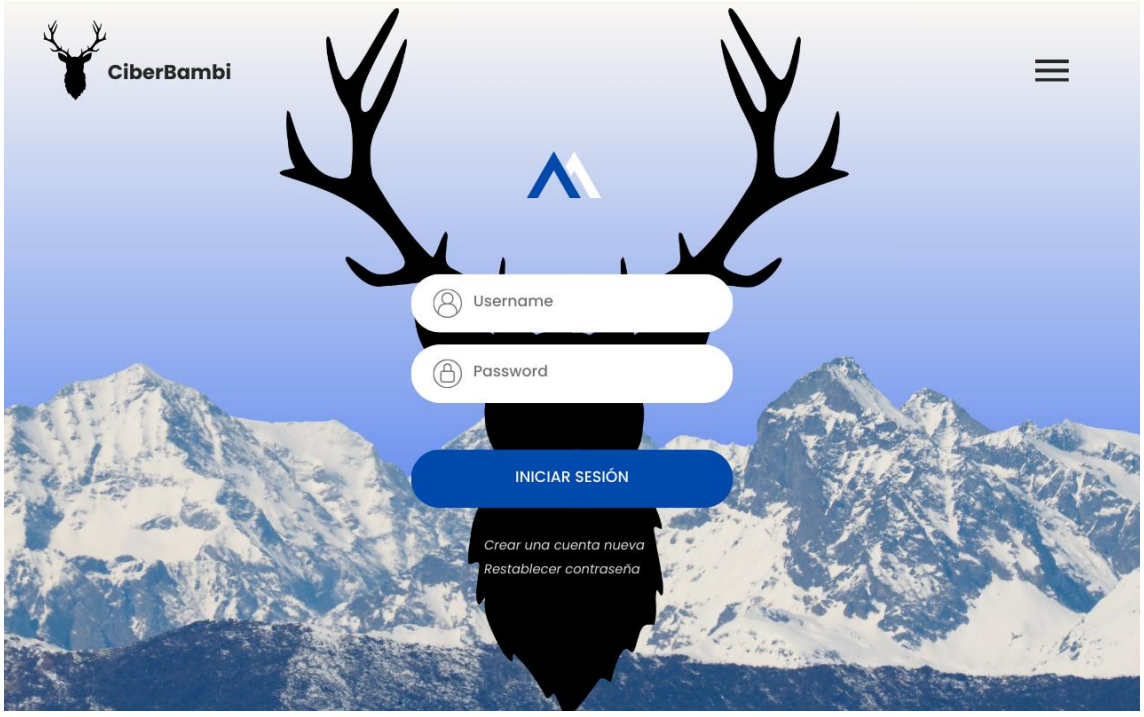
PROYECTO INTERMODULAR ASIX

Ciberbambi

Documento de Buenas Prácticas de Seguridad en WordPress



Configurado por Adam Valien y documentado por Sergi Couto.

Miembros:

Adam Valien, Adam Ahmadi y Sergi Couto.

Índice de contenido

1. Introducción

El presente documento tiene como objetivo definir e implementar un conjunto de **buenas prácticas de seguridad** en un entorno WordPress, complementadas mediante el uso de **seis plugins especializados**.
Estas medidas permiten reforzar el sistema, reducir vulnerabilidades habituales y mejorar la protección frente a ataques comunes como fuerza bruta, inyecciones, spam o fugas de información.

2. Plugins Seleccionados e Implementación de Buenas Prácticas

2.1. Plugin de Seguridad Integral

Wordfence Security

Este plugin ofrece un conjunto de herramientas de seguridad como firewall, análisis de malware, limitación de accesos indebidos y bloqueo de IP maliciosas. Su motor de detección se actualiza de forma frecuente para responder ante amenazas nuevas.

Buenas prácticas aplicadas

- Activar el **Firewall en modo extendido** para obtener una protección más profunda.
- Programar un **escaneo automático semanal**.
- Configurar **2FA para los administradores**.
- Habilitar el sistema de **bloqueo de intentos de login**

2.2. Plugin de Copias de Seguridad

UpdraftPlus

Permite generar copias de seguridad automáticas y almacenarlas en servicios remotos como Google Drive, Dropbox o S3. Facilita además la restauración de archivos ante fallos o ataques.

Buenas prácticas aplicadas

- Establecer **copias diarias de la base de datos** y semanales de los archivos.
- Guardar las copias al menos en **dos ubicaciones externas**.
- Verificar una **restauración cada trimestre** para confirmar que las copias son funcionales.
- Mantener un **histórico de al menos 3 versiones**.

2.3. Plugin de Control de Acceso y Autenticación

WP 2FA

Habilita la autenticación en dos factores para todos los usuarios, añadiendo una capa extra frente a accesos no autorizados.

Buenas prácticas aplicadas

- Obligar a que los perfiles de administración y edición activen **2FA**.
- Configurar un método alternativo (códigos de recuperación).
- Bloquear usuarios que no completen el registro seguro en un plazo definido.
- Registrar auditorías de accesos.

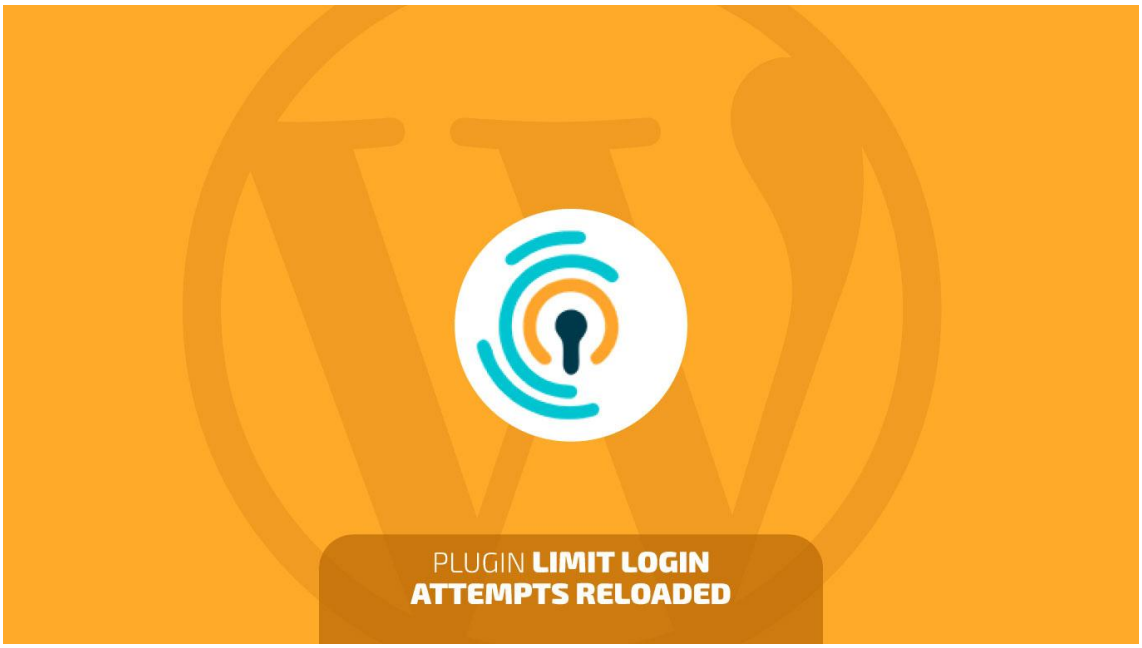
2.4. Plugin de Optimización y Seguridad del Login

Limit Login Attempts Reloaded

Protege el panel de administración limitando los intentos fallidos de login, evitando ataques de fuerza bruta.

Buenas prácticas aplicadas

- Reducir el número máximo de intentos a **3 fallos** antes del bloqueo.
- Configurar un bloqueo progresivo (por ejemplo: 15 min → 1 h → 24 h).
- Integrar bloqueo de IP sospechosas con servicios externos.
- Activar notificaciones por correo ante intentos reiterados.



2.5. Plugin de Seguridad en Formularios y Anti-Spam

Akismet Anti-Spam

Filtra automáticamente comentarios y formularios para evitar spam, contenido malicioso o enlaces peligrosos.

Buenas prácticas aplicadas

- Activar el filtro estricto de spam.
- Revisar periódicamente el registro de comentarios bloqueados.
- Combinarlo con un **captcha adicional** para formularios públicos.
- Evitar mostrar comentarios sin moderar.

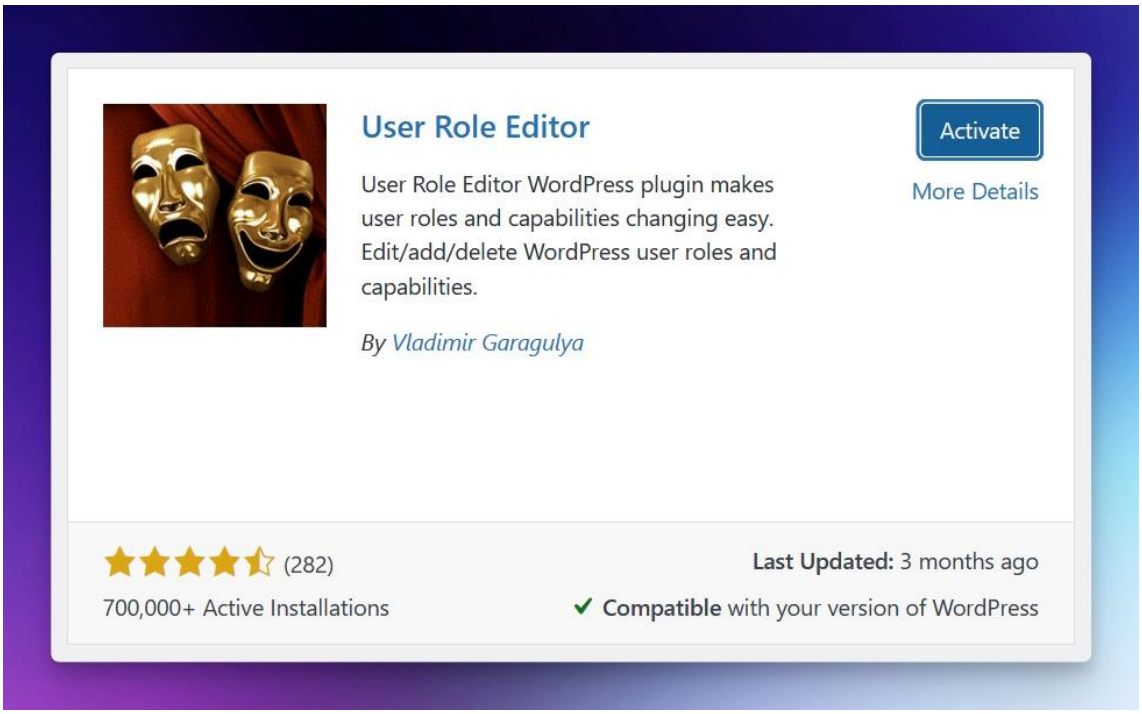
2.6. Plugin de Gestión de Permisos y Roles

User Role Editor

Permite ajustar con detalle los permisos de cada rol en WordPress, evitando que usuarios con funciones menores accedan a áreas críticas.

Buenas prácticas aplicadas

- Aplicar el **principio de privilegio mínimo**.
- Crear roles específicos para tareas concretas (por ejemplo, “editor de blog”, “gestor de soporte”).
- Revisar permisos cada trimestre o tras cambios del personal.
- Evitar que usuarios no técnicos tengan acceso a plugins o archivos del sistema.



3. Buenas Prácticas Generales de Seguridad en WordPress

Independientemente de los plugins instalados, se recomienda seguir estas normas:

3.1. Actualizaciones

- Mantener **WordPress, temas y plugins siempre actualizados**.
- Evitar temas o plugins sin soporte activo.

3.2. Contraseñas y usuarios

- Usar contraseñas robustas (mínimo 12 caracteres, combinando tipos).
- Deshabilitar el usuario “admin”.
- Revisar accesos inactivos y eliminarlos.

3.3. Hardening del servidor

- Proteger el archivo **wp-config.php** con permisos correctos (640).
- Deshabilitar edición de archivos desde el panel (DISALLOW_FILE_EDIT).
- Activar HTTPS mediante Let’s Encrypt o similar.

3.4. Monitorización

- Habilitar alertas por correo para:
    - Cambios de plugins
    - Logins fallidos
    - Modificaciones en archivos del sistema

3.5. Copias de seguridad verificada

- Asegurar redundancia en copias: remoto + local.
- Mantener versiones históricas.

4. Conclusión

La implementación combinada de los seis plugins seleccionados, junto con las buenas prácticas expuestas, permite obtener una plataforma WordPress mucho más segura, estable y resistente frente a ataques comunes.
Estas medidas constituyen una base sólida para entornos profesionales y educativos.