Nikto

Nikto es una escaner de vulnerabilidades Open Source o de fuente abierta, el cual está escrito en el lenguaje Perl.

proporciona la capacidad de escanear servidores web en busca de vulnerabilidades. Realiza más de 6,400 verificaciones por archivos o scripts potencialmente peligrosos, realiza 1,200 pruebas para versiones desactualizadas de servidores, y verifica cerca de 300 problemas específicos a versiones de servidores web.

Para ejecutarlo ponemos: nikto -h 10.10.10.128 -p8080

CMSeek

Detección básica de CMS de más de 20 CMS

Exploraciones avanzadas de WordPress – Detecta la versión, usuarios, busca vulnerabilidades de versión y mucho más.

Sistema modular de fuerza bruta – Utiliza módulos de fuerza bruta pre-hechos y lo mejor es que puedes crear tu propio módulo.

Instalación y uso

git clone https://github.com/Tuhinshubhra/CMSeeK

cd CMSeeK

python3 cmseek.py - es para entrar en el menú

si queremos realizar la búsqueda desde la consola sin entrar en el menú

cmseek -u 192.168.0 .50 --random-agent

Cada escaneo se guarda dentro de la carpeta Result

LFI – Local file inclusión

Esta técnica consiste en incluir ficheros locales, es decir, archivos que se encuentran en el mismo servidor de la web con este tipo de fallo.

Tenemos que encontrar la vulnerabilidad y explotarla.