

Informe de Vulnerabilidad

Permisos incorrectos en wp-config.php

WordPress - Archivo de configuración con credenciales de base de datos

Fecha del registro: 8 de enero de 2026 (America/New_York)

Sistema: Debian (VM) - Ruta analizada: /var/www/html/wp-config.php

Objetivo

Verificar si el archivo **wp-config.php**, que contiene credenciales críticas de la base de datos, está expuesto a usuarios no autorizados por permisos demasiado permisivos; y documentar la evidencia antes y después de la corrección.

Comandos utilizados

```
sudo find /var/www -name wp-config.php -type f 2>/dev/null
sudo ls -l /var/www/html/wp-config.php
sudo stat /var/www/html/wp-config.php
sudo namei -l /var/www/html/wp-config.php
```

Hallazgos

Elemento	Antes (vulnerable)	Después (corregido)
wp-config.php	0777 (-rwxrwxrwx) Propietario: www-data Grupo: www-data	0640 (-rw-r-----) Propietario: root Grupo: www-data
/var/www/html	0777 (drwxrwxrwx) (Escritura pública)	0755 (drwxr-xr-x) (Sin escritura pública) (según namei -l)

Evidencia - Antes

Salida relevante (resumen):

```
-rwxrwxrwx 1 www-data www-data 3017 Sep 30 2024 /var/www/html/wp-config.php
Access: (0777/-rwxrwxrwx)  Uid: ( 33/www-data)   Gid: ( 33/www-data)

f: /var/www/html/wp-config.php
drwxr-xr-x root    root    /
drwxr-xr-x root    root    var
drwxr-xr-x root    root    www
drwxrwxrwx www-data www-data html
-rwxrwxrwx www-data www-data wp-config.php
```

Impacto / Riesgo

Confidencialidad: con 0777, cualquier usuario local podía leer credenciales (DB_USER/DB_PASSWORD) y otros secretos del sitio.

Integridad: con escritura pública, un usuario no autorizado podía modificar **wp-config.php** e inyectar código o alterar la configuración.

Superficie de ataque: permisos 0777 en el directorio del sitio facilitan la manipulación de archivos web y el compromiso del servicio.

Corrección aplicada

```
sudo chown root:www-data /var/www/html/wp-config.php
sudo chmod 640 /var/www/html/wp-config.php
sudo chmod 755 /var/www/html
```

Evidencia - Después

Salida relevante (verificación):

```
-rw-r----- 1 root www-data 3017 Sep 30 2024 /var/www/html/wp-config.php
Access: (0640/-rw-r-----)  Uid: (  0/   root)   Gid: ( 33/www-data)

f: /var/www/html/wp-config.php
drwxr-xr-x root    root    /
drwxr-xr-x root    root    var
drwxr-xr-x root    root    www
drwxr-xr-x www-data www-data html
-rw-r----- root    www-data wp-config.php
```

Conclusión

La vulnerabilidad quedó confirmada por permisos 0777 en **wp-config.php** y en el directorio **/var/www/html**.

Tras ajustar propietario y permisos a 0640 (root:www-data) y restringir el directorio a 0755, el archivo sensible deja de ser accesible/modificable por usuarios no autorizados, reduciendo significativamente el riesgo de exposición y manipulación de credenciales.