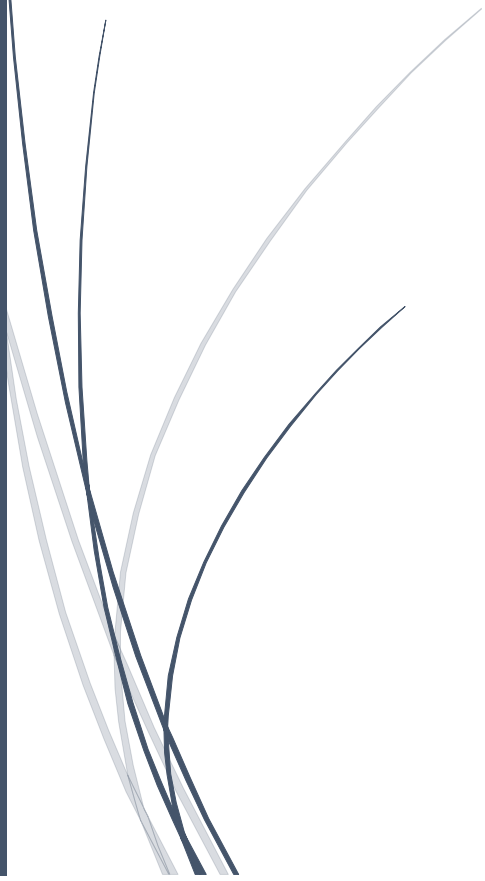
25-10-2016

Comparativo.

Escáner de vulnerabilidades en DRUPAL. (DruSpawn)

PBSC 10ª generación.



- Fernando Castañeda G.

Comparativo de herramientas en el mercado.

Nombre	URL	Características.
Drupal Security Scan	https://hackertarget.com/drupal-security-scan/	Se trata de una herramienta en línea, su funcionamiento consiste en ingresar el objetivo a escanear en un formulario. Muestra: • Si se trata de una instalación de Drupal. • Directorios expuestos. • Reputación del sitio en google. • Prueba una cuenta de administrador. • Muestra los archivos js • Muestra iframes en la página. No genera reportes descargables.
Droopescan	https://github.com/droope/droopescan	Hace una enumeración a partir de un escaneo a un CMS, puede detectar instalaciones de Drupal, Wordpress y Joomla. Muestra: • Versión. • Temas y módulos. • Archivos de configuración comunes. No incluye más funcionalidades, y no genera un reporte además de lo que se muestra en la terminal.
Drupalscan	https://raz0r.name/drupalscan/	Hace una enumeración a partir de un escaneo a instalaciones de Drupal. Muestra: • Versión. • Temas y módulos. • Archivos de configuración comunes. Solo funciona con versiones de Drupal 6 para atrás, no genera reportes.
CMSmap	https://github.com/dionach/CMSmap	Hace una enumeración a partir de un escaneo a un CMS, puede detectar instalaciones de Drupal, Wordpress y Joomla. Muestra: • Módulos y temas. • Versiones • Ataques de fuerza bruta. • Genera un reporte en texto plano • Se puede seleccionar un user agent especifico.

		• Capacidad de escanear diversos objetivos. Esta herramienta es de las mejores disponibles.
Version Check Extension.	http://www.whitefirdesign.com/version-check?pk_campaign=VC-Chrome	Extensión de google Chrome que averigua el tipo de CMS, su versión aproximada y si se encuentra actualizado. Tiene un costo de 630 MXN.
DruSpawn	https://github.com/f99942/DruSpawn	Herramienta por medio de línea de comandos que escanea instalaciones de Drupal con el fin de evaluar su seguridad. Muestra: • Versión del CMS así como vulnerabilidades para la versión. • Directorios y archivos de configuración expuestos. • Módulos y temas, así como vulnerabilidades de existir para módulos y temas encontrados. • CVEs para vulnerabilidades encontradas. • Implementación de proxy. • Implementación de tor como proxy. • Generación de reportes en formato HTML. • Referencias a las vulnerabilidades para implementar solución en el reporte. • Scripts de ataque de diccionario y denegación de servicio por xmlrpc • Capacidad de extensión de la herramienta a través de scripts programados por el usuario. • Generación de base de datos de vulnerabilidades de Drupal durante la instalación. • Fácil instalación. • Compatible con diversas distribuciones de GNU/Linux • Documentación incluida en el repositorio.