Instalación DVWA en nuestra Kali

Nos convertimos en root

Entramos en /var/www/html

git clone https://github.com/digininja/DVWA.git

Le damos permisos 777 a todo el directorio: chmod -R 777 DVWA

Entramos dentro del directorio DVWA y en el subdirectorio config

Cambiamos el nombre del archivo que hay dentro por config.inc.php

Editamos el archivo y ponemos en db_user un usuario y en db_password una contraseña que nos acordemos.

Inicializamos mysql

Entramos como usuario root a mysql

Creamos un usuario con el nombre que pusimos en el archivo config y su contraseña: create user 'miguel'@'127.0.01' identified by '123456';

Ahora le damos todos los permisos a ese usuario:

grant all privileges on dvwa.* to 'miguel'@'127.0.0.1' identified by '123456';

Ahora vamos a configurar php: cd /etc/php

Nos metemos en el directorio de la versión que tenga.

Nos metemos en el directorio apache2

Editamos php.ini y modificamos allow_url_include = on

Arrancamos apache2

Y ya ponemos en la barra de direcciones del mozilla en directorio/setup.php

WPScan

Wpscan y la --url opción y especifique la URL del sitio de WordPress para escanearlo con WPScan.
wpscan --url http://ejemplo.com

Si un sitio web ha hecho un buen trabajo ofuscando su información de WordPress, WPScan puede decirnos que no se está ejecutando wordpress, para obligar a WPScan a escanearlo de todas formas usams:
wpscan --url http://ejemplo.com –force

Algunos sitios también pueden cambiar sus complementos predeterminados o directorios de contenido wp. Para ayudar a WPScan a encontrar estos directorios, puede especificarlos manualmente con las opciones --wp-content-diry . --wp-plugins-dirHemos completado un par de directorios de ejemplo a continuación, así que asegúrese de reemplazarlos.

wpscan --url http://example.com --force --wp-content-dir newcontentdir --wp-plugins-dir newcontentdir/apps

Escanear temas vulnerables: Te permitirá escanear todos los temas y plugin instalados, para analizar si alguno de ellos tiene alguna vulnerabilidad ya conocida.
wpscan --url http(s)://tu-dominio.com -e vt

Escanear usuarios: Te hará una enumeración con todos los usuarios encontrados en el Wordpress de la víctima.
wpscan --url http(s)://your-domain.com --enumerate u

Fuerza Bruta para obtener las contraseñas de los usuarios:
wpscan --url http(s)://your-domain.com -e u –passwords /usr/share/wordlist/rockyou.txt