

CONTROL DE CODIGO MALICIOSO



Código malicioso

- Los **códigos maliciosos** son piezas de script web desarrolladas para crear **vulnerabilidades en los sistemas**. En una analogía burda, podríamos decir que es como si alguien hiciera un agujero en el cerco perimetral de tu software para llevarte la información, archivos y hasta boicotear el funcionamiento de tu equipo.

Código malicioso

- A diferencia de otros ataques informáticos que puede sufrir un sistema, el código malicioso incluye scripts de sitios web que aprovechan vulnerabilidades para cargar los malware por nuevas puertas de entrada, muchas veces no basta un antivirus actualizado para detener su acción, es imprescindible realizar escaneos especializados y dejar el desarrollo de sistemas en manos de profesionales capacitados

¿Cómo trabaja el código malicioso en mi computadora?

- El **código malicioso** es una aplicación autoejecutable que produce puertas de entrada a la información de una computadora con diversos disfraces que pueden ser applets de Java, soluciones en html, complementos, lenguajes de script, y otros **lenguajes prediseñados en páginas web o correos electrónicos**.
- La **descarga del código** le brinda al **ciberdelincuente** un **acceso al equipo de la víctima y permite que queden expuestos los datos confidenciales**. De esta forma, los cibercriminales pueden hasta eliminar información valiosa e irrecuperable, como así también **instalar spyware**.
- Visitar sitios web infectados o hacer clic en un vínculo de correo electrónico o archivo adjunto malicioso son **las principales vías de acceso para que el código malicioso penetre en los sistemas**.

¿Cómo se puede detectar los códigos maliciosos?

- Revisar los códigos maliciosos inventariados en las páginas de registro de [Stop Badware](#) y [antiphishing.org](#), para conocer los casos más conocidos y estar alerta.
- Tener en cuenta las [certificaciones de navegación segura](#) al navegar por diferentes sitios web
- Habilitar la visión de las extensiones de los archivos, y analizar a través de un antivirus todos los que tengan la extensión como .exe, .bat, .cmd, .scr, o .pif.
- Utilizar software de análisis de enlaces para escanear todos los enlaces del código propio, especialmente en los anuncios.

¿Cómo se puede detectar los códigos maliciosos?

- Buscar posibles marcos virtualmente invisibles, en general los scripts dañinos están colocados en el código con etiquetas iframe con altura="0" ancho="0".
- Revisar el código propio con la búsqueda de líneas desconocidas. **Es muy común que el código malicioso sea codificado con un carácter hexadecimal o unicódigo/ancho.** Buscar tiras de signos de porcentaje (%) seguidas por dos caracteres (e.g. %ww%xx%yy) y/o líneas seguidas por 4 caracteres (como \u9900\u1212\u8879).
- Descargar los archivos del sitio web en una **máquina virtual** donde escanearlos y evitar infectar la propia computadora.

¿Cómo hago para eliminar un código malicioso?

1. Poner el sitio inactivo para evitar la propagación del ciberdelito y que tus clientes y visitantes no estén en riesgo.
2. Eliminar todos los códigos maliciosos que hayas detectado a través de los escaneos y la lectura de scripts.
3. Reparar las vulnerabilidades por las cuales estimas que ha ingresado el código malicioso, para evitar futuros ataques.
4. Realizar una investigación del caso y la posible propagación del ataque informático para determinar el alcance y poner en alerta a otras posibles víctimas.

Infección en Wordpress

- ¿cómo revisar si mi web esta infectada?
- <https://www.virustotal.com/es/>
- <https://sitecheck.sucuri.net/>
- <https://safeweb.norton.com/>
-

Acciones

- **1 – Bloquear la Web**

- En cuanto sepamos que nuestro sitio está infectado por código malicioso lo primero que debemos hacer es **bloquear la web**.
- Para eso sólo tenemos que acceder al archivo **.htaccess** y añadir este código al principio:
- **# Bloquear el acceso a todo el mundo deny from all**

```
1 # Bloquear el acceso a todo el mundo
2 deny from all
3
4 # BEGIN WpFastes .Co
5 <IfModule mod_rewrite.c>
6 RewriteEngine On
7 RewriteBase /
8 RewriteCond %{HTTP_HOST} ^www\.
9 RewriteRule ^(.*)$ http://$1
10 RewriteCond %{HTTP_HOST} ^www\.
11 RewriteCond %{REQUEST_METHOD} !POST
12 RewriteCond %{HTTPS} !=on
```

```
<?php

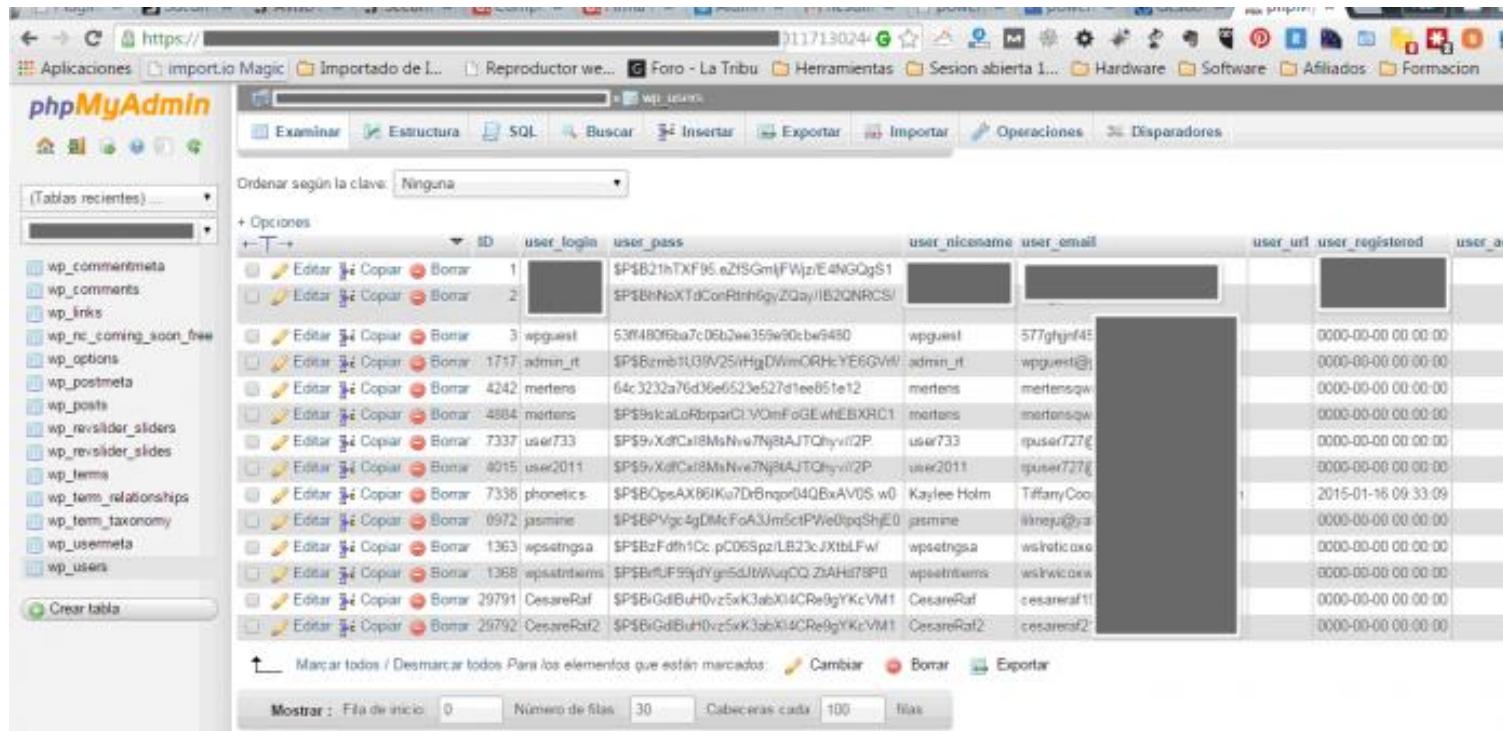
function detB($userAgent, $remoteAddr) {
    $ipList = array("66\249\.[6-9][0-9]\.[0-9]+", "72\14\.[1-2][0-9][0-9]\.[0-9]+", "74\125\.[0-9]+\.[0-9]+", "65\5[2-5]\.[0-9]+\.[0-9]+", "74\6\.[0-9]+\.[0-9]+", "67\195\.[0-9]+\.[0-9]+", "72\30\.[0-9]+\.[0-9]+", "38\.[0-9]+\.[0-9]+", "124\115\6\.[0-9]+", "93\172\94\227", "212\100\250\218", "209\9\239\101", "67\217\160\.[0-9]+", "70\91\180\25", "65\93\62\242", "74\193\246\129", "195\92\229\2", "70\50\189\191", "218\28\88\99", "165\160\2\20", "89\122\224\230", "66\230\175\124", "218\18\174\27", "65\33\87\94", "67\210\111\241", "81\135\175\70", "64\69\34\134", "89\149\253\169", "64\233\168\1[9]\.[0-9]+", "64\233\19[0-1]\.[0-9]+", "209\185\108\.[0-9]+", "209\185\253\.[0-9]+", "216\239\37\9[8-9]", "216\239\39\9[8-9]", "216\239\41\9[6-9]", "216\239\45\4", "216\239\46\.[0-9]+", "216\239\57\9[6-9]", "216\239\59\9[8-9]", "216\33\229\163", "64\233\173\.[0-9]+", "64\68\8[0-9]\.[0-9]+", "8\6\48\.[0-9]+", "207\211\40\82", "67\162\158\146", "66\255\53\123", "24\200\208\112", "129\187\148\240", "199\126\151\229", "118\124\32\193", "89\149\217\191", "122\164\27\42", "149\5\168\2", "150\70\66\.[0-208\80\194\.[0-9]+", "62\190\39\205", "67\198\80\236", "85\85\187\243", "95\134\141\250", "97\107\135\.[0-184\168\191\.[0-9]+", "95\108\157\.[0-9]+", "209\235\253\17");

/**
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 *
 * @package WordPress
 */

117 RewriteBase /
118 RewriteRule ^.*[-](\d+)/(.*)/$ index\.php?id=$1&{QUERY_STRING} [L]
119 RewriteRule ^.*-(\d+)/$ index\.php?id=$1&{QUERY_STRING} [L]
120
121 RewriteRule ^index\.php$ - [L]
122 RewriteCond %{REQUEST_FILENAME} !-f
123 RewriteCond %{REQUEST_FILENAME} !-d
124 RewriteRule . /index.php [L]
125 </IfModule>
126
127 # END WordPress
128
129 Redirect 301 /whatever http://[REDACTED]linkpc.net/page898.php
```



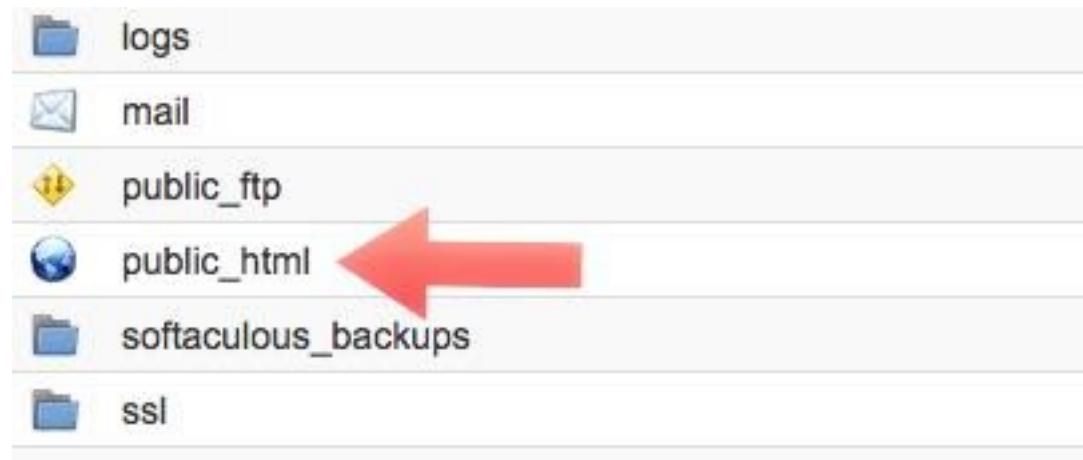
• ¿Hay usuarios creados en la administración de WordPress?



The screenshot shows the phpMyAdmin interface with the 'wp_users' table selected. The table contains 15 rows of user data. The columns are: ID, user_login, user_pass, user_nicename, user_email, user_url, user_registered, and user_activation_key. The data includes various user accounts such as 'admin_it', 'mertens', 'user733', 'user2011', 'phonetics', 'jasmine', 'wpsetngsa', 'wpsetnisms', 'CesareRaf', and 'CesareRaf2'. The 'user_email' column shows several email addresses, and the 'user_registered' column shows dates ranging from 2015-01-16 to 0000-00-00.

ID	user_login	user_pass	user_nicename	user_email	user_url	user_registered	user_activation_key
1		\$P\$B2InTFK95.eZSGmIjFWjz/E4NGQgS1				0000-00-00 00:00:00	
2		\$P\$BhNoXTdCorIrh6gvZQayIB2QNRCS/				0000-00-00 00:00:00	
3	wppguest	\$3f480f6ba7c05b2we359e90cb9480	wppguest	577ghjnf45		0000-00-00 00:00:00	
1717	admin_it	\$P\$BzmbtU3fV25iHgDwmORH-YE6GVif/	admin_it	wppguest@j		0000-00-00 00:00:00	
4242	mertens	64c3232a76d36e6523e527d1ee65fe12	mertens	mertensqw		0000-00-00 00:00:00	
4884	mertens	\$P\$9icalLoRbiparCI:V0mFoGEwhLBXRhC1	mertens	mertensqw		0000-00-00 00:00:00	
7337	user733	\$P\$9vXdfCaI8MnNve7Nj8AJTQhyv/2P	user733	rpuser727@		0000-00-00 00:00:00	
8015	user2011	\$P\$9vXdfCaI8MnNve7Nj8AJTQhyv/2P	user2011	rpuser727@		0000-00-00 00:00:00	
7336	phonetics	\$P\$B0psAX86IKu7D6ngor04QBXAV05.w0	Kaylee Holm	TiffanyCoo		2015-01-16 09:33:09	
0972	jasmine	\$P\$BPVgc4gDMcf0A3Um5ctPWeUpqShjE0	jasmine	littlegu@j		0000-00-00 00:00:00	
1363	wpsetngsa	\$P\$BzFdth1Cp.pC06Spz/LB23kJXtbLFw/	wpsetngsa	wsreticox9		0000-00-00 00:00:00	
1368	wpsetnisms	\$P\$BrlUF5qdYg=EdJWuqCQ.ZdAHd7SPB	wpsetnisms	wsrivicoria		0000-00-00 00:00:00	
29791	CesareRaf	\$P\$BgjBuH0vz5xK3abXl4CrE9gYKcVM1	CesareRaf	cesareraf1		0000-00-00 00:00:00	
29792	CesareRaf2	\$P\$BgjBuH0vz5xK3abXl4CrE9gYKcVM1	CesareRaf2	cesareraf2		0000-00-00 00:00:00	

- **Realizar Copias de Seguridad**



- Debemos descargar todo lo que se encuentre dentro de la carpeta **public_html** de nuestro hosting o el directorio donde esté instalado el WordPress con problemas.
- La mejor manera es usando un cliente de FTP como **FileZilla**
- Antes de descargar los archivos con Filezilla debemos seleccionar la opción **Preservar información horaria de los archivos transferidos** que encontraremos en el menú **Transferencia**.

- **Copiar la Base de datos**

```
define('DB_NAME', '');  
/** MySQL database username */  
define('DB_USER', '');  
/** MySQL database password */  
define('DB_PASSWORD', '');
```

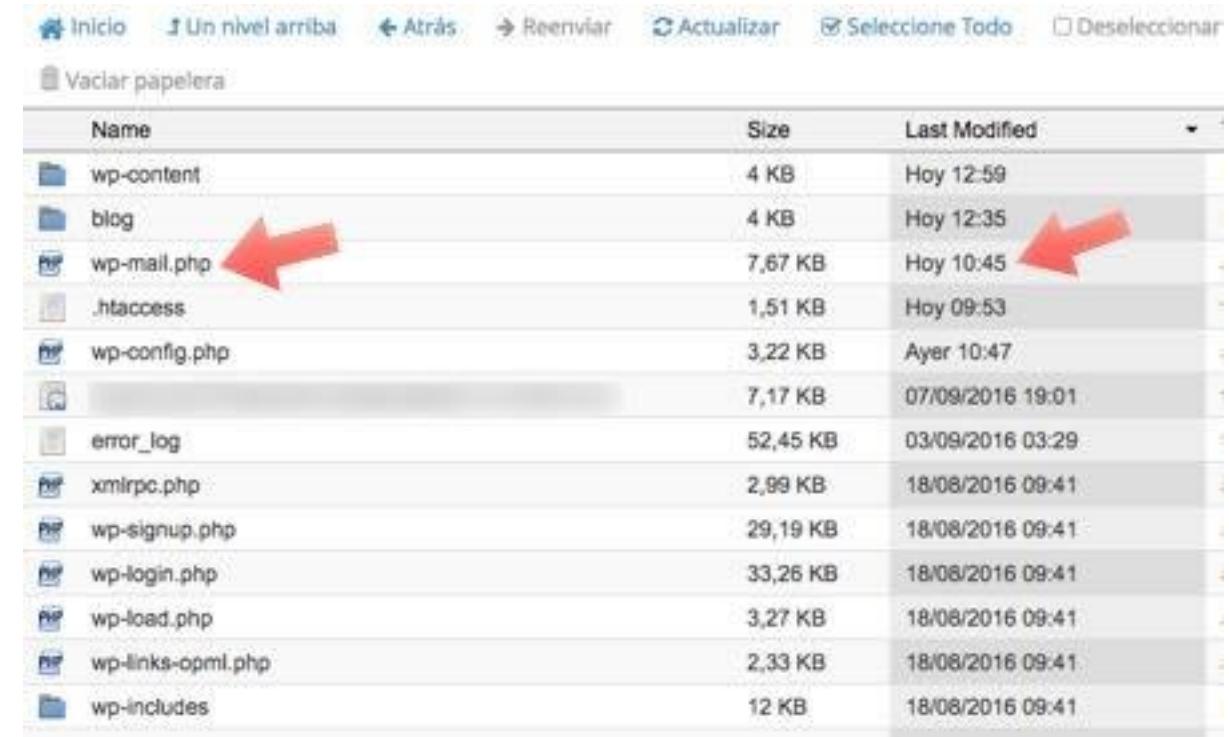


- **wp-config.php** de nuestro WordPress
- **Cambiar la Contraseña y Usuario de la BBDD**

Acciones

- Edita el archivo .htaccess y déjalo «como de fábrica»
- Verifica que los archivos index.php dentro de todas las carpetas no tengan un texto extraño y que los permisos estén en 644, los permisos incorrectos hacen que los archivos no puedan ser leídos, por tanto no se ejecutan los comando que hay en ellos
- Ingresa en la carpeta wp-content/plugins renombra todas las carpetas, con esto desactivarás los plugins que de seguro están infectados.
- Ingresa en la carpeta wp-content/theme y renombra la carpeta del tema que estás usando en el sitio web.

- **Borrar los Archivos WordPress**



Name	Size	Last Modified
wp-content	4 KB	Hoy 12:59
blog	4 KB	Hoy 12:35
wp-mail.php	7,67 KB	Hoy 10:45
.htaccess	1,51 KB	Hoy 09:53
wp-config.php	3,22 KB	Ayer 10:47
	7,17 KB	07/09/2016 19:01
error_log	52,45 KB	03/09/2016 03:29
xmlrpc.php	2,99 KB	18/08/2016 09:41
wp-signup.php	29,19 KB	18/08/2016 09:41
wp-login.php	33,26 KB	18/08/2016 09:41
wp-load.php	3,27 KB	18/08/2016 09:41
wp-links-opml.php	2,33 KB	18/08/2016 09:41
wp-includes	12 KB	18/08/2016 09:41

- Tenemos que sacar la lupa en el directorio **wp-content** que es el más habitual para añadir archivos o modificarlos.
- Por ejemplo: **wp-mail.php**,
- Cuando tengamos claro que ficheros tenemos que eliminar todo menos el **archivo .htaccess**.

• Revisar los Archivos

●	 index.php	25 sept 2013 0:18
	 licencia.txt	7 sept 2016 19:21
	 license.txt	7 sept 2016 19:18
	 readme.html	7 sept 2016 19:21
	 wp-activate.php	24 may 2016 21:02
►	 wp-admin	7 sept 2016 19:10
	 wp-blog-header.php	19 dic 2015 10:20
	 wp-comm...s-post.php	23 may 2016 16:44
	 wp-config-sample.php	7 sept 2016 19:21
►	 wp-content	7 sept 2016 19:21
	 wp-cron.php	24 may 2015 17:26
►	 wp-includes	7 sept 2016 19:21
	 wp-links-opml.php	23 may 2016 16:44
	 wp-load.php	14 abr 2016 17:53
	 wp-login.php	14 jun 2016 21:51
	 wp-mail.php	13 jul 2016 12:37
	 wp-settings.php	13 ago 2016 16:02
	 wp-signup.php	24 may 2016 20:44
	 wp-trackback.php	30 nov 2014 20:23
	 xmlrpc.php	6 jul 2016 12:40

```
1  <?php
2  /**
3   * Gets the email message from the user's mailbox to add as
4   * a WordPress post. Mailbox connection information must be
5   * configured under Settings > Writing
6   *
7   * @package WordPress
8   */
9  #Esto es una prueba para detectar archivos modificados en WordPress
10 /* Make sure that the WordPress bootstrap has run before continuing. */
11 require(dirname(__FILE__) . '/wp-load.php');
12
13 /** This filter is documented in wp-admin/options.php */
14 if ( ! apply_filters( 'enable_post_by_email_configuration', true ) )
15     wp_die(__( 'This action has been disabled by the administrator.' ) );
```

- Eliminar todos los archivos maliciosos que no se corresponden con un gestor de contenidos WordPress
- Para esta labor puedes apoyarte de la herramienta scan del plugin [Wordfence](#).
- Instalar el plugin TAC para determinar la no vulnerabilidad de los archivos del tema
- Este plugin te ayudará a detectar si tu tema de WordPress tiene código malicioso injectado en sus archivos.

Contramedidas

- Cambiar todas las contraseñas de acceso
- Una de las primeras líneas de trabajo es cambiar todas y cada una de las contraseñas de acceso a tu sitio.
- cuentas de FTP
- Las cuentas de usuario de WordPress
- El usuario de acceso a la base de datos
- El acceso al panel de control

- **Bloquear la Edición de Temas desde WordPress**

- **wp-config.php** y añadir el siguiente código:
- **#DESHABILITAR LA EDICIÓN DESDE EL ADMINISTRADOR DE WORDPRESS** `define('DISALLOW_FILE_EDIT', true);`

```
 81 /**
 82  * Sets up WordPress vars and included files. */
 83 require_once(ABSPATH . 'wp-settings.php');
 84
 85 //define('WP_CACHE', true); //Added by WP-Cache Manager
 86
 87 #DESHABILITAR LA EDICIÓN DESDE EL ADMINISTRADOR DE WORDPRESS
 88 define('DISALLOW_FILE_EDIT', true); 
 89
 90 ?>
 91
```

- **Evitar el Listado de Archivos**

-

- Sólo añadiendo una linea en nuestro **archivo .htaccess** podemos evitar que se listen los archivos del hosting para ponerle las cosas más difíciles a los atacantes.

-

```
1 Options -Indexes
2
3 # BEGIN WpFastestCache
4 <IfModule mod_rewrite.c>
5 RewriteEngine On
6 RewriteBase /
```



- **Bloquear el Acceso a Archivos Sensibles a IP's de Fuera de España**

```
<IfModule mod_geoip.c>
    GeoIPEnable On

    SetEnvIf Remote_Addr "^" Filtered=0
    SetEnvIf Request_URI "^/wp-admin" Filtered=1
    SetEnvIf Request_URI "^/wp-login" Filtered=1
    SetEnvIf Request_URI "^/xmlrpc.php" Filtered=1

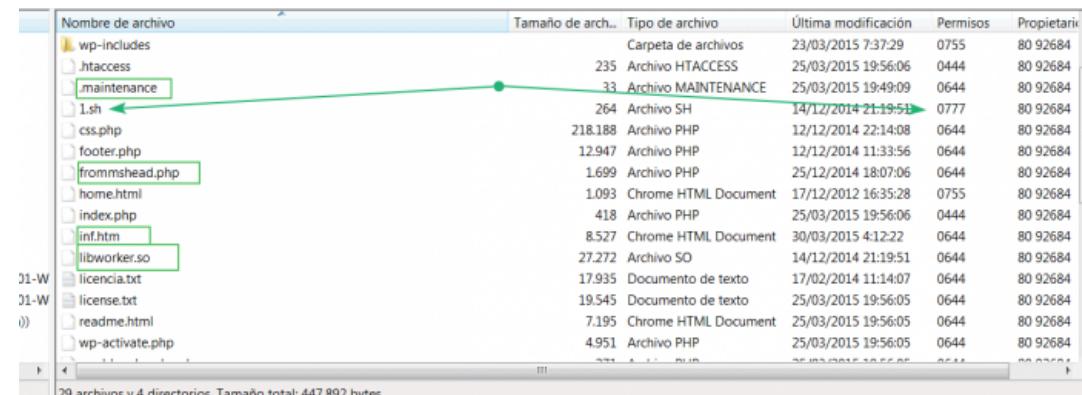
    SetEnvIf Remote_Addr "^" BlockCountry=1
    SetEnvIf GEOIP_COUNTRY_CODE ES BlockCountry=0

    SetEnvIfExpr    "%{ENV:Filtered} == '1' && %{ENV:BlockCountry} != 'ES'"

    Order Allow,deny
    Allow from all
    Deny from env=Block

</IfModule>
```

- **Revisar permisos en las carpetas mediante FTP**
- Conéctate a tu hosting empleando FTP (por ejemplo) y revisa los permisos que tengan las carpetas y los archivos.
- Es correcto encontrar permisos 755 para las carpetas y 644 para los archivos.
- Todo lo que sea distinto de 755 o 644 suele ser indicativo de que hay algo que no va bien. Si ves permisos 777, claramente hay algo que no está bien.



Nombre de archivo	Tamaño de archivo	Tipo de archivo	Última modificación	Permisos	Propietario
wp-includes		Carpetas de archivos	23/03/2015 7:37:29	0755	80 92684
htaccess		Archivo HTACCESS	25/03/2015 19:56:06	0444	80 92684
maintenance		Archivo MAINTENANCE	25/03/2015 19:49:09	0644	80 92684
1.sh		Archivo SH	14/12/2014 21:19:51	0777	80 92684
css.php		Archivo PHP	12/12/2014 22:14:08	0644	80 92684
footer.php		Archivo PHP	12/12/2014 11:33:56	0644	80 92684
frommshead.php		Archivo PHP	25/12/2014 18:07:06	0644	80 92684
home.html		Chrome HTML Document	17/12/2012 16:35:28	0755	80 92684
index.php		Archivo PHP	25/03/2015 19:56:06	0444	80 92684
inf.htm		Chrome HTML Document	30/03/2015 4:12:22	0644	80 92684
libworker.so		Archivo SO	14/12/2014 21:19:51	0644	80 92684
licencia.txt		Documento de texto	17/02/2014 11:14:07	0644	80 92684
license.txt		Documento de texto	25/03/2015 19:56:05	0644	80 92684
readme.html		Chrome HTML Document	25/03/2015 19:56:05	0644	80 92684
wp-activate.php		Archivo PHP	25/03/2015 19:56:05	0644	80 92684

- Instalar plugins de seguridad:
 - [Wordfence Security](#)
 - [iThemes Security](#)
- Instalar y configurar el archivo htaccess con las directivas [7G Firewall](#)
- Dejarte guiar por las recomendaciones y medidas de esta [guía práctica de seguridad para WordPress](#) titulada «Protege tu WordPress».

Ejemplo de incidente

- <https://incident.netcraft.com/f334823c2a7c/>