Web

- [Énumération/Web] Cheat-sheet
- [Énumération/Web] LFI - RFI

[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>
```

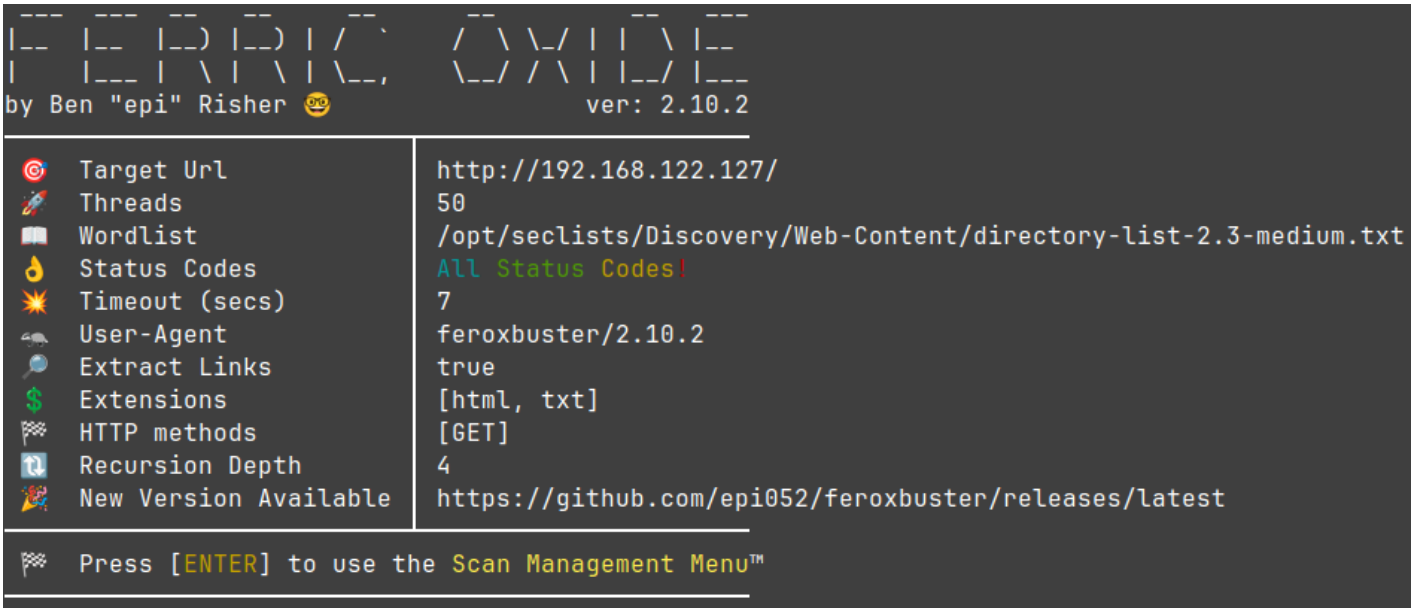
Fuzzing

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



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>
```

[Énumération/Web] LFI - RFI

Introduction

Les vulnérabilités **LFI** pour *Local File Inclusion* et **RFI** pour *Remote File Inclusion* sont très dangereuses puisqu'elles peuvent aboutir à des RCE dans certains cas ou l'affichage de fichiers systèmes comme /etc/shadow et /etc/passwd .

Ces failles reposent sur la possibilité pour l'utilisateur d'un site web de pouvoir appeler un fichier dont il ne doit pas avoir accès initialement.

Là où la LFI se contente de pouvoir appeler des fichiers locaux au serveur web, la RFI permet d'ouvrir un fichier distant.



LFI Finder Tool

Un outil très pratique qui permet d'énumérer les LFI disponibles d'une application web :

https://github.com/capture0x/LFI-FINDER