

[Énumération/Web] Cheat-sheet

Introduction

Des outils permettent l'énumération de serveur web comme **Gobuster**, **Dirbuster**, **Nikto** ou **Wfuzz**.



Gobuster

Files and directories

Voici comment utiliser gobuster pour trouver les **fichiers** et **répertoires** sur un serveur web :

```
gobuster dir -w <WORDLIST_PATH> -u <URL>
```

Subdomains

Voici comment utiliser gobuster pour trouver les **sous-domaines** sur un serveur web :

```
gobuster dns -w <WORDLIST_PATH> -u <URL>
```

Fuzzing

Voici comment utiliser gobuster pour tester des **paramètres** sur un serveur web :

```
gobuster dns -w <WORDLIST_PATH> -u <URL/<PAGE>.php?PARAMETER=FUZZ>
```

Feroxbuster

- <https://github.com/epi052/feroxbuster>

```
-- -- -- -- -- /_/_   _/_ \_/_ |/_/_   _/_ \_/_
|_| |_| |_| |_| |_| /_/_   _/_ \_/_ |/_/_   _/_ \_/_
by Ben "epi" Risher 🐼                               ver: 2.10.2
```

🎯 Target Url	http://192.168.122.127/
🚀 Threads	50
📖 Wordlist	/opt/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
💧 Status Codes	All Status Codes!
⚡ Timeout (secs)	7
☂ User-Agent	feroxbuster/2.10.2
🔍 Extract Links	true
💰 Extensions	[html, txt]
🏁 HTTP methods	[GET]
🏠 Recursion Depth	4
🌈 New Version Available	https://github.com/epi052/feroxbuster/releases/latest

🏁 Press [ENTER] to use the Scan Management Menu™

L'outil se veut être un clone de gobuster en allant plus vite et avec une interface plus agréable.

Directories

```
feroxbuster -w <WORDLIST> --url <URL>
```

Files

```
feroxbuster -w <WORDLIST> --url <URL> -x <EXT1> [EXT2]
```

Par exemple vous pouvez utiliser les options suivantes : **-x html php js txt**.

La wordlist sélectionnée doit correspondre à ce que vous cherchez (fichiers/dossiers).

WFuzz

Voici comment faire du fuzzing :

```
wfuzz -c -z file,<WORDLIST> --hc 404 <URL>
```

Revision #7

Created 11 October 2023 15:15:25 by Elieroc

Updated 28 June 2024 08:17:41 by Elieroc