Debian

INFORME DE VULNERABILIDADES

MIÉRCOLES, 7 DE MAYO DE 2025

CONTROL DE DOCUMENTO

Versión	Fecha	Autor	Descripción
1.0	05/07/2025	Javier Pérez, Moisés Adamuz	Versión Inicial

ÍNDICE

INFORMACIÓN GENERAL

ALCANCE

4geeks nos ha ordenado realizar pruebas de seguridad en el siguiente alcance:

- Validación de la robustez de contraseñas en servicios SSH mediante ataques de fuerza bruta.
- Evaluación de mecanismos de autenticación en WordPress y control de contraseñas.
- Revisión de la exposición de archivos de configuración sensibles como wp-config.php.
- Verificación de seguridad en el acceso remoto y modificación de parámetros del sitio WordPress.
- Inspección de la posibilidad de modificación directa de la base de datos WordPress.
- Análisis de la exposición de usuarios mediante enumeración con herramientas como WPScan.
- Revisión de mecanismos anti-brute force en el acceso al panel de WordPress.

ORGANIZACIÓN

Las actividades de prueba se realizaron entre 01/05/2025 y 05/05/2025.

RESUMEN EJECUTIVO

Durante el ejercicio de evaluación de seguridad realizado sobre la máquina objetivo, se identificaron múltiples vectores de ataque que permitieron el compromiso completo del sistema y del entorno WordPress instalado.

En primer lugar, un escaneo de red reveló servicios expuestos, entre ellos un servicio SSH vulnerable a ataques de fuerza bruta. Aprovechando esta debilidad, se logró acceder como usuario `root` mediante credenciales débiles.

Una vez con acceso privilegiado al sistema, se detectaron configuraciones inseguras en la aplicación WordPress. Fue posible acceder al archivo `wp-config.php`, exponiendo las credenciales de base de datos. A través de estas, se modificó directamente la contraseña del usuario administrador del CMS, lo que permitió acceso completo al panel de administración.

Además, se observó la capacidad de enumerar usuarios válidos de WordPress sin restricciones, y la ausencia de mecanismos efectivos de defensa contra ataques de fuerza bruta en el login de WordPress.

Principales vulnerabilidades identificadas:

- Acceso root por fuerza bruta vía SSH.
- Exposición de credenciales en `wp-config.php`.
- Modificación directa de la contraseña del administrador en la base de datos.
- Configuración remota del dominio WordPress.
- Enumeración de usuarios del CMS.
- Ausencia de protección ante intentos de autenticación repetidos.

Estas vulnerabilidades, combinadas, permitieron comprometer completamente el servidor, alterar su funcionamiento, y tomar control de la aplicación web.

RESUMEN DE VULNERABILIDADES

Se han descubierto las siguientes vulnerabilidades

Criticidad	ID	Vulnerabilidad	Ámbito afectado
Critical	IDX-002	Acceso root por fuerza bruta vía SSH	Servidor SSH
Medium	VULN-005	WordPress para acceso remoto	CMS Wordpress
Medium	VULN-003	Cambio directo en base de datos WordPress	Base de datos MySQL.
Medium	VULN-001	Acceso a credenciales vía wp-config.php	CMS Wordpress
Medium	VULN-006	Enumeración de usuarios	CMS Wordpress
Low	IDX-004	Intento fallido contra WordPress	CMS Wordpress

DETALLES TÉCNICOS

WORDPRESS PARA ACCESO REMOTO

CVSS	Medium		CVSSV3 SCORE	6.0
CVSSV3 CRITERIOS	Attack Vector :	**Local**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**High**
	Required Privileges :	**High**	Integrity :	**High**
	User Interaction :	**None**	Availability :	**None**
ÁMBITO AFECTADO	CMS Wordpress			
DESCRIPCIÓN	Tras acceder como root, se editó el archivo wp-config.php de WordPress para permitir la administración remota desde otra máquina de la red.			
OBSERVACIÓN	Se configuró el sitio para que respondiera a peticiones desde otra IP ('192.168.1.54'), lo cual facilitó el acceso al panel de administración.			
DETALLES				
REMEDIACIÓN	Revisar periódicamente los archivos críticos de configuración de WordPress. Usar sistemas de monitorización de integridad de archivos (FIM).			
REFERENCIAS	CWE-264: Permissions, Privileges, and Access Controls https://wordpress.org/support/article/editing-wp-config-php/			

ACCESO ROOT POR FUERZA BRUTA VÍA SSH

CVSS	Critical		CVSSV3 SCORE	9.8
CVSSV3 CRITERIOS	Attack Vector :	**Network**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**High**
	Required Privileges :	**None**	Integrity :	**High**
	User Interaction :	**None**	Availability :	**High**
ÁMBITO AFECTADO	Servidor SSH			
DESCRIPCIÓN	Se obtuvo acceso como root mediante un ataque de fuerza bruta con Hydra, explotando el uso de contraseñas débiles en el servicio SSH.			

Observación	El usuario root tenía configurada una contraseña débil ('123456'). Hydra logró autenticarse exitosamente a través del puerto 22 (SSH).
Detalles	
Remediación	Deshabilitar acceso SSH directo a root, implementar autenticación por clave pública, establecer políticas de contraseñas robustas y utilizar firewalls para restringir accesos SSH.
Referencias	CWE-521: Weak Password Requirements https://owasp.org/www-community/attacks/Brute_force_attack

Cambio directo en base de datos WordPress

CVSS	**Medium**		**CVSSv3 Score**	**6.7**
CVSSv3 criterios	Attack Vector :	**Local**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**High**
	Required Privileges :	**High**	Integrity :	**High**
	User Interaction :	**None**	Availability :	**High**
Ámbito Afectado	Base de datos MySQL.			
Descripción	Modificación de contraseña del usuario administrador mediante consulta SQL directa.			
Observación	La contraseña fue cambiada directamente desde la base de datos usando una consulta SQL, lo que permitió burlar los mecanismos normales de autenticación.			
Detalles				
Remediación	Control de integridad de base de datos, monitoreo de cambios en las tablas de usuarios y habilitar mecanismos de alerta.			
Referencias	CWE-269: Improper Privilege Management https://wordpress.org/support/article/resetting-your-password/#through-phpmyadmin			

Intento fallido contra WordPress

CVSS	**Low**		**CVSSv3 Score**	**3.7**
CVSSv3 criterios	Attack Vector :	**Network**	Scope :	**Unchanged**
	Attack Complexity :	**High**	Confidentiality :	**Low**
	Required Privileges :	**None**	Integrity :	**None**
	User Interaction :	**None**	Availability :	**None**

Ámbito Afectado	CMS Wordpress
Descripción	Ataque de fuerza bruta fallido sobre el usuario wordpress-user.
Observación	El sistema respondió con códigos HTTP 200/302 sin indicios de bloqueo de IP ni detección de múltiples intentos.
Detalles	
Remediación	Implementar rate-limiting, captcha, bloqueo temporal y monitoreo de accesos sospechosos.
Referencias	CWE-307: Improper Restriction of Excessive Authentication Attempts https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

Acceso a credenciales vía wp-config.php

CVSS	**Medium**		**CVSSv3 Score**	**6.0**
CVSSv3 criterios	Attack Vector :	**Local**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**High**
	Required Privileges :	**High**	Integrity :	**High**
	User Interaction :	**None**	Availability :	**None**
Ámbito Afectado	CMS Wordpress			
Descripción	Se accedió al archivo wp-config.php que contenía las credenciales de acceso a la base de datos.			
Observación	El archivo wp-config.php era accesible desde el entorno con privilegios root, lo cual permitió obtener usuario, contraseña y nombre de la base de datos.			
Detalles				
Remediación	Restringir permisos de archivos críticos, aplicar políticas de mínimo privilegio y usar variables de entorno para credenciales.			
Referencias	CWE-538: Insertion of Sensitive Information into Log File / Config File https://wordpress.org/support/article/hardening-wordpress/#securing-wp-config-php			

Enumeración de usuarios

CVSS	**Medium**		**CVSSv3 Score**	**5.3**
CVSSv3 criterios	Attack Vector :	**Network**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**Low**

	Required Privileges :	**None**	Integrity :	**None**
	User Interaction :	**None**	Availability :	**None**
ÁMBITO AFECTADO	CMS Wordpress			
DESCRIPCIÓN	Enumeración de usuarios válidos a través de WPScan.			
OBSERVACIÓN	El sitio web no bloqueaba la enumeración de usuarios, lo que permitió obtener nombres de usuarios válidos.			
DETALLES				
REMEDIACIÓN	Restringir el listado de usuarios, bloquear endpoints de enumeración, implementar detección de escaneos.			
REFERENCIAS	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor https://owasp.org/www-community/attacks/Enumeration			