

Seguridad en WordPress

WPHardening

Daniel Maldonado / @elcodigok



OWASP
LATAM
2017
LATIN AMERICA TOUR

Daniel Maldonado

Ing. en Computación, Analista de Sistemas y Técnico
Informático, SysAdmin, Certificado Tecnologías
MikroTik, Consultor de Seguridad y **Activista del
Software Libre**

@elcodigok



Cacería de Spammers

www.caceriadespammers.com.ar

27.9%

de toda la web

+49.800

Plugins

+18.000

Themes

111.000 base de datos de Wordpress públicas

13/03/2014

vulnerabilidad 0-day en el script TimThumb

25/06/2014

Ataques de fuerza bruta en Wordpress utilizando XML-RPC

28/07/2014

Exploit for stealing backups on WP sites with WP-DB-Backup v2.2.4 plugin

22/11/2014

06/12/2016 se publica WordPress 4.7

11/01/2017 v4.7.1 corrige 8 fallos de Seguridad.

26/01/2017 v4.7.2 corrige 3 fallos de Seguridad.

06/03/2017 v4.7.3 corrige 6 fallos de Seguridad.

20/04/2017 v4.7.4.

Seguridad Informática

El Principio KISS

... las cosas simples y fáciles de entender suelen tener mejor aceptación que las complejas ...

Leyes de Fortificación

- Mínimo Punto de Exposición (**MPE**)
- Mínimo Privilegio Posible (**MPP**)
- Defensa en Profundidad (**DP**)

Configurar WordPress al extremo

Configurar la Base de datos

```
define('DB_NAME', 'NombreBaseDeDatos');  
define('DB_USER', 'UsuarioBaseDeDatos');  
define('DB_PASSWORD', 'contrasena');  
define('DB_HOST', 'localhost');  
define('DB_CHARSET', 'utf8');
```

llevarlo fuera del proyecto

Modificar el prefix de tablas

```
$table_prefix = 'wph419_';
```

Agregar un firewall

limitar conexiones en .htaccess

Limitar la memoria

```
define('WP_MEMORY_LIMIT', '64M');
```

Descativar wp-cron.php

```
define('DISABLE_WP_CRON', false);
```

Forzar el uso de Certificados SSL

```
define('FORCE_SSL_LOGIN', true);  
define('FORCE_SSL_ADMIN', true);
```

Cambiar los permisos en Archivos y Directorios

Desactivar el Debugging mode

```
define('WP_DEBUG', false);
```

**Evitar la navegación por
Directorios**

Analizar código estático de Plugins y Themes

Desactivar la edición de Plugins y Themes

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

Seguridad

Evitar Fingerprinting

Evitar Enumeración

Reparar Full Path Disclosure

Escaneo de Malware

Inventario de librería

Modificar archivos estáticos

*.css y *.js

Políticas de Actualización

Actualizaciones

- Core de WordPress **4.7.4**
- Plugins
- Themes
- Componente de los Themes

Entorno de Producción y Desarrollo

Ejecutar las Actualizaciones

Documentar las Actualización

- Fecha y Hora de Actualización
- Responsable de la Actualización
- Componentes Actualizados
- Nuevas Versiones

WPHardening

WPHardening

- Herramienta de línea de comando *UNIX
- Escrita en Lenguaje Python 2.7
- Licencia GPLv3
- Automatización de Cambios
- Generador de Archivo
- Versión estable v1.5



WPHardening

v1.6

WPHardening

1. Validación de Proyecto WordPress
2. Asignación de Permisos
3. Eliminación de Componentes
4. Creación de robots.txt
5. Eliminación de Fingerprinting
6. Búsqueda de librerías TimThumb
7. Generador de Archivo de Configuración
8. Eliminación de Versión
9. Plugins de Seguridad
10. Creación de archivos Index
11. Escaneo de Malware

WPHardening v1.6

1. Compresión *.css y *.js
2. Asignación de Usuario y Grupos
3. Enumeración de malware
4. Integración con Travis CI
5. Compatibilidad con versiones anteriores
6. Código fuente normalizado a PEP8
7. Creación de Archivo LOG
8. Implementación de 6G Firewall
9. Desactivar REST API

Como obtener WPHardening

```
$ git clone https://github.com/elcodigok/wphardening.git
```

DEMO

Chequear un Proyecto en WordPress

```
$ ./wphardening.py -d /home/path/wordpress -v
```


Cambiar permisos en Archivos y Directorios

```
$ ./wphardening.py -d /home/path/wordpress --chmod -v
```

Eliminar Archivos que no se utilizan

```
$ ./wphardening.py -d /home/path/wordpress --remove -v
```

Generador de Archivo Robots.txt

```
$ ./wphardening.py -d /home/path/wordpress --robots -v
```

Remover todos los Fingerprinting

```
$ ./wphardening.py -d /home/path/wordpress --fingerprinting -v
```

Chequear librería TimThumb

```
$ ./wphardening.py -d /home/path/wordpress --timthumb -v
```

Creación de Archivos Index

```
$ ./wphardening.py -d /home/path/wordpress --indexes -v
```

Descarga de Plugins Recomendados

```
$ ./wphardening.py -d /home/path/wordpress --plugins
```

Generador del Archivo wp- config.php

```
$ ./wphardening.py -d /home/path/wordpress --wp-config
```


Eliminación de Versión de WordPress

```
$ ./wphardening.py -d /home/path/wordpress --delete-version -v
```

Combinando todas las opciones

```
$ ./wphardening.py -d /home/user/wordpress -c -r -f -t --wp-col
```

Mecanismo de Monitoreo

Análisis Cualitativo y Cuantitativo

Control de Versiones

Adoptar metodologías de Desarrollo

Entornos de Prueba y Entornos de Producción

BACKUPS

... el **47%** de las empresas **nunca** realiza copias de seguridad de sus datos ...

Conclusiones.

Revisar las Configuraciones

Ejecutar las Actualizaciones

Plan de Backup

Está TODO por hacer

I + D

Investigación + desarrollo

Buscar ...

Niveles de Seguridad Aceptables



[HackersClub.academy](https://hackersclub.academy)

Instalación en 5'

Instalación Segura en 7'

Muchas Gracias.

- Ing. Daniel Maldonado
- @elcodigok
- info@danielmaldonado.com.ar
- caceriadespammers.com.ar