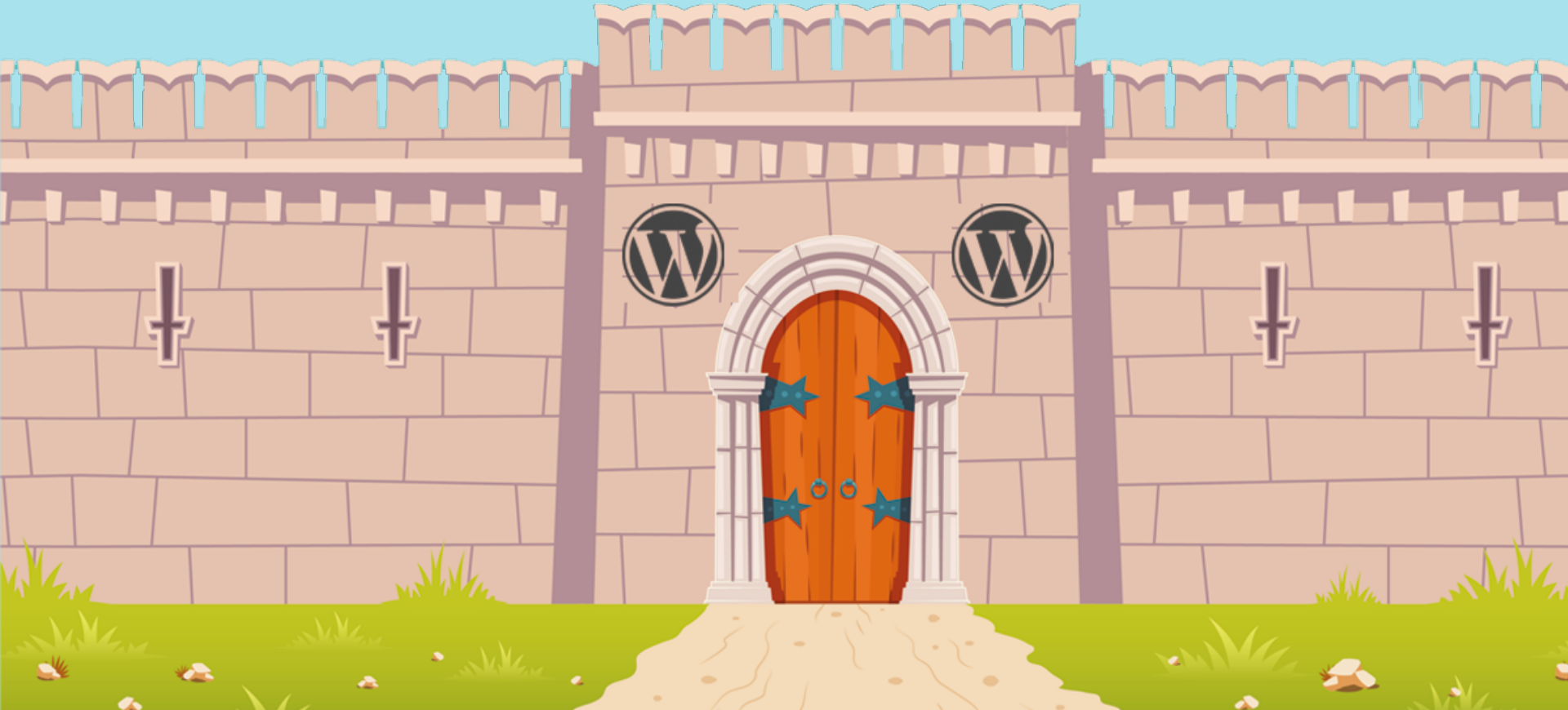
10 consejos para mantener mi WordPress Seguro

Lidia Arroyo Vargas

Proteger nuestro sitio como protegeriamos nuestro castillo



WordPress

¿Es Seguro?

¿WordPress es Seguro?

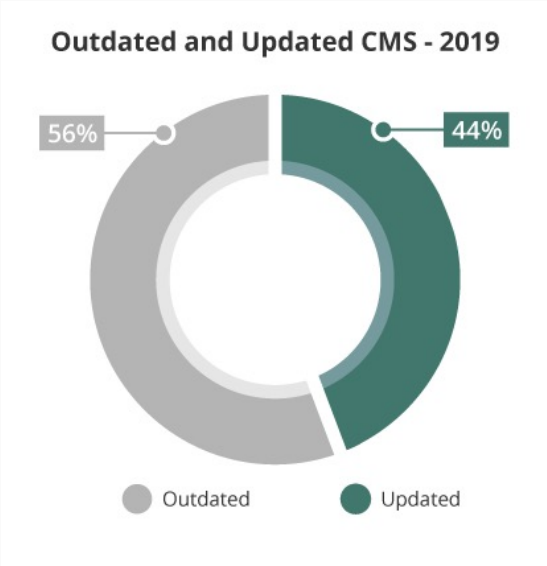
- 60.8% mercado CMS
- 500 sitios al día
- 40% sitios web
- 58.000 plugins
- CMS mayor crecimiento

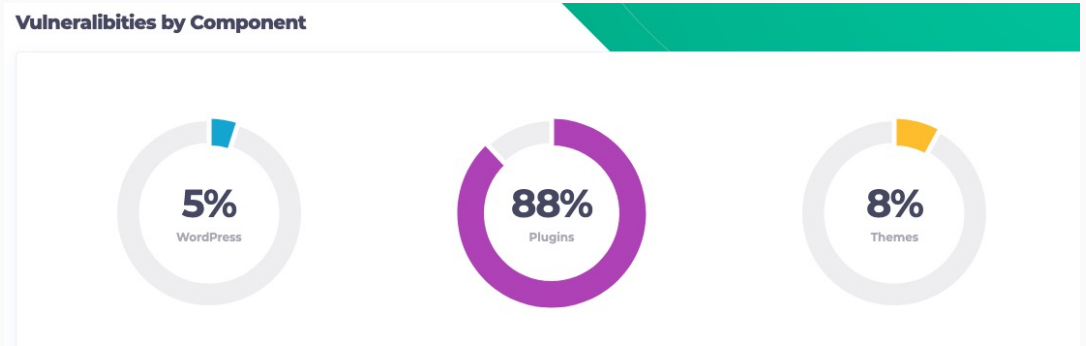
CMS con más usuarios

Blanco de los Atacantes

¿Qué puede hacer mi sitio NO SEGURO?

- Software obsoleto
- Plugins desactualizados
- Temas, plantillas



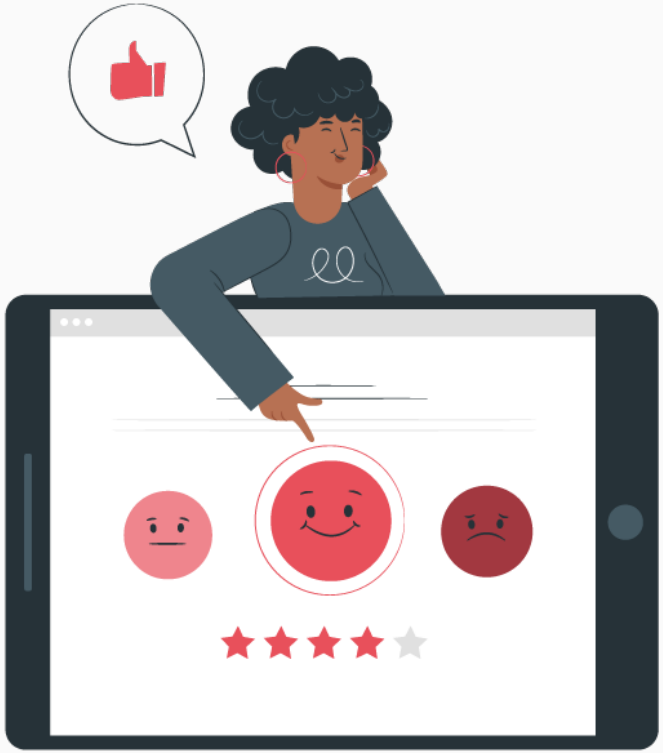


Fuente: https://wpscan.com/statistics

- Hospedajes deficientes con tecnología obsoleta

Fuente: https://blog.sucuri.net/2020/01/hacked-website-threat-report-2019.html

¿Porqué debo tomar medidas de seguridad?



Posicionamiento

Clientes

Ataques más comunes

Ataques de Fuerza Bruta

Programas automáticos

Acceden al administrador

Combinaciones Posibles

No tienen limitador de login
Primer usuario que utilizan:
”admin”

Inyección de SQL

Filtración código BD

Alterar el funcionamiento

Formularios

Campos de Comentarios

Otros

Malware

Código malicioso se inyecta a través de un tema infectado, complementos o script obsoleto.

Cross-site scripting

Ataque XSS, carga de código JS malicioso, recopila datos y redirige a otros sitios maliciosos.

Ataques DDoS

Denegación de servicio distribuido, gran volumen de solicitudes a un servidor web, hace el servidor lento y finalmente lo bloquea.

Versiones PHP

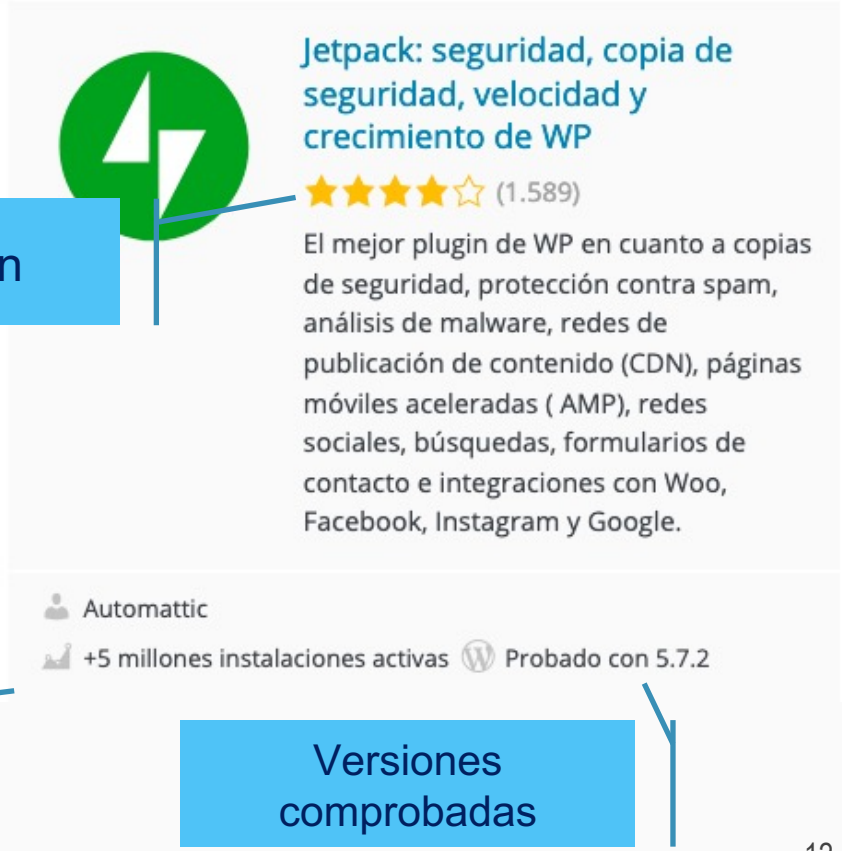
Versiones antiguas de PHP causan incompatibilidad

¿Qué hago?

1. Plugins y temas actualizados y confiables

Antes de instalar

- Verificarlo primero
- No descargar plugins de pago que ofrezcan totalmente gratis en Internet.
- Entrar periódicamente y mantenerlos actualizados.



2. Copias de Seguridad

Tener respaldado completamente tu sitio

Copia de seguridad periódica y automática

3. Contraseña

Débil: 6 – 15 caracteres
Fuerte: 16 – 36 caracteres

- Símbolos
- Números
- minúsculas
- Mayúsculas
- Cambiarla cada cierto tiempo.

No usar la misma contraseña en varios proyectos.

¿Qué hago cuando tengo más usuarios?

- Suscriptor
- Autor
- Editor
- etc

Forzarlos a generar contraseñas seguras

- Caducidad de la contraseña
- Forzar cambio de contraseña
- Fuerza: longitud mínima y máxima.
- Restricciones (A,a,#,1)
- Muestra la seguridad de la contraseña.
- Obliga a todos los usuarios a cumplir con la política configurada.
- Restablecimiento a un clic

https://es.wordpress.org/plugins/password-policy-manager/

4. Ruta de Acceso al *Admin* de WordPress

midominio.com/wp-admin

Cambiar la ruta de ingreso

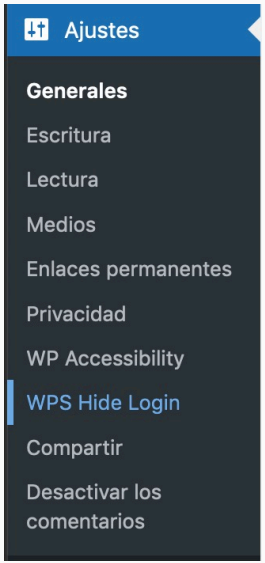
No utilizar el usuario: *admin*

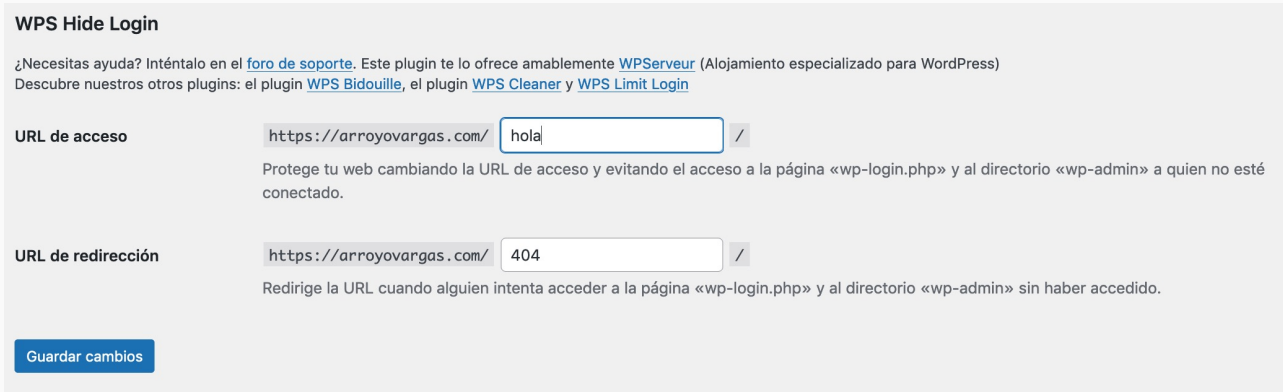
WPS Hide Login

Permite cambiar la URL del Login

Ventajas

- No hace cambios en la BD
- En caso de desactivarlo, la configuración de WP será la misma que antes.
- Disminuye los ataques de fuerza bruta





5. Firewall y Antivirus

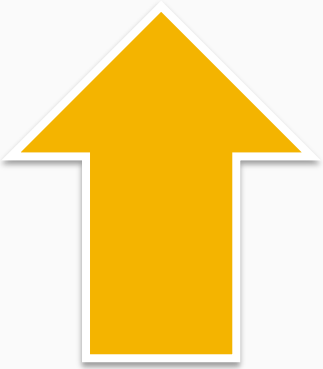
- Monitoreo de seguridad activa
- Análisis de archivos
- Análisis de malware
- Monitoreo de la blacklist
- Endurecimiento de seguridad
- Firewalls
- Protección ante ataques de fuerza bruta
- Notificaciones cuando se detecta una amenaza a la seguridad

+ Popular

- Sitio Web

+ Ataques

- Inserción de Código



Opciones

Versión gratuita, limitada

- Auditoría de actividad
- Monitoreo archivos
- Listas negras
- Notificaciones Seguridad

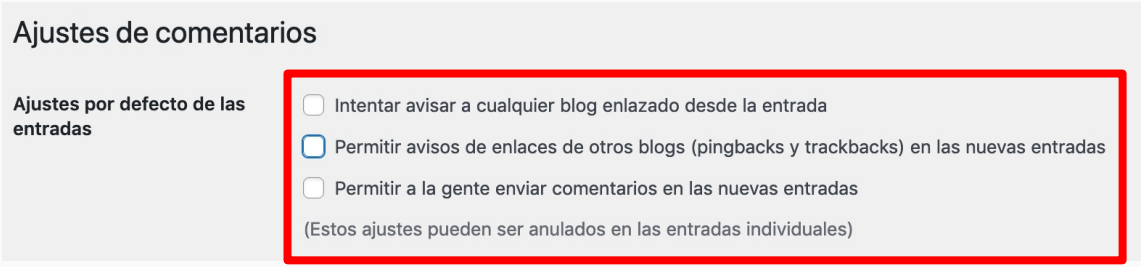
Versión gratuita muy completa

- Firewall – Bloqueo de país, manual de IP, protección de fuerza bruta
- Escaneo de malware
- Amenazas de tiempo real y spam
- Monitoreo tráfico en vivo
- Notificación de actualizaciones

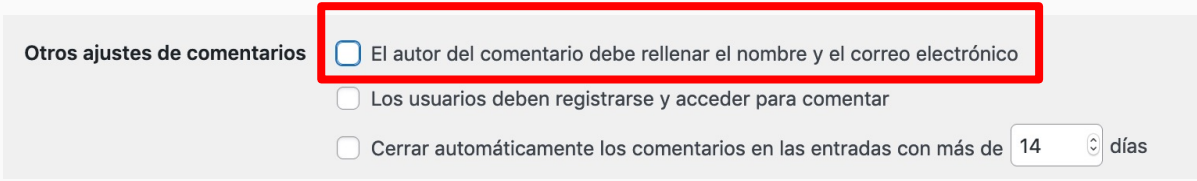
6. Controlar o bloquear el spam de los comentarios

Ajustes / Comentarios

Desactivar los comentario



Apagar los comentarios anónimos

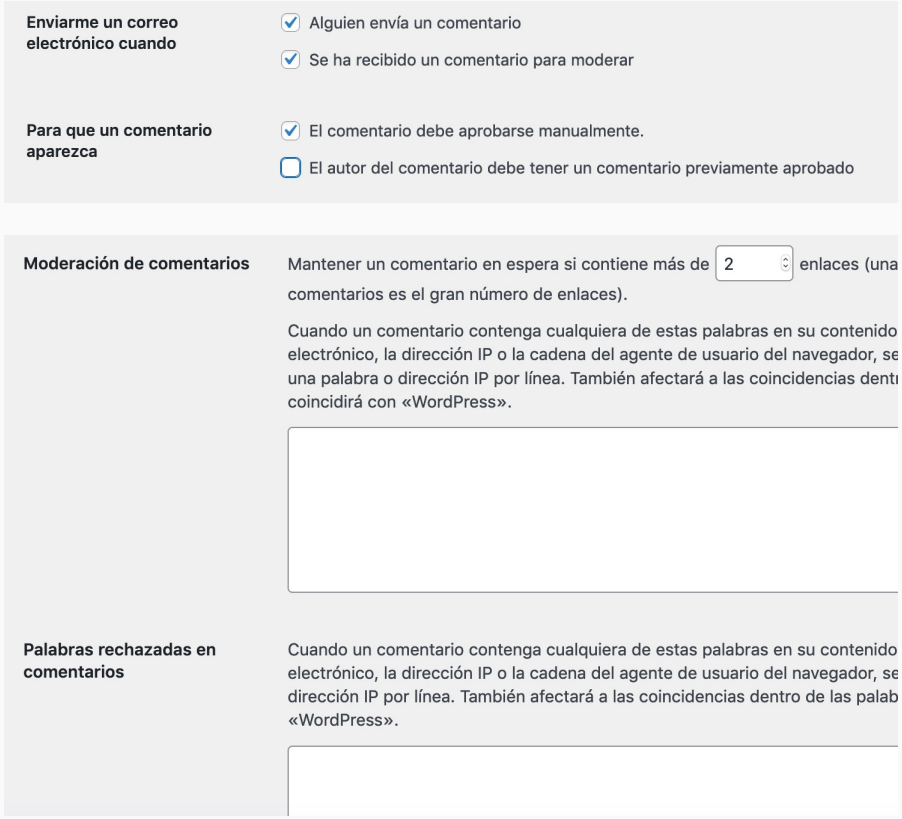


6. Controlar o bloquear el spam de los comentarios

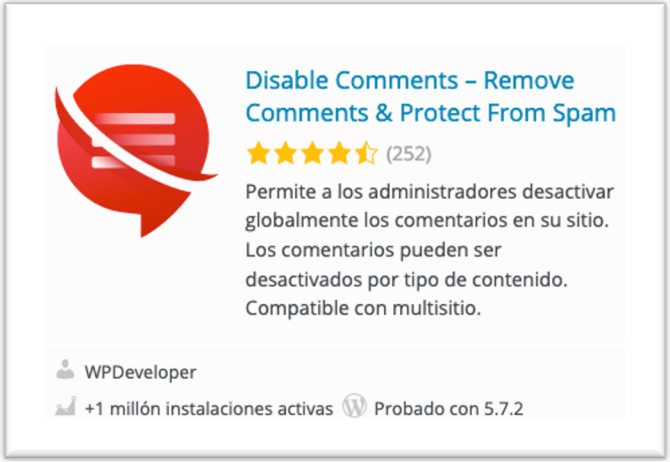
Ajustes / Comentarios

Habilitar la moderación de comentarios

Crear una lista negra de palabras



No quiero comentarios en mi sitio



- Reduce ataques por inyección SQL

Ajustes / Desactivar comentarios

7. Formularios de contacto

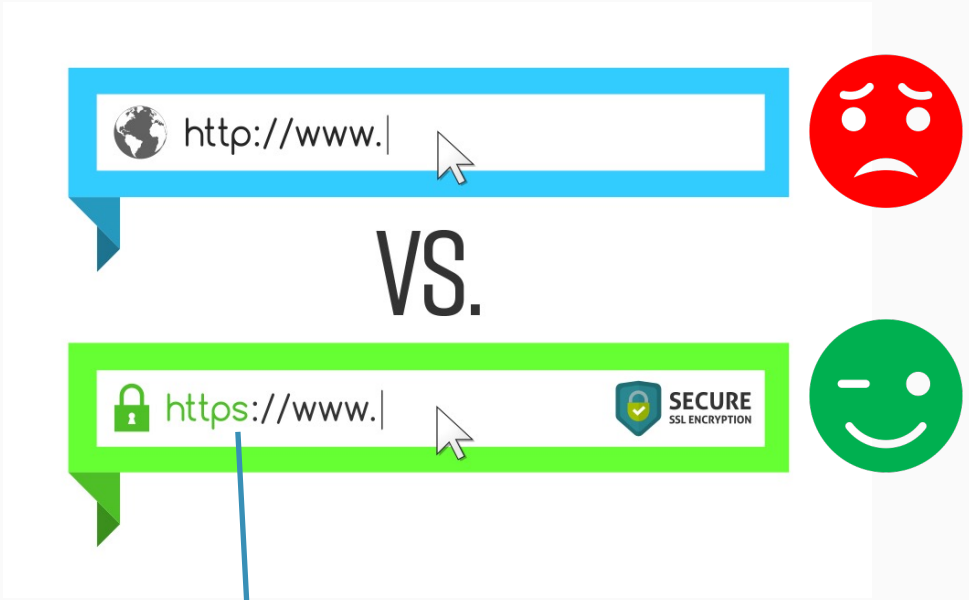
- Asegúrese que los que entran a su castillo lo hacen con buenas intenciones
- Elija un plugin para el spam del formulario.
- Use reCAPTCHA
- Honeypot: un campo oculto para el usuario, pero visible para los robots, cuando lo ven, lo rellenan. Cuando esto sucede la información es bloqueada.

- Múltiples formularios
- Compatible con Akismet, Honeypot
- Integración con reCAPTCHA

8. Certificado de Seguridad SSL

Datos cifrados de extremo a extremo.

SSL = Secure Sockets Layer



S = Secure

Contrate un proveedor de hospedaje que le brinde el certificado de seguridad.

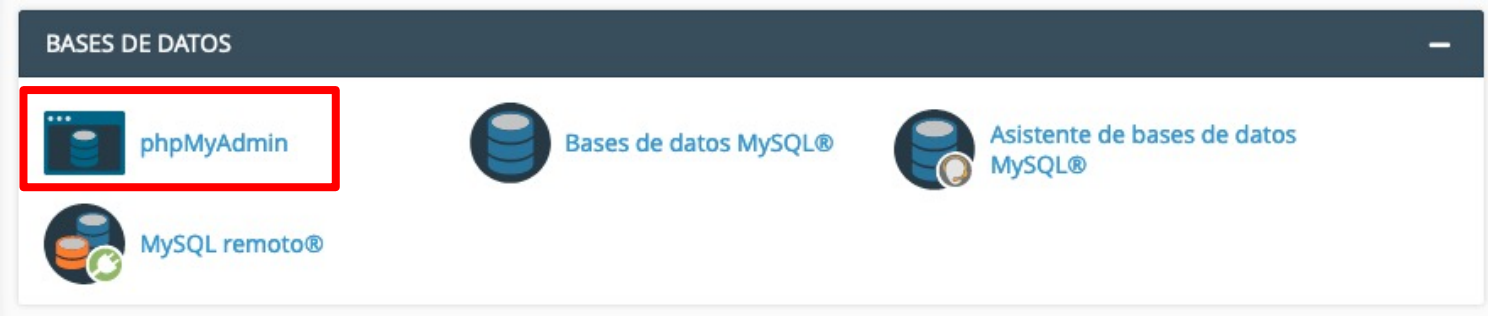
9. Proteger la Base de Datos

Cambiar el prefijo wp_ de la BD

1. Archivo wp_config.php

```
/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'my_';
```

2. Cambiar los nombres de las tablas: Panel hospedaje / phpMyAdmin

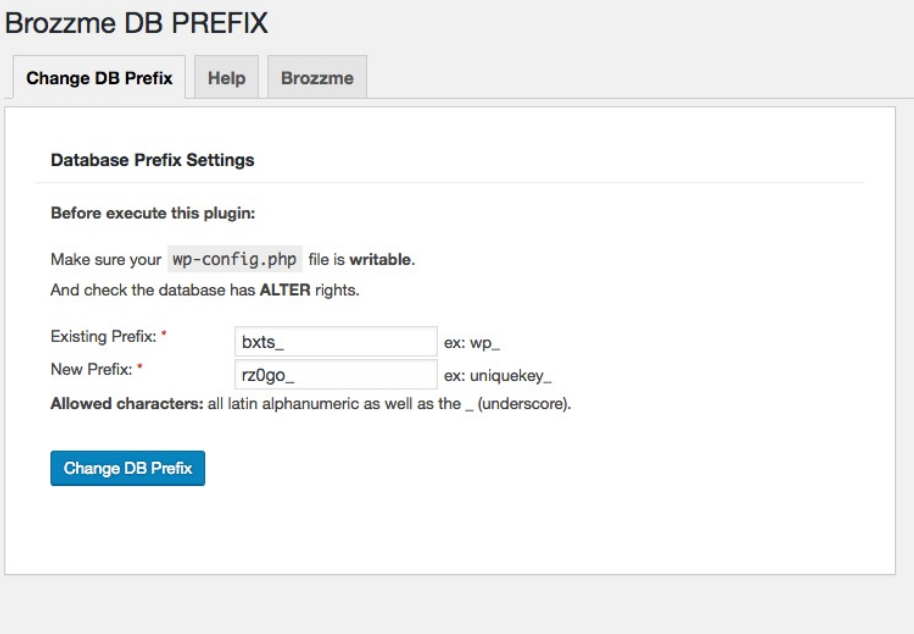


Más fácil

Brozzme DB Prefix & Tools Addons

★★★★★ (26)

Easily change your WordPress DB prefix, save time, increase security.



Ventajas

- Para usuarios que no quieren tocar código.
- Se puede desactivar y eliminar después de hacer el cambio.

Importante

Copia de Seguridad antes de realizar este tipo de cambios.

10. WordPress Actualizado

Utiliza siempre la última versión de WP.

Actualiza periódicamente tu WordPress.

Importante

Copia de Seguridad antes de realizar actualizaciones mayores

Conclusión

1. Plugins y temas actualizados
2. Copias de Seguridad
3. Contraseñas fuertes
4. Ruta de login y Rey protegido
5. Firewall & Antivirus
6. Comentarios protegidos o deshabilitados.
7. Formularios de contacto protegidos
8. Certificado de seguridad
9. BD protegida
10. WordPress actualizado

=

Solo después de que los usuarios hayan sido engañados, realmente prestarán atención a la capacitación.

Todd Fitzgerald

Gracias!!!

lidia@arroyovargas.com
@lidarroy