Seguridad WordPress: 25 Plugins Esenciales

Si utiliza un sitio web de WordPress, su seguridad debe ser su principal preocupación. En la mayoría de los casos, los blogs de WordPress están en peligro debido a que algubos de sus archivos y/o plugins son obsoletos, estos son trazables y es una invitación abierta a los piratas informáticos. Para empezar, asegúrese de que siempre está al día con la última versión de WordPress. Pero hay más. En el post de hoy, voy a gustaría compartir con ustedes algunos plugins útiles, así como algunos consejos para endurecer la seguridad de WordPress.

WP DB Backup

WP DB Backup es una herramienta fácil de usarque le permite realizar copias de seguridad de las tablas de bases de datos de WordPress con sólo unos pocos clics.

WP Security Scan

Con este plugin, el escaneo de su sitio de WordPress será una tarea sencilla. Este plugin encuentra las vulnerabilidades en su sitio y ofrece consejos útiles sobre la eliminación de

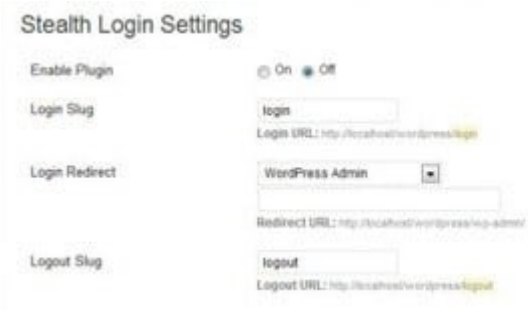
ellos.

Ask Apache Password Protect

Este plugin no controla WordPress o se involucra con su base de datos, sino que utiliza lo verdadero y rapido de las características incorporadas de seguridad , para agregar múltiples capas de seguridad a tu blog.

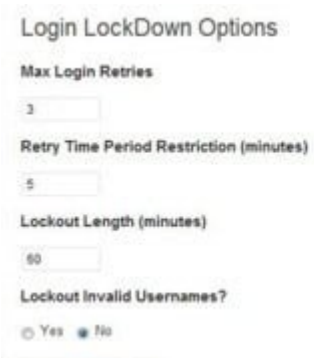
Stealth Login

El stealth Login le ayudará a crear direcciones URL personalizadas para inicio de sesión, el registro y cerrar la sesión de WordPress.



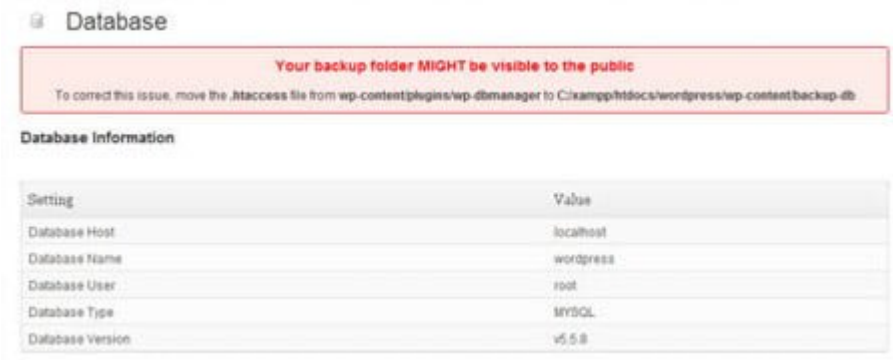
Login Lockdown

Login Lockdown le ayudará a bloquear los intentos para un período de tiempo para acceder a su panel de administración después de varios intentos fallidos.



WP-DB Manager

Esta es otro gran plugin que le permite administrar su base de datos de WP. Podría ser utilizado como una alternativa al Administrador de copia de seguridad de WordPress.

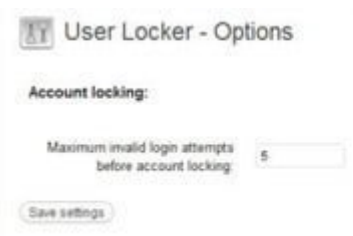


Admin SSL Secure Plugin

Otro plugin para mantener a su panel de administración segura. Actúa sobre el cifrado SSL y es muy útil contra hackers o personas que tratan de obtener acceso no permitidos a su panel.

User Locker

Si usted quiere evitar la fuerza bruta para el hackeo de su sitio, entonces el plugin User Locker es el adecuado para usted. Se basa en el mismo sistema Login Lockdown, sin embargo, es un plugin con puntuación 5 estrellas de WP que tiene una gran fama entre sus usuarios.



Limit Login Attempts

Limit Login Attempts bloquea la dirección de internet que hace otro intento después de que se alcance el límite especificado en reintentos, lo que hace difícil un ataque de fuerza bruta o imposible.

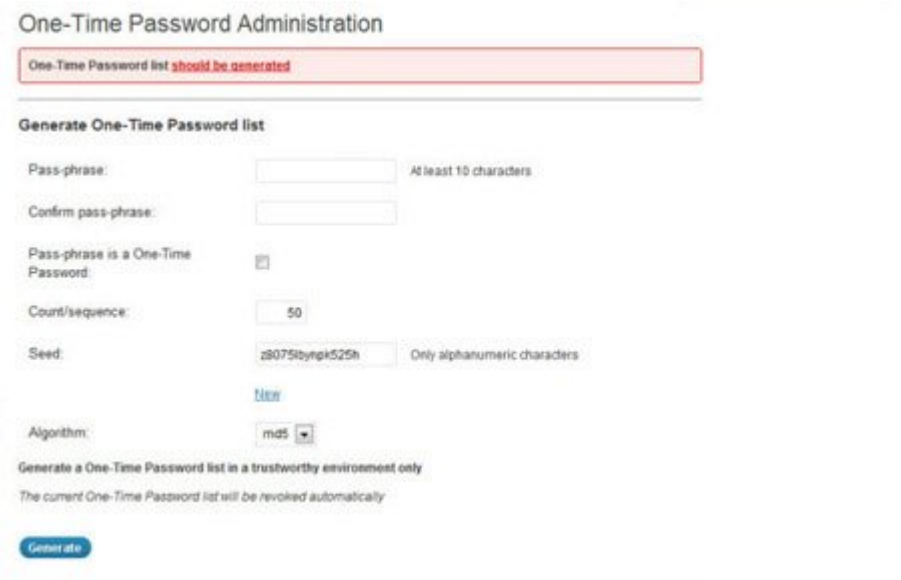
Login Encrypt

Login Encrypt es un plugin de seguridad. Utiliza una combinación compleja de emcriptado DES y RSA para asegurar el proceso de inicio de sesión al panel de administración.

One Time Password

Este plugin única le ayudará a establecer una contraseña una sola vez para su nombre de usuario, a fin de evitar el

registro de usuarios no deseados desde cibercafés o cosas así.

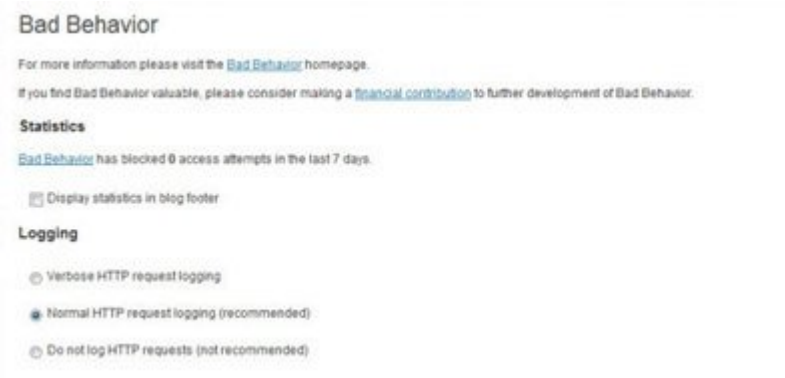


Antivirus

Antivirus es un plugin de seguridad muy popular, que le ayudará a mantener tu blog asegurado contra bots, virus y malwares.

Bad Behavior

Bad Behavior es el plugin que le ayuda a combatir con los molestos spammers. El plug-in no sólo le ayudará a prevenir mensajes de spam en su blog, sino que también tratará de limitar el acceso al spammer a su blog, por lo que no será capaz incluso de leerlo.

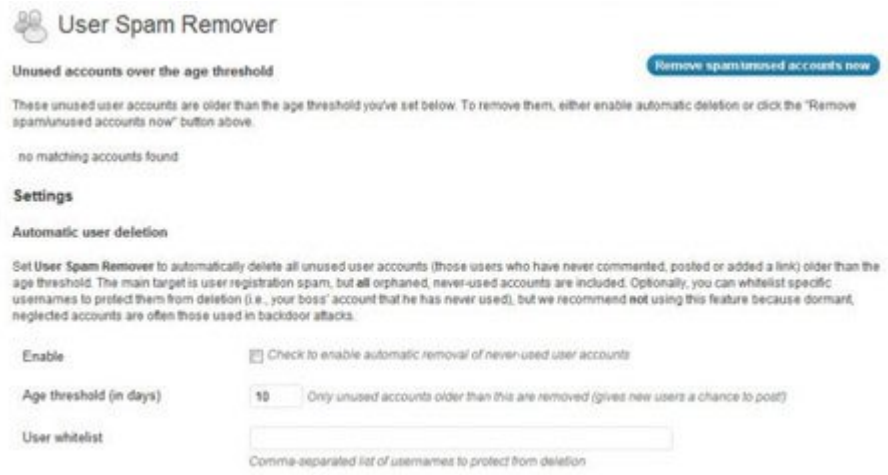


Exploit Scanner

Examina los archivos y bases de datos de su instalación de WordPress en busca de signos que pueden indicar que los archivos o la base de datos ha sido víctima de los hackers. Incluso si es otro plugin de exploración, vale la pena intentarlo.

User Spam Remover

El nombre del plug-in indica sus funciones, un plugin popular, que le ayudará a prevenir y eliminar los mensajes spam no deseados.



[Block Bad Queries]

Este plugin intenta bloquear todas las consultas maliciosas en el servidor y en el WordPress. Funciona en segundo plano, la comprobación de cadenas con solicitudes excesivamente largas (es decir, mayor que 255 caracteres), así como la presencia de cualquiera de las sentencias «eval (» o «base 64» en la URI de la solicitud.