FORMAS DE SEGURIZAR WORDPRESS

La seguridad de tu blog en WordPress es muy importante. Una gran atención se requiere para que tu blog en WordPress esté seguro de los hackers. Se requiere que pongas atención en la seguridad de tus blogs para no dejar ninguna puerta abierta a los hackers. Si un hacker esta absolutamente determinado a entrar a tu blog entonces probablemente tendrá éxito, pero puedes proteger a tu blog de los hackers con los siguientes tips, consejos, trucos, etc. que te voy a contar.

Son 21 consejos que puedes aplicar para que tu blog sea más impenetrable que la caja fuerte de la reserva federal de EEUU.

1. Mantén actualizado tu WordPress

Siempre en la última actualización de WordPress vienen las soluciones a varios problemas de seguridad de éste. Si no actualizas tu blog de WordPress a la última versión, los hackers aprovecharán las brechas de seguridad de la versión antigua de WordPress y podrán entrar fácilmente a tu blog.

2. Haz un BackUp de tu base de datos y de tus archivos periódicamente

Hacer un BackUp (respaldo) de tu Base de Datos y de tus archivos es muy importante para prevenir que se pierdan tus datos en un posible ataque de los hackers o cuando tu servidor se caiga.

Un plugin excelente para manejar y automatizar los respaldos de tu base de datos es WP-DBManager. Este automáticamente creará el backup de la base de datos y lo enviará al correo que se disponga en la configuración del plugin.

3. Utiliza una contraseña difícil

Nunca utilizas tu nombre u otro dato personal en la contraseña, pues serían fáciles de descubrir. Una contraseña fuerte es esencial para un usuario con privilegios de administrador. por eso al elegir una contraseña para tu blog asegura de que:

- Sea alfanumérico, o sea, contenga tanto números como letras.
- Tenga tango mayúsculas como minúsculas.
- Contenga caracteres como ¬ ! #$%…

4. Asígnale los permisos correctos (CHMOD) a las carpetas de tu servidor

Para hacer esto deberías utilizar el plugin WP Security Scan. Este plugin te ayudará a saber si tienes los permisos más seguros para tus carpetas de WordPress en el servidor.

5. Evita la exploración de las carpetas

Es vital prohibir que tus visitantes puedan explorar las carpetas de tu sitio. Por ejemplo debemos evitar que si escribes *http://www.tusitio.com/wp-admin/* se vean todos los archivos en esa carpeta.

Para evitar esto solo debes añadir la siguiente línea de código en el archivo .htaccess de la carpeta raíz de tu servidor:

```
01 Options All -Indexes
```

6. Utiliza el archivo robots.txt para deshabilitar el acceso

El archivo robots.txt se utiliza para para decirle a los buscadores que carpetas de tu sitio no quieres que explore el robot del buscador. Por ejemplo deberías desactivar la búsqueda en la carpeta "*/plugins*" y "*/wp-admin*". Solo debes copiar el siguiente texto en un archivo del bloc de notas y llamarlo "robots.txt" y subirlo a la carpeta raíz de tu sitio de WordPress:

```
#
User-agent: *
Disallow: /cgi-bin
Disallow: /wp-admin
Disallow: /wp-includes
Disallow: /wp-content/plugins/
Disallow: /wp-content/cache/
Disallow: /wp-content/themes/
Disallow: */trackback/
Disallow: */feed/
Disallow: /*/feed/rss/$
Disallow: /category/*
```

7. Protege la carpeta "/plugins"

Los plugins que utilizas pueden decirle mucho a un usuario malicioso sobre tu sitio así que es mejor esconderlos. Para esto solo debes crear un archivo en el Bloc de Notas sin ningún contenido y guardarlo como "*index.html*" y luego sube este archivo a la carpeta "*/wp-content/plugins/*".

8. Revisa tus comentarios

Todos sabemos como los spammers llenan los blogs de comentarios si no existe una moderación o un filtro anti-spam. Estos comentarios spam pueden contener enlaces a sitios potencialmente dañinos los cuales pueden afectar a nuestros inocentes lectores e incluso afectar al blog. Aquí hay algunos plugins que deberías instalar para evitar el spam en los comentarios de tu blog:

- Akismet: Maravilloso plugin para la protección anti-spam. Este revisa tus comentarios con el servicio web de Akismet para ver si parece spam o no y deja que revises si ese comentario marcado es spam o no.
- Math Comment Spam Protection: Le pregunta al lector antes de comentar una simple pregunta mátemática. Esto para probar que el visitantes es humano en vez de un robot de spam.
- reCAPTCHA: Este plugin utiliza el ya conocido método de ingresar los caracteres que ves en la imágen para comprobar si eres humano o un robots spam.

9. Cambia el prefijo de la Base de Datos

Para hacer que tu base de datos sea más segura deberías cambiar el prefijo de ésta. Por defecto todas las tablas tienen el prefijo "*wp_*" y deber ser cambiado por algo un poco más difícil de adivinar, algo como "*t45s4w_*".

Primero el prefijo debe ser cambiado en el archivo *wp-config.php*:

```
01 $table_prefix = 't45s4w_'; // Solo utiliza números, letras y guión bajo.
```

Luego debes cambiar el nombre de las tablas de la base de datos con el nuevo prefijo, para esto debes ejecutar la siguiente sentencia SQL en tu base de datos (probablemente en PhpMyAdmin):

```
01 RENAME TABLE wp_comments to t45s4w_comments;
02 RENAME TABLE wp_links to t45s4w_links;
03 RENAME TABLE wp_options to t45s4w_options;
04 RENAME TABLE wp_postmeta to t45s4w_postmeta;
05 RENAME TABLE wp_posts to t45s4w_posts;
06 RENAME TABLE wp_terms to t45s4w_terms;
07 RENAME TABLE wp_term_relationships to t45s4w_term_relationships;
08 RENAME TABLE wp_term_taxonomy to t45s4w_term_taxonomy;
09 RENAME TABLE wp_usermeta to t45s4w_usermeta;
10 RENAME TABLE wp_users to t45s4w_users;
```

Y luego debes ejecutar la siguiente sentencia SQL para que WordPress funcione correctamente:

```
01 UPDATE t45s4w_options SET option_name = REPLACE(option_name,
'wp_', 't45s4w_');
02 UPDATE t45s4w_usermeta SET meta_key = REPLACE(meta_key, 'wp_',
't45s4w_');
```

10. Restringe el acceso de archivos de la carpeta *wp-content*

La carpeta *wp-content* contiene los archivos de tu theme, las imágenes que has subido y los plugins. WordPress no accede a estos archivos vía HTTP. Las únicas peticiones desde un explorador web deberían ser a archivos de imágen, javascript, css y xml.

Por esta razón debes restringir la carpeta "*wp-content*" para que solo se permitan ver esos archivos y ninguno más.

Crea un archivo en el Bloc de Notas, guárdalo como ***.htaccess***, añádele las siguientes líneas y súbelo a la carpeta *wp-content* de tu instalación de WordPress:

```
01 Order deny,allow
02 Deny from all
03 <Files ~ ".(php|lock|xml|css|jpe?g|png|gif|js)$">
04 Allow from all
05 </Files>
```

11. Bloquea el acceso a la carpeta *wp-admin*

Puedes limitar el acceso a ciertas direcciones IP para que no puedan entrar a la carpeta wp-admin, excepto las IP's que tu quieras (Si no sabes la dirección IP de tu computador, esta página te puede servir: What Is My IP) . Para esto debes crear un archivo ***.htaccess*** en la carpeta *wp-admin* con las siguientes líneas:

```
01 AuthUserFile /dev/null
02 AuthGroupFile /dev/null
03 AuthName "Access Control"
03 AuthType Basic
04 order deny,allow
05 deny from all
06 # Dirección IP de mi Casa
07 allow from 00.000.000.00
08 #Dirección IP del Trabajo
09 allow from 00.000.000.000
10 allow from 000.000.00.000
12 # Dirección IP de la Casa de mi Tía
13 allow from 000.000.0.00
```

Solo debes reemplazar los (000.000.000.000) con las IP's verdaderas para permitir el acceso mediante ellas.

12. Protege el archivo *wp-config.php*

El archivo *wp-config.php* contiene toda la información que WordPress necesita para acceder a tu base de datos. Proteger este archivo es muy importante.

Para esto, añadimos las siguientes líneas de código al archivo .htaccess de la carpeta raíz del servidor de WordPress:

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```

Esto prevendrá que cualquier robot o persona pueda entrar directamente en este archivo.

13. Utiliza las claves secretas de autenticación en *wp-config.php*

Estas claves secretas son usadas para que tu contraseña sea más difícil de adivinar mediante la fuerza bruta. Simplemente visita WordPress Key Generator y copia las 8 claves en las siguientes líneas del archivo *wp-config.php*:

```
define('AUTH_KEY', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('SECURE_AUTH_KEY', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('LOGGED_IN_KEY', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('NONCE_KEY', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('AUTH_SALT', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('SECURE_AUTH_SALT', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('LOGGED_IN_SALT', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('NONCE_SALT', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
```

14. Mueve el archivo *wp-config.php*

Desde WordPress 2.6 se puede mover la ubicación del archivo wp-config.php de la carpeta raíz de la instalación de WordPress. Simplemente mueve tu archivo wp-config.php a cualquier carpeta que se encuentre en la carpeta raíz de tu instalación y WordPress automáticamente buscará este archivo por todas las carpetas si no puede encontrarlo en la carpeta raíz.

15. Cambia el usuario "*admin*" por otro

Hacer esto pondrá mucho más difícil entrar a tu blog a usuarios maliciosos. Solo debes ejecutar la siguiente sentencia SQL en tu base de datos (No olvides poner tu propio usuario donde dice "*Tu Nuevo Usuario*"):

```
01 UPDATE wp_users SET user_login = 'Tu Nuevo Usuario' WHERE user_login = 'admin';
```

16. Protege tu blog de inyecciones de código

El siguiente código protege a tu blog de inyecciones de código que modifican las variables GLOBALS y _REQUEST de PHP. Pega esto en el archivo .htaccess del servidor:

```
01 Options +FollowSymLinks
02 RewriteEngine On
03 RewriteCond %{QUERY_STRING} (\<|%3C).*script.*(\>|%3E) [NC,OR]
04 RewriteCond %{QUERY_STRING} GLOBALS(=|\[|\%[0-9A-Z]{0,2}) [OR]
06 RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})
07 RewriteRule ^(.*)$ index.php [F,L]
```

17. No muestres la versión de tu WordPress

Cuando muestras la versión que tienes de WordPress puedes darle información a usuarios maliciosos sobre si tu blog esta actualizado o no. Si es una versión antigua, ellos pueden utilizar los errores que tenga dicha versión y apoderarse de tu blog.

WordPress automáticamente publica este dato en tu theme. La siguiente línea de código le dice a WordPress que no publique este dato, pégala en el archivo *functions.php* de tu theme:

```
01 <?php remove_action('wp_head', 'wp_generator'); ?>
```

18. Limita los intentos de ingreso al Panel de Administración

A veces el hacker cree que sabe nuestra contraseña, o ha desarrollado un script para adivinarla. En este caso necesitas limitar la cantidad de veces que un usuario puede equivocarse al ingresar sus datos de ingreso. Puedes hacer esto fácilmente con el plugin Login Lockdown, que bloqueará a un usuario por tanto tiempo si ha ingresado mal los datos después de tantas veces.

19. Utiliza un ingreso seguro

Los usuarios de WordPress que tienen el SSL (SSL es un protocolo criptográfico que blinda la comunicación entre redes) habilitado para su dominio, deberían utilizar este canal encriptado para acceder al Panel de Administración.

Para esto solo debes poner el siguiente código en el archivo *wp-config.php*:

```
01 define('FORCE_SSL_ADMIN', true);
```

Recuerda que no todos los hosting tienen habilitada la opción de SSL, así que debes asegurarte primero de tener habilitada esta opción.

20. No muestres errores de ingreso

Cuando ingresas un usuario o contraseña incorrecta, sale un mensaje de error en la página de ingreso. Así que si el hacker ingresa un dato correcto, el mensaje de error le ayuda´ra a identificarlo. entonces, es recomendable que elimines completamente ese mensaje de error.

Ingresa el siguiente código en el archivo *functions.php* de tu theme:

```
01 add_filter('login_errors',create_function('$a', "return null;"));
```

21. Elimina los plugins innecesarios

Siempre asegúrate de eliminar los plugins que no estés utilizando pues pueden crear agujeros de seguridad que pueden ser aprovechados fácilmente por usuarios maliciosos.

Espero que esta guía te haya sido de ayuda para mantener completamente segura tu instalación de WordPress.