Alcapdemy:
Curso de Fuzzing Web

1.Fuzzing Web

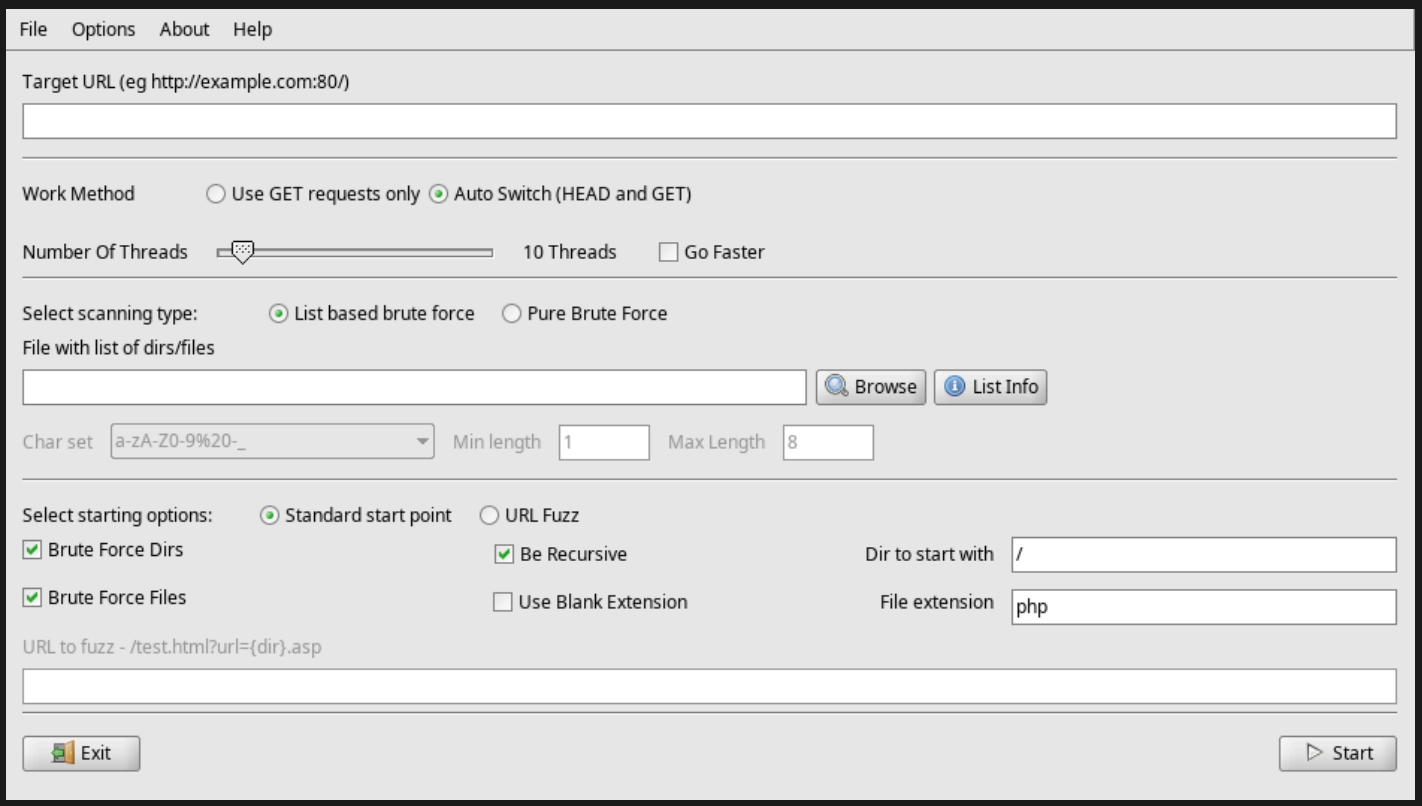
El fuzzing web es una técnica que consiste en descubrir directorios ocultos dentro de una web usando herramientas de fuerza bruta

2.Herramientas para hacer fuzzing web

-Gobuster: `gobuster dir -u https://ejemplo.com -w /usr/share/wordlists/diccionario.txt -x php,js,html`

> Dir: indica que es un ataque de directorio
> -u: indica la url
> -w: indica la ruta del diccionario
> -x: indica el tipo de archivo que quieres que busque en los directorios que encuentre (este parámetro es opcional)

-Dirbuster: esta es una herramienta con interfaz gráfica:



> Target URL: debemos de introducir la url de la página que queramos hacerle fuzzing

> Number of threads: seleccionamos la velocidad del ataque en hilos

> File with list of dirs/files: debemos de introducir la ruta del diccionario con el que vayamos a realizar el ataque

> Dir to start with: si queremos buscar más directorios dentro de un directorio, si no sabemos ningún directorio lo dejaremos como está (/)

> File extension: si queremos que dentro del directorio que encuentre, busque archivos del tipo que le indiquemos

> Start: comenzara el ataque

-Wfuzz: `wfuzz -c —-hc=404 -w /usr/share/wordlists/diccionario.txt https://ejemplo.com/FUZZ`

> -c: indica que queremos usar colores (opcional)

> -w: indica la ruta del diccionario

> url de la página: cuando pongamos la url de la página es importante poner la palabra “FUZZ” donde quieras hacer fuzzing