#M03: Conceptos básicos de Seguridad en WordPress

Ya conocemos a **WordPress**, un CMS (**Sistema de Gestión de Contenidos)**, que permite crear un entorno de trabajo para la creación y administración de contenidos.

Hemos estado viendo algunos aspectos muy interesantes y herramientas que nos **facilitan** la creación de páginas web con este sistema con cierta soltura.

Hoy conoceremos algunos conceptos básicos de seguridad que nos ayudarán a proteger ese proyecto en el que hemos estado trabajando, para prevenir en la medida de lo posible que la web sea vulnerada por los continuos ciberataques a los que está expuesta.

No todo queda en el diseño de la web. La seguridad es algo más efímero, pero importante.

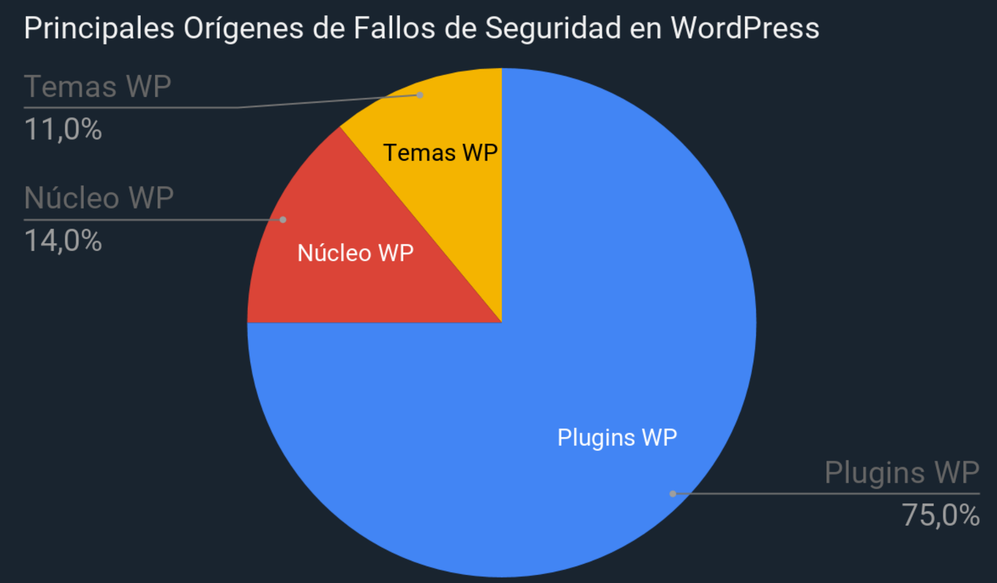
Algunos datos

¿Es WordPress Seguro?

Principales Orígenes de Fallos de Seguridad

Según un informe reciente de wpvulndb.com y wpscan.org, de las 2.837 vulnerabilidades de seguridad conocidas de WordPress en su base de datos:

- 75% son de plugins de WordPress
- 14% son del núcleo de WordPress
- 11% son de los temas para WordPress



5 Aspectos principales de Seguridad de WordPress

1- Ataques de Fuerza Bruta

2- Vulnerabilidades de inclusión de archivos

3- Inyecciones SQL

4- Cross-Site Scripting (XSS)

El 84% de todas las vulnerabilidades de seguridad en toda Internet se denominan ataques XSS o Cross-Site Scripting. Las más comunes se encuentran en los plugins de WordPress.

5- **Malware**: Software Malicioso

El malware es un código que se utiliza para obtener acceso no autorizado a un sitio web con el fin de recopilar datos confidenciales.

¿Qué hace que tu sitio de WordPress sea vulnerable?

1- Contraseñas débiles

2- Plugins o Temas desactualizados

3- Uso de plugins y temas de fuentes no confiables

4- No tener un plugin de seguridad y el sitio configurado correctamente

5- Uso de Hosting Compartido de Mala Calidad

Es muy tentador eso de elegir alojamiento web gratis o muy barato, pero nos puede salir muy caro por otro lado. No vale la pena jugársela.

¿A mí quién me va a hackear?

Pensar que somos un botín pequeño: un grave error.

Los ataques en muchas ocasiones están orientados a propagar software malicioso, páginas de phishing, cobros fraudulentos, redirecciones, publicidad maliciosa o spam.

Para tales cometidos, el objetivo del malware infeccioso queda cubierto con el mero hecho de hacerse con los recursos del servidor.

Cuanto más insignificantes nos creemos que somos con nuestra web, más vulnerables nos volvemos, porque tendemos a bajar la guardia y de eso se aprovechan los atacantes.

> **“El propio hecho de existir una falla de seguridad en una web será el motivo en sí mismo para que ésta sea detectada e infectada. Normalmente por bots.”**

OK: ¿Cómo nos protegemos?

10 Acciones que puedes realizar para proteger tu sitio WordPress

1- Usa contraseñas FUERTES: Largas y complejas
2- Mantén tu sitio de WordPress actualizado
3- Configura los permisos adecuados en tu servidor: En archivos y carpetas
4- Instala un plugin de seguridad *
5- Habilita la autenticación de dos factores *
6- Ejecuta escaneos de malware programados *
7- Activa la protección de fuerza bruta de WordPress *
8- Ten un plan de copias de seguridad fiable y fácil de usar: Automático y Manual
9- Instala solo plugins y temas de buena reputación
10- Mantente informado/a sobre las últimas noticias de seguridad WordPress

*(* normalmente ofrecido por el plugin de seguridad)*

¡Muchas gracias!

A todos por asistir

1. ¿Preguntas?
2. ¿Dudas?
3. ¿Cuestiones?

WordPress Marina Alta

Agradecemos a nuestros patrocinadores

KNOWHERE

anatex rotulaciones

SiteGround

avellà GRÀFIQUES