Tomás Sierra Campos
@Tomycant

WORDCAMP MADRID Abril 2017

¿SEGURO QUE CREO WEBS SEGURAS?

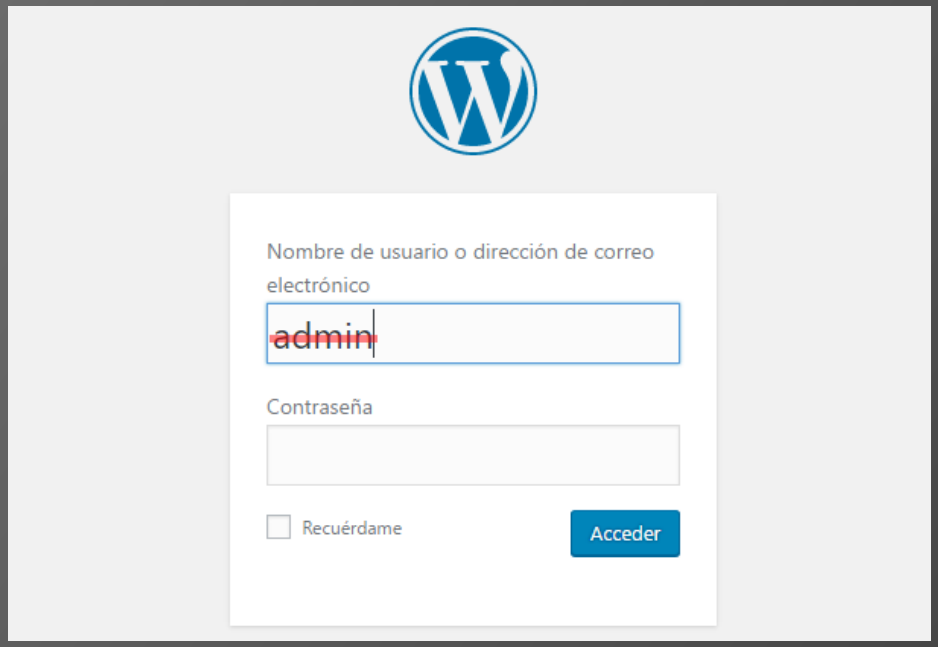


Parámetros esenciales de seguridad que todo WordPress debería tener:

1.- Esconder la ruta de acceso al panel de control

Parámetros esenciales de seguridad que todo WordPress debería tener:

2.- No usar usuario “admin”



Parámetros esenciales de seguridad que todo WordPress debería tener:

3.- Modificar la ID del usuario administrador

dymweb.es/?autor=1

dymweb.es/author/admin/

Parámetros esenciales de seguridad que todo WordPress debería tener:

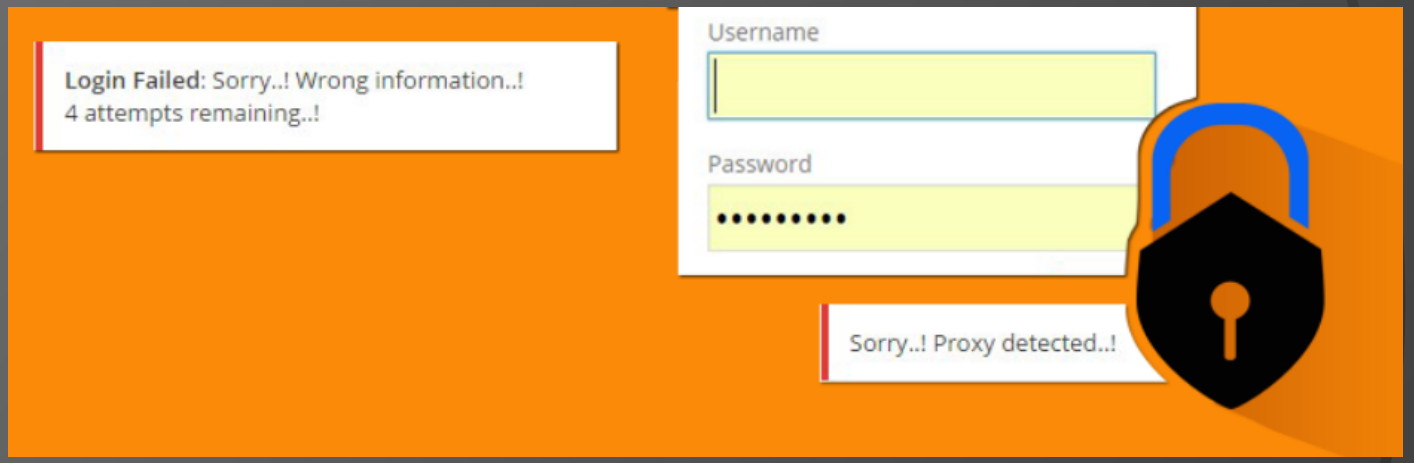
4.- Modificar prefijos de la bbdd

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

Plugins como Sucuri, Acunetix WP Security, Ithemes Security, etc.

Parámetros esenciales de seguridad que todo WordPress debería tener:

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



Plugins:
Limit login attemps...
Wordfence, Sucuri, All In One WP Security & Firewall...

Herramientas para auditar WordPress:

HERRAMIENTAS ONLINE

WPDOCTOR: https://www.wpdoctor.es/
WHATWPTHEMEISTHAT: http://whatwpthemeisthat.com/

DEMOS ONLINE DE AMBAS HERRAMIENTAS

Herramientas para auditar WordPress:

CONSOLA DE COMANDOS

Herramientas para auditar WordPress:

CONSOLA DE COMANDOS

CMSMAP: para WordPress, Joomla y Drupal

Comandos: *python cmsmap.py -h*

```
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#
```

Herramientas para auditar WordPress:

CONSOLA DE COMANDOS

CMSMAP: para WordPress, Joomla y Drupal

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:

CONSOLA DE COMANDOS

Otras herramientas

PLECOST
CMSScanner

Herramientas para auditar WordPress:

CONSOLA DE COMANDOS

DEMOS:

Con plugin de seguridad
Sin plugin de seguridad

Fortificar WordPress
ANTES DE LA INSTALACIÓN:

WPHARDENING

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 fingerpinting: 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

www.tomassierra.com

@Tomycant

https://www.facebook.com/tomas.profesor.3