WordPress

Twitter: @marianoingerto
Facebook: mpiestudio
Blog: www.estudiompi.com.ar/blog/

¿Porqué hacerlo?

Una de las razones más habituales para no prestar atención a la seguridad pensar que nunca seremos un blanco de ataque porque no tenemos un blog o una web conocida, o nuestra información es publica y creamos que no tiene valor, sin embargo la mayoría de los ataques no son para destruir o robar datos de los sitios sino infectarlos con malware, que es por decirlo de una manera simple: virus para la web.

¿Como eligen a una pagina para ser atacada? Casi siempre peinando Internet de forma automatizada mediante programas buscando sitios que cumplan ciertos requisitos, por ejemplo que tengan un WordPress instalado, preferiblemente desactualizado o de una versión especifica ya que contiene un agujero de seguridad conocido listo para explotarlo y que les sirva como punto de entrada, en cada momento millones de paginas webs son atacadas en forma constante con el fin de infectar esos sitios, no por su contenido sino para usarla para alojar Malware, para enviar spam o para lanzar ataques a otras webs y un sin fin de actividades delictivas.

¿Qué hacer?

No utilices el prefijo wp_ para la base de datos

- Desde el primer momento de la instalación de WordPress hay que especificar una serie de información que hay que introducir para que WordPress se comunique con la base de datos.

- Por defecto, en esta pantalla el prefijo ofrecido es wp_, de manera que tus tablas quedarán tal que wp_options, wp_comments, wp_posts, etc.

No utilices el prefijo wp_ para la base de datos

- Y, por supuesto, esto es algo que todo hacker sabe, y es **información gratuita que damos a cualquier posible atacante**.

- Así que **el primer lugar donde debemos empezar a asegurar WordPress es antes incluso de instalarlo**, en este paso: cambiamos el prefijo para las tablas por defecto (wp_) por otro a elección, lo que queramos. Lo importante no es lo largo o complicado que sea sino que, al menos, no dejes el prefijo por defecto.

A continuación deberás introducir los detalles de conexión a tu base de datos. Si no estás seguro de esta información contacta con tu proveedor de alojamiento web.

Nombre de la base de datos	nombre_base_datos	El nombre de la base de datos en la que quieres ejecutar WordPress.
Nombre de Usuario	nombre_de_usuario	Tu usuario de MySQL
Contraseña	contraseña_base_datos	...y tu contraseña de MySQL.
Servidor de la base de datos	localhost	Deberías poder acceder desde tu servidor web si `localhost` no funciona.
Prefijo de tabla	wp_	Si quieres ejecutar varias instalaciones de WordPress en una sola base de datos cambia esto.

Enviar

cambia el prefijo de tabla

No utilices el usuario admin para acceder a WordPress

- Otra de las decisiones que tenemos que tomar durante la instalación de WordPress **es el nombre del primer usuario para acceder a la administración de nuestra web**, usuario que por defecto tendrá permisos totales de gestión de la misma.

- En el momento de elegir el nombre de tu primer usuario para acceder a WordPress no elijas aquellos nombres comunes para esta tarea, como *admin*, *Admin*, *root*, etc., ya que son los primeros que comprobará un hacker que quiera tomar posesión de tu web.

Hola

¡Bienvenido al famoso proceso de instalación de WordPress en cinco minutos! Simplemente completa la información siguiente y estarás a punto de usar la más enriquecedora y potente plataforma de publicación personal del mundo.

Información necesaria

Por favor, debes facilitarnos los siguientes datos. No te preocupes, siempre podrás cambiar estos ajustes más tarde.

Título del sitio Mi nueva web WordPress

cualquier nombre menos root, admin o Admin

Nombre de usuario Lo que sea menos admin

Los nombres de usuario pueden tener únicamente caracteres alfanuméricos, espacios, guiones bajos, guiones medios, puntos y el símbolo @.

Contraseña S4&2hrJgs(l!F8KL4& Ocultar

Fuerte

siempre contraseñas fuertes

Importante: Necesitas esta contraseña para acceder. Por favor, guárdala en un lugar seguro.

Tu correo electrónico

Comprueba bien tu dirección de correo electrónico antes de continuar.

Privacidad Permitir a los buscadores que indexen el sitio

Instalar WordPress

Utiliza una contraseña fuerte

- Cuanto más fácil de recordar (para nosotros) sea una contraseña, también será más fácil que los sistemas automáticos de acceso por fuerza bruta de los atacantes la consigan.

- WordPress, en sus últimas versiones, incorpora un generador de contraseñas seguras y te “sugiere” utilizarlas. Ésta será siempre la mejor opción. Podemos, no obstante, poner una contraseña sencilla, e insegura, pero sería **el principal y más importante error de seguridad** de todos los posibles.

Utiliza una contraseña fuerte

- Actualmente todos los navegadores ofrecen la posibilidad de recordar las contraseñas. Así que usemos siempre contraseñas seguras, que contengan letras en minúsculas, mayúsculas, números y caracteres especiales.

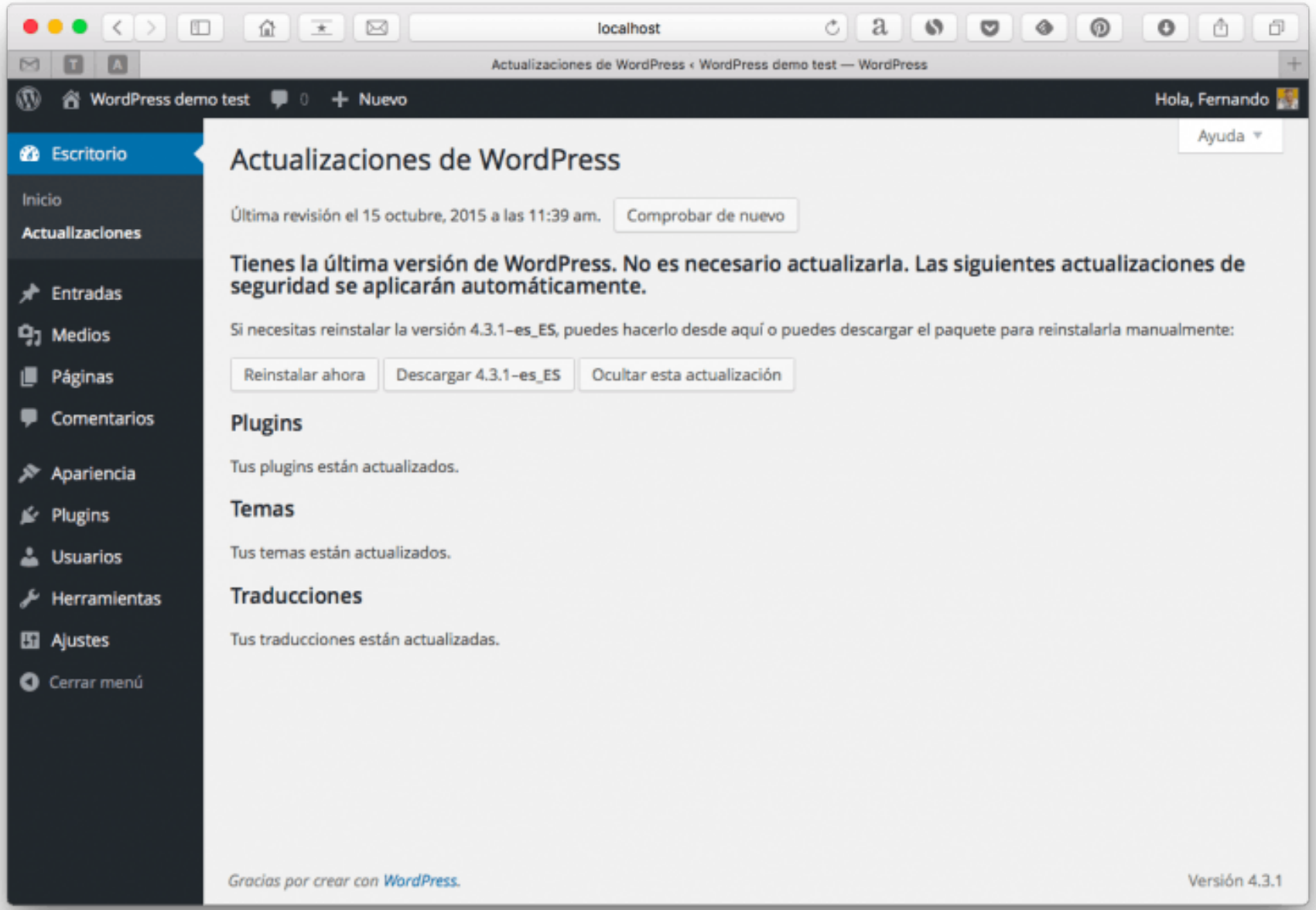
- Dos herramientas útiles:

Forzando el cambio de contraseñas cada 30 días
Reiniciando todas las contraseñas

Usa siempre la última versión de WordPress

- Si hay algo peligroso es trabajar en red con software obsoleto o no suficientemente actualizado. **Los hackers suelen atacar principalmente sitios con versiones antiguas, no actualizadas**, pues suelen ser más vulnerables al no incorporar la suficiente protección a tipos de ataque conocidos.

- Afortunadamente, WordPress ofrece un sistema de actualizaciones automáticas, tanto para el mismo núcleo de WordPress como para plugins y temas.


localhost
Actualizaciones de WordPress ‹ WordPress demo test — WordPress
WordPress demo test
0
Nuevo
Hola, Fernando
Escritorio
Inicio
Actualizaciones
Entradas
Medios
Páginas
Comentarios
Apariencia
Plugins
Usuarios
Herramientas
Ajustes
Cerrar menú
Ayuda
Actualizaciones de WordPress
Última revisión el 15 octubre, 2015 a las 11:39 am.
Comprobar de nuevo
Tienes la última versión de WordPress. No es necesario actualizarla. Las siguientes actualizaciones de seguridad se aplicarán automáticamente.
Si necesitas reinstalar la versión 4.3.1–es_ES, puedes hacerlo desde aquí o puedes descargar el paquete para reinstalarla manualmente:
Reinstalar ahora
Descargar 4.3.1–es_ES
Ocultar esta actualización
Plugins
Tus plugins están actualizados.
Temas
Tus temas están actualizados.
Traducciones
Tus traducciones están actualizadas.
Gracias por crear con WordPress.
Versión 4.3.1

Usa siempre la última versión de WordPress

- Por defecto, no deberemos preocuparnos de las actualizaciones de mantenimiento y seguridad de WordPress, pues las hace sin tu intervención. Simplemente avisará cuando se haya actualizado. Pero sí deberemos realizar, aunque sea con un simple clic, las actualizaciones a las versiones denominadas “mayores”.

- Por ejemplo, no hace falta tu intervención para actualizar de la versión 4.3.1 a la 4.3.2, WordPress las actualiza por ti. Pero sí desde la 4.3.x a la 4.4, aunque el proceso sea tan rápido y tan sencillo como pulsar un botón.

Actualiza los plugins instalados

- WordPress es seguro, y es normal que así sea porque hay una gran comunidad que se ocupa de su mantenimiento, desarrollo y crecimiento, pero no pasa lo mismo con los plugins.

- Por muy utilizado que sea un plugin, muchas veces detrás hay un único programador que, por razones obvias, no dispone de los recursos ni el tiempo necesarios para tener siempre su plugin al día.

Actualiza los plugins instalados

- La principal vía de entrada de ataques a una instalación WordPress es en su mayoría a través de plugins sin actualizar.
- WordPress nos ofrece un sistema de aviso y actualizaciones automáticas de los plugins instalados.
- En caso de no utilizar plugins del directorio oficial es posible que WordPress no identifique automáticamente si hay actualizaciones disponibles. En ese caso deberemos estar pendiente de la web del desarrollador.

Actualiza el tema activo

- Igualmente importante es usar siempre una versión actualizada del tema activo, pues los hackers saben que no se suelen cambiar muy a menudo, lo que les da tiempo para aprender de su código e inventarse modos de hacerte la vida más complicada e incluso meterte en problemas.

- Si usas un tema del directorio oficial, de nuevo, WordPress te avisará de las actualizaciones. Y si utilizas uno adquirido en otro sitio deberemos estar pendiente de las noticias de su creador para actualizarlo.

No utilices plugins o temas obsoletos

- Una de las más importantes fuentes de vulnerabilidad son los plugins y temas obsoletos o abandonados por sus desarrolladores. Frecuentemente debemos comprobar si se han actualizado recientemente y, en caso contrario, buscar una alternativa que ofrezca las mismas prestaciones.

- Si utilizamos temas y plugins del directorio oficial de WordPress encontraremos toda la información disponible, como la fecha de la última actualización y la compatibilidad con las últimas versiones de WordPress.

No utilices plugins o temas obsoletos

- Además, el directorio oficial de WordPress retira automáticamente plugins y temas que no se hayan actualizado durante más de dos años, lo que supone una garantía adicional.

- En caso de utilizar temas y plugins descargados de otros sitios deberenos comprobarlo en su propia web e instalar manualmente cualquier actualización.

Borra los plugins y temas que no utilices

- Es un peligro tener instalados plugins y temas inactivos, por la sencilla razón de que les prestaremos menos atención al no estar activos. No solo ocupan espacio en tu alojamiento sino que suponen una vía de entrada a posibles vulnerabilidades en tu web.

- El único tema no activo que deberiamos dejar instalado es el último tema por defecto de WordPress, ya que si WordPress detecta un problema en tu tema activo y no puede cargarlo intentará activar automáticamente el tema por defecto si lo encuentra instalado.

Descarga plugins y temas de sitios seguros

- El sitio más seguro para descargar plugins y temas es el directorio oficial, en cuyas direcciones hay versiones actualizadas, comprobadas y seguras de los últimos desarrollos. Son los temas y plugins que podemos instalar desde el instalador incluido en WordPress, y que también podemos visitar en las siguientes direcciones:

- https://es.wordpress.org/plugins/

- https://es.wordpress.org/themes/

Descarga plugins y temas de sitios seguros

- Además, hay mercados de temas y plugins como Envato, Woothemes o Elegant Themes, de gran calidad y cuidado por sus productos.

- Por supuesto, nunca debemos descargar plugins y temas de las redes P2P como Torrent o eMule, suelen estar todos infectados de virus y malware.

Haz copias de seguridad

- Si hay una regla fija en la seguridad es que da igual las medidas que apliquemos, siempre habrá alguna vulnerabilidad nueva para la que no estemos protegidos, siempre iremos un paso por detrás de los ataques malintencionados.

- Así que, en caso de desastre, lo único que nos puede salvar de una eventual pérdida de todo nuestro contenido es disponer de copias de seguridad.

Haz copias de seguridad

- Debemos comprobar que nuestro proveedor de alojamiento web disponga de copias de seguridad automáticas completas.

- Y, además, instalar un plugin de copias de seguridad como BackWPup, que te permite programar distintas tareas de copia de seguridad, pudiendo guardar tus copias en otro servidor, enviarlas por email, o incluso automatizar su guardado en servicios Cloud como DropBox, Amazon S3 o Google Drive, entre otros.

Haz copias de seguridad

- Debemos comprobar que nuestro proveedor de alojamiento web disponga de copias de seguridad automáticas completas.

- Y, además, instalar un plugin de copias de seguridad como BackWPup, que te permite programar distintas tareas de copia de seguridad, pudiendo guardar tus copias en otro servidor, enviarlas por email, o incluso automatizar su guardado en servicios Cloud como DropBox, Amazon S3 o Google Drive, entre otros.

Haz copias de seguridad

Por Inpsyde GmbH

Instala un plugin de seguridad

- Muchas de las medidas de protección que podemos aplicar a nuestra instalación de WordPress vienen incluidas en plugins especializados en asegurar WordPress.

- La mayoría de ellos contienen ajustes para evitar ataques de fuerza bruta, inyecciones de código y modificaciones de archivos de sistema, incluyendo sistemas de aviso para que estés informado de cualquier posible ataque en curso.

Instala un plugin de seguridad

- Muchas de las medidas de protección que podemos aplicar a nuestra instalación de WordPress vienen incluidas en plugins especializados en asegurar WordPress.

- La mayoría de ellos contienen ajustes para evitar ataques de fuerza bruta, inyecciones de código y modificaciones de archivos de sistema, incluyendo sistemas de aviso para que estés informado de cualquier posible ataque en curso.

Instala un plugin de seguridad

- Los más recomendables son los siguientes:

- WordFence
- iThemes Security
- Bulletproof

iThemes Security

iThemes Security

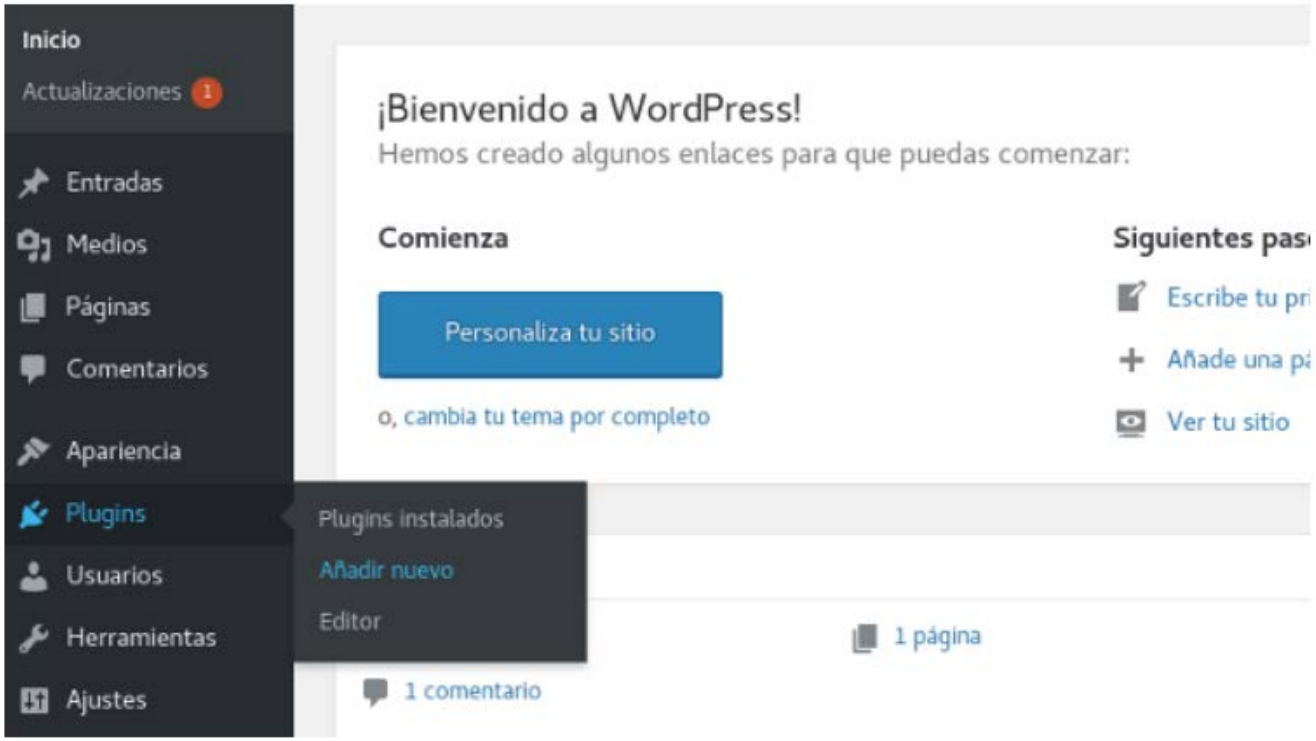
Cómo configurar iThemes Security (better WP security)

Hay varios vectores de ataques que se suele utilizar para vulnerar una web, el gestor de contenido desactualizado, plugins en la misma condición, incluso hasta el theme, es decir hasta el diseño del sitio puede ser vulnerado y usado como punto de entrada para infectar la web, por dicha razón siempre es fundamental actualizar WordPress, la instalación y los plugins que usemos.

En el caso de WordPress afortunadamente tenemos plugins de muy buena calidad que nos ayudaran a proteger nuestro sitio, tal es el caso de **iThemes Security** un fantástico complemento, muy completo que si bien tiene una versión de pago aun en su versión gratuita incluye funciones avanzadas y muy útiles, y de esta ultima versión gratuita es de la que vamos a mostrar hoy.

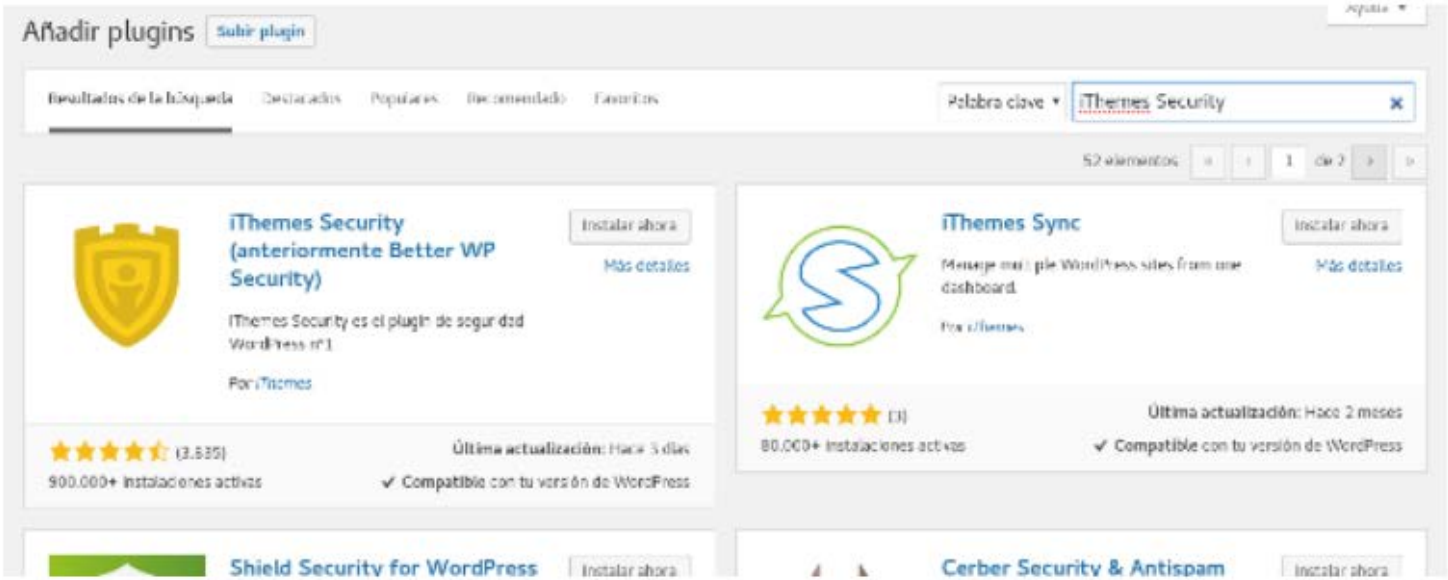
iThemes Security

Para instalar el plugin es muy fácil, luego de ingresar a nuestro administrador WordPress vamos a plugins, luego a Añadir Nuevo.

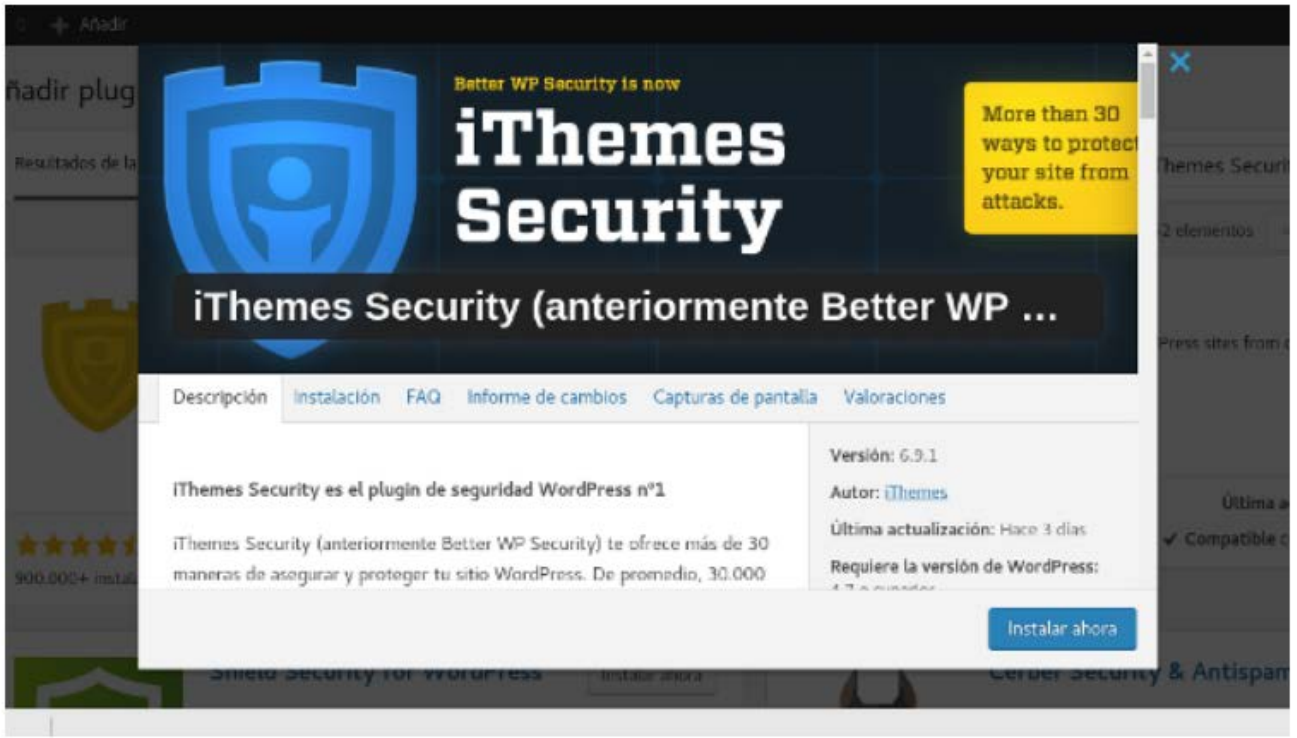


iThemes Security

En el buscador de la derecha escribimos **iThemes Security** y presionamos enter, cuando lo encontremos pulsamos en **Instalar Ahora** y seguimos los pasos de instalación

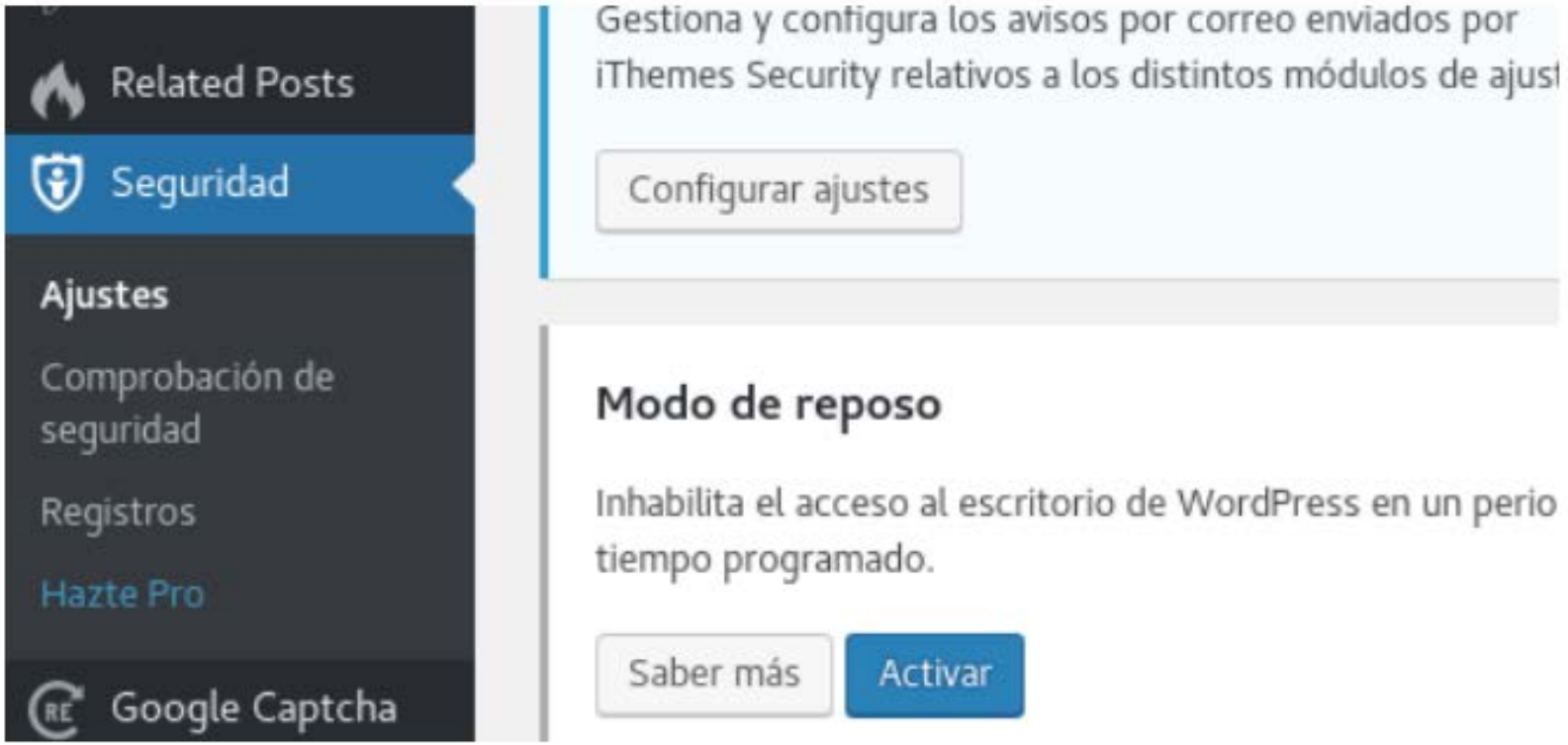


iThemes Security



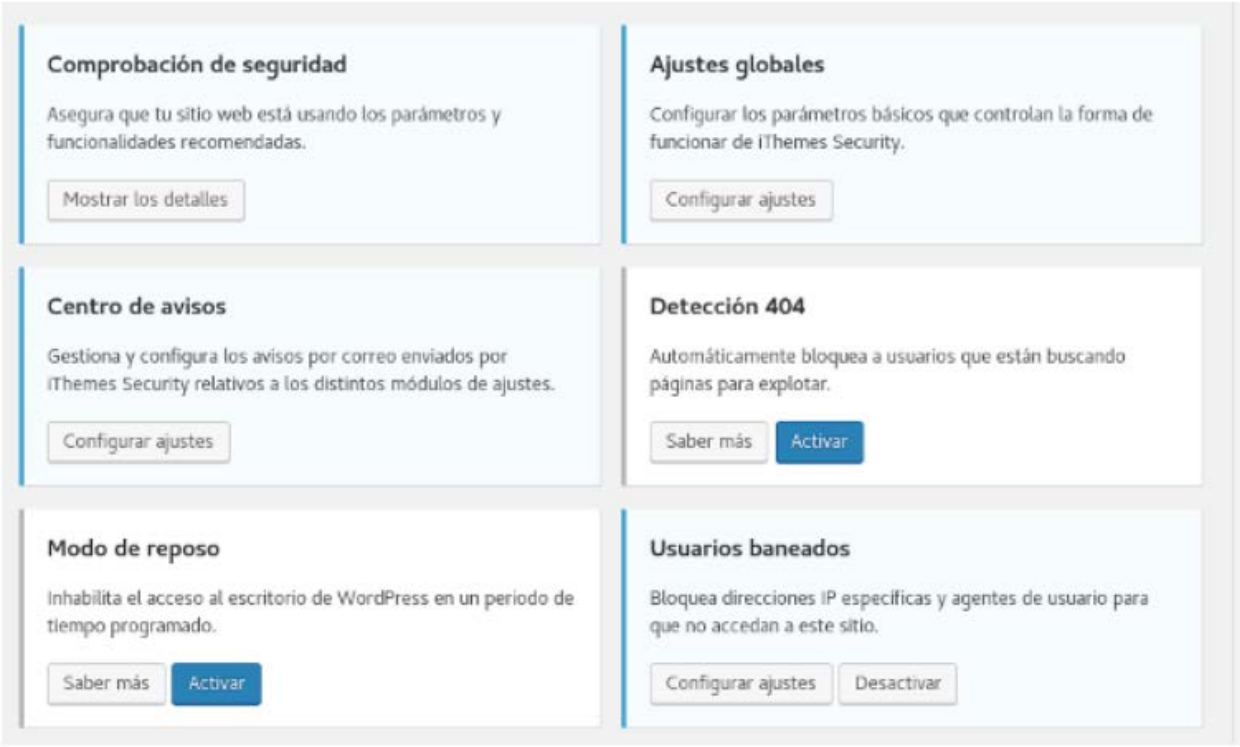
En este punto ya tenemos el plugin instalado y listo para configurar, desde el menú de la izquierda vamos a la opción **Seguridad** y nos mostrara la pantalla principal de configuración de nuestro plugin

iThemes Security



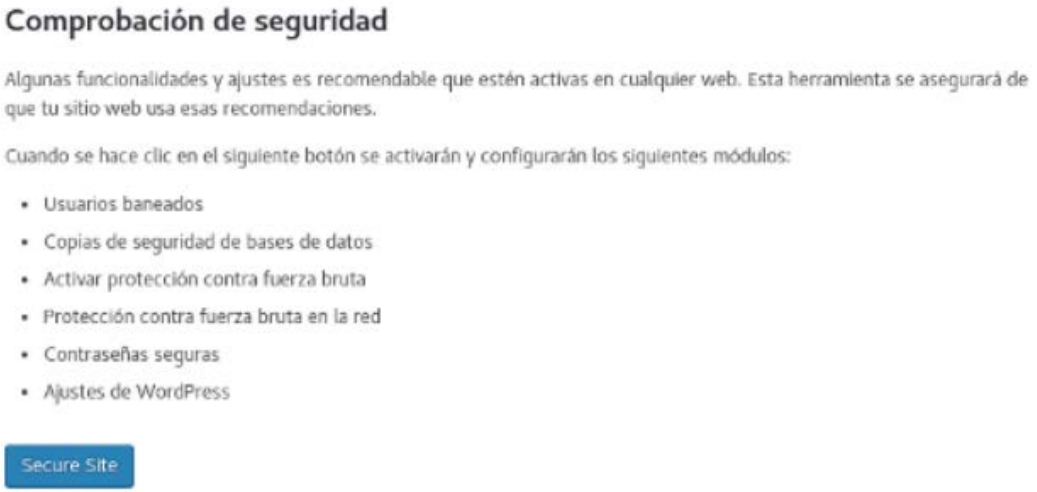
iThemes Security

Desde este panel podemos configurar todo el plugin, las opciones son bastante extensas, vamos a repasar los puntos mas importantes como por ejemplo la comprobación de seguridad en la cual si nos apareciera algo en amarillo o en rojo nos conviene arreglarlo, por eso dentro de **Comprobación de seguridad** pulsamos **Mostrar los Detalles**.



iThemes Security

En la imagen anterior vemos la opción comprobación de seguridad, una vez que ingresemos nos aparecerá la siguiente ventana de abajo de este texto, indicándonos que se va a comprobar, una vez que pulsemos el botón **Secure Site** se iniciara el proceso, luego nos mostrara los resultados de, si nos aparece los tics en verde quiere decir que esta todo bien, si aparece en otro color nos conviene revisar de que se trata y solucionarlo dado que son recomendaciones básicas aunque muy importantes.



iThemes Security

Una vez analizado el punto anterior todavía hay otras configuraciones que también nos conviene revisar y ajustar como son las secciones de **Activar protección contra fuerza bruta**, **Ajustes del Sistema** y **Ajustes de WordPress**

iThemes Security

Activar protección contra fuerza bruta

Una de las principales desventajas de WordPress en cuanto a seguridad es que permite a un atacante probar una y otra vez contraseñas al azar para ver si con alguna puede abrir el sitio, puede llegar a probar cientos de contraseñas por segundo así que con suficiente tiempo un atacante puede "adivinar" nuestra contraseña, esto es lo que se conoce como ataque de fuerza bruta, por suerte este plugin cuenta con protección contra este tipo de ataques limitando la cantidad de contraseñas erróneas que un atacante puede introducir y luego bloquearlo, esto lo podemos configurar desde **Activar protección contra fuerza bruta** .

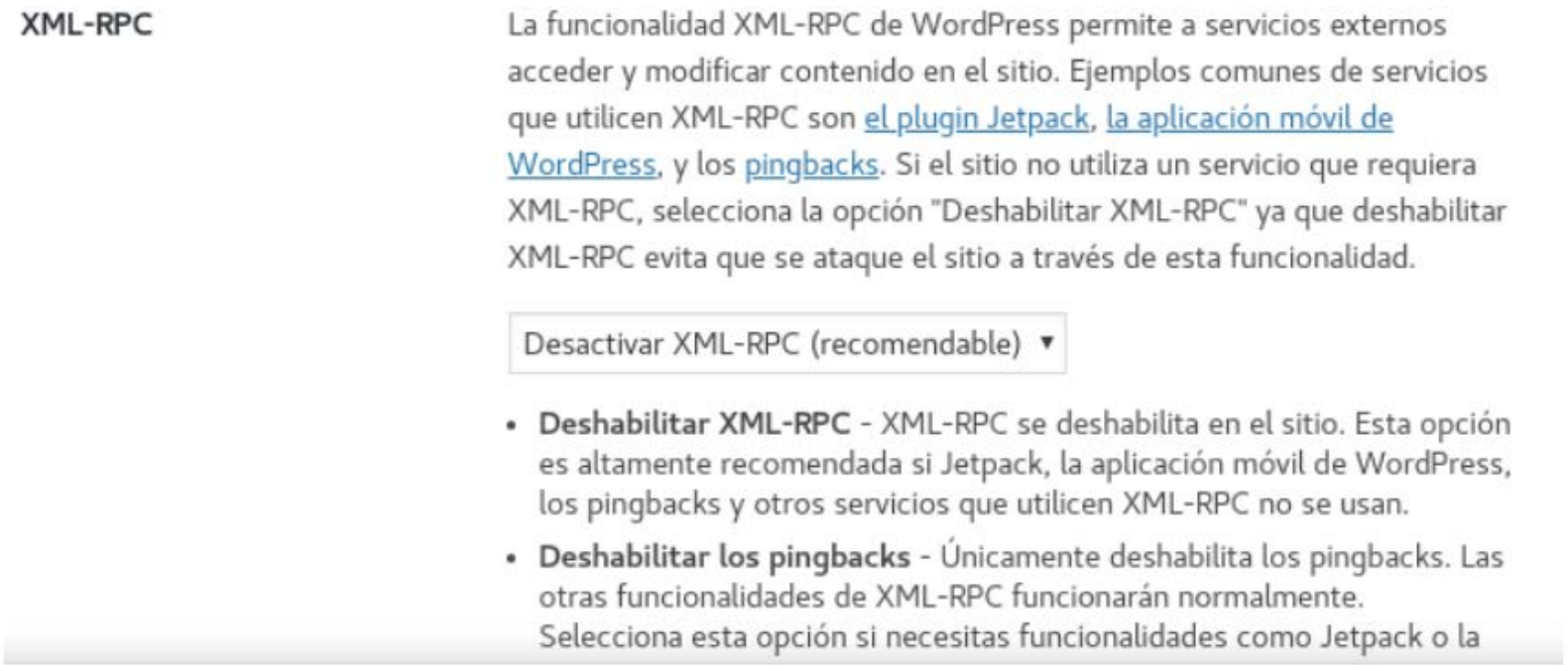
iThemes Security

Ajustes del sistema y Ajustes de WordPress

Dentro de **Ajustes de Wordpress** hay dos valor que nos conviene ajustar porque son susceptibles de ataques por fuerza bruta al igual que el login y estos son las opciones de **XML-RPC** y **Múltiples intentos de autenticación por petición XML-RPC**, si nuestro sitio no hace uso de **XML-RPC** nos conviene desactivarlo por lo que lo marcamos como **Desactivar XML-RPC.**

En el caso de **Múltiples intentos de autenticación por petición XML-RPC** marcamos la opción **Bloquear** ya este es uno de los principales blancos de ataques de fuera bruta, tal como muestra la siguiente imagen.

iThemes Security



Con resto de los ajustes hay que tener cuidado debido a que si bien detienen ataques también pueden bloquear otros plugins así que sino tenemos claro que es entonces es mejor dejarlo con la configuración por defecto.

iThemes Security

Detección de cambios de archivo

La detección cambios en los archivos es una utilidad interesante aunque puede resultar un tanto molesta también dependiendo de como usemos el sitio, la función consiste en controlar día a día todos los archivos que cambian en el sitio y te mostrara una lista, si nuestro sitio no subimos contenido seguido es muy útil para detectar Malware por ejemplo.

Sin embargo si subimos archivos o fotos seguido o usamos un plugin de cache por ejemplo, la lista de archivo modificados diariamente puede contener cientos o incluso miles de archivos modificados todos los días lo que puede volverse complicado de comprobar diariamente, la recomendación es habilitarlo y si nos molesta podremos des habilitarlo mas tarde igual.

iThemes Security

Copias de seguridad de bases de datos

Una de las tareas mas importantes de cada webmaster es realizar respaldos periódicos de nuestro sitio por si ocurre un desastre, desde aquí puedes programar la realización de copias de seguridad de la base de datos y configurar donde y como quieres guardarlos.

Conclución

Siguiendo estos sencillos pasos daremos un gran salto en cuanto a seguridad de nuestro sitio aunque todavía este plugin tiene mucho más por ofrecer, hay muchas mas funciones por descubrir que podremos ir configurando a medida que lo vayamos conociendo mejor.

¡Gracias!

¿Preguntas?