

# Enumeración de aplicaciones web

## Gobuster

Escaner de directorios, es veloz pero las búsquedas no son recursivas. Tiene 4 modos:

- dir: Busca directorios por fuerza bruta
- dns: Modo de fuerza bruta para enumeración de subdominios DNS
- vhost: modo de fuerza bruta de host virtual o enumeración de hosts virtuales.
- s3: Enumeración de fuerza bruta en depósitos S3 de AWS

## Burp Suite

Reune herramientas especializadas en pruebas de penetración de aplicaciones web. Hay 2 versiones:

- Community edition (KALI): actua como porxi http para interceptar tráfico de red, permite analizar, modificar, aceptar o rechazar todas las solicitudes y respuestas de la aplicación
- Professional (PortSwigger): Software de pago que también incluye:
  - Escáner de tipos de vulnerabildiades web
  - Módulo spider para detección de contenido indexado
  - Programas para hacer fuzzing
  - Funciones colaborativas

Burp Suite contiene las siguientes herramientas:

- Target: Permite fijar un objetivo y construir un siteMap a partir de el.
- Proxy: Proxi entre el navegador e internet que permite einterceptar peticiones e inspeccionar el tráfico
- Intruder: Permite automatizar procesos
  - Fuzzing de aplicaciones
  - Ataques de fuerza bruta
  - Ataques SQLi
  - XSS
  - Enumeración de usuarios y directorios
- Repeater: Permite manipular peticiones interceptadas, modificando parámetros y cabeceras.
- Sequencer: Permite analizar la aleatoriedad de los tokens de sesión. Útil para obtener cookies y tokens CSRF por fuerza bruta
- Decoder: Utilizado para codificar y decodificar parámetros, URLs y hashes.

From:

<http://knoppia.net/> - **Knoppia**

Permanent link:

[http://knoppia.net/doku.php?id=master\\_cs:int:tm6v2](http://knoppia.net/doku.php?id=master_cs:int:tm6v2)

Last update: **2026/05/18 18:19**



