Tabla de contenidos:

Tabla de contenidos: **1**

Introducción **2**

Instalando WordPress **2**

Accediendo a sus tablas de WordPress *2*

Cambiando el prefijo a sus tablas de WordPress **3**

Antes de instalar *3*

Cambio manual *3*

A través de WP Prefix Table Changer *4*

Preparando el Blog **5**

Cambiando su nombre de usuario administrador *5*

Crear un nuevo usuario de acceso limitado *6*

Reforzando su instalación de WP **7**

Restringiendo wp-content y wp-includes *7*

Restringiendo wp-admin *7*

Bloqueando todas las IP menos la suya 7

Contraseña obligatoria - .htpasswd *7*

El archivo .htaccess 8

El archivo .htpasswd 8

Extensiones IMPRESCINDIBLES **8**

WPIDS – Detecte intrusiones *8*

WordPress Plugin Tracker – ¿Está usted actualizado? *9*

Escáner de seguridad online de WordPress *10*

Fin **10**

Introducción

Este documento le proporciona toda la información necesaria para mejorar la seguridad de su blog. Intentaremos describir los pasos de una manera fácil y comprensible sin mucha jerga técnica, para que pueda seguirlos fácilmente y no se encuentre con problemas para aplicar estos cambios para asegurar su blog. Toda la información puede encontrarse en BlogSecurity.net; este documento sirve como una guía compacta para asegurar su blog. Nos esforzaremos para mantener este documento actualizado, así que visítenos regularmente.

Si tiene preguntas, problemas, ideas o cualquier otra cosa relacionada con este documento, siéntase libre de contactarnos.

Importante: Antes de usar cualquiera de las técnicas descritas en este documento, por favor, realice una copia de seguridad completa de sus archivos de WP y su base de datos. Consulte nuestros "5 pasos a prueba de fallos para actualizar WordPress" si necesita ayuda.

Instalando WordPress

Accediendo a sus tablas de WordPress

Antes incluso de que comience a instalar su blog es importante elegir el tipo adecuado de usuario de base de datos con los permisos correctos. La idea tras este paso "vital" es usar un usuario de base de datos limitado para administrar su blog. En el caso de que su blog sea comprometido, el atacante luchará para escalar su privilegios fuera de su blog (p. ej. el resto del servidor o la cuenta de alojamiento).

Nota: Nunca deje que una aplicación web accede a la base de datos con un usuario root. En pocas palabras, se estaría buscando problemas.

Su cuenta de usuario no debería tener privilegios globales de SQL así como acceso limitado a la base de datos donde sus tablas de WordPress residen. Para realizar las tareas diarias es suficiente darle a su usuario los siguientes permisos:

> *Para datos: SELECT, INSERT, UPDATE, DELETE*
> *Para estructuras: CREATE, ALTER, DROP*

Si solo se le permite ejecutar una base de datos en su cuenta de alojamiento web, pero puede crear múltiples usuarios dentro de esta base de datos, cree un usuario cuyo acceso esté limitado a las tablas de WordPress, hablando claro. Los privilegios deberían ser:

> *Para datos: SELECT, INSERT, UPDATE, DELETE*
> *Para estructuras: ALTER*

¿Por qué estamos haciendo esto?, es por su propia seguridad, para que si un atacante obtiene acceso a su blog y puede realizar consultas, estas consultas estén entonces limitadas sólo a su instalación de WordPress y no al resto de sus bases de datos.

Cambiando el prefijo a sus tablas de WordPress

Para mitigar amenazas de inyección SQL debería cambiar el prefijo predeterminado de WordPress de wp_ a algo **más aleatorio** como *4i32a_*. A menudo los atacantes usan vulnerabilidades públicas en Internet. Estas vulnerabilidades suelen confiar en el hecho de que la mayoría de instalaciones de WordPress usan el prefijo de tabla, "wp_". Cambiando esto hará más difícil para un atacante ejecutar vulnerabilidades satisfactoriamente.

Para reconocer fácilmente que prefijo pertenece a qué aplicación web puede mantener algo de la aplicación en el prefijo, como *wp_4i32a_* o *wp4i32a_*. Es importante modificarlo, para que un atacante no pueda adivinar fácilmente su prefijo de WordPress.

Antes de instalar

Si acaba de empezar a instalar WordPress este paso es bastante fácil de llevar a cabo, todo lo que necesita es cambiar esta línea del archivo **WP-CONFIG.PHP** :

```
$table_prefix = 'wp_';
```

a algo diferente, como nuestro ejemplo:

```
$table_prefix = '4i32a_';
```

Después de eso puede simplemente ejecutar la rutina de instalación de WordPress y todas las tablas y campos de WordPress serán creados con su prefijo **diferente** de WordPress.

Cambio manual

Si quiere cambiar el prefijo de las tablas en una instalación existente requiere unos pocos pasos adicionales. Esto suele ser un proceso tedioso y se explica más abajo, de todos modos, para una solución rápida consulte la siguiente sección.

El primer paso es abrir su archivo **WP-CONFIG.PHP** y cambiar esa línea:

```
$table_prefix = 'wp_';
```

Para usar el ejemplo anterior de nuevo, estamos usando el prefijo *4i32a_* así que nuestra línea se verá como esta:

```
$table_prefix = '4i32a_';
```

Ahora que esto está hecho necesitamos renombrar todas las tablas de WordPress para que coincidan con el nuevo prefijo, para conseguirlo necesitamos ejecutar una consulta SQL [1] dentro de un interfaz web como PHPMyAdmin o similar, ya que WordPress no permite cambiar el prefijo directamente.

Así que estas tablas:

[1] Ejemplo de consulta: *RENAME TABLE wp_categories TO 4i32a_categories*

> *wp_categories, wp_comments, wp_link2cat, wp_links, wp_options, wp_post2cat, wp_postmeta, wp_posts, wp_usermeta, wp_users*

Se convertirán en estas:

> *4i32a_categories, 4i32a_comments, 4i32a_link2cat, 4i32a_links, 4i32a_options, 4i32a_post2cat, 4i32a_postmeta, 4i32a_posts, 4i32a_usermeta, 4i32a_users*

Ahora puede pensar que hemos acabado, ¿es así?. Pero ese no es el caso. WordPress también incluye algunos valores con el prefijo de las tablas. Para poder usar su blog primero necesitamos cambiarlos.

Necesitamos cambiar dentro de la tabla wp_options[2] el valor de un registro para el campo option_name de *wp_user_roles* a *4i32a_user_roles*[3].

Ahora necesita sustituir otros dos[4] valores en esta tabla: wp_usermeta.
Los valores *wp_autosave_draft_ids* y *wp_user_level* para el campo meta_key necesitan ser cambiados al nuevo prefijo: *4i32a_autosave_draft_ids* y *4i32a_user_level*.

¡Eso es!. **Pero BlogSecurity ha hecho esto todavía más fácil con** WP Prefix Table Changer.

A través de WP Prefix Table Changer

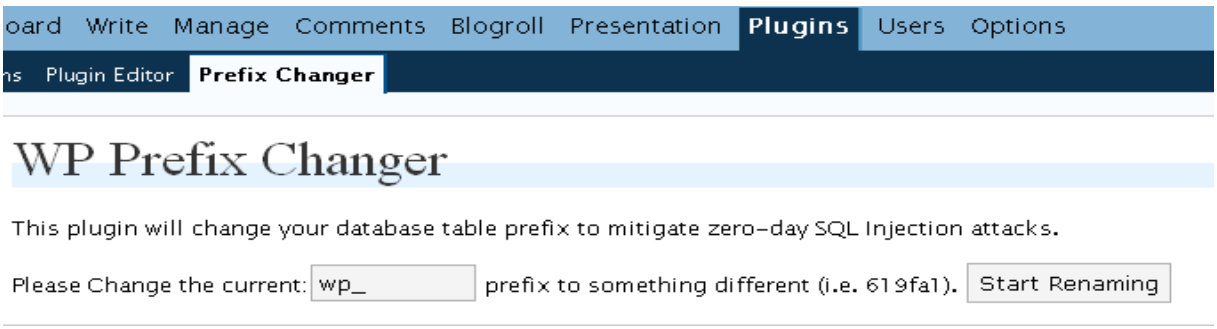
Hemos creado una extensión llamada WP Prefix Table Changer, la cual automatiza el proceso completo de renombrar sus tablas de WordPress y las entradas de las tablas mencionadas.

Después de que descargue la extension desde BlogSecurity.net, solo necesita extraer los archivos a su carpeta plugins de WordPress, que debería ser **WORDPRESS/WP-CONTENT/PLUGINS**. Después de esto necesita entrar al área de administración de WP y activar la extensión WP Prefix Table Changer. Tras la activación aparecerá una nueva pestaña de submenú dentro de la página de extensiones llamada Prefix Changer, haga clic en ella. En esa página verá lo siguiente:

[2] Se usa el prefijo predeterminado, para evitar confusiones que podrían ocurrir si hubiésemos usado el nuevo prefijo

[3] *UPDATE 4i32a_options SET option_name='4i32a_user_roles' WHERE option_name='wp_user_roles' LIMIT 1*

[4] **Nota**: puede ser que estos campos no existan actualmente, ya que son creados cuando se necesitan, una vez que son creados obtienen el valor correcto automáticamente



Como puede ver este blog está usando el prefijo predeterminado de la base de datos de WP. Ahora cambie ese prefijo mostrado a algo **aleatorio, sin significado** como nuestro anterior ejemplo *4i32a_*. Una vez hecho, simplemente haga clic en el botón 'Start Renaming' y la extensión empezará a renombrar todos los nombres de tabla de wp_ a su palabra aleatoria seleccionada. Debería tenerse en cuenta que las tablas de componentes de terceros también se cambian, ya que también necesitan el nuevo prefijo.

El ultimo paso de la extensión es cambiar el prefijo dentro del archive **WP-CONFIG.PHP** .

Obtendrá un mensaje de si este proceso ha sido satisfactorio o ha fallado. Si el proceso ha sido satisfactorio el archivo **WP-CONFIG.PHP** será configurado como solo lectura (**644**) por razones de seguridad, si el proceso falló normalmente es porque el archivo ya era de sólo lectura. Así que si el proceso falla todo lo que necesita es abrir el archivo **WP-CONFIG.PHP** manualmente y cambiar el prefijo de las tablas a su nuevo prefijo aleatorio.

Preparando el Blog

Ahora su blog está instalado y se han tenido en cuenta al excelentes aspectos fundamentales de seguridad, ¡bien hecho!. Para seguir vamos a realizar algunos cambios sus usuarios de WP, para mejorar la seguridad.

Cambiando su nombre de usuario administrador

Debería renombrar su cuenta de administración predeterminada de **admin** a algo más difícil de adivinar, ya que todas las versiones de WP disponibles actualmente son vulnerables a la enumeración de usuarios. Cambiando la cuenta de administración predeterminada a otro nombre ayudará a mitigar los ataques de contraseña por fuerza bruta.

Nota: Debe asumir que el atacante conoce su nombre de usuario. Por tanto, asegúrese de que ha elegido una contraseña sólida.

Inicie sesión con su cuenta de administrador y cree un nuevo usuario, el cual tendrá el rol de administrador. Proporciónele una contraseña (algo que no sea fácil de adivinar, con caracteres no alfanuméricos) etcétera , puede usar el mismo email que para su Antigua cuenta de administrador, ya que vamos a borrar esa.

Después de que la cuenta haya sido creada necesita cambiar la cuenta que está usando actualmente. Ahora ha iniciado sesión con la nueva cuenta de administrador. Es hora de desprenderse de su antigua cuenta de administrador.

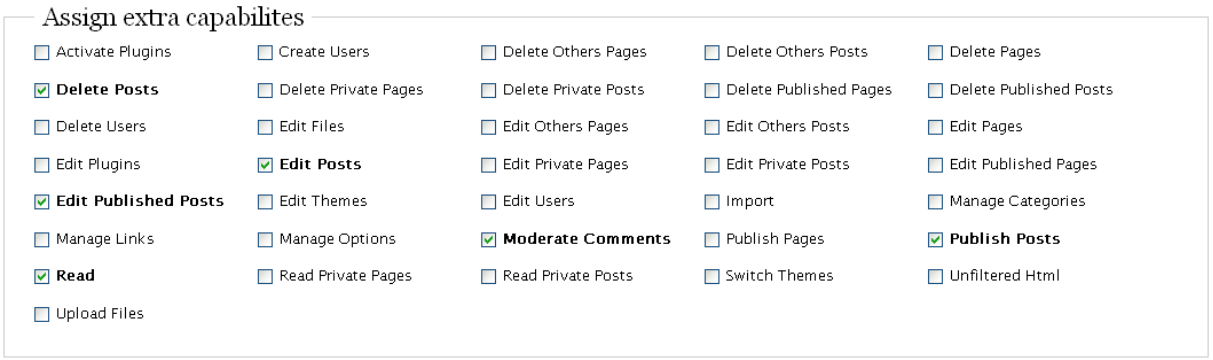
Crear un nuevo usuario de acceso limitado

Antes de comenzar con este paso debería proporcionarse a si mismo una copia la extensión Role Manager por im-web-gefunden. Esta extensión le habilitará para fijar permisos de WP granulares para cada usuario. Después de que active la extensión, cree una nueva cuenta de usuario con las funciones que prefiera.

Contra menos cosas sea posible hacer con su cuenta de usuario más segura será; su nuevo usuario no debería tener un rol mayor que el de colaborador.

El rol de colaborador puede no tener permisos suficientes de manera predeterminada, por eso hemos instalado antes la extensión Role Manager. Esa extensión permite fijar **permisos adicionales** para cada usuario que no los tendría normalmente con su rol, puede cambiar los permisos de un rol o incluso crear nuevos roles.

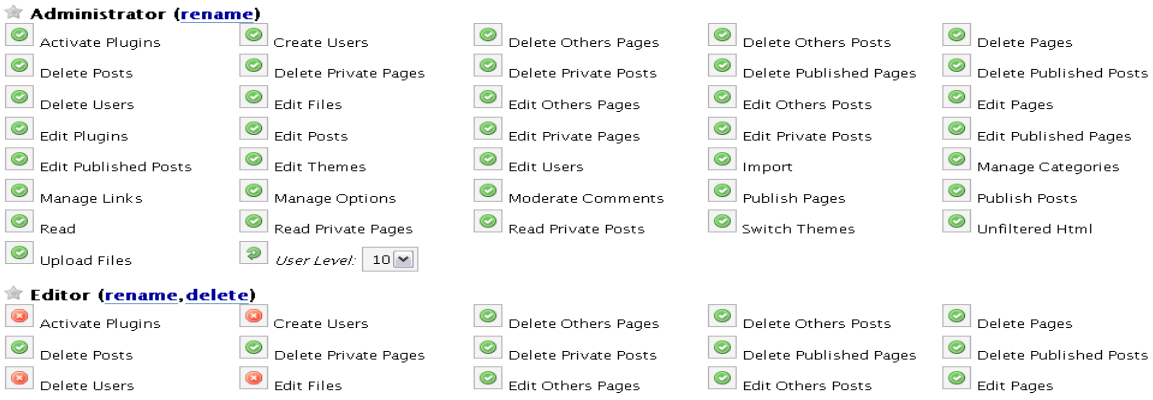
Para seguir un estándar sugerimos que a los nuevos usuarios se les de nivel de acceso "contributor", de todos modos, esta extensión le permite muchísima más flexibilidad. Como se ve debajo.



Ver: Información de Role Manager.

Si usted tiene múltiples usuarios, es mejor cambiar los permisos para el rol adicional, o quizás debería incluso crear un nuevo rol como usted quiera que puedan actuar los usuarios y dejar los roles normales como están.

Al crear usuarios, sea cauteloso de permitir a usuarios en los que no confía acceso a capacidades como "subir archivos", "acceso general a extensiones", "editar archivos/páginas/entradas", "importar" y "HTML sin filtrar", ya que estas capacidades dan al usuario muchísimo poder. En dos palabras sea prudente.



Cambiando los permisos del rol con Role Manager

Reforzando su instalación de WP[5]

Este capítulo tratará acerca de como proteger su área de administración de accesos no autorizados. Este paso es más fácil de llevar a cabo para blogs de un solo usuario, y puede ser un verdadero suplicio para blogs con múltiples usuarios. Usted tiene que decidir si quiere si quiere cargar con eso para asegurar su blog o no, pero debería.

Restringiendo wp-content y wp-includes

En este paso vamos a limitar el acceso a estos directorios, principalmente vamos a denegar de forma general todo, excepto las peticiones de imágenes, CSS y algunos archivos JavaScript.

Necesita poner este código para las carpetas **WP-CONTENT** y **WP-INCLUDES** en su archivo **.HTACCESS**:

```
Order Allow,Deny
Deny from all
<Files ~ ".(css|jpe?g|png|gif|js)$">
 Allow from all
</Files>
```

Nota: Puede que quiera añadir acceso a archivos PHP ”específicos” para ciertas plantillas y extensiones.

Restringiendo wp-admin

Bloqueando todas las IP menos la suya

Si usted administra un blog de un único usuario, puede que quiera restringir el acceso a través de IP a su directorio **WP-ADMIN**. Asegúrese de que tiene una dirección IP estática (una que no cambia) antes de hacer esto. El archivo **.HTACCESS** dentro de **WP-ADMIN** debería parecerse a este:

```
Order deny,allow
Allow from a.b.c.d #That’s your static IP
Please add some example for allowed ip ranges
Deny from all
```

Guarde el archivo e intente acceder a la carpeta wp-admin a través de un proxy web; debería ser bloqueado si todo está funcionando correctamente. Después de eso intente acceder directamente con su IP (a.b.c.d).

Si todo funciona correctamente **WP-ADMIN** estará ahora restringido solo a la(s) IP(s) de su elección.

Contraseña obligatoria - .htpasswd

Ciertamente la opción preferida es usar protección por contraseña. Esto significa que usted puede seguir accediendo a su directorio de administración desde cualquier sitio, no obstante, añade una capa adicional de seguridad.

[5] El artículo original puede encontrarse aquí: http://blogsecurity.net/WordPress/article-210607/

El archivo .htaccess

El archivo **.HTACCESS** dentro de **WP-ADMIN** debería parecerse a algo así:

> *AuthUserFile /srv/www/user1/.htpasswd #this file should be outside your webroot.*
> *AuthType Basic*
> *AuthName "Blog"*
> *require user youruser #making this username difficult to guess can help mitigate password brute force attacks.*

El archivo .htpasswd

Este archivo[6] debería, como ya se ha mencionado, ser colocado en algún lugar fuera de su directorio web, lo ideal es un directorio por encima de el. Para generar la contraseña encriptada puede usar: http://www.euronet.nl/~arnow/htpasswd/ pero también hay otros cuantos disponibles, simplemente introduzca su usuario y la contraseña tal cual en este formulario y entonces escriba el código resultante en el archivo **.HTPASSWD** , su archivo debería parecerse a este:

> *Yourusr:$a983seJ/a25.Aa*

Ahora pruébelo para ver si todo está funcionando; si ese no es el caso, vuelva a escribir la contraseña encriptada.

Extensiones IMPRESCINDIBLES

No todas las extensiones son potencialmente un riesgo adicional de seguridad. Este listado de extensiones puede mejorar enormemente la seguridad de su blog.

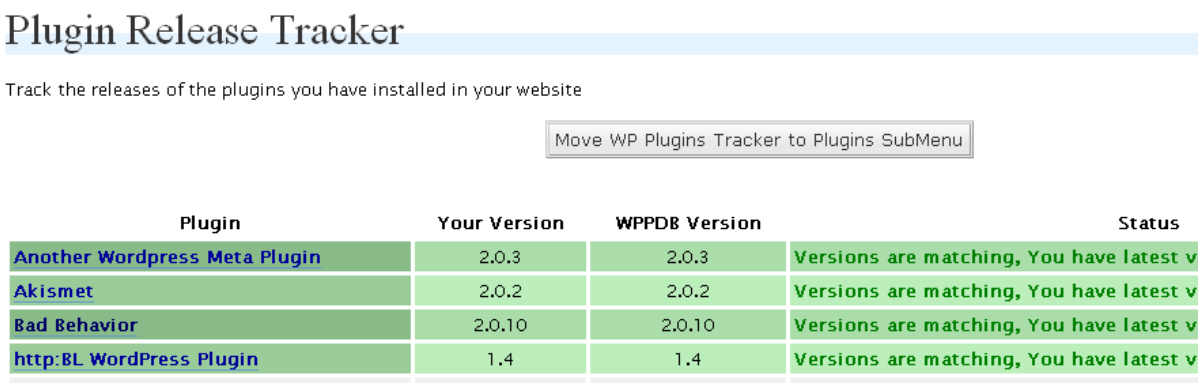
WPIDS – Detecte intrusiones

BlogSecurity ha portado PHPIDS (Sistema de Detección de Intrusos) a WordPress. PHPIDS es capaz de detectar varios intentos de intrusión. Usamos esta facilidad para bloquear ataques peligrosos. Cada intrusión es registrada en la base de datos, para que pueda realizar un seguimiento y tomar las precauciones que sean necesarias. Le será posible recibir un email si el impacto es mayor que un valor definido (cada intrusión tiene su propia puntuación de riesgo). También puede bloquear la IP del atacante por un número determinado de días no tiene una puntuación baja, de todos modos, en todos los casos WPIDS intentará sanear la introducción de datos maliciosa. Puede obtener su copia desde el sitio web oficial de PHPIDS. Nota: Para ser capaz de usar esta extensión necesita tener al menos PHP 5.1.6 o superior. Pronto será publicada una nueva versión de WPIDS que incluirá el reciente añadido de BlogSecurity, WP-Lockdown, así que permanezca atento.

[6] Puede encontrar más información acerca de ese archivo aquí: http://httpd.apache.org/docs/1.3/mod/mod_auth.html

WordPress Plugin Tracker – ¿Está usted actualizado?

Si acaba de instalar su blog y todas las extensiones desde el sitio web del desarrollador ya debería estar ejecutando la última versión. Debería instalar la extensión WordPress Plugin Tracker para estar al tanto de si usted está usando las últimas versiones de las extensiones. Después de que haya instalado y activado la extensión, ejecútelo para ver si está usando la versión actual de sus extensiones. Debería ver algo como esto:



Plugin Release Tracker

Track the releases of the plugins you have installed in your website

Move WP Plugins Tracker to Plugins SubMenu

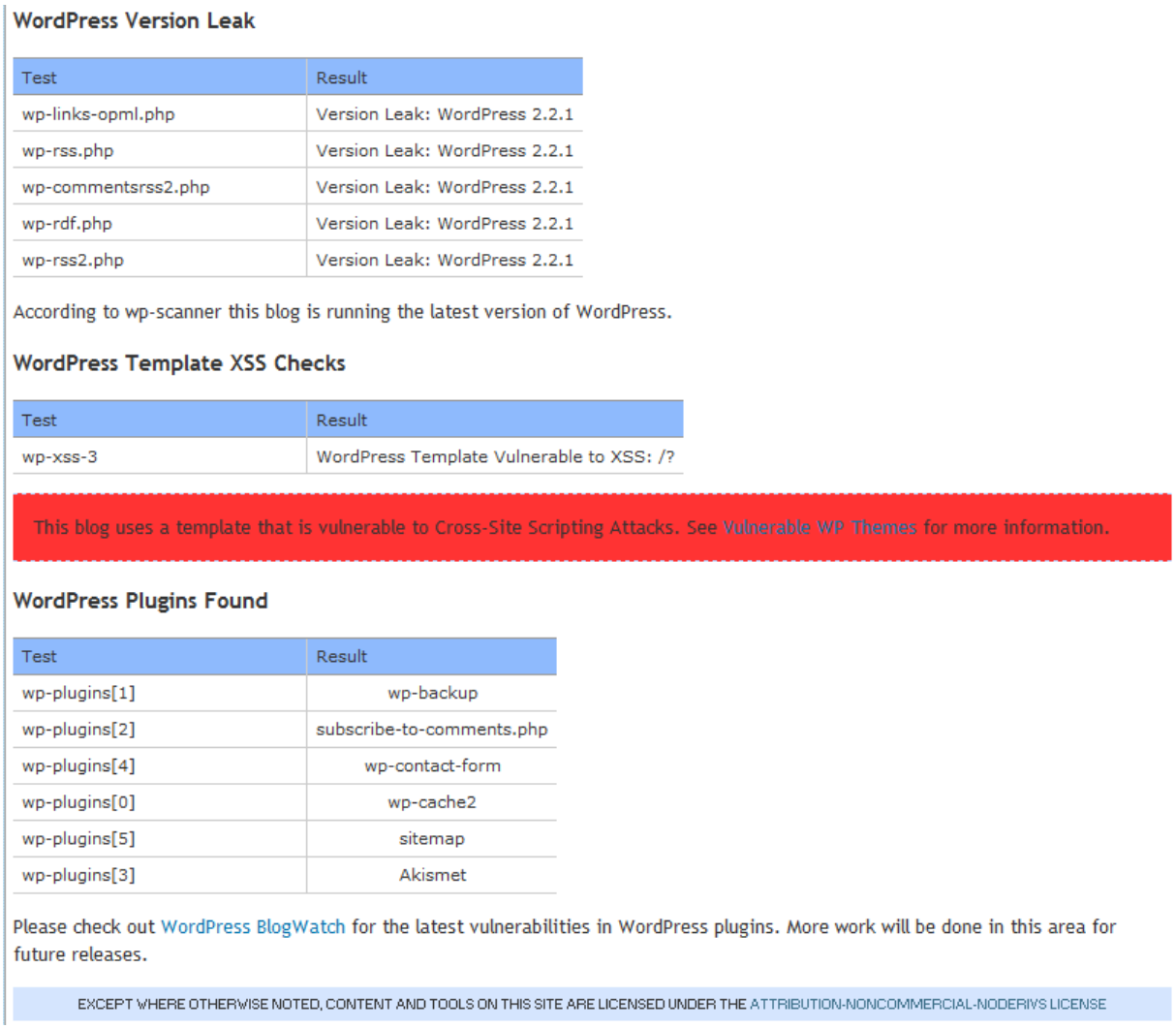
Plugin	Your Version	WPPDB Version	Status
Another Wordpress Meta Plugin	2.0.3	2.0.3	Versions are matching, You have latest v
Akismet	2.0.2	2.0.2	Versions are matching, You have latest v
Bad Behavior	2.0.10	2.0.10	Versions are matching, You have latest v
http:BL WordPress Plugin	1.4	1.4	Versions are matching, You have latest v

Así es la apariencia de la página de ejemplo de Plugin Release Tracker

Si algunas extensiones no están actualizadas, se le notificará acerca de ello y haciendo clic en el título de la extensión a la izquierda, será llevado fácilmente a la página de la extensión donde podrá obtener la actualización. Así es fácil mantener su blog actualizado.

Escáner de seguridad online de WordPress

BlogSecurity ha escrito una herramienta de comprobación de seguridad en WordPress, para comprobar si su blog tiene debilidades de seguridad habituales. Es excelente enumerando extensiones, comprobando vulnerabilidades de XSS y mucho más.



WordPress Version Leak

Test	Result
wp-links-opml.php	Version Leak: WordPress 2.2.1
wp-rss.php	Version Leak: WordPress 2.2.1
wp-commentsrss2.php	Version Leak: WordPress 2.2.1
wp-rdf.php	Version Leak: WordPress 2.2.1
wp-rss2.php	Version Leak: WordPress 2.2.1

According to wp-scanner this blog is running the latest version of WordPress.

WordPress Template XSS Checks

Test	Result
wp-xss-3	WordPress Template Vulnerable to XSS: /?

This blog uses a template that is vulnerable to Cross-Site Scripting Attacks. See Vulnerable WP Themes for more information.

WordPress Plugins Found

Test	Result
wp-plugins[1]	wp-backup
wp-plugins[2]	subscribe-to-comments.php
wp-plugins[4]	wp-contact-form
wp-plugins[0]	wp-cache2
wp-plugins[5]	sitemap
wp-plugins[3]	Akismet

Please check out WordPress BlogWatch for the latest vulnerabilities in WordPress plugins. More work will be done in this area for future releases.

WP-Scanner es un servicio online gratuito y ha comprobado más de 5000 blogs hasta la fecha. Consulte más información aquí.

Fin

Hemos llegado al final de nuestro documento de referencia. Esperamos que lo haya disfrutado, y que haya tenido éxito implementando estos pasos de seguridad vitales. Siempre es un placer obtener opiniones y sus experiencias, así que por favor contacte con nosotros.

Traductor: Samuel Aguilera http://agamum.net/blog/