

WORDPRESS

A PRUEBA DE BALAS

Una charla sobre seguridad
y buenas prácticas en WordPress

Aura Lila Gutiérrez Tejada

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 que esta de moda

- Ransomware ("CTB-Locker")
- Encriptan el sitio web, modifican el index
- Piden a cambio bitcoin para desenscriptarlo



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 guardes tus respaldos en el servidor
- Soluciones de terceros como:
<http://vaultpress.com>

Respaldo

DASHBOARD


BACKUPS

SECURITY

STATS

ACTIVITY

SETTINGS

 BACKUPS

Jump to a month... ▾

Backup Now

August 2013

				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

July 2013

		1	2	3	4	5	6
7	8	9	10	11	12	13	
14	15	16	17	18	19	20	
21	22	23	24	25	26	27	
28	29	30	31				

June 2013

							1
2	3	4	5	6	7	8	
9	10	11	12	13	14	15	
16	17	18	19	20	21	22	
23	24	25	26	27	28	29	
30							

May

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

WP Administrado

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

.htaccess

- Desactiva la navegación de directorios
Options All Indexes
- Importante si quieres 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

wp-config.php

- Protege tu archivo
wpconfig.php
- Cambia los permisos
chmod 400 wp-config.php

Más permisos

- Directorios: 705
- Archivos: 640
- Excepciones:
wpconfig.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
- No pongas como nombre de usuario admin
- Administrador no debe publicar

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

Contraseñas

- Usa contraseñas seguras y cámbialas periódicamente
- Evita contraseñas cortas, nombres comunes, datos personales

Contraseña

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

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

Contraseña

- 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/>

Cortafuegos

- 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

llaves secretas

```
define('AUTH_KEY', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.  
define('SECURE_AUTH_KEY', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.  
define('LOGGED_IN_KEY', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.  
define('NONCE_KEY', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.  
define('AUTH_SALT', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.  
define('SECURE_AUTH_SALT', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.  
define('LOGGED_IN_SALT', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.  
define('NONCE_SALT', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
```

```
define('AUTH_KEY', 'm$:I,yR)[/ShpFLb&8kTsRTEz)HEw6p@?Cs%B@Q8wYi+XPX*~e4v+KzOU0So)]V1');  
define('SECURE_AUTH_KEY', 'xEtu>S9Y,]cG!j:XP!80>9Xzd`/QVtb%92Uhrqa9-K:W- nG& EA o</};}!0H`#');  
define('LOGGED_IN_KEY', 'b- OMNM!N)cK9n8q3D85}b.?U@~GL| -b7%tsY#;t|^ -:gb&Da*9[WPR+LY%$|=%0b');  
define('NONCE_KEY', 'NXeWY3yjxxqx_Xv?CAaltC>Tm7- QP:l$^E*bAyqhK;B!aC;G:_^gQgd]#<Ou6@`~');  
define('AUTH_SALT', '|6dLH]mew=YI3D80r-X<+<a+S| (~/>gU7IPE#qW=79A% gXHZ>5P%x{cufK5Z:gF');  
define('SECURE_AUTH_SALT', '77l*LOa*Q9|B/KM#Hr<bh?Al}h8MoL_`hF/1G|8Lek#7u+b2o&C=Q;IF&IA,zcbi');  
define('LOGGED_IN_SALT', '_VhX1S$rVpg&TMbe{F/M+s]!}OxX^E+w$QNCuG>R)2#rOKjVoT,d[Bd;e?S~b8&?');  
define('NONCE_SALT', 'Ufv|SMG}U/t@L=)uaYG) -~I8DkF||DC|x/N?%SlBOf|f9nA=4(|$u8~<_+P&0ch-');
```


Cortafuegos

- Bloquea las amenazas de seguridad comunes como Googlebots falsos, exploraciones maliciosas y botnets








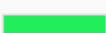
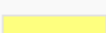
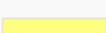
Cortafuegos

- iThemes Security (antes Better WP Security) restringe el acceso a nivel de Apache

<http://wordpress.org/plugins/better-wp-security/>



WordPress File Permissions

Relative Path	Suggestion	Value	Result	Status
/	= 755	0755	OK	
/wp-includes/	= 755	0755	OK	
/wp-admin/	= 755	0755	OK	
/wp-admin/js/	= 755	0755	OK	
/home/confidencial/confidencial.com.ni/wp-content/themes	= 755	0755	OK	
wp-content/plugins	= 755	0755	OK	
wp-content	= 755	0755	OK	
wp-content/uploads	= 755	0755	OK	
wp-config.php	= 444	0644	WARNING	
.htaccess	= 444	0644	WARNING	
Relative Path	Suggestion	Value	Result	Status

Ban Hosts

58.96.177.210
124.231.247.60
85.98.252.230

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

Your Site Activity in Real-Time ON

[Learn more about Wordfence Live Traffic](#)

Wordfence Live Activity: Wordfence used 116.61MB of memory for scan. Server peak memory usage was: 139.94MB

All Hits Humans Registered Users Crawlers Google Crawlers Pages Not Found Logins and Logouts Top Consumers Top 404s

 **Denver, United States** arrived from <https://www.wordfence.com/signup-thanks/> and visited <https://www.wordfence.com/manage-wordfence-api-keys/>

3/25/2015 4:20:59 PM (3 months 29 days ago) IP: [96.88.81.90](#) [block] Hostname: 96-88-81-90-static.hfc.comcastbusiness.net

Browser: Chrome version 41.0 running on Win7

Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.101 Safari/537.36

[\[Block this IP\]](#) — [\[Block this network\]](#) — [\[Run WHOIS on 96.88.81.90\]](#) — [\[See recent traffic\]](#)

 **Ukraine** visited <http://www.wordfence.com/>

3/25/2015 4:20:56 PM (3 months 29 days ago) IP: [82.144.213.118](#) [block] Hostname: ip.82.144.213.118.stat.volia.net

Browser: Safari version 8.0 running on MacOSX

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/600.4.10 (KHTML, like Gecko) Version/8.0.4 Safari/600.4.10

[\[Block this IP\]](#) — [\[Block this network\]](#) — [\[Run WHOIS on 82.144.213.118\]](#) — [\[See recent traffic\]](#)

 **Denver, United States** arrived from <https://www.wordfence.com/wordfence-signup/> and visited <https://www.wordfence.com/signup-thanks/>

3/25/2015 4:20:42 PM (3 months 29 days ago) IP: [96.88.81.90](#) [block] Hostname: 96-88-81-90-static.hfc.comcastbusiness.net

Browser: Chrome version 41.0 running on Win7

Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.101 Safari/537.36

[\[Block this IP\]](#) — [\[Block this network\]](#) — [\[Run WHOIS on 96.88.81.90\]](#) — [\[See recent traffic\]](#)


 **Valladolid, Spain** arrived from <https://www.google.com/> and visited <https://www.wordfence.com/docs/how-to-clean-a-hacked-wordpress-site-using-wordfence/>

3/25/2015 4:20:39 PM (3 months 29 days ago) IP: [81.43.238.30](#) [block] Hostname: 30.red-81-43-238.staticip.rima-tde.net

Browser: Chrome version 40.0 running on Win7

Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2150.0 Iron/40.0.2150.0 Safari/537.36

[\[Block this IP\]](#) — [\[Block this network\]](#) — [\[Run WHOIS on 81.43.238.30\]](#) — [\[See recent traffic\]](#)

 **Dronnten, Netherlands** arrived from https://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&sqi=2&ved=0CCEQFjAA&url=https%3A%2F%2Fwww.wordfence.com%2Fdocs%2Fhow-to-clean-a-hacked-wordpress-site-using-wordfence%2F&ei=kBgTve8Bg_FSxSWBiAM&usg=AFQjCNFk0UdINI8IsnHdgBf8G73dbA0aVg&sig2=2cV3Q7-ovYaVqQm_BEeK9A&bvm=bv.89217033.d.ZWU and visited <https://www.wordfence.com/docs/how-to-clean-a-hacked-wordpress-site-using-wordfence/>

3/25/2015 4:20:37 PM (3 months 29 days ago) IP: [87.195.246.154](#) [block] Hostname: fiber-087-195-246-154.solcon.nl

Browser: Firefox version 36.0 running on Win8.1

Mozilla/5.0 (Windows NT 6.3; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0

[\[Block this IP\]](#) — [\[Block this network\]](#) — [\[Run WHOIS on 87.195.246.154\]](#) — [\[See recent traffic\]](#)

An anime-style illustration. On the left, a blonde girl with long hair is shown from the chest up, smiling with her eyes closed. On the right, a red-haired girl with pigtails is standing, wearing a blue hoodie with a white circular logo, a yellow and orange pleated skirt, and white socks with orange stripes. She is holding a small yellow cat with orange ears and a long orange tail. The background is a warm, golden-yellow color with soft, abstract shapes.

Gracias :)

Presentación basada en: Wordpress a pruebas de balas,
Wordcamp 2014, por Leandro Gomez