wordpress

- /vía: http://wpzine.com/wordpress-security-hacks-and-tricks/
- /vía: http://www.katharsix.com/la-seguridad-en-wordpress-algunos-consejos/
- /vía: http://www.katharsix.com/la-seguridad-en-wordpress-algunos-consejos-ii/

- WordPress multisite

securizar

- cambiar usuario «admin»
- tener el WP actualizado
- usar contraseñas fuertes
- aplicar el perfil correspondiente al trabajo a realizar - administrador no ha de ser el perfil por defecto para todos
- quitar versión de WP, añadiendo una función en el fichero **functions.php**:

```
function no_generator() { return ''; }
add_filter( 'the_generator', 'no_generator' );
```

- Desactivar XML-RPC (plugin → **Disable XML-RPC-API**)
  - https://www.wpbeginner.com/plugins/how-to-disable-xml-rpc-in-wordpress/
  - https://www.fortinet.com/blog/threat-research/gotrim-go-based-botnet-actively-brute-forces-wordpress-websites
  - https://unaaldia.hispasec.com/2022/12/gotrim-la-red-de-bots-que-busca-controlar-cuentas-de-administrador-de-wordpress.html

  ```
  wget https://fruitsmontmany.cat/wp-json/wp/v2/users
  ```

trucos

- obligar método https VS ftp al actualizar:

  wp-config.php

  ```
  define('FS_METHOD', 'direct');
  ```

recover & debugging

- desactivar plugins:https://www.ostraining.com/blog/wordpress/disable-a-wordpress-plugin/
  - `wp-content/plugins`, rename
  - DBB → wp-options → active_plugins
- DEBUG:https://wordpress.org/support/article/debugging-in-wordpress/

plugins

- Activity Log
- All in One WP Security
- Asesor de Cookies
- Akismet, el antispam
- Broken Link Checker
- Contact Form 7 (formularios de contacto sencillos)
- Limit Login attempts
- Easy HTTPS redirection
- Email Log
- Font Awesome
- Google Analytics
- Google Analytics dashboard for WP
- Loginizer Security
- MailPoet newsletters
- Media Library Organizer
- ~~miniOrange 2 factor auth.~~
- Obfuscate Email
- PHP Compatibility Checker
- User Groups
- User Groups restrictions
- Secure WordPress
- WP 2FA - Two-factor authentication for WordPress
- WP Construction Mode (diferentes opciones para poner la página «en obras»)
- WP Database Backup
- WP Email Template lite
- WP Forms Lite
- WPS Hide Login
- WP Maintenance mode
- WordPress Firewall 2
- WP Super Cache
- YouTube

sistemas

- borrar ficheros y carpetas de instalación:
  - /readme.html
  - /wp-admin/install.php
- proteger fichero wp-config.php

.htaccess

```
<Files wp-config.php>
   order allow,deny
   deny from all
</Files>
```

- Si es posible, permitir acceso ADMIN solo desde ciertas IPs a los directorios **wp-admin**, **wp-includes**

.htaccess

```
# my ip address only
order deny,allow
allow from 213.27.244.178
```

```
allow from 62.97.72.29
deny from all
```

  - No permite acceder a las imágenes desde los buscadores, habría que excluir **wp-includes/upload**

- evitar el acceso a ficheros:

.htaccess

```
# disable directory browsing
    Options All –Indexes
```

- controlar acceso a directorio UPLOADS o UPGRADE, permitiendo solo ciertos tipos de ficheros

.htaccess

```
# seguridad de subida de archivos en carpeta
<Files ~ ".*\..*">
    Order Allow,Deny
    Deny from all
</Files>
<FilesMatch
"\.(jpg|jpeg|jpe|gif|png|bmp|tif|tiff|doc|pdf|rtf|xls|numbers|odt|pages|k
ey|zip|rar)$">
    Order Deny,Allow
    Allow from all
</FilesMatch>
```

  - http://ayudawordpress.com/seguridad-en-la-carpeta-uploads-de-wordpress/

From:
https://miguelangel.torresegea.es/wiki/ - **miguel angel torres egea**

Permanent link:
https://miguelangel.torresegea.es/wiki/web:security:wordpress?rev=1704355004

Last update: **03/01/2024 23:56**