Seguridad WordPress

Más vale prevenir que limpiar (un crackeo)

JavierCasares.com | WPdanger.com | WPBarcelona.com

@JavierCasares | @WPdanger | @WPBarcelona | #WPBarcelona

Antes de nada…

La seguridad absoluta no existe…

…aquí voy a enseñarte algunas medidas extra que debes tener en cuenta a la hora de trabajar con un WordPress.

Hay muchos puntos de ataque. Si tienes un proyecto importante, ten alguien en el equipo que se encargue de la seguridad, por ejemplo, tu SysAdmin.

Un poco de autobombo

Guía de Seguridad WordPress (PDF)

[ISBN: 9788469756560]

https://www.javiercasares.com/wpseguridad/

Licencia EUPL 1.2, así que es Open Source.

WPdanger

https://www.wpdanger.com/

Herramienta de análisis de seguridad gratuita.

Mis opiniones son mías

Aquí voy a recomendar muchas cosas… eso no significa que lo que yo diga sea la verdad absoluta.

Si te recomiendo algo es porque **mi experiencia** me dice que eso es mejor que otras opciones que he probado, pero no he probado todo.

“Seguridad”

La **seguridad informática** (ciberseguridad o seguridad de tecnologías de la información) es el área relacionada con la informática y la telemática que se enfoca en la **protección de la infraestructura computacional y todo lo relacionado con esta** y, especialmente, la **información contenida en una computadora o circulante a través de las redes** de computadoras.

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para **minimizar los posibles riesgos a la infraestructura o a la información.**

La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

https://es.wikipedia.org/wiki/Seguridad_informática

Alojamiento de WordPress

- Hosting Compartido / *Managed*
    llámalo Cloud, Virtual…
- Hosting Dedidado / *UnManaged*
    llámalo VPS, Amazon…

¿Quién se encarga de configurar y mantener la máquina? ¿Otro o tú?

Haz backup de tu máquina (bases de datos, configuraciones, ficheros…) fuera de la máquina.

Confianza

Tu sitio web necesita confianza.

Si tus usuarios no confían:
¡Adiós!

La seguridad protege la confianza.

¿Qué infraestructura pedir?

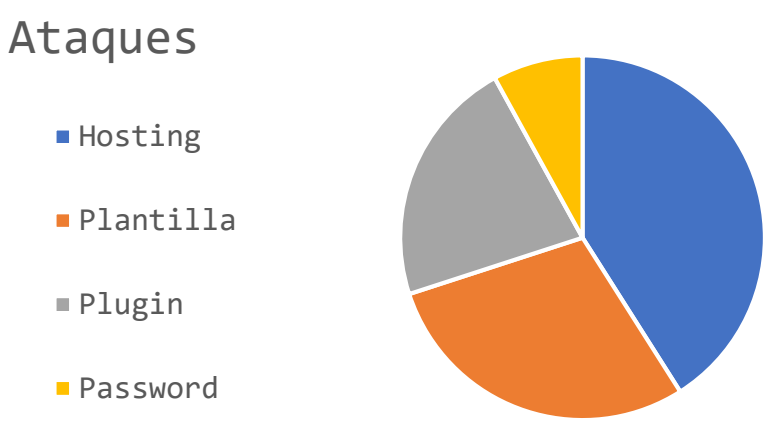
Servidor Web:			
	nginx	>= 1.10	1.12
Lenguaje:			
	PHP	>= 7.0	7.2
Base de Datos:			
	MySQL	>= 5.6	5.7
	MariaDB	>=10.0	10.2
Certificado:			
	TLS	>= 1.2	1.2 (2048 bits)

https://wordpress.org/about/requirements/

Actualiza, frecuentemente

PHP, nginx, Apache HTTPD, MySQL, MariaDB, Certificados, Sistema Operativo…

TODO ESTO también ha de actualizarse.



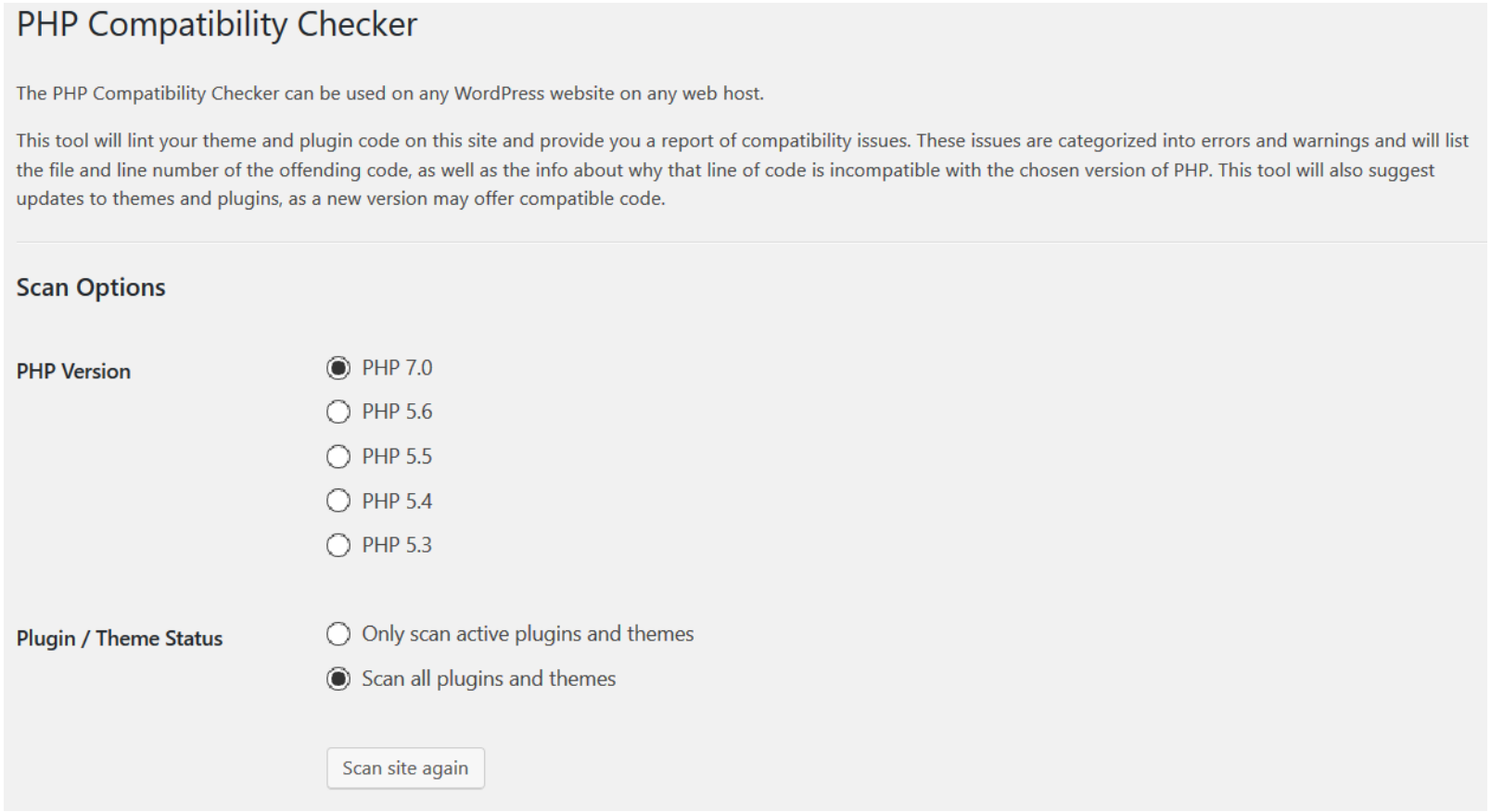
- Prográmate un día a la semana para realizar actualizaciones de todo el sistema.
- Suscríbete a listas de correo, feeds… para estar al día de los paquetes que utilizas.
- ¡Recuerda! Cuando aparece un paquete de seguridad, también aparece la documentación del agujero.

[esto sirve tanto para el sistema como para el software]

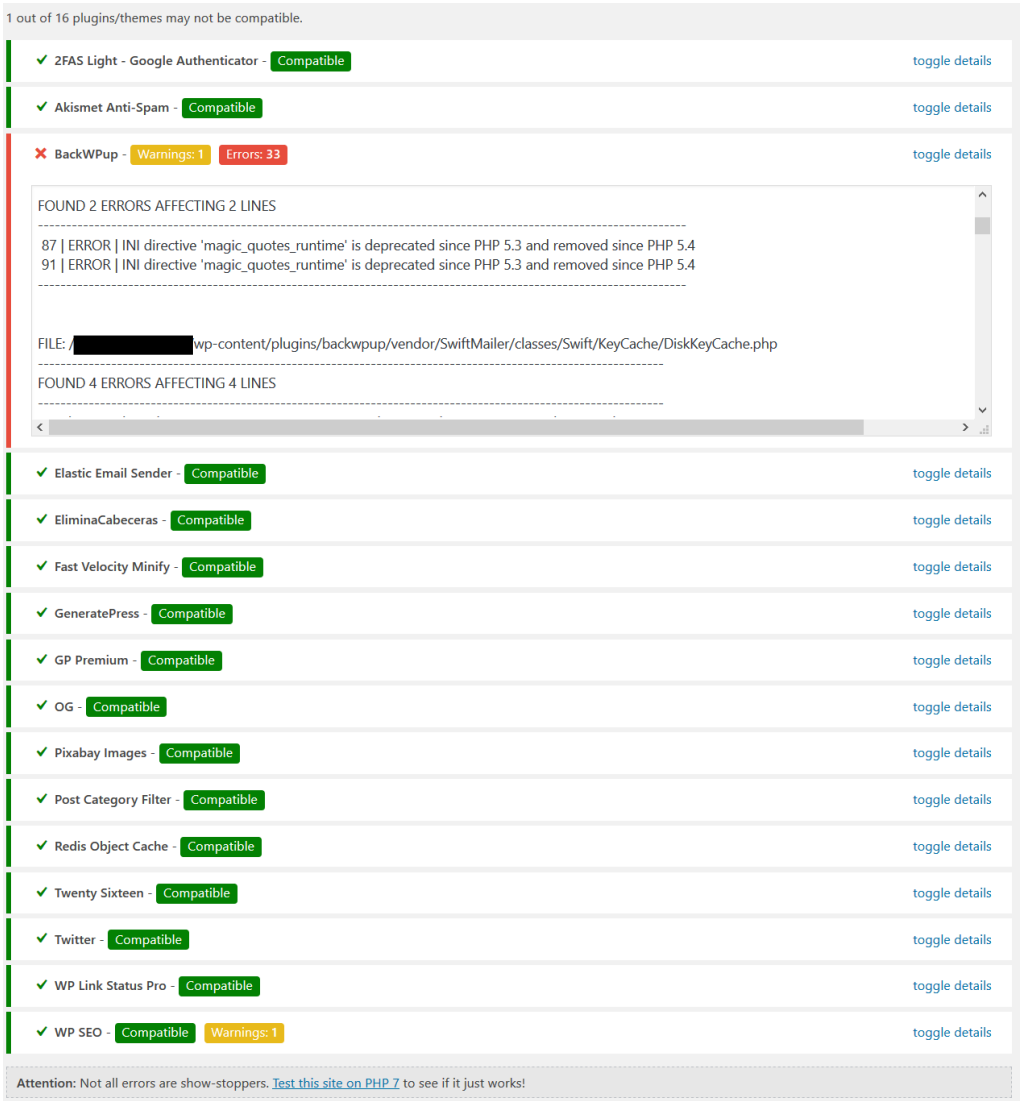
@JavierCasares | @WPdanger

WP Compatibility Checker

https://wordpress.org/plugins/php-compatibility-checker/



WP Compatibility Checker



Versión mínima de PHP

En los últimos tiempos WordPress ha añadido un campo que indica la **versión mínima de PHP necesaria** para que funcionen algunos elementos (por ejemplo, los plugins).

https://make.wordpress.org/plugins/2017/08/29/minimum-php-version-requirement/

```
=== 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
```

WordPress Tide project

En cada evento WordPress aparece la pregunta de:

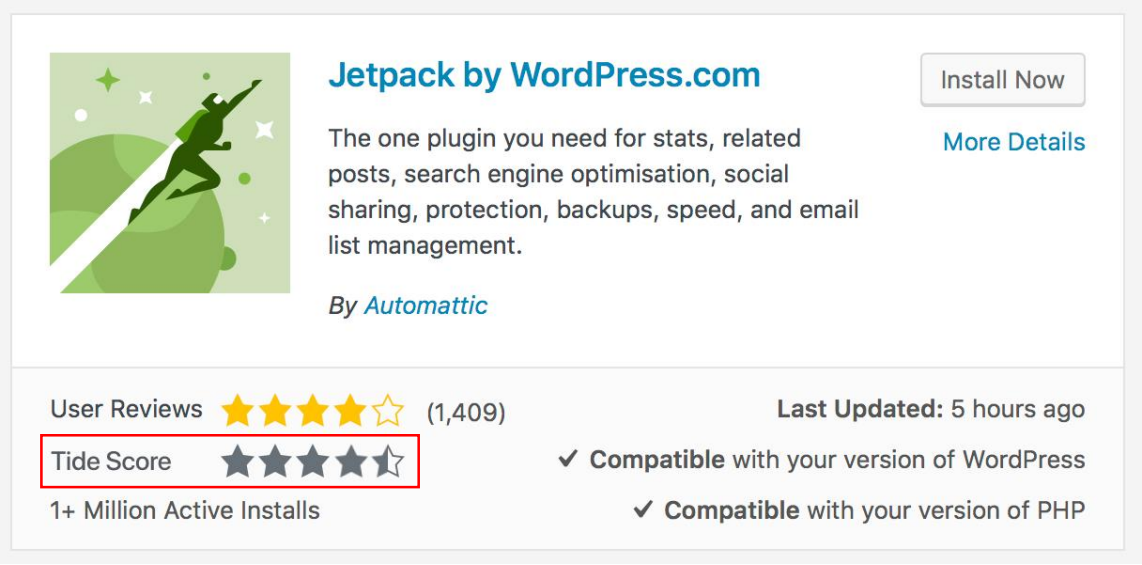
¿Qué plugin me recomiendas para {tema}?

Hay más de 53.000 plugins en wordpress.org, por lo que se hacía necesario un sistema que revise y analice de forma automática todos los plugins.

Para eso aparece el proyecto Tide.

WordPress Tide project

Tide is a service, consisting of an API, Audit Server, and Sync Server, working in tandem to run a series of automated tests against the WordPress.org plugin and theme directories. Through the Tide plugin, the results of these tests are delivered as an aggregated score in the WordPress admin that represents the overall code quality of the plugin or theme. A comprehensive report is generated, equipping developers to better understand how they can increase the quality of their code.



WordPress Tide project

Lecturas sobre Tide:

- https://make.wordpress.org/tide/

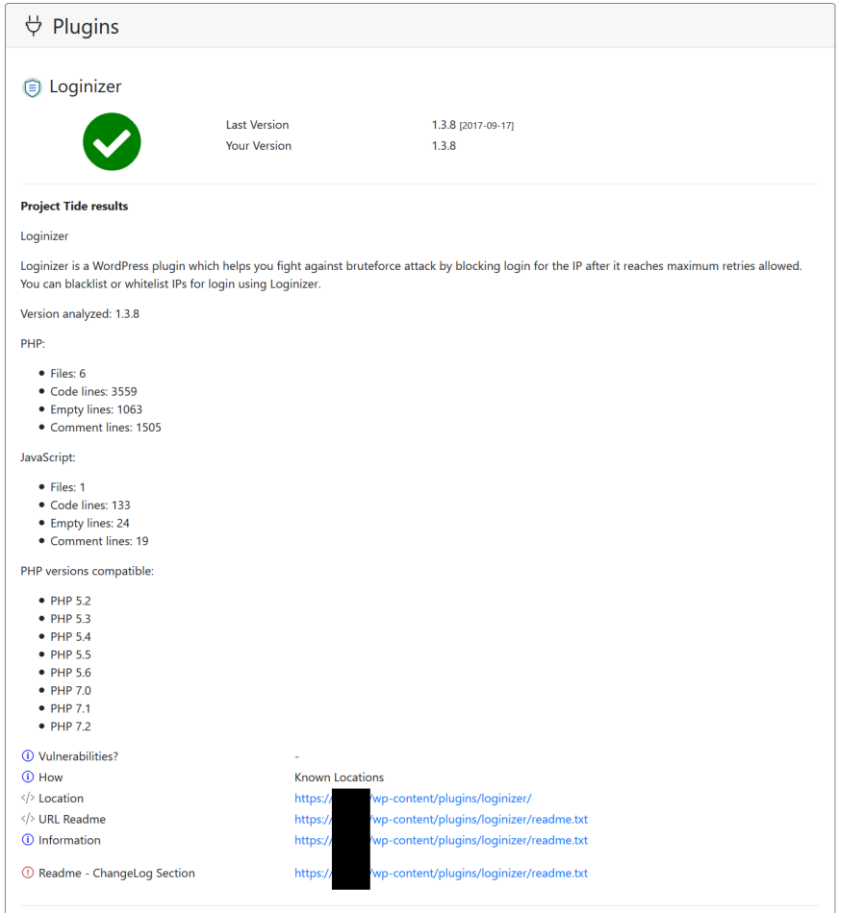
- https://xwp.co/tide-a-path-to-better-code-across-the-wordpress-ecosystem/

- https://wptavern.com/tide-project-aims-to-audit-and-score-wordpress-themes-and-plugins-based-on-code-quality

- Slack: #tide (los martes a las 22:00 UTC)

WordPress Tide en WPdanger

- Información de plugins y plantillas.
- Versión del plugin que ha sido analizada.
- Ficheros, líneas de código, vacías y comentadas por tipo de código (PHP, HTML, CSS, JSON, markdown…)
- Lista de versiones compatibles seguras.
- Aún está en “Alpha”, pero si añades [&tide] a tu *análisis* de WPdanger verás esa información.



¡Déjate de mandangas!

Venga, ahora sí.

Dejemos la teoría y vayamos a la práctica…

Mantén WordPress actualizado

Actualiza el *core* de WordPress automáticamente (no sólo las *minor versions*, sino las *major* también).

[/wp-config.php]

```
define('WP_AUTO_UPDATE_CORE', true);
```

[/wp-config.php]

```
define('WP_AUTO_UPDATE_CORE’, minor);
```

O hazlo todo manualmente:

[/wp-config.php]

```
define('AUTOMATIC_UPDATER_DISABLED', true);
```

Mantén WordPress actualizado

No sólo el *core*, sino *plugins*, *themes* y *translations*.

Añade este plugin a la carpeta [/wp-content/mu-plugins/]

http://bit.ly/wpdanger-autoupdater

```
add_filter('auto_update_core', '__return_true');
add_filter('auto_update_plugin', '__return_true');
add_filter('auto_update_theme', '__return_true');
add_filter('auto_update_translation', '__return_true');
add_filter('auto_core_update_send_email', '__return_false');
```

Mantén WordPress actualizado

¡Atención!

Si tienes una configuración compleja de WordPress

(por ejemplo con plugins “complicados” como WooCommerce o similares)

es mejor que hagas las actualizaciones manualmente en un entorno *sandbox*.

Si todo funciona correctamente, entonces haz las actualizaciones en producción.

¿Problemas con la actualización? *WP-Rollback*
https://wordpress.org/plugins/wp-rollback/

Mantén WordPress “des”actualizado

Si tienes una instalación compleja, y vas a programarte revisiones manuales, desactiva todo.

```
add_filter('auto_update_core', '__return_false');
add_filter('auto_update_plugin', '__return_false');
add_filter('auto_update_theme', '__return_false');
add_filter('auto_update_translation', '__return_false');
add_filter('auto_core_update_send_email', '__return_false');
```

Permisos de ficheros

- Carpetas 750
- Archivos 640
- wp-config.php 400
- readme.html 000

Si quieres que WordPress tenga permisos de escritura en el wp-config.php, ponle 600.

¡Atención!
Nunca des permisos 777 a la carpeta /wp-content/

Tras la instalación

Bloquea los ficheros

/wp-admin/install.php

/wp-admin/setup-config.php

```
location ~* ^/wp-admin/(install|setup-config).php {
  deny all;
}
```

Edición de ficheros

¿Quieres evitar que nadie toque los CSS, *themes* o *plugins*? No los dejes.

[/wp-config.php]

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

Bloquear PHP en carpetas de media

¿Para qué necesitamos PHP en el /wp-content/?

En Apache HTTPD (dentro del fichero .htaccess en la carpeta [/wp-content/uploads/]):

```
<Files *.php>
  deny from all
</Files>
```

Bloquear PHP en carpetas de media

En nginx:

```
location ~* /wp-includes/.*\.php$ {
  deny all;
  access_log off;
  log_not_found off;
}
location ~* /wp-content/.*\.php$ {
  deny all;
  access_log off;
  log_not_found off;
}
location ~* /(?:uploads|files)/.*\.php$ {
  deny all;
  access_log off;
  log_not_found off;
}
```

Acceso a la base de datos

Da sólo los permisos necesarios para el usuario de WordPress:

```
GRANT ALTER, CREATE, DELETE, DROP, INDEX, INSERT, SELECT, UPDATE ON tu_database.* TO 'tu_usuario'@'10.0.0.1' IDENTIFIED BY 'tu_contraseña’;
```

- Acceso que no permita eliminar la base de datos.
- Acceso sólo a tu base de datos
- Acceso sólo a un usuario desde una IP
- Uso de una contraseña de al menos 24 caracteres con letras (mayúsculas y minúsculas), números y caracteres especiales.

Prefijo de la tabla

- No uses el prefijo por defecto [wp_]
- Si tu web es example.com, no uses de prefijo [example_]
- Crea un “algo” aleatorio de letras (minúsculas) y números (no el primer carácter):

[c2712m_]
[jgriyz_]
[ah8zhl_]

[/wp-config.php]

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

Utiliza las *Security Keys*

https://api.wordpress.org/secret-key/1.1/salt/

Configura las Security Keys en el /wp-config.php

```
define('AUTH_KEY', 'l3Yk-= V+N@M&`=-skp,[F?Mp1vN|.tQ-mCQr-_YrUJ-');
define('SECURE_AUTH_KEY', 'u[G-;-XPjovJ_hy?v`IWUgf(/7mGy1R>Na.~Yld(jg~W');
define('LOGGED_IN_KEY', '-gQS^SH+{qCXb_=aBI=Q~x|aq@8`HU:Tt<XJ(j8KX>x*');
define('NONCE_KEY', 'iY]*URXkUJ5o=J0Q/b,P;%ULl1`v3x=>+#F]S|z&^<bz');
define('AUTH_SALT', 'FWlh^z8L;s4`*r>7H#*(iA!OWV9^X#^#m-A&>;!lz@(X');
define('SECURE_AUTH_SALT', 'oZ#3S6d{pjeTb.lxLy2uQec=Cs?oWRRm% *(U7!QFQ%(q');
define('LOGGED_IN_SALT', '=oMWAYx1UVXaZRK?slW}_q9Fbbjw7Bi|Ca|QLst^64/zF');
define('NONCE_SALT', '|)<Z~_/gf[.iiec-M/HM@|xW28LMIc%e<bn^og9+LVv1C');
```

Evita cambios de configuración

[/wp-config.php]

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

No se puede cambiar

Usa un certificado TLS

En todo el sitio navegarás con HTTPS.

La configuración de un certificado dependerá de tu servidor, gestionado o no.

Existe una cosa llamada Let’s Encrypt.

NOTA:

Los certificados actuales y seguros son TLS y no SSL, aunque habitualmente se les llama de la misma manera.

Acceso de usuarios al WP-Admin

Los Nombres de Usuario (*login*) deberían ser “algo más seguros” y predecibles de lo que suelen serlo…

¿Por qué en vez de usar…

[javier]

…no usar…

[Javier Casares]

…que es un nombre “más complejo”?

Acceso de usuarios al WP-Admin

Los usuarios son “tontos”, en general, porque usan contraseñas poco seguras, algo bastante ¿inevitable?.

- Fuerza contraseñas seguras

Usa generadores de contraseñas y no “tú con tu teclado”:
passwordsgenerator.net

- Longitud: 24 caracteres
- Incluir símbolos, números, mayúsculas, minúsculas…

Acceso de usuarios al WP-Admin

Si tienes varios WordPress, recuerda no usar la misma contraseña entre ellos.

Es sencillo saber si tienes más de un sitio web, y si comprometes uno de ellos, intenta evitar los otros usando contraseñas distintas.

Recuerda que tu usuario y contraseña es probable que circule por Internet ya…

1400 Million Clear Text Credentials Discovered in a Single Database

Acceso de usuarios al WP-Admin

Para evitar acceso indeseados, que usen doble verificación (2FA). Tras su usuario y contraseña, necesitarán introducir un código extra que les dará su teléfono móvil.

- 2FAS Light
- Magic Password
- Loginizer

No uses verificación por SMS, usa una App.

Acceso de usuarios al WP-Admin

Pero también es interesante evitar floods o ataques, por lo que también puedes bloquear la cantidad de intentos que un usuario tiene disponibles en un espacio de tiempo:

-Limit Login Attempts

O desconéctalos si no usan el panel:

-Idle User Logout

Hay varios plugins de estos, algunos antiguos, otros más nuevos. Prueba varios y usa el que mejor se adapte a ti.

Acceso de usuarios al WP-Admin

Evita decir si un usuario o contraseña es válido o inválido. Cuando fallas al poner una contraseña dirás si el usuario es correcto o no. Evítalo.

```
function disable_wordpress_login_errors() {
  return 'Meeeeec!';
}
add_filter('login_errors', 'disable_wordpress_login_errors');
```

Acceso de usuarios al WP-Admin

Cuando se crea WordPress lo hace con el usuario “ID=1”. Configura tu sitio, y cuando acabes puedes cambiar la numeración de los usuarios vía SQL:

```
ALTER TABLE wp_users AUTO_INCREMENT = 128;
```

Una vez hayas hecho esto, crea un nuevo usuario administrador, y elimina el primer usuario que creaste.

Con este sistema dejarás de tener los “ID” iniciales y habitualmente atacables vía URL:

```
&autor=1
```

Unifica los CSS y JavaScript…

Sí, esto va muy bien para Web Performance pero…

WordPress incluye por defecto la versión de tu instalación en ficheros CSS y JavaScript.

Si quieres evitarlo (y de paso optimizar la carga), concatena y comprime.

[/wp-config.php]

```
define('CONCATENATE_SCRIPTS', true);
define('COMPRESS_CSS', true);
define('COMPRESS_SCRIPTS', true);
```

…o un plugin, elimina “ver=“

Con un plugin puedes buscar el parámetro “ver” y que lo elimine:

```
add_filter('style_loader_src', 'wpdanger_remove_ver', 9999, 2);
add_filter('script_loader_src', 'wpdanger_remove_ver', 9999, 2);

function wpdanger_remove_ver($src, $handle) {
  $handles = ['style’,’script’];
  if(strpos($src, 'ver=') && !in_array($handle, $handles, true))
    $src = remove_query_arg('ver', $src);
  return $src;
}
```

Ocultar cabeceras inconvenientes

Añade este plugin a la carpeta [/wp-content/mu-plugins/]

http://bit.ly/wpdanger-headers

```
remove_action('set_comment_cookies', 'wp_set_comment_cookies');
add_filter('show_admin_bar','__return_false');
add_filter('the_generator', '__return_false');
remove_action('wp_head', 'adjacent_posts_rel_link', 10, 0);
remove_action('wp_head', 'adjacent_posts_rel_link_wp_head', 10, 0);
remove_action('wp_head', 'feed_links', 2);
remove_action('wp_head', 'feed_links_extra', 3);
remove_action('wp_head', 'rsd_link');
remove_action('wp_head', 'wlwmanifest_link');
remove_action('wp_head', 'wp_generator');
remove_action('wp_head', 'wp_shortlink_wp_head', 10, 0);
```

Evitar ataques mediante XML-RPC

¿No sabes qué es el XML-RPC?
Pues eso es que ni lo usas ni te hace falta.

Añade este plugin a la carpeta [/wp-content/mu-plugins/]

http://bit.ly/wpdanger-xmlrpc

Apache HTTPD (dentro del fichero .htaccess):

```
<Files xmlrpc.php>
  order deny, allow
  deny from all
  allow from 8.8.8.8
</Files>
```

En nginx (dentro del fichero de configuración del sitio):

```
location = /xmlrpc.php {
  limit_except POST {
    deny all;
  }
  allow 8.8.8.8;
  access_log off;
  log_not_found off;
}
```

Copias de Seguridad

Existen decenas de plugins de copias de seguridad / *backup* para WordPress.

https://wordpress.org/plugins/tags/backup/

El que yo uso es BackWPup, que permite guardar en local, Dropbox, Amazon S3, Azure…

NOTA:

Configura la frecuencia de tus copias de seguridad según hayan cambios en tu sitio. Al menos uno por semana.

Seguridad activa

Usa un *firewall*. Puedes usar un sistema compatible con el propio WordPress (en modo plugin) como:

- Wordfence
- Sucuri

Están bien como herramientas de análisis, pero no me gusta tarerlos siempre, porque suelen generar incompatibilidades con el resto del sistema.

¿Por qué no pides a tu hosting un WAF (Web application firewall)?

Herramientas para Webmasters

Baidu 百度站长平台

https://zhanzhang.baidu.com/

Google Search Console

https://www.google.com/webmasters/

Bing Webmaster Tools

https://www.bing.com/toolbox/webmaster

REDbot

https://redbot.org/

DNSBL

http://www.dnsbl.info/

Yandex Webmaster

https://webmaster.yandex.com/

Activa la caché

Aunque es difícil controlar un ataque DDoS, puedes mitigarlo.

[/wp-config.php]

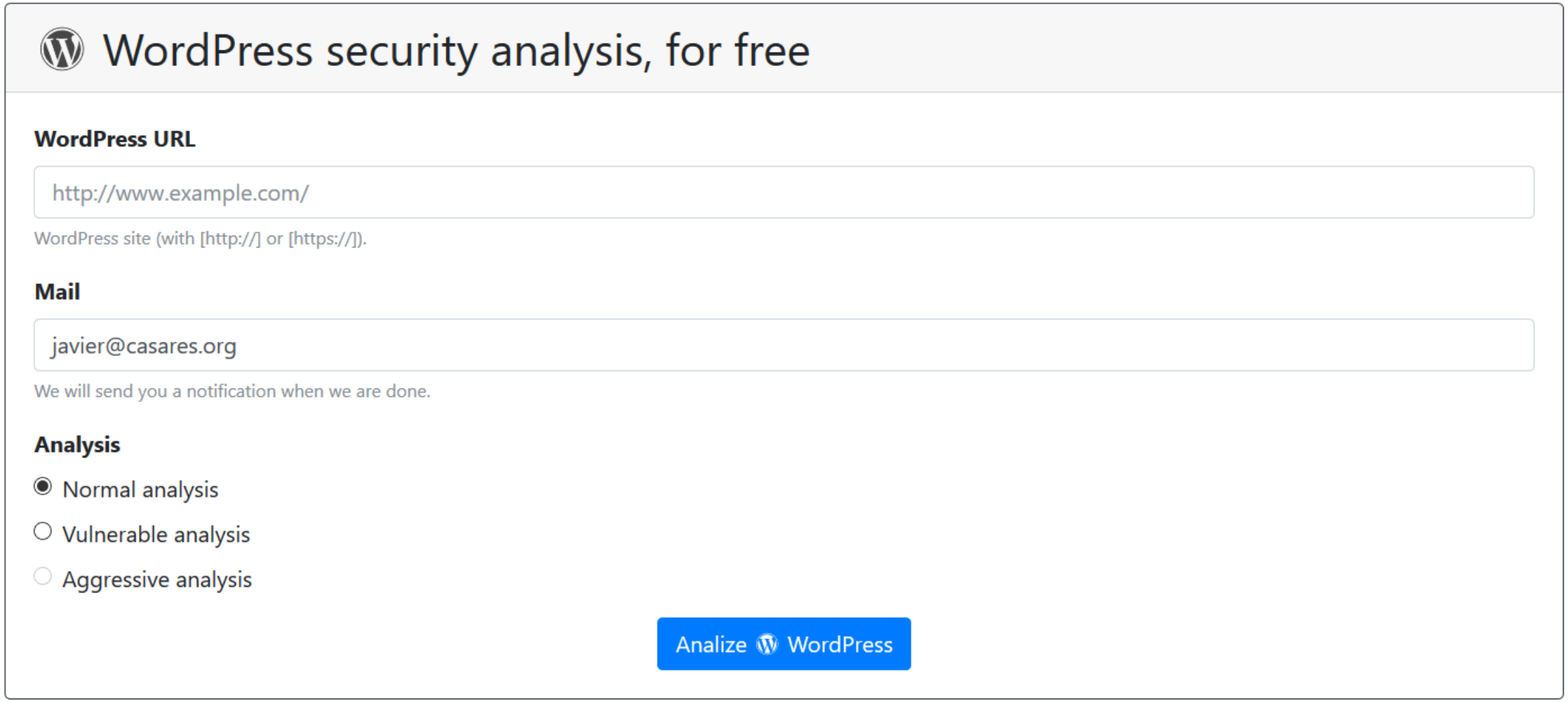
```
define('WP_CACHE', true);
```

Utiliza sistemas de almacenamiento complementarios como:

- memcached
- Redis

Comienza tu propia aventura

www.wpdanger.com



Sentido Común

Dicen que el sentido común es el menos común de los sentidos, y por eso te pido un poco de él.

La seguridad en general es compleja, no hay nada 100% seguro, y por eso hay que aplicar todos estos consejos y códigos con cabeza, sabiendo el porqué los vas a aplicar y no simplemente copiando y pegando líneas de código “porque sí”.

Checklist

- [x] Leer WPdanger: Guía de Seguridad para WordPress
- [ ] Haz una copia de seguridad
- [ ] Actualiza WordPress
- [ ] Elimina plugins y plantillas que no utilices
- [ ] Actualiza plugins, plantillas y traducciones
- [ ] Revisa que todos los usuarios que tienes, son los que han de estar
- [ ] Instala un complemento de “2FA” (doble verificación de acceso)
- [ ] Revisa los permisos en los ficheros del sistema
- [ ] Instala un certificado TLS si no usas HTTPS
- [ ] Activa las herramientas para Webmasters
- [ ] Activa la caché
- [ ] Haz una copia de seguridad (sí, otra vez)

WP-CLI es tu amigo

¿Quieres un pequeño sistema de actualización / mantenimiento con WP-CLI?

https://www.casares.blog/wp-cli-mantenimiento-seguridad/

$ reviso la versión de la instalación de WP-CLI

```
wp cli version
```

$ compruebo si hay actualizaciones disponibles de WP-CLI

```
wp cli check-update
```

$ actualizo WP-CLI a su última versión

```
wp cli update
```

WP-CLI es tu amigo

$ entro en la carpeta de la instalación que quiero analizar

```
cd /carpeta/de/instalacion/wordpress/
```

$ verifico que no haya nada "raro" instalado en el core

```
wp core verify-checksums
```

$ listo la configuración del wp-config

```
wp config get
```

$ listo la lista de usuarios

```
wp user list
```

WP-CLI es tu amigo

$ reviso la versión del WordPress

```
wp core version
```

$ compruebo si hay una nueva versión del WordPress

```
wp core check-update
```

$ actualizo a la última versión del WordPress

```
wp core update --path="/carpeta/de/instalacion/wordpress/"
```

$ verifico que no haya nada "raro" instalado en el core

```
wp core verify-checksums
```

WP-CLI es tu amigo

$ hago una lista de todos los plugins instalados

```
wp plugin list --path="/carpeta/de/instalacion/wordpress/"
```

$ listo todos los plugins que tienen actualizaciones

```
wp plugin update --dry-run --all --
path="/carpeta/de/instalacion/wordpress/"
```

$ actualizo todos los plugins que tienen actualizaciones

```
wp plugin update --all --path="/carpeta/de/instalacion/wordpress/"
```

WP-CLI es tu amigo

$ hago una lista de todas las plantillas instaladas

```
wp theme list --path="/carpeta/de/instalacion/wordpress/"
```

$ listo todas las plantillas que tienen actualizaciones

```
wp theme update --dry-run --all --
path="/carpeta/de/instalacion/wordpress/"
```

$ actualizo todas las plantillas que tienen actualizaciones

```
wp theme update --all --path="/carpeta/de/instalacion/wordpress/"
```

WP-CLI es tu amigo

$ hago una lista de todos los idiomas instalados

```
wp language core list --status=installed
```

$ listo todos los idiomas que tienen actualizaciones

```
wp language core update --dry-run --
path="/carpeta/de/instalacion/wordpress/"
```

$ actualizo todos los idiomas que tienen actualizaciones

```
wp language core update --path="/carpeta/de/instalacion/wordpress/"
```

WP-CLI es tu amigo

$ elimino todos los transients caducados

```
wp transient delete --expired
```

$ compruebo el prefijo del WordPress

```
wp db prefix
```

$ verifico el tamaño de la base de datos del WordPress

```
wp db size
```

$ optimizo la base de datos del WordPress

```
wp db optimize
```

‘Cosas’ en el tintero…

- Revisión de código (sobre todo del que tú desarrollas).
- User role levels / management.
- WAF (Web Application Firewall) a nivel de hosting.
- Acceso SSH / FTP sólo vía VPN o por una IP fija.
- Bases de datos (¿y ficheros?) aisladas (red IP privada).
- Fuentes de datos fiables (plugins, plantillas, etcétera…).
  - Vale que WordPress es Open Source y GPL, pero si te descargas algo de un sitio no-oficial, al menos revisa el código para saber qué haces.
- Cómo recuperar un sitio infectado o comprometido.
  - Puedes leer esta entrada en los foros de WordPress: https://es.wordpress.org/support/topic/limpiar-un-wordpress-infectadohackeado/
- Ataques vía comentarios / spam.

Seguridad WordPress

Más vale prevenir que limpiar (un crackeo)

JavierCasares.com | WPdanger.com | WPBarcelona.com

@JavierCasares | @WPdanger | @WPBarcelona | #WPBarcelona