

# 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:

The screenshot shows the Dirbuster web application interface. At the top, there is a menu bar with 'File', 'Options', 'About', and 'Help'. Below this is a 'Target URL (eg http://example.com:80/)' input field. The 'Work Method' section has two radio buttons: 'Use GET requests only' and 'Auto Switch (HEAD and GET)'. The 'Number Of Threads' section has a slider set to 10 Threads and a 'Go Faster' checkbox. The 'Select scanning type:' section has two radio buttons: 'List based brute force' and 'Pure Brute Force'. Below this is a 'File with list of dirs/files' input field with 'Browse' and 'List Info' buttons. The 'Char set' dropdown is set to 'a-zA-Z0-9%20-\_', with 'Min length' set to 1 and 'Max Length' set to 8. The 'Select starting options:' section has two radio buttons: 'Standard start point' and 'URL Fuzz'. There are four checkboxes: 'Brute Force Dirs', 'Be Recursive', 'Brute Force Files', and 'Use Blank Extension'. The 'Dir to start with' input field is set to '/', and the 'File extension' input field is set to 'php'. At the bottom, there is a 'URL to fuzz - /test.html?url={dir}.asp' input field. The interface has an 'Exit' button on the bottom left and a 'Start' button on the bottom right.

> 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