
WORDCAMP
LAS PEÑITAS

WORDPRESS
A PRUEBA DE BALAS

Una charla sobre seguridad
y buenas prácticas en WordPress

WordPress a prueba de balas

- Bájatelo! http://monchito.net/wordpress-seguro
- Compártelo! Licencia CC-BY-SA 3.0

@leogg

desarrollador web

activista software libre

No te engañes!

- La seguridad absoluta no existe
- Alguien quiere entrar a tu sitio web sin tu permiso
- Alguien va a tratar de entrar a tu sitio web sin permiso

Lo importante...

- Conoce los riesgos
- Conoce las herramientas
- No seas un blanco fácil!

Web hosting

- Búscate un buen web hosting
- No te vayas por lo más barato
- No tengas miedo de cambiar
- http://wordpress.org/hosting/

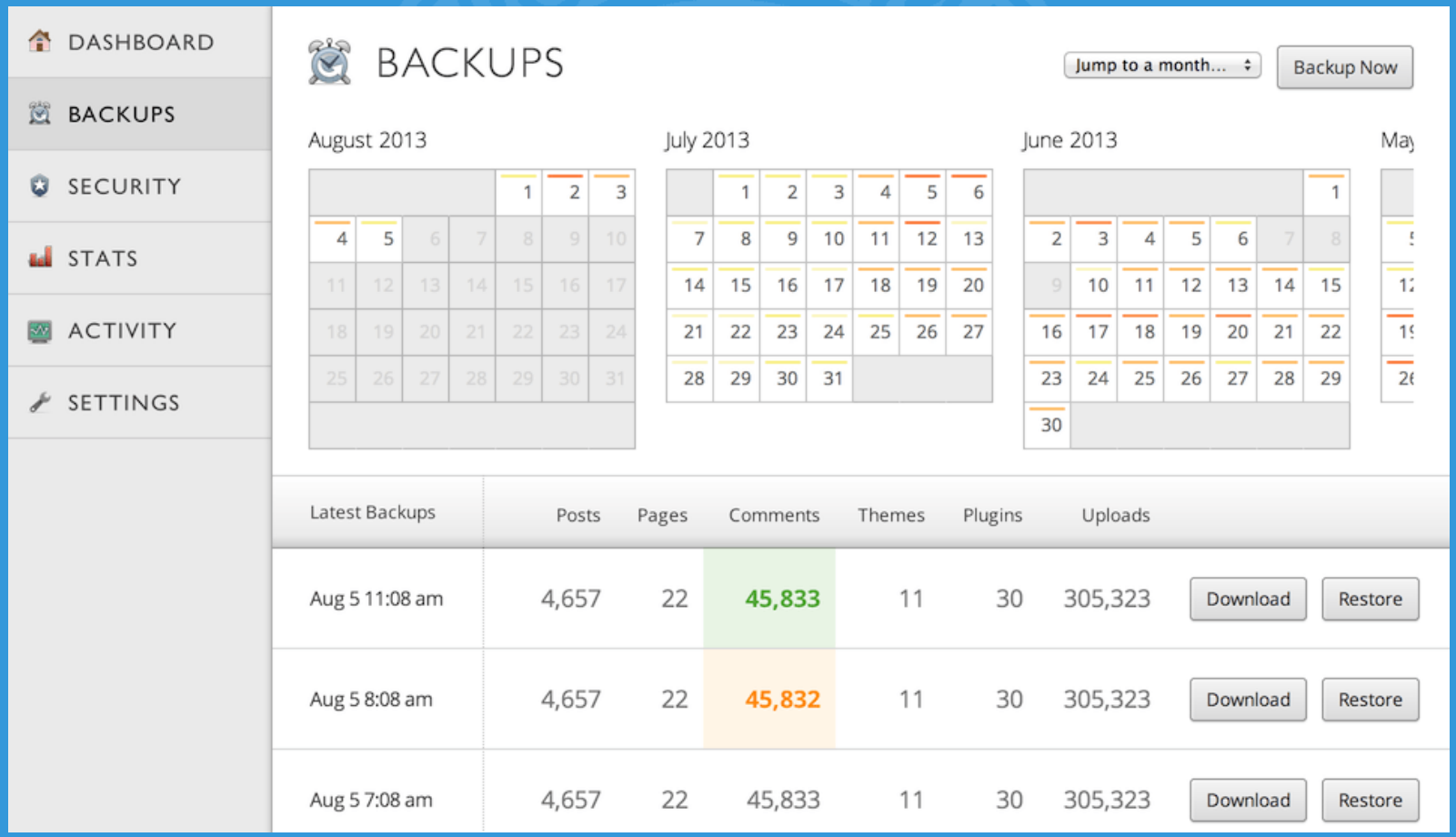
Respaldos

- Respalda tu sitio regularmente
- No es suficiente con los respaldos de tu proveedor
- No guardes tus respaldos en el servidor

Soluciones de terceros

- http://vaultpress.com/
- Respaldos automatizados
- Restaura tu sitio con un solo click
- Alertas de seguridad

VaultPress


DASHBOARD
BACKUPS
SECURITY
STATS
ACTIVITY
SETTINGS
BACKUPS
Jump to a month...
Backup Now
August 2013
July 2013
June 2013
Latest Backups
Posts
Pages
Comments
Themes
Plugins
Uploads
Aug 5 11:08 am
4,657
22
45,833
11
30
305,323
Download
Restore
Aug 5 8:08 am
4,657
22
45,832
11
30
305,323
Download
Restore
Aug 5 7:08 am
4,657
22
45,833
11
30
305,323
Download
Restore

¿Qué respaldar?

- El sistema de archivos (temas, plugins, archivos core de WordPress, medios)
- La base de datos (entradas, páginas, comentarios, etc.)

Actualizaciones

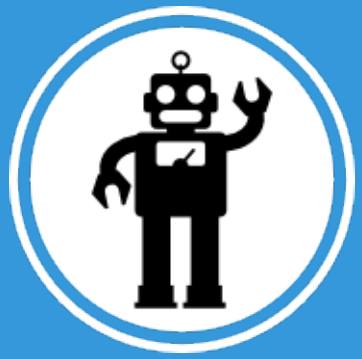
- No hay excusas para no actualizar tu sitio web
- Actualiza WordPress
- Actualiza tus plugins
- Actualiza tus temas

Si no sabes lo que haces,
las manitos quietas

- insane raspu

WP Administrado

- Hosting WordPress
- Respaldo y actualizaciones
- Optimización del sitio web
- Protección ante amenazas
- Busca un experto local



Robots.txt

- Prohíbe que los robots indexen directorios importantes

```
User-agent: *
Disallow: /wp-*
```

- http://www.robotstxt.org/

.htaccess

- Desactiva la navegación de directorios

  ```
  Options All -Indexes
  ```

- Importante si queres evitar la búsqueda de plugins vulnerables/sin actualizar

wp-admin

- Protege tu directorio `wp-admin`
- Limita el acceso al directorio por dirección IP en el `.htaccess`
- Usa una contraseña de acceso
- Renombra el directorio

wp-config.php

- Protege tu archivo `wp-config.php`
- Cambia los permisos `chmod 400 wp-config.php`
- Mueve el archivo a otro directorio

Más permisos

- Directorios: `705`
- Archivos: `640`
- Excepciones:
  `wp-config.php`
  `index.php`
- http://ss64.com/bash/chmod.html

Seguridad por obscuridad

- La seguridad por obscuridad NO es un reemplazo de buenas prácticas de seguridad. Úselas sabiamente, y solo como una capa adicional de seguridad.

Seguridad por obscuridad

- Cambia la cuenta administrativa
- En una instalación nueva, crea una cuenta admin nueva
- En una instalación existente, modifícalo en la base de datos
- Administrador no debe publicar!

Seguridad por obscuridad

- Cambia el prefijo de las tablas en la base de datos
- Muchos atacantes asumen que el prefijo de las tablas es `wp_`
- Edita el archivo `wp-config.php`

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

Seguridad por obscuridad

- Cambia la URL del formulario de inicio de sesión
- Muchos atacantes y bots buscan `/wp-login.php`
- Limita la cantidad de intentos de acceso

El 38% de las personas prefieren limpiar el inodoro antes de cambiar a una nueva contraseña

http://mashable.com/2012/08/23/password-overload/

Contraseñas

- Usa contraseñas seguras y cámbialas periódicamente
- Evita contraseñas cortas, nombres comunes, datos personales o leetspeak (`n0 35tam05 3n 105 n0v3ntas!`)

Contraseñas

- Contraseña mala: `migatotom12`
- Contraseña buena: `MgT12/Urdmh03;`

Contraseñas

- Contraseña mala: `migatotom12`
- Contraseña buena: `MgT12/Urdmh03;`

`Mi gato Tom 12 años. Un regalo de mi hermana 2003.`

Contraseñas

- No uses la misma contraseña más de una vez
- Asegúrate que tus usuarios sigan las buenas prácticas
- Usa gestores de contraseñas como KeePass http://keepass.info/

Contraseñas

- Utiliza autenticación en dos pasos
- Algo que sabes + Algo que tienes
- Algo que sabes (contraseña)
  Algo que tienes (móvil)
- http://wordpress.org/plugins/tags/two-factor-authentication

Llaves secretas

- Genera llaves secretas!
- Dificulta el crackeo de las contraseñas de usuario
- Añaden encriptación a las cookies de sesión

Llaves secretas

- Edita `wp-config.php`
- Genera tus llaves en https://api.wordpress.org/secret-key/1.1/salt/
- Copia y pega tus llaves en el archivo de configuración

Dentro de dos años, el problema del spam se habrá resuelto

- Bill Gates (2004)

http://www.informationweek.com/spam-will-be-solved-in-2-years--gates/d/d-id/1022817

Cortafuegos

- Bloquea las amenazas de seguridad comunes como Googlebots falsos, exploraciones maliciosas y botnets
- Protección adicional al cortafuegos de tu servidor web

Cortafuegos

- iThemes Security (antes Better WP Security) restringe el acceso a nivel de Apache
- http://wordpress.org/plugins/better-wp-security/

Cortafuegos

- WordFence trabaja a nivel de WordPress, mientras éste se está cargando
- http://wordpress.org/plugins/wordfence/

Cortafuegos

- Escaneo de archivos, temas y plugins para comprobar su integridad
- Almacenamiento en caché, autenticación de dos pasos y monitoreo de tráfico en tiempo real

La tostada siempre cae
por el lado de la mantequilla

- Ley de Murphy

Después de un ataque

- ¡Mi sitio ha sido comprometido! ¿Y ahora que hago?
- Revisa primero tu computadora, busca y limpia cualquier malware que encuentres

Después de un ataque

- Haz un respaldo del sitio infectado para su posterior análisis
- Busca una copia de respaldo limpia para restaurar el sitio

Después de un ataque

- Cambia las contraseñas de usuario, base de datos y FTP
- Cambia todas tus claves secretas
- Actualiza tu sitio, temas y todos los plugins instalados

Después de un ataque

- Realiza una auditoría post-mortem
- Revisa la copia infectada e investiga el ataque a tu sitio
- http://codex.wordpress.org/FAQ_My_site_was_hacked

Recomendaciones

- http://codex.wordpress.org/Hardening_WordPress
- http://wpsecure.net/