

# REPORTE DE VULNERABILIDADES

## EN WORDPRESS

### Escaneo de Nmap en busca de vulnerabilidades:

```
(kali㉿kali)-[~]
└─$ nmap -sV 10.0.2.15 --script=vuln
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-10 21:26 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00097s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.62 ((Debian))
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Apache/2.4.62 (Debian)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-enum:
|   /wordpress/: Blog
|_  /wordpress/wp-login.php: Wordpress login page.
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Del escaneo de Nmap, se pueden extraer varias conclusiones:

1. Se encontró un puerto abierto, específicamente el puerto 80/tcp que está ejecutando el servicio HTTP con Apache httpd 2.4.62 (Debian).
2. Enumeración de HTTP:
  - /wordpress/: Se detectó la presencia de un blog de WordPress.
  - /wordpress/wp-login.php: Se detectó la página de inicio de sesión de WordPress.

### Conclusiones y Potenciales Vulnerabilidades

- **El Servidor:** La versión detectada (2.4.62) es reciente, pero siempre es bueno verificar si hay vulnerabilidades disponibles.
- **Seguridad en WordPress:** Aunque no se han detectado vulnerabilidades en el escaneo de Nmap, la presencia de WordPress nos indica que es importante realizar un análisis de vulnerabilidades en plugins y temas. Es importante realizar un escaneo más profundo y específico en WordPress, buscando versiones vulnerables de plugins o configuraciones inseguras.

## Objetivo del Escaneo de WordPress

URL Escaneada	IP del Objetivo
http://10.0.2.15/wordpress/	10.0.2.15

## Vulnerabilidades Detectadas

### 1. XML-RPC Habilitado

Descripción	Impacto	Ubicación
El archivo xmlrpc.php permite realizar llamadas remotas a la API de WordPress, lo que puede ser explotado para:	<ul style="list-style-type: none"><li>- Ataques de fuerza bruta</li><li>- Amplificación DDoS</li></ul>	http://10.0.2.15/wordpress/xmlrpc.php

### 2. Archivo readme.html Expuesto

Descripción	Impacto	Ubicación
El archivo readme.html expone información sobre la versión de WordPress utilizada.	Facilita ataques dirigidos basados en vulnerabilidades conocidas de esa versión.	http://10.0.2.15/wordpress/readme.html

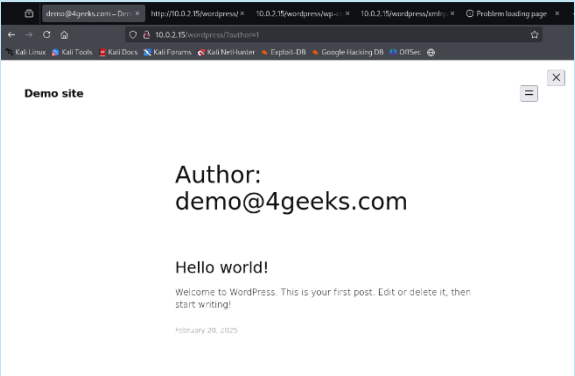
### 3. WP-Cron Habilitado

Descripción	Impacto	Ubicación
wp-cron.php gestiona tareas programadas en WordPress, pero puede ser utilizado en ataques DDoS.	Consumir recursos del servidor, afectando el rendimiento del sitio.	http://10.0.2.15/wordpress/wp-cron.php

4. Página de Inicio de Sesión Predeterminada

Descripción	Impacto	Ubicación
La página de inicio de sesión /wp-login está en su ruta por defecto, lo que facilita ataques de fuerza bruta.	Incrementa el riesgo de accesos no autorizados si se descubren credenciales válidas.	http://10.0.2.15/wordpress/wp-login

5. Usuarios expuestos

Descripción	Impacto	Ubicación
La enumeración de usuarios permite descubrir nombres de usuario válidos al solicitar la URL con el parámetro “?author=X”. Si el usuario existe, el servidor responde con una dirección válida que incluye el nombre del usuario	Facilita ataques de fuerza bruta al conocer los nombres de usuario válidos	http://10.0.2.15/wordpress/?author=1 

Versiones Detectadas

Versión de WordPress	Fecha de Lanzamiento	Estado	Método de Detección
6.7.2	11 de febrero de 2025	Última	curl -s -X GET http://10.0.2.15/wordpress/   grep '<meta name="generator"'

## Recomendaciones

Recomendación	Acción Sugerida
<b>Deshabilitar XML-RPC</b>	Utilizar un plugin de seguridad o añadir reglas en el archivo .htaccess para bloquear su acceso.
<b>Eliminar o restringir el acceso a readme.html</b>	Eliminar este archivo o hacerlo inaccesible desde el público.
<b>Proteger el acceso a WP-Cron</b>	Limitar el acceso a wp-cron.php o deshabilitarlo si no es necesario.
<b>Ocultar la página de inicio de sesión</b>	Cambiar la URL /wp-admin utilizando un plugin como <b>WPS Hide Login</b> .
<b>Fortalecer la seguridad de cuentas</b>	Habilitar contraseñas fuertes, 2FA y limitar intentos de inicio de sesión.
<b>Mantener todo actualizado</b>	Garantizar que WordPress, plugins y temas estén siempre actualizados con las últimas versiones.