

WordPress, webinar seguridad

- Nominalia: <https://www.escueladeinternet.com/>
- <https://www.escueladeinternet.com/seguridad-wordpress-hackeo>

vulnerabilidades

- en themes o plugins
- en núcleo WP
- PHP → versión > 8.1
- robo credenciales/suplantación
- fugas de información (logs de error que exponen información sensible)

Amenazas

- Malware y puertas traseras
- DDOS y fuerza bruta
- inyección SQL
- XSS
- subidas de ficheros no controladas
- secuestro de sesiones (no https o mal configurado)
- redirecciones maliciosas
- ataques por IA

prácticas recomendadas

- Actualizar core, plugins, temas...
 - eliminar aquellos que no se usan (el código PHP está ahí)
 - no instalar plugins abandonados (más de 9 meses sin actualizarse)
- Instalar de sitios oficiales o confiables
- PHP 8.1
- acceso seguro
 - limitar número de accesos erróneos
 - 2FA
 - cambiar usuario «admin»
 - contraseñas largas y únicas
 - roles apropiados
- sistema de archivos
 - 664 archivos
 - 600 wp-config.php
 - 400 .htaccess
 - 755 carpetas
 - desactivar feed rss y atom
 - desactivar XML-RPC
 - ocultar versión WP
 - borrar archivos de identificación de WP (readme, license)
 - deshabilitar la exploración de directorios
- Debug y log de errores
 - desactivar por defecto
 - wp-config.php

- .htaccess
- Copias de seguridad
 - diarios
 - guardar fuera del servidor (sobre todo cambios importantes)
 - algun plugin para copia interna de restauración rápida
- Monitorizar
 - algún plugin de activity log
 - alertas por mail para acciones críticas
 - análisis malware y cambio de archivos
 - escanear semanalmente
- Otros:
 - cambiar prefijo BDD
 - cabeceras de seguridad
 - deshabilitar enumeración de usuarios
 - themeforest + envato (para tener temas actualizados de ese sitio de temas. Hay que vincular con la cuenta que compró el tema)

ejemplo práctico

analisis

- Herramientas → Salud del sitio → Información
 - Wordpress
 - versión
 - Tema activo
 - versión
 - Servidor
 - versión PHP
 - versión servidor web
- plugin **WordFence**
 - desactivar **pausar actualizaciones en vivo cuando la ventana pierde el foco**
 - opciones de exploración y planificación → alta sensibilidad
 - iniciar nueva exploración → listado de vulnerabilidades
 - plugin sin soporte:
 - alternativas equivalentes
 - buscar solución a través de IA (claude.ia, por ejemplo)

actualizaciones

- borrar caché antes de actualizar para detectar errores producidos por una actualización (WP Fastest Cache)
- activar plugin de mantenimiento (WP Maintenance)
- Escritorio → actualizaciones
 - plugins (no actualizar todas de golpe, dificulta localizar un error)
 - temas
 - nucleo WP

corrección vulnerabilidades

securización

procedimiento actualización

1. vaciar cache si se usa alguna
2. modo mantenimiento
3. plugins
4. temas
5. core

preventivo

- .htaccess
- XML-RPC-API
- cambiar «admin»

plugins

- eliminar los que no se usan

recomendados

- WordFence (seguridad)
- GOTMLS (seguridad)
- WP Maintenance (Modo mantenimiento)
- Disable XML-RPC-API
 - Per Neatma
 - Per Amin Nazemi

From:
<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:
<https://miguelangel.torresegea.es/wiki/web:security:wordpress:seguridad?rev=1760953286>

Last update: 20/10/2025 02:41

