

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 algunos 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 usar que le permite realizar copias de seguridad de las tablas de bases de datos de WordPress con sólo unos pocos clics.

Backup



[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.

The image shows a 'Setup Password Protection' form. It has a 'Create User' section with an 'Admin Email' field containing 'alvaris924@gmail.com' and a note: 'Username and Password sent here in case you forget it.'. Below are 'Username' and 'Password (twice)' fields. The 'Authentication Scheme' section has a 'Choose Scheme' label and two radio buttons: 'Digest' (selected) and 'Basic'. A note at the bottom says: 'This is the mechanism by which your credentials are authenticated (Digest is strongly preferred)'

[Stealth Login](#)

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

Stealth Login Settings

Enable Plugin On Off

Login Slug
Login URL: <http://localhost/wordpress/login>

Login Redirect
Redirect URL: <http://localhost/wordpress/wp-admin/>

Logout Slug
Logout URL: <http://localhost/wordpress/logout>

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.

Login LockDown Options

Max Login Retries

Retry Time Period Restriction (minutes)

Lockout Length (minutes)

Lockout Invalid Usernames? Yes No

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.

Database

Your backup folder MIGHT be visible to the public

To correct this issue, move the .htaccess file from wp-content/plugins/wp-dbmanager to C:\xampp\htdocs\wordpress\wp-content\backup-db

Database Information

Setting	Value
Database Host	localhost
Database Name	wordpress
Database User	root
Database Type	MySQL
Database Version	v5.5.8

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.

Admin SSL Configuration

Enable SSL

You must have a Private SSL certificate correctly installed or enabling this option will render your site inaccessible.

Secure my site with SSL

Additional URLs

Admin SSL forces wp-login.php and wp-admin/profile.php to be secured (these are the pages on which you can enter a password). When HTTPS is being used, the content and includes directories are also secured. Here you can add other URLs to be secured by Admin SSL.

URL List

One URL per line. Your blog URL is http://localhost/wordpress/, so to secure http://localhost/wordpress/some_page.php, add 'some_page.php' to the box below. To secure all your admin URLs, add 'wp-admin/', etc

```
wp-comments-post.php
wp-admin/plugins.php?page=akismet-key-config
```

Warning: depending on how other plugins are written, this feature may not work properly on a Shared SSL setup.
Attempting to secure a blog post or page will cause a redirection error. Single posts and pages cannot be secured - to secure your entire blog, disable Admin SSL and change your blog URL on the 'Settings' page.

Secure additional URLs only if user is signed in

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.

User Locker - Options

Account locking:

Maximum invalid login attempts before account locking:

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.



The screenshot shows the 'Limit Login Attempts Settings' interface. It includes a 'Statistics' section with 'Total lockouts' set to 'No lockouts yet'. The 'Options' section contains several input fields: 'Lockout' with '4 allowed retries', 'minutes lockout' with '20', 'lockouts increase lockout time to' with '4' and 'hours' with '24', and 'hours until retries are reset' with '12'. The 'Site connection' section shows 'It appears the site is reached directly (from your IP: 127.0.0.1)' and radio buttons for 'Direct connection' (selected) and 'From behind a reverse proxy'.

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.



The screenshot shows the 'Login Encryption Options' interface. It features a 'Reset your RSA Key' section with a 'Reset it >' button. Below is the 'Your own numbers' section with input fields for 'P number:' and 'Q number:', and a 'Create it >' button. The 'Using your own key' section has input fields for 'Modulus', 'Public Key', and 'Private Key'. A note at the bottom states: 'Note: Put the decimal form of the key. If you've it in hexadecimal form, you can transform the numbers here:'. Below the note is a 'Transform to Decimal' section with an input field and a 'Transform' button. At the bottom is a 'Save Key >' button.

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.

One-Time Password Administration

One-Time Password list **should be generated**

Generate One-Time Password list

Pass-phrase: At least 10 characters

Confirm pass-phrase:

Pass-phrase is a One-Time Password:

Count/sequence:

Seed: Only alphanumeric characters

[New](#)

Algorithm:

Generate a One-Time Password list in a trustworthy environment only
The current One-Time Password list will be revoked automatically

Antivirus

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

AntiVirus

Completed scan

Permalinks back door check All clear
Danger

Manual scan

Settings

Enable the daily antivirus scan

Alternate email address:

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.

Bad Behavior

For more information please visit the [Bad Behavior](#) homepage.

If you find Bad Behavior valuable, please consider making a [financial contribution](#) to further development of Bad Behavior.

Statistics

[Bad Behavior](#) has blocked 0 access attempts in the last 7 days.

Display statistics in blog footer

Logging

Verbose HTTP request logging

Normal HTTP request logging (recommended)

Do not log HTTP requests (not recommended)

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.

Exploit Scanner

This script searches through your WordPress install for signs that may indicate that your website has been compromised by hackers. It does NOT remove anything, this is left for the user to do.

Search for suspicious styles: (`<!--[if]-->` and `<!--[endif]-->` can be used to hide spam, but may cause many false positives)

Upper file size limit: KB (files larger than this are skipped and will be listed at the end of scan)

Number of files per batch: (to help reduce memory limit errors the scan processes a series of file batches)

[Run the Scan](#)

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.



User Spam Remover

Unused accounts over the age threshold

[Remove spam/unused accounts now](#)

These unused user accounts are older than the age threshold you've set below. To remove them, either enable automatic deletion or click the "Remove spam/unused accounts now" button above.

no matching accounts found

Settings

Automatic user deletion

Set User Spam Remover to automatically delete all unused user accounts (those users who have never commented, posted or added a link) older than the age threshold. The main target is user registration spam, but all orphaned, never-used accounts are included. Optionally, you can whitelist specific usernames to protect them from deletion (i.e., your boss' account that he has never used), but we recommend **not** using this feature because dormant, neglected accounts are often those used in backdoor attacks.

Enable

Check to enable automatic removal of never-used user accounts

Age threshold (in days)

10

Only unused accounts older than this are removed (gives new users a chance to post)

User whitelist

Comma-separated list of usernames to protect from deletion

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.