WordPress es seguro

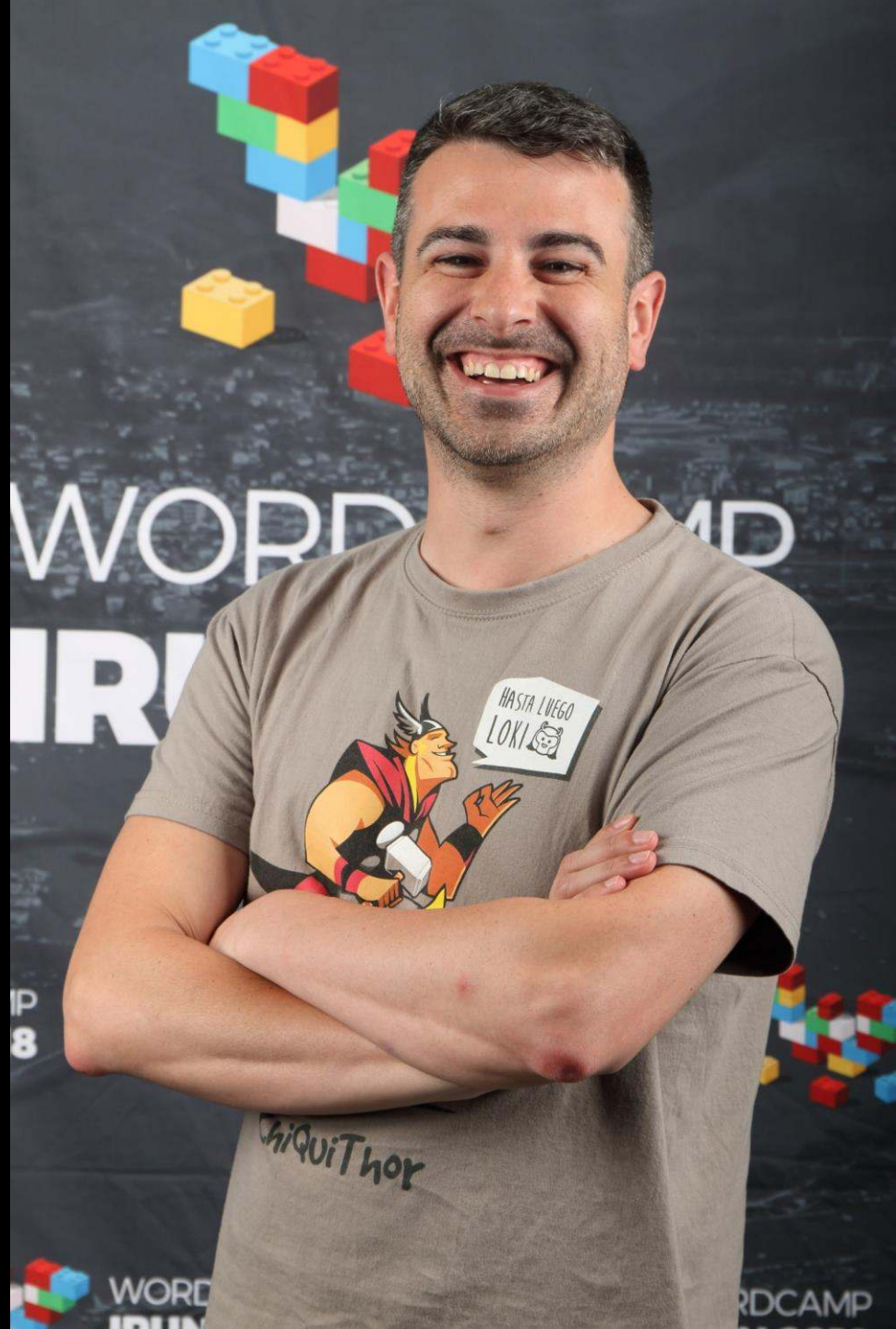
pero el ser humano no

¡Hola!

javiercasares.com
@JavierCasares

www.wpdanger.com
code.wpdanger.com

"Si trabajas en Internet,
aprende cómo funciona Internet"



pregunta…

¿Cuál es la primera regla
de la seguridad en WordPress?

respuesta…

Hacer backups

pregunta…

¿Quién de aquí
prueba sus backups?

respuesta…

Si haces backups pero no los pruebas, tienes **Backup Schrödinger.**

pregunta…

¿Cuál es la segunda regla
de la seguridad en WordPress?

respuesta…

Actualizar

La seguridad, en temas

-Hosting
-Base de Datos
-WordPress
-Seguridad Activa
-Desarrolladores

NOTA: sé que al principio es bastante técnico, pero luego se relaja ☺

Hosting

Alojamiento Web

- ¿Cuál es el alojamiento web más adecuado para mi?
  - ¿Sé de sistemas?
  - ¿Necesito recursos?
- Elegir entre *hosting* compartido y *hosting* dedicado.
- Mantén en hora tu servidor (no, no es broma).

Versiones

Sistema Operativo	Versión
CentOS	7.5
Debian	9.5
Fedora	28
FreeBSD	11.2
Ubuntu	18.04

Servidor Web	Versión
Apache HTTPD	2.4.34
nginx	1.15

Versiones

Base de Datos	Versión
MariaDB Server	10.3
MySQL Community Server	8.0
Percona Server for MySQL	5.7

Lenguaje de Programación	Versión
PHP	7.2

Certificado de Encriptación	Versión
TLS	1.2

Certificado TLS

- ¿Usas HTTPS?
  - Si no, estás jod***.

- Instala un certificado TLS y fuerza a WordPress su uso:

```
define('FORCE_SSL_LOGIN', true);
define('FORCE_SSL_ADMIN', true);
```

Permisos de ficheros

- Carpetas 750
- Ficheros 640
- wp-config.php 400
- robots.txt 400
- readme.html 000

.htaccess

```
<files wp-config.php>
  deny from all
</files>
<files readme.html>
  deny from all
</files>
<files license.txt>
  deny from all
</files>
```

nginx

```
location ~ \.php$ {
  location ~ wp-config {
    deny all;
  }
  location ~ /xmlrpc.php {
    limit_except POST {
      deny all;
    }
  }
}
location ~* readme.(html|txt) {
  deny all;
}
location ~* ^license.txt {
  deny all;
}
```

Bloquear PHP en "uploads"

- ¿Para qué quieres ejecutar PHP en la carpeta /wp-content/uploads/?

```
<Files ~ ".+\.php">
  Deny from all
</Files>
```

Base de Datos

Acceso

- ¿Has de dar acceso completo…

```
GRANT ALL ON tu_database.* TO 'tu_usuario'@'localhost' IDENTIFIED BY
'tu_contraseña';
```

- …o solo el necesario?

```
GRANT ALTER, CREATE, DELETE, DROP, INDEX, INSERT, SELECT, UPDATE ON
tu_database.* TO 'tu_usuario'@'10.0.0.2' IDENTIFIED BY 'tu_contraseña';
```

Prefijo de las tablas

- Hasta hace un tiempo WordPress usaban como prefijo de las tablas

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

- ¿Por qué no lo complicas un poco?

```
$table_prefix = 'c2712m_';
```

Copias antiguas

- Mantén tu base de datos limpia de contenidos antiguos

```
define('EMPTY_TRASH_DAYS', 1);

define('WP_POST_REVISIONS', 5);
define('WP_POST_REVISIONS', false);
```

¿Realmente te equivocas tanto?

WordPress

Security Keys

- Revisa tener algo así en tu wp-config.php

```
define('AUTH_KEY',         'H(e|_(4$+FIs2;7%F181${EZG`)r7i)/QM0_hqdG^w>oA]cLS##P[LT?Q+[OQ>5b');
define('SECURE_AUTH_KEY',  'VCT8<=l3Kk`F+[Re9<=DWQELT-E_TmSoZr|1hBk<+M71::HqISK(|N3BWp}Xcj!:');
define('LOGGED_IN_KEY',    '-#/TGnhzT]t*T%wc )y-@l4r]%Aw&Sl l*,|im%7y^`UQu+qOp-[-_c!gbeK->B#');
define('NONCE_KEY',        '-KOAqd;N PK=PN(y@eFfC6xC8uhp|4xTbL7}q!xz[j+`-~Hv+7v*8=Z/bkNren~&');
define('AUTH_SALT',        '%XSIsn|.<b#O:|2mpsu?hL]YH=;,0u`n U)w$|`]|X~2Bhg`jaiO+W;*?FJ*sYF)');
define('SECURE_AUTH_SALT', 'QSsi_M+uO=1m+;Le+qC%<,&wKGStAWs=-m@uwmxz+3mr[J-{2YuF/cx]1j rs,1S');
define('LOGGED_IN_SALT',   '~.YkVZ |+?ii6tSg.T|1oz/Pgt. )LgiE3Bq2=>:iA]r&-8:Ik=(@(1)V|YkA(M%');
define('NONCE_SALT',       'XgU.{]_?W)B#+$gREcqFprR=4z]` OQ9IN>6i#~f*fIMA=Y*#sEKWGL}/q|R0|~B’);
```

¿Por qué no ir actualizándolas de tanto en tanto?

Para eso tienes [Salt Shaker](). 

Cabeceras inconvenientes

- WordPress deja muchos rastros en meta-datos del HTML.
  - Versión de WordPress
  - Linking interno
  - Feeds
  - ...

1. Descarga el plugin (descomprime el fichero ZIP).
2. Accede por FTP a la carpeta [/wp-content/mu-plugins/]. Si no tienes esta carpeta, créala.
3. Sube por FTP el fichero [wpdanger-headers.php] a la carpeta [/wp-content/mu-plugins/].
4. Cuando entres en el panel de administración de tu WordPress, en la zona de Plugins tendrás una sección nueva de plugins Imprescindibles donde aparecerá. Recuerda que al ser Imprescindible no podrás activarlo ni desactivarlo.

https://code.wpdanger.com/wordpress/cabeceras-inconvenientes/

Versión en CSS y Javascript

- Los CSS y JavaScript suelen incluir el parámetro "ver=" al final de sus direcciones.

1. Descarga el plugin (descomprime el fichero ZIP).
2. Accede por FTP a la carpeta [/wp-content/mu-plugins/]. Si no tienes esta carpeta, créala.
3. Sube por FTP el fichero [wpdanger-ver.php] a la carpeta [/wp-content/mu-plugins/].
4. Cuando entres en el panel de administración de tu WordPress, en la zona de Plugins tendrás una sección nueva de plugins Imprescindibles donde aparecerá. Recuerda que al ser Imprescindible no podrás activarlo ni desactivarlo.

https://code.wpdanger.com/wordpress/ocultar-version/

Post instalación

- Bloquea los ficheros de instalación de WordPress
  - [/wp-admin/setup-config.php]
  - [/wp-admin/install.php]

```
<Files ~ "^(install|setup-config).php">
Deny from all
</Files>
```

Edición de ficheros

- Que tus usuarios no te amarguen el día.
  - Que no puedan editar ficheros CSS, plantillas, plugins ni nada…
  - Que no puedan añadir plugins o plantillas.

```
define('DISALLOW_FILE_EDIT', true);
define('DISALLOW_FILE_MODS', true);
```

URL del sitio

- Que tus usuarios no te amarguen el día.
  - Que no cambien por error la URL de tu sitio...

```
define('WP_SITEURL', 'https://www.example.com');
define('WP_HOME', 'https://www.example.com');
```

XML-RPC

- Gracias al XML-RPC podemos utilizar algunas apps externas como Open Live Writer o herramientas como IFTTT e incluso la propia App de WordPress para Android o iOS.
- El problema es que esto tiene problemas desde casi el inicio de los días…

1. Descarga el plugin (descomprime el fichero ZIP).
2. Accede por FTP a la carpeta [/wp-content/mu-plugins/]. Si no tienes esta carpeta, créala.
3. Sube por FTP el fichero [wpdanger-xmlrpc.php] a la carpeta [/wp-content/mu-plugins/].
4. Cuando entres en el panel de administración de tu WordPress, en la zona de Plugins tendrás una sección nueva de plugins Imprescindibles donde aparecerá. Recuerda que al ser Imprescindible no podrás activarlo ni desactivarlo.

https://code.wpdanger.com/wordpress/xml-rpc/

Acceso a wp-admin

- ¡Hemos de entrar! Pero que haya una puerta no significa que todo el mundo tenga la llave.
  - Bloqueo por IP o usuario/contraseña
  - Cambio de dirección URL del wp-admin
  - Ataques de fuerza bruta
    Para evitar ataques, Limit Login Attempt.
  - Desconexión automática
    Para desconectar, Inactive Logout.

Acceso a wp-admin

- Cuando intentas acceder al panel de administración y al poner tu usuario o contraseña da un error, ese mensaje deja entrever si lo que ha fallado es el usuario y contraseña, o solo la contraseña (de forma que implícitamente estás diciendo que ese usuario sí que existe).

1. Descarga el plugin (descomprime el fichero ZIP).
2. Accede por FTP a la carpeta [/wp-content/mu-plugins/]. Si no tienes esta carpeta, créala.
3. Sube por FTP el fichero [wpdanger-login.php] a la carpeta [/wp-content/mu-plugins/].
4. Cuando entres en el panel de administración de tu WordPress, en la zona de Plugins tendrás una sección nueva de plugins Imprescindibles donde aparecerá. Recuerda que al ser Imprescindible no podrás activarlo ni desactivarlo.

https://code.wpdanger.com/wordpress/acceso-wpadmin/

Actualizaciones automáticas

- ¿Quieres que WordPress se actualice al 100% sin pedirte permiso? Esto incluye el propio WordPress, plantillas, plugins, traducciones…

1. Descarga el plugin (descomprime el fichero ZIP).
2. Accede por FTP a la carpeta [/wp-content/mu-plugins/]. Si no tienes esta carpeta, créala.
3. Sube por FTP el fichero [wpdanger-autoupdater.php] a la carpeta [/wp-content/mu-plugins/].
4. Cuando entres en el panel de administración de tu WordPress, en la zona de Plugins tendrás una sección nueva de plugins Imprescindibles donde aparecerá. Recuerda que al ser Imprescindible no podrás activarlo ni desactivarlo.

https://code.wpdanger.com/wordpress/actualizaciones-automaticas/

Actualizaciones automáticas

- Pero tal vez quieras que no se actualice nada, y ponerte en la agenda semanal una tarea que es revisarlo.

1. Descarga el plugin (descomprime el fichero ZIP).
2. Accede por FTP a la carpeta [/wp-content/mu-plugins/]. Si no tienes esta carpeta, créala.
3. Sube por FTP el fichero [wpdanger-noautoupdater.php] a la carpeta [/wp-content/mu-plugins/].
4. Cuando entres en el panel de administración de tu WordPress, en la zona de Plugins tendrás una sección nueva de plugins Imprescindibles donde aparecerá. Recuerda que al ser Imprescindible no podrás activarlo ni desactivarlo.

https://code.wpdanger.com/wordpress/actualizaciones-automaticas/

¿Cuándo se actualizó ese plugin o plantilla?

- Está muy bien actualizar los complementos (plugins) o las plantillas (themes) pero ¿por qué instalas un complemento que hace más de un año que no se actualiza?

- Está claro que hay plugins que seguramente por su funcionalidad no requieren de grandes cambios, pero simplemente por mantener las fechas y los datos de testeo actualizados, cualquier desarrollador de un plugin o theme debería actualizar los datos.

- Y es que todos los complementos llevan interiormente un dato que debería estar al día: versión "hasta la que se ha probado". Si van apareciendo versiones y versiones de WordPress y el programador del plugin no va probando en esas nuevas versiones su funcionamiento ¿quién lo va a hacer?

Usuarios: el nombre

- ¿Es más seguro este usuario?

javier

- ¿O este otro?

Javier Casares

Usuarios: la contraseña

- Tu contraseña ya está pública en Internet:

[1400 Million Clear Text Credentials Discovered in a Single Database]

- ¿Qué podemos considerar hoy una contraseña segura? Pues probablemente una de 24 caracteres alfanuméricos y con símbolos. A partir de ahí, lo que queramos. Y es que hay varias reglas a seguir cuando hablemos de una contraseña; la primera y más importante: ser lo más única y aleatoria posible.
- Otro detalle importante es que las contraseñas es mejor generarlas con sistemas aleatorios y no "tú con tu teclado", debido a que no es tan aleatorio como podría parecer.
- Puedes por ejemplo probar a generar una contraseña con la herramienta Password Generator y forzarla con Force Strong Passwords.

https://code.wpdanger.com/general/contrasenas/

Usuarios: 2FA (doble verificación)

- ¿Sabéis en los casinos esa máquina que genera códigos cada minuto?
  Pues eso.
- La idea es instalar un plugin de doble verificación, obligatorio para todos los usuarios, de forma que una vez el usuario haya accedido con su usuario y contraseña (más o menos segura) te pedirá una nueva clave numérica que se genera cada minuto y que sólo estará configurada en tu dispositivo móvil.
- Incluso, existen sistemas aún más avanzados, como el Magic Password, en el que sólo necesitarás una App para Android o iOS y no una contraseña.

Usuarios: intentos de acceso masivos

- Aunque una contraseña segura y doble verificación es suficiente para que nadie pueda entrar en tu WordPress mediante sistemas de fuerza bruta, puede ser un poco cansado que se estén ejecutando miles de solicitudes de acceso. Es por esto que podemos plantear la instalación de un plugin que cuando detecte este tipo de ataques los bloquee. Podemos instalar un Firewall o tenemos sistemas que se limitan a controlar los intentos de acceso de la zona de acceso.

Emoji

- WordPress integra los Emoji desde hace muchas versiones, convirtiendo los iconos de texto en imagen. Pero este sistema implica algunos problemas de detección de versiones que, si no los utilizas en tus textos, no tiene mucho sentido dejar activos.

1. Descarga el plugin (descomprime el fichero ZIP).
2. Accede por FTP a la carpeta [/wp-content/mu-plugins/]. Si no tienes esta carpeta, créala.
3. Sube por FTP el fichero [wpdanger-emoji.php] a la carpeta [/wp-content/mu-plugins/].
4. Cuando entres en el panel de administración de tu WordPress, en la zona de Plugins tendrás una sección nueva de plugins Imprescindibles donde aparecerá. Recuerda que al ser Imprescindible no podrás activarlo ni desactivarlo.

https://code.wpdanger.com/wordpress/emoji/

Analiza tus enlaces

- En muchas ocasiones los enlaces dejan de funcionar o se redirigen a sitios de, digámoslo finamente, dudosa calidad.
- Es por eso que es muy recomendable utilizar algún complemento que analice los enlaces rotos.
- Pero no sólo los enlaces que tú publicas, sino aquellos que te hacen referencia. Los trackbacks (sitios webs que te enlazan y aparecen como comentarios) también pueden falsificarse simplemente para hacer spam o para llevar a tus usuarios a sitios poco seguros. Para estos casos puedes desactivarlos, o verificar que cuando se produce uno, realmente te han enlazado desde allí.

Seguridad Activa

Copias de seguridad

- ¿Cuál era la primera regla de seguridad? Los backups.
- Hay una decena de plugins de backup, yo uso:
  - BackWPup
- Sólo tenéis que buscar [backup] y tendréis un centenar de resultados. ¿Cuál es el mejor? El que os funcione bien.

- Haced copias diarias si publicáis con cierta frecuencia o semanales si menos. Siempre, al menos, uno semanal.

Firewall / WAF

- Podemos activar determinadas herramientas de seguridad activa que intenten evitar “lo más en tiempo real posible” ataques o cambios.
- Bloquear ataques (firewall) y bloquear cambios de ficheros (malware).

Firewall

Wordfence

Sucuri

Cloudflare

Malware

Wordfence

Sucuri

Herramientas para Webmasters

- No voy a poner la infinidad de herramientas, pero sí algunas importantes que, entre otras cosas, te pueden ayudar a encontrar detalles de la seguridad en tu WordPress.
  - Baidu 百度站长平台
  - Bing Webmaster Tools
  - DNSBL
  - Google Search Console
  - REDbot
  - Yandex Webmaster

Auditor

- Existen varios plugins que realizan esta tarea, cada uno con mayor o menor configuración y opciones.
  - Activity Log
  - Audit Trail
  - Simple History
  - Stream
  - User Activity Log
  - WP Document Revisions
  - WP Security Audit Log

Desarrolladores

Versión mínima de PHP

- ¿Eres desarrollador de plugins? Desde agosto de 2017, tienes "algunas obligaciones".

```
=== Plugin Name ===
Contributors: (this should be a list of wordpress.org userid's)
Donate link: http://example.com/
Tags: comments, spam
Requires at least: 4.6
Tested up to: 4.8
Requires PHP: 5.6
Stable tag: 4.3
License: GPLv2 or later
License URI: https://www.gnu.org/licenses/gpl-2.0.html
```

¿Te vienes a la *WordCamp Barcelona*?
5 y 6 de octubre de 2018
#WCBCN
barcelona.wordcamp.org

¡Gracias!

www.WPdanger.com

code.WPdanger.com