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?

Vì đường dẫn /blog đã được quét ở bài **Page Fuzzing**

nên ở đây ta sẽ bắt đầu quét từ /forum

```bash

ffuf -w /root/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -u http://94.237.58.147:49864/forum/FUZZ -recursion -recursion-depth 1 -e .php -v

/'\_\_\_\ /'\_\_\_\ /'\_\_\_\

/\ \\_\_/ /\ \\_\_/ \_\_ \_\_ /\ \\_\_/

\ \ ,\_\_\\ \ ,\_\_\/\ \/\ \ \ \ ,\_\_\

\ \ \\_/ \ \ \\_/\ \ \\_\ \ \ \ \\_/

\ \\_\ \ \\_\ \ \\_\_\_\_/ \ \\_\

\/\_/ \/\_/ \/\_\_\_/ \/\_/

v2.1.0-dev

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

:: Method : GET

:: URL : http://94.237.58.147:49864/forum/FUZZ

:: Wordlist : FUZZ: /root/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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 279ms]

| URL | http://94.237.58.147:49864/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: 283ms]

| URL | http://94.237.58.147:49864/forum/#

\* FUZZ: #

[Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 284ms]

| URL | http://94.237.58.147:49864/forum/.php

\* FUZZ: .php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 288ms]

| URL | http://94.237.58.147:49864/forum/# or send a letter to Creative Commons, 171 Second Street,

\* FUZZ: # or send a letter to Creative Commons, 171 Second Street,

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 288ms]

| URL | http://94.237.58.147:49864/forum/# Attribution-Share Alike 3.0 License. To view a copy of this.php

\* FUZZ: # Attribution-Share Alike 3.0 License. To view a copy of this.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 287ms]

| URL | http://94.237.58.147:49864/forum/# license, visit http://creativecommons.org/licenses/by-sa/3.0/

\* FUZZ: # license, visit http://creativecommons.org/licenses/by-sa/3.0/

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 288ms]

| URL | http://94.237.58.147:49864/forum/# or send a letter to Creative Commons, 171 Second Street,.php

\* FUZZ: # or send a letter to Creative Commons, 171 Second Street,.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 288ms]

| URL | http://94.237.58.147:49864/forum/#

\* FUZZ: #

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 292ms]

| URL | http://94.237.58.147:49864/forum/# 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: 290ms]

| URL | http://94.237.58.147:49864/forum/# Copyright 2007 James Fisher.php

\* FUZZ: # Copyright 2007 James Fisher.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 289ms]

| URL | http://94.237.58.147:49864/forum/# on at least 3 different hosts.php

\* FUZZ: # on at least 3 different hosts.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 291ms]

| URL | http://94.237.58.147:49864/forum/# Copyright 2007 James Fisher

\* FUZZ: # Copyright 2007 James Fisher

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 292ms]

| URL | http://94.237.58.147:49864/forum/# directory-list-2.3-small.txt.php

\* FUZZ: # directory-list-2.3-small.txt.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 296ms]

| URL | http://94.237.58.147:49864/forum/#

\* FUZZ: #

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 293ms]

| URL | http://94.237.58.147:49864/forum/# on at least 3 different hosts

\* FUZZ: # on at least 3 different hosts

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 294ms]

| URL | http://94.237.58.147:49864/forum/

\* FUZZ:

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 297ms]

| URL | http://94.237.58.147:49864/forum/#.php

\* FUZZ: #.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 299ms]

| URL | http://94.237.58.147:49864/forum/#.php

\* FUZZ: #.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 301ms]

| URL | http://94.237.58.147:49864/forum/#.php

\* FUZZ: #.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 300ms]

| URL | http://94.237.58.147:49864/forum/# Attribution-Share Alike 3.0 License. To view a copy of this

\* FUZZ: # Attribution-Share Alike 3.0 License. To view a copy of this

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 299ms]

| URL | http://94.237.58.147:49864/forum/# Suite 300, San Francisco, California, 94105, USA..php

\* FUZZ: # Suite 300, San Francisco, California, 94105, USA..php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 302ms]

| URL | http://94.237.58.147:49864/forum/#

\* FUZZ: #

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 300ms]

| URL | http://94.237.58.147:49864/forum/# This work is licensed under the Creative Commons.php

\* FUZZ: # This work is licensed under the Creative Commons.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 303ms]

| URL | http://94.237.58.147:49864/forum/# Priority-ordered case-sensitive list, where entries were found

\* FUZZ: # Priority-ordered case-sensitive list, where entries were found

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 301ms]

| URL | http://94.237.58.147:49864/forum/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.php

\* FUZZ: # license, visit http://creativecommons.org/licenses/by-sa/3.0/.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 303ms]

| URL | http://94.237.58.147:49864/forum/# directory-list-2.3-small.txt

\* FUZZ: # directory-list-2.3-small.txt

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 297ms]

| URL | http://94.237.58.147:49864/forum/# 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: 298ms]

| URL | http://94.237.58.147:49864/forum/index.php

\* FUZZ: index.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 303ms]

| URL | http://94.237.58.147:49864/forum/#.php

\* FUZZ: #.php

[Status: 200, Size: 21, Words: 1, Lines: 1, Duration: 295ms]

| URL | http://94.237.58.147:49864/forum/flag.php

\* FUZZ: flag.php

```

Kết quả thu được file flag.php có size=21 còn lại các đường dẫn khác thì size =0

Sử dung curl để xem phản hồi của đường dẫn <http://94.237.58.147:49864/forum/flag.php>

```bash

curl <http://94.237.58.147:49864/forum/flag.php>

```

A screenshot of a computer

Description automatically generated

P/s: HTB{fuzz1n6\_7h3\_w3b!}