

UCTechPro Marzo 2018



@TomyCant

Alta Seguridad en WordPress



Tomás Sierra Campos



- Trabajo en el departamento de seguridad de “Netkia” (Grupo PITMA)
- Maestro de Ed. Primaria, formador y desarrollador web.
- Organizador el **congreso de seguridad Sh3llcon**
- Organizador de la **WordCamp Santander** y miembro activo de la comunidad WordPress de España.
- Mas de 4000 horas de formación en Congresos, cursos y talleres.

Podéis encontrarme en las redes como

  @TomyCant

 tomassierra.com

Parámetros esenciales de seguridad que todo WordPress debería tener:

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);
```

Parámetros esenciales de seguridad que todo WordPress debería tener:

Mantén WordPress actualizado

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

Añade estas líneas en un archivo .php de la carpeta
[/wp-content/mu-plugins/]

```
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');
```

Parámetros esenciales de seguridad que todo WordPress debería tener:

Permisos de ficheros

- Carpetas 755
- Archivos 644
- readme.html 000

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

Nunca des permisos 777 a la carpeta /wp-content/

Parámetros esenciales de seguridad que todo WordPress debería tener:

Edición de ficheros

Evita que nadie toque los CSS, themes o plugins

[/wp-config.php]

Edición

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

Actualización

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

Parámetros esenciales de seguridad que todo WordPress debería tener:

Usa un certificado TLS

En todo el sitio navegarás con HTTPS.

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

Let's Encrypt.

NOTA:

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

Parámetros esenciales de seguridad que todo WordPress debería tener:

Modificar prefijos de la bbdd

Modificar el prefijo por defecto **wp_**
por algo como **lsdjdujm_**

Plugins como:

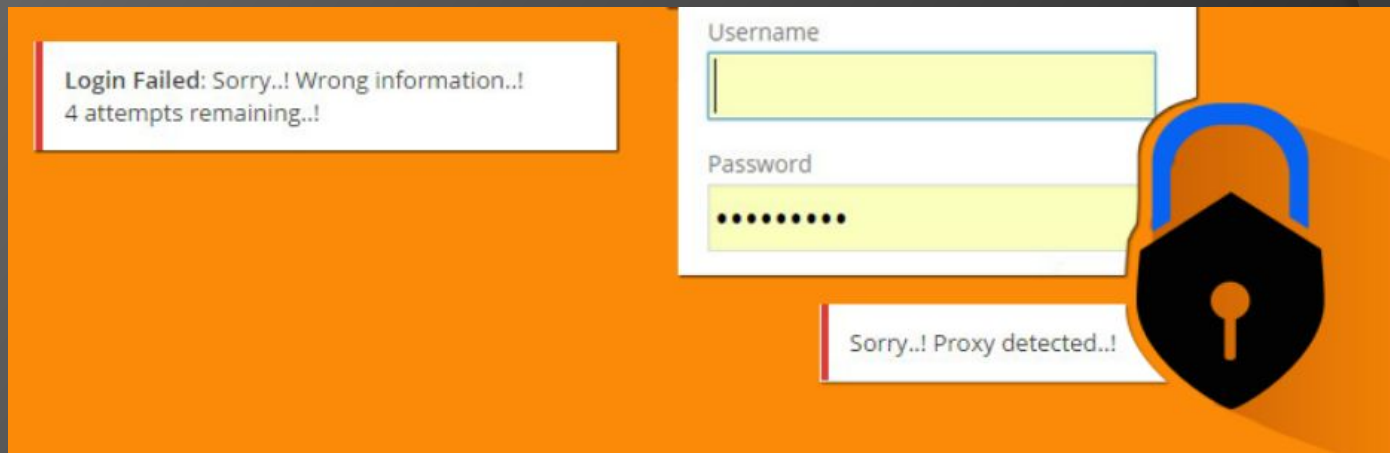
All in one WP Security & Firewall

Sucuri

Ithemes Security...

Parámetros esenciales de seguridad que todo WordPress debería tener:

5.- Limitar el número de intentos de acceso al panel de control.



Plugins:

Limit login attempts...

Wordfence, Sucuri, All In One WP Security & Firewall...

Parámetros esenciales de seguridad que todo WordPress debería tener:

No usar usuario “admin”, “nombredemiweb”, etc.



Nombre de usuario o dirección de correo electrónico

~~admin~~

Contraseña

☐ Recuérdame

Acceder

Parámetros esenciales de seguridad que todo WordPress debería tener:

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

Parámetros esenciales de seguridad que todo WordPress debería tener:

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;%ULI1`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@|xW28LMlc%e<bn^og9+LVv1C');
```

Parámetros esenciales de seguridad que todo WordPress debería tener:

Ocultar cabeceras inconvenientes

Añade un plugin a la carpeta [/wp-content/mu-plugins/] con las siguientes líneas

```
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);
```

Parámetros esenciales de seguridad que todo WordPress debería tener:

Unifica los CSS y JavaScript...

Sí, esto va muy bien para WPO 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);
```

Parámetros esenciales de seguridad que todo WordPress debería tener:

Copias de Seguridad

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

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

NOTA:

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

Parámetros esenciales de seguridad que todo WordPress debería tener:

Editar reglas del .HTACCESS

```
# proteger wpconfig.php
<files wp-config.php>
    order allow,deny
    deny from all
</files>
# proteger htaccess
<files .htaccess>
    order allow,deny
    deny from all
</files>
# proteger xmlrpc
<Files xmlrpc.php>
    Order Deny,Allow
    Deny from all
</Files>
# proteger Readme
<Files readme.html>
    Order Deny,Allow
    Deny from all
</Files>
```

PLUGINS DE SEGURIDAD



HERRAMIENTAS PARA AUDITAR WORDPRESS

Herramientas para auditar WordPress:

HERRAMIENTAS ONLINE

WPDOCTOR:

<https://www.wpdoctor.es/>

WPDOCTOR:

<https://www.wpdanger.com/>

WHATWPTHEMEISTHAT:

<http://whatwpthemeisthat.com/>

Herramientas para auditar WordPress:

LÍNEA DE COMANDOS

Herramientas para auditar WordPress: LINEA DE COMANDOS



DEMOS:

Con plugin de seguridad

Sin plugin de seguridad

Herramientas para auditar WordPress: CONSOLA DE COMANDOS

CMSMAP

para WordPress, Joomla y Drupal

Herramientas para auditar WordPress: CONSOLA DE COMANDOS

```
root@tomas-netkia:/home/tomas/CMSmap# python cmsmap.py -h
CMSmap tool v0.6 - Simple CMS Scanner
Author: Mike Manzotti mike.manzotti@dionach.com
Usage: cmsmap.py -t <URL>
Targets:
  -t, --target      target URL (e.g. 'https://example.com:8080/')
  -f, --force       force scan (W)ordpress, (J)oomla or (D)rupal
  -F, --fullscan    full scan using large plugin lists. False positives and slow!
  -a, --agent       set custom user-agent
  -T, --threads     number of threads (Default: 5)
  -i, --input       scan multiple targets listed in a given text file
  -o, --output      save output in a file
  --noedb          enumerate plugins without searching exploits

Brute-Force:
  -u, --usr         username or file
  -p, --psw         password or file
  --noxmlrpc       brute forcing WordPress without XML-RPC

Post Exploitation:
  -k, --crack       password hashes file (Require hashcat installed. For WordPress and Joomla only)
  -w, --wordlist    wordlist file

Others:
  -v, --verbose     verbose mode (Default: false)
  -U, --update      (C)MSmap, (W)ordpress plugins and themes, (J)oomla components, (D)rupal modules, (A)ll
  -h, --help       show this help

Examples:
  cmsmap.py -t https://example.com
  cmsmap.py -t https://example.com -f W -F --noedb
  cmsmap.py -t https://example.com -i targets.txt -o output.txt
  cmsmap.py -t https://example.com -u admin -p passwords.txt
  cmsmap.py -k hashes.txt -w passwords.txt
root@tomas-netkia:/home/tomas/CMSmap#
```

Comandos: *python cmsmap.py -h*

Herramientas para auditar WordPress: LINEA DE COMANDOS

Comandos:

`python cmsmap.py -t http://dymweb.es`

Escaneo simple de vulnerabilidades

```
root@tomas-netkia:/home/tomas/CMSmap# python cmsmap.py -t http://dymweb.es
[-] Date & Time: 11/04/2017 15:22:58
[-] Target: http://dymweb.es
[M] Website Not in HTTPS: http://dymweb.es
[I] Server: Apache/2.4.10 (Debian)
[L] X-Frame-Options: Not Enforced
[I] Strict-Transport-Security: Not Enforced
[I] X-Content-Security-Policy: Not Enforced
[I] X-Content-Type-Options: Not Enforced
[L] No Robots.txt Found
[I] CMS Detection: Wordpress
[I] Wordpress Version: 4.6
[I] Wordpress Theme: twentysixteen
[-] Enumerating Wordpress Usernames via "Feed" ...
[-] Enumerating Wordpress Usernames via "Author" ...
[M] User de Mentira
[M] Website vulnerable to XML-RPC Brute Force Vulnerability
[I] Autocomplete Off Not Found: http://dymweb.es/wp-login.php
[-] Default WordPress Files:
[I] http://dymweb.es/readme.html
[I] http://dymweb.es/license.txt
[I] http://dymweb.es/wp-includes/images/crystal/license.txt
[I] http://dymweb.es/wp-includes/images/crystal/license.txt
[I] http://dymweb.es/wp-includes/js/plupload/license.txt
[I] http://dymweb.es/wp-includes/js/tinymce/license.txt
[I] http://dymweb.es/wp-includes/js/swfupload/license.txt
[I] http://dymweb.es/wp-includes/ID3/license.txt
[I] http://dymweb.es/wp-includes/ID3/readme.txt
[I] http://dymweb.es/wp-includes/ID3/license.commercial.txt
[-] Searching Wordpress Plugins ...
[-] Searching Wordpress TimThumbs ...
[I] Checking for Directory Listing Enabled ...
[-] Date & Time: 11/04/2017 15:24:15
[-] Completed in: 0:01:17
root@tomas-netkia:/home/tomas/CMSmap#
```

Herramientas para auditar WordPress: LINEA DE COMANDOS

Otras herramientas

PLECOST

CMSScanner

WPScan

Fortificar WordPress: ANTES DE LA INSTALACIÓN:

WPHARDENING



Fortificar WordPress ANTES DE LA INSTALACIÓN:

```
root@tomas-netkia: /home/tomas/ZAP_2.6.0

  W P H a r d e n i n g  ( )
Fortify the security of any WordPress installation.
Caceria de Spammers - http://www.caceriadespammers.com.ar

/home/tomas/Escritorio/wordpress -
  This project directory is a WordPress.

chmod on Directories
  All directories drwxr-xr-x (755)

chmod on Files
  All files -rw-r--r-- (644)

Deleted WordPress versions
  Modified: wp-includes/default-filters.php
  // This is a function that removes versions of WordPress.
  function delete_version_wp() {
    return "";
  }
  add_filter('the_generator', 'delete_version_wp');

Deleted fingerprinting WordPress
  All changes implemented.

Created file wp-config-wphardening.php
  Name of the database > bbdd
  Name of the User > user
  Password of the user > password
  Host [localhost] >
  Table prefix [wph_] > wpgjsyh_
  Language [es_ES] >
  Memory Limit [64M] > 128
  Disable wp-cron.php? [y/n] > n
  Your host provider gives you SSL certificate? [y/n] > n
  Enable Multisite? [y/n] > n
  Auto update Core? [y/n] >

Create Indexes Files
  All index.php files were created.

Not Found file library Timthumb in /home/tomas/Escritorio/wordpress/
```


Fortificar WordPress ANTES DE LA INSTALACIÓN:

WPHARDENING

Escaneo rápido de vulnerabilidades:

```
python wphardening.py -d /home/tomas/Escritorio/wordpress -v
```

- Configura los permisos adecuados a toda la raíz de archivos.
- Elimina los ficheros y directorios no utilizados.
- Crea un robots.txt personalizado.
- Elimina fingerprinting: huellas de seguimiento y la información de versión.
- Crea un índice de ficheros.
- Descarga e instala varios plugins relacionados con la seguridad.
- Genera un nuevo archivo wp-config.php.

Todos los Comandos:

```
python wphardening.py -d /home/path/to/wordpress -c -r -f -t --wp-config --indexes --plugins -o /home/user/wphardening.log
```

Descarga github: <https://github.com/elcodigok/wphardening>

Más info: <http://www.caceriadespammers.com.ar>



MUCHAS GRACIAS



tomassierra.com



[@Tomycant](https://twitter.com/Tomycant)



<https://www.facebook.com/tomycant>



WORDPRESS

