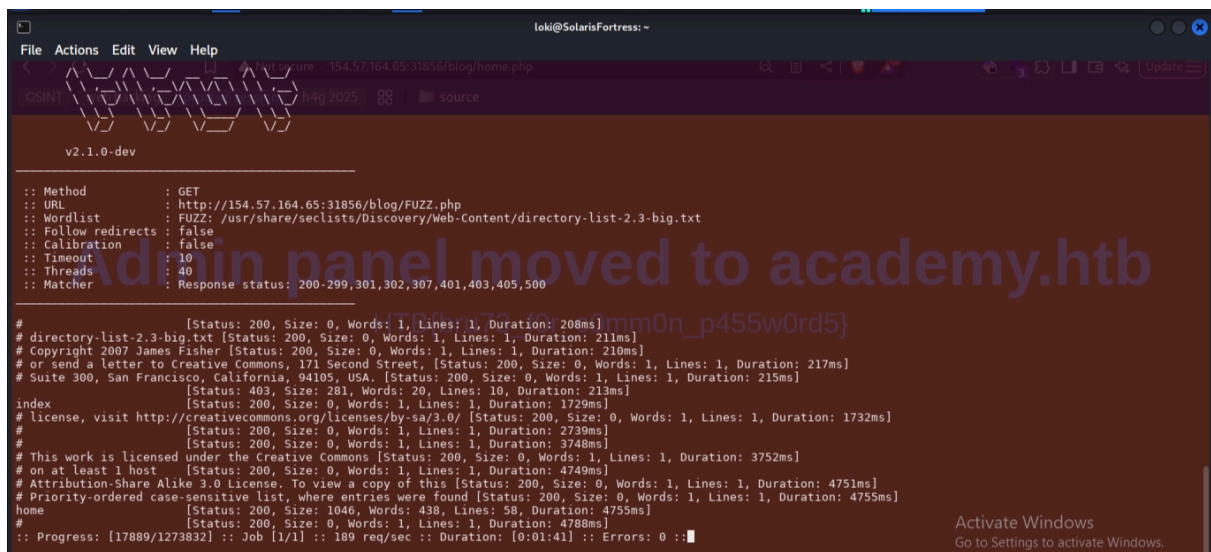
v2.1.0-dev

:: Method: GET
:: URL: http://154.57.164.65:31856/blog/FUZZ.php
:: Wordlist: FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
:: Follow redirects: false
:: Calibration: false
:: Timeout: 10
:: Threads: 40
:: Matcher: Response status: 200-299,301,302,307,401,403,405,500

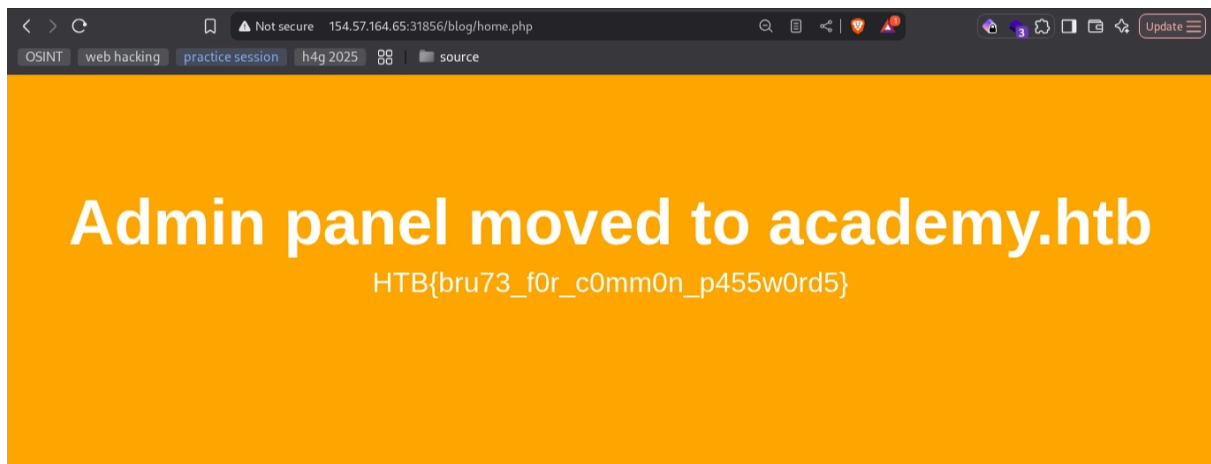
# [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 208ms]
# directory-list-2.3-big.txt [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 211ms]
# Copyright 2007 James Fisher [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 210ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 217ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 215ms]
# [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 213ms]
index [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 1729ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 1732ms]
# [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 2739ms]
# [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 3748ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 3752ms]
```

```
ffuf -w /opt/useful/seclists/Discovery/Web-Content/director
y-list-2.3-small.txt:FUZZ \
-u http://SERVER_IP:PORT/blog/FUZZ.php
```

A valid page named `home` was discovered.



When accessed in the browser:



`http://SERVER_IP:PORT/blog/home.php`

The flag was visible on the page.


Recursive Fuzzing

Question:

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?

Questions

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


 Cheat Sheet

Target(s): 154.57.164.76:31491 🚩

Life Left: 39 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_w3bl}

 Submit

 Hint

flag : HTB{fuzz1n6_7h3_w3bl}

process:

Initial command

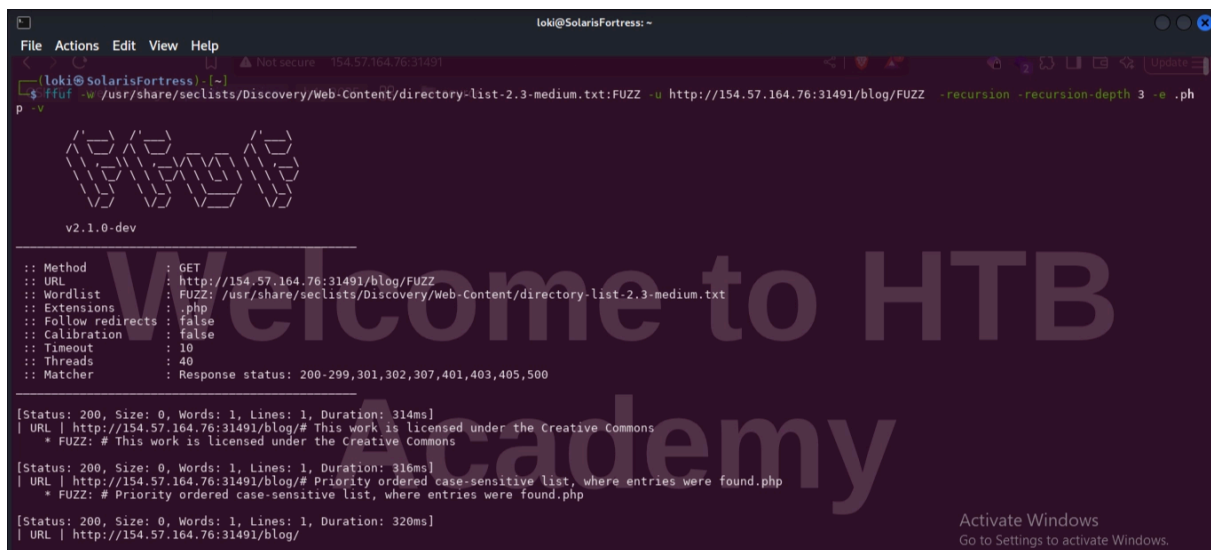
```
ffuf -w /opt/useful/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ \
-u http://SERVER_IP:PORT/FUZZ \
-recursion -recursion-depth 1 \
-e .php \
-v
```

Option breakdown

- **w** Specifies the wordlist and assigns the keyword **FUZZ**.
- **u** Target URL. **FUZZ** is replaced with each word from the wordlist.
- **recursion** Enables recursive scanning (fuzzes inside discovered directories).
- **recursion-depth 1** Limits recursion to one level deep (main directories + direct subdirectories).
- **e .php** Appends **.php** to each word (e.g., **admin** → **admin.php**).
- **v** Verbose output (shows full URLs in results).

After multiple attempts, I successfully located the flag.

I first tested the **blog** directory but did not find the flag there.

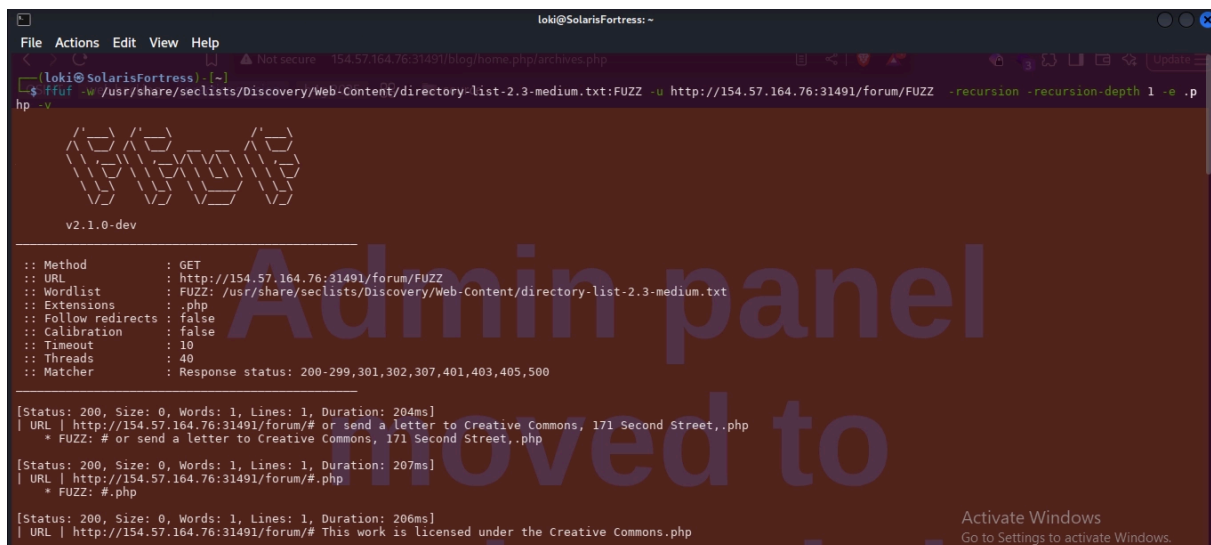


```
loki@SolarisFortress: ~  
File Actions Edit View Help  
154.57.164.76:31491  
[loki@SolarisFortress:~]$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt:FUZZ -u http://154.57.164.76:31491/blog/FUZZ -recursion -recursion-depth 3 -e .php -v  
v2.1.0-dev  
:: Method : GET  
:: URL : http://154.57.164.76:31491/blog/FUZZ  
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  
:: Extensions : .php  
:: 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: 314ms]  
| URL | http://154.57.164.76:31491/blog/# This work is licensed under the Creative Commons  
* FUZZ: # This work is licensed under the Creative Commons  
[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 316ms]  
| URL | http://154.57.164.76:31491/blog/# Priority ordered case-sensitive list, where entries were found.php  
* FUZZ: # Priority ordered case-sensitive list, where entries were found.php  
[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 320ms]  
| URL | http://154.57.164.76:31491/blog/  
Activate Windows  
Go to Settings to activate Windows.
```

Command

```
ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt:FUZZ \  
-u http://154.57.164.76:31491/blog/home.php/FUZZ \  
-recursion -recursion-depth 3 \  
-e .php \  
-v
```

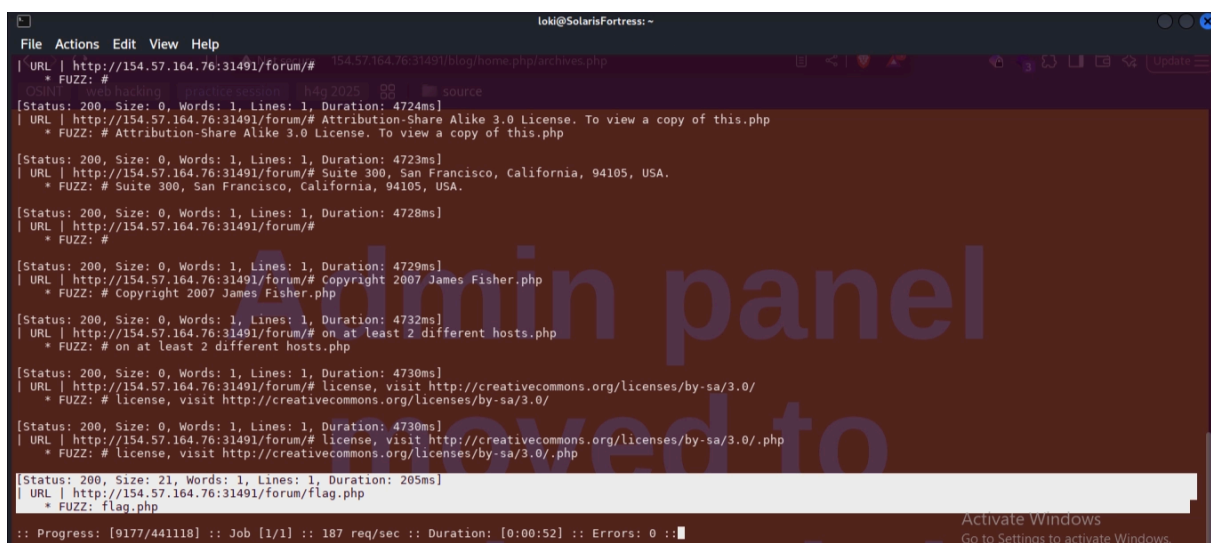
Since the blog path did not contain the flag, I proceeded to test the **forum** directory.



Command

```
ffuf -w /usr/share/seclists/Discovery/Web-Content/directory
-list-2.3-medium.txt:FUZZ \
-u http://154.57.164.76:31491/forum/FUZZ \
-recursion -recursion-depth 1 \
-e .php \
-v
```

The scan revealed `flag.php`.



```
[Status: 200, Size: 21, Words: 1, Lines: 1, Duration: 205m
s]
```

```
| URL | http://154.57.164.76:31491/forum/flag.php  
* FUZZ: flag.php
```

I then navigated to the URL in the browser:



```
http://154.57.164.76:31491/forum/flag.php
```

The flag was successfully retrieved.