Seguridad WordPress Avanzada

Recapitulemos

-Contraseña mejorada
-Nombre de usuario mejorado
-Prefijo de base de datos
-Ocultar la versión de WordPress
-Bloqueos por .htaccess
-Cambios en ficheros
-Escaneo de usuarios
-Certificados de Seguridad TLS
-Copias de Seguridad

Y ahora ¿qué?

Ya hemos visto los básicos... ahora toca lo complejo.

Diferenciemos

Hemos de diferenciar el tipo de usuario que soy:
-Inicial
-Avanzado
-Experto

Hemos de diferenciar el tipo de alojamiento:
-Compartido y gestionado por otro
-Soy *Juan Palomo* y lo gestiono yo

Alojamiento

Hora

Sí, la hora, el reloj...

Asegúrate que tu servidor tiene la hora correctamente. Como preferencia, lo mejor es usar una configuración UTC.

Versiones

Sistema Operativo	Versión
CentOS	7.14xx
Debian	9.5
Fedora	28
FreeBSD	11.x
Ubuntu	18.04

Servidor Web	Versión
Apache HTTPD	2.4.3x
nginx	1.15.x

Versiones

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

Lenguaje de Programación	Versión
PHP	7.2

Certificado de Encriptación	Versión
TLS	1.2

Permisos de ficheros

- Carpetas 755
- Ficheros 644
- 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';
```

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<+M7l::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’);
```

Actualízalas de tanto en tanto, que para eso tienes Salt Shaker.

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>
```

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 no 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 actualizó un plugin o plantilla?

¿Por qué instalas un complemento que hace más de un año que no actualiza?

Cualquier desarrollador de plugin o theme debería actualizar los datos de última versión soportada.

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?

2FA (doble verificación)

La idea es instalar un plugin de doble verificación, obligatorio para todos los usuarios.

Existen sistemas aún más avanzados, como el Magic Password, en el que sólo necesitarás una App para Android o iOS y no una contraseña.

Analiza tus enlaces

Utiliza algún complemento que analice los enlaces rotos y no envíes a tus usuarios a posibles sitios maliciosos.

Pero no sólo los enlaces que tú publicas, sino aquellos que te hacen referencia.

Para estos casos puedes desactivarlos, o verificar que cuando se produce uno, realmente te han enlazado desde allí.

Seguridad Activa

Actualizar

Obvio, sí.

Muchos no actualizan "porque un plugin deja de funcionar". Si es así: cambia de plugin.

WordPress es seguro si todos los componentes están al día, mantenidos y actualizados.

Copias de seguridad

Hay que tener copias, y tener alguna probada (sino tendrás *Backup Schrödinger*).

- Puedes usar un plugin para tener una copia. Es importante que tu alojamiento web haga copias.
  - Ten copias completas fuera del alojamiento.
  - Que tu alojamiento tenga copias completas.
  - Ten copias incrementales, si es posible.

Firewall / WAF

Hay que tener una capa de seguridad que evite ataques, o sea, un FireWall.

Tu alojamiento debería ofrecerte un sistema de seguridad de Firewall.

Si no te lo da, hazlo mediante un plugin tipo Wordfence, Sucuri, All in One...

Anti Malware y Anti Virus

Evitemos que hagan cambios en nuestro software si consiguen acceder.

Tu alojamiento debería ofrecerte un sistema de seguridad AntiMalware y AntiVirus.

Si no te lo da, hazlo mediante un plugin tipo Wordfence, Cerber, Sucuri, iThemes...

Herramientas para Webmasters

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

Controla los cambios que se hacen en tu sitio.

- Activity Log
- Audit Trail
- Simple History
- Stream
- User Activity Log
- WP Document Revisions
- WP Security Audit Log

¡Gracias!

JavierCasares.com

WPdanger.com