

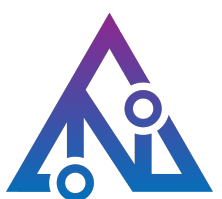
# Partial Fuzzing w/ Short Names



# Logical fuzzing of files and folders

- After running Shortname Enumeration on your target, you may end up with output like so:

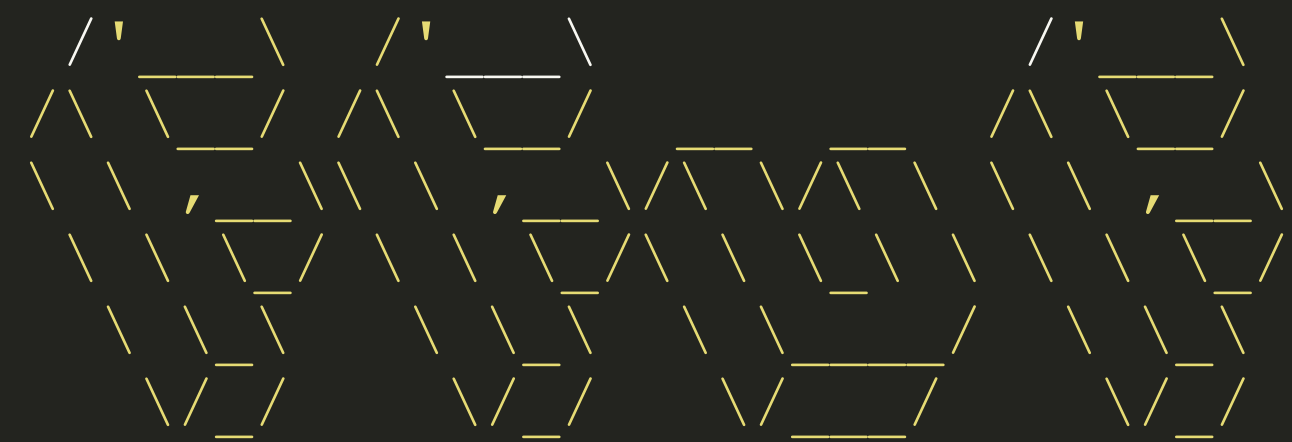
```
> go run cmd/shortscan/main.go http://redacted/
Shortscan v0.4 // an IIS short filename enumeration tool by bitquark
Target: http://redacted/
Running: Microsoft-IIS/8.5 (ASP.NET v4.0.30319)
Vulnerable: Yes!
-----
ASPNET~1          ASPNET?          ASPNET_CLIENT
LIDSDI~1          LIDSDI?
LIDSSE~1          LIDSSE?
LIDSTE~1          LIDSTE?
EASYFI~1          EASYFI?
-----
Finished! Requests: 250; Retries: 0; Sent 48277 bytes; Received 105151 bytes
```



# Logical fuzzing of files and folders

- Try and find the most logical cut off point.
- For example, for ffuf, you would put use the following fuzzing pattern:
  - LIDSDI\_\_\_\_\_ → LIDSFUZZ
  - LIDSSE\_\_\_\_\_ → LIDSFUZZ
  - EASYFI\_\_\_\_\_ → EASYFUZZ
- `./ffuf -w final_wordlist.txt -D -e asp,aspx,ashx,asmx -t 1000 -c -u http://redacted/lidsFUZZ`

```
SSH: shubs@mothership ~/w/ffuf-brute $ ./ffuf -w final_fucking_wordlist.txt -D -e asp,html,aspx,ashx,asmx \
-t 1000 -c -u http://redacted/lidsFUZZ
```



v1.1.0

```
:: Method : GET
:: URL : http://redacted/lidsFUZZ
:: Wordlist : FUZZ: final_fucking_wordlist.txt
:: Extensions : asp html aspx ashx asmx
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 1000
:: Matcher : Response status: 200,204,301,302,307,401,403
```

```
test [Status: 301, Size: 154, Words: 9, Lines: 2]
TEST [Status: 301, Size: 154, Words: 9, Lines: 2]
Test [Status: 301, Size: 154, Words: 9, Lines: 2]
display [Status: 301, Size: 157, Words: 9, Lines: 2]
Display [Status: 301, Size: 157, Words: 9, Lines: 2]
Service [Status: 301, Size: 150, Words: 9, Lines: 2]
:: Progress: [700801/700801] :: Job [1/1] :: 4800 req/sec :: Duration: [0:02:26] :: Errors: 0 ::
```