Mejorar el desempeño de tu WordPress

La Seguridad en Internet siempre ha sido tan importante como su seguridad personal. Si usted está haciendo dinero a través de tu blog o página web, la seguridad de su sitio web se vuelve tan importante como la seguridad de su cuenta bancaria. Por suerte, WordPress se esfuerza por garantizar una mejor seguridad con cada nueva versión. Además, hay un montón de plug-ins que puede utilizar para fortalecer su seguridad en el sitio web o blog.

La parte más interesante es que la optimización de un blog de WordPress o sitio web para una mejor seguridad requiere solo ajustes pequeños. Estos son algunos de los consejos más interesantes y eficaces para ayudarle a asegurar su sitio web contra el robo de información, las violaciones, las intrusiones e intercepción.

Forzar uso de SSL

Secure Sockets Layers o SSL son algoritmos criptográficos que se utilizan para proteger la comunicación a través de Internet. Es un protocolo muy utilizado sobre todo en los sitios web de comercio electrónico. Lo bueno es que si bien la seguridad de su blog o sitio web, sólo necesita un poco de conocimiento técnico. Con SSL implementado, los hackers e intrusos no pueden escuchar, manipular o falsificar los datos, incluso si tienen la posibilidad de acceder a él. Puede sonar como una exageración, pero muchos desarrolladores lo consideran como el epítome de la seguridad en Internet. Por no hablar, un certificado SSL hará que su sitio web / blog parece más creíble y confiable, incluso para usuarios que no son expertos en tecnología.

Ahora siga estos pasos para forzar el uso de SSL en su sitio

web.
Abra el archivo ***wp-config.php*** en el directorio de archivos. Este es el archivo de configuración más importante en todo el directorio. Una vez abierto, pegue el siguiente fragmento de código en el archivo ***wp_config.php***.

[code lang=»php»]
/* Enable SSL Encryption */
define (‘FORCE_SSL_LOGIN’, true);
define (‘FORCE_SSL_ADMIN’, true);
[/code]

Guarde y cierre el archivo. El Cifrado SSL está habilitado en área de administración de su sitio web. El área de administración ahora carga con “https” en lugar de “http“. Como la mayoría de sitios web requieren información confidencial para ser utilizado sólo en el área de administración, la activación de SSL para la interfaz no es necesario.
Protección contra Inyecciones de secuencias de comandos

Inyección SQL se ha convertido en una de las principales amenazas a los sitios web hoy en día. En la inyección de script, los atacantes inyectan una pieza de código malicioso en las variables de entrada del usuario que luego son analizadas y ejecutadas por el servidor SQL. Incluso una sola página infectada puede poner todo el sitio web en riesgo y podría dañar todos los datos.

Con el fin de proteger su sitio web contra este tipo de ataques, debe proteger **PHP GLOBALS** y variables **_REQUEST**. Puede hacerlo siguiendo las instrucciones indican a continuación.

Abra el archivo “**.htaccess**” en el directorio de archivos de tu instalación de WordPress. Ahora pega el siguiente código.

Options +FollowSymLinks

RewriteEngine On

```
RewriteCond %{QUERY_STRING} (\&lt;|%3C).*script.*(\&gt;|%3E) [NC,OR]

RewriteCond %{QUERY_STRING} GLOBALS(=|\[|\%[0-9A-Z]{0,2}) [OR]

RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})

RewriteRule ^(.*)$ index.php [F,L]
```

Este código comprobará la petición de entrada para cualquier script que intenta modificar el valor de PHP GLOBALS o variables _REQUEST. Si se detecta un ataque, el código se bloquea la solicitud y devuelve un error 403.

Un punto importante a mencionar aquí es que editar el archivo ".htaccess" no se recomienda hasta que esté absolutamente seguro de que está haciendo de la manera correcta.
Sin embargo, si usted tiene una copia de seguridad del archivo y base de datos, entonces usted puede editar sin ningún tipo de preocupaciones.

Si está utilizando un servidor nginx, entonces usted tendrá que hacer uso de otros métodos para asegurar su sitio. Esto se debe a ".htaccess" no está soportado por el servidor nginx.
Protección contra el Rascadores Contenido y hotlinking

El contenido ha sido siempre el rey pero con Panda y el Pingüino, el contenido es cada vez mas importante. Su contenido está siempre en peligro de ser plagiado por otros. Esto es válido para todos los tipos de contenido, como texto e imágenes. Contenido de desguace también implica imagen hotlinking, que a su vez debilita ancho de banda del servidor.
La verdad es que sólo unas pocas personas ponen suficiente esfuerzo y dedicación para generar contenido original de alta calidad. Si usted ha pasado por todo el trabajo duro, usted debe proteger su contenido contra raspadores. Hágalo, siguiendo el siguiente procedimiento.
Abra el archivo single.php y llegar a la línea en la que aparece el título. Todo lo que necesitas hacer es reemplazar

esa línea con el siguiente código.

```
[code lang=»php»]
<h1>
<a href="<?php the_permalink(); ?>">
<?php the_title(); ?>
</a>
</h1>
[/code]
```

Este código coloca un enlace en el título de su post. Por lo tanto, cuando los scrappers utilizan su contenido junto con el título, el post robado tendra un link que lo dirigira al mismo.

Para hotlinkers, crear una imagen con el nombre de nohotlink.jpg y subirlo a la carpeta Imágenes. Abra el archivo ".htaccess" y pega el siguiente código. Antes de hacer esto, usted debe colocar la imagen en la carpeta Imágenes.

```
RewriteEngine On

#Replace ?mysite\.com/ with your blog url

RewriteCond %{HTTP_REFERER} !^http://(.+\.)?mysite\.com/ [NC]

RewriteCond %{HTTP_REFERER} !^$

#Replace /images/nohotlink.jpg with your &quot;don't hotlink&quot; image url

RewriteRule .*\.(jpe?g|gif|bmp|png)$ /images/nohotlink.jpg [L]
```

La página hot-linking ahora mostrará cualquier imagen que haya nombrado como nohotlink.jpg. Una vez más, hacer esto con mucho cuidado y asegúrese de tener copias de seguridad necesarias ya que editar el archivo "***.htaccess***" puede ser riesgoso.

Actualizaciones WordPress

Una de las mejores maneras y más simples para asegurar su

sitio de WordPress es actualizar regularmente el software. Al igual que cualquier otro programa, WordPress a menudo configura medidas de seguridad, y libera nuevas actualizaciones.

Protección contra ataques de fuerza bruta

WordPress no pone restricciones a los intentos de conexión si se proporciona una contraseña incorrecta. Sin embargo, los intentos ilimitados hace que sea más fácil para un hacker romper la clave y garantizar el ingreso. Por lo tanto, se debe limitar el número de intentos de inicio de sesión. Para ello, descargue el plug-in disponible en el sitio de WordPress, y extraerlo en el directorio wp-content/plugin. El plug-in se puede activar desde la interfaz de administración.

Contraseñas seguras

La mayoría de la gente tiene la costumbre de aplicar el primer procedimiento más difícil en lugar de los más sencillos. Igual es el caso con las contraseñas que estableció para su cuenta de administrador. Trate de elegir una contraseña compleja que es alfanumérico y contiene signos de puntuación también. Además, cambiar el nombre de usuario de la 'admin' cuenta a otra cosa.

Errores en Acceso

WordPress muestra un nombre de usuario o contraseña inválida si los datos de acceso son erroneos Esto debería ser desactivada para que los hackers no pueden seguir su proceso. Esto puede hacerse escribiendo la línea siguiente en el archivo ***functions.php.***

```
[code lang=»php»]
add_filter('login_errors',  create_function('$a',  "return null;"));
[/code]
```

Prefijo de Base de datos

Los prefijos de todas las bases de datos son los mismos de forma predeterminada, por lo que son conocidos a los demás. Usted debe cambiar a fin de aumentar la seguridad. Esto se puede hacer añadiendo la línea dada en el archivo ***wp-config.php.***

[code lang=»php»]
$table_prefix = ‘wp_a123456_’;
[/code]

Permisos de archivos

Al igual que las bases de datos, los permisos para los archivos también son los mismos para todos los usuarios hasta que los cambie. Usted debe agregar esta línea de código para evitar el acceso no deseado de todos los archivos .

chmod who=permissions filename

Tema y Plug-in de edicion

El tema y el plug-in de edicion debe estar deshabilitada para que nadie pueda modificar su contenido. Abra el archivo wp-config.php y pega la siguiente línea.

[code lang=»php»]
define(‘DISALLOW_FILE_EDIT’, true);
[/code]