



VISIBILIDAD WEB UNAM

LA IMPORTANCIA DE LAS RESTRICCIONES DE ACCESO A DIRECTORIOS Y ARCHIVOS





MAYO 2020

Importancia de las restricciones de acceso a directorios

Un aspecto básico de seguridad que se debe de contemplar en la administración de un sitio web, es evitar que el servidor muestre el listado de los archivos contenidos en directorios públicos.



<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory			-
 license.txt	2019-01-02 02:07	19K	
 readme.html	2019-04-09 04:29	7.3K	
 wp-activate.php	2019-01-12 12:11	6.8K	
 wp-config-sample.php	2019-01-08 10:00	2.8K	
 wp-config.php	2017-12-07 17:00	3.1K	
 wp-content/	2012-01-08 22:31	-	
 wp-includes/	2019-05-21 23:54	-	
 xmlrpc.php	2018-08-17 07:21	3.0K	

Apache/2.4.18 (Ubuntu) Server at demo.tecadmin.net Port 80

Listado de archivos de un directorio no protegido

En la imagen se observa que en lugar de presentar una página web, se muestra el contenido del directorio, esto le permite al usuario el acceso del sitio para que descargue, visualice o ejecute los archivos o scripts de programación sin restricción alguna.

Además, también se muestra información sobre la plataforma tecnológica que se está utilizando, incluso la versión exacta del servidor (en este caso Apache 2.4.18) y, con ello, la posibilidad de aprovechar las vulnerabilidades específicas para esa versión.

Existen diversos mecanismos para evitar exponer el listado de archivos y directorios, así como información sensible sobre el servidor. A continuación se enlistan algunas de ellas:

1. Archivo *index.html*

Para algunos casos incluir un archivo *index.html* en cada directorio del sitio es suficiente para evitar que se muestre su contenido y solucionar el problema. Si no se trata de un sitio web con múltiples directorios y subdirectorios, podría ser una solución rápida.

Sin embargo, esto no siempre resulta ser una solución práctica o viable. Dependiendo del tamaño del sitio, se puede llegar a tener una cantidad muy grande de directorios que se tendrían que contemplar y sería un problema incluir un archivo para cada directorio y subdirectorio.

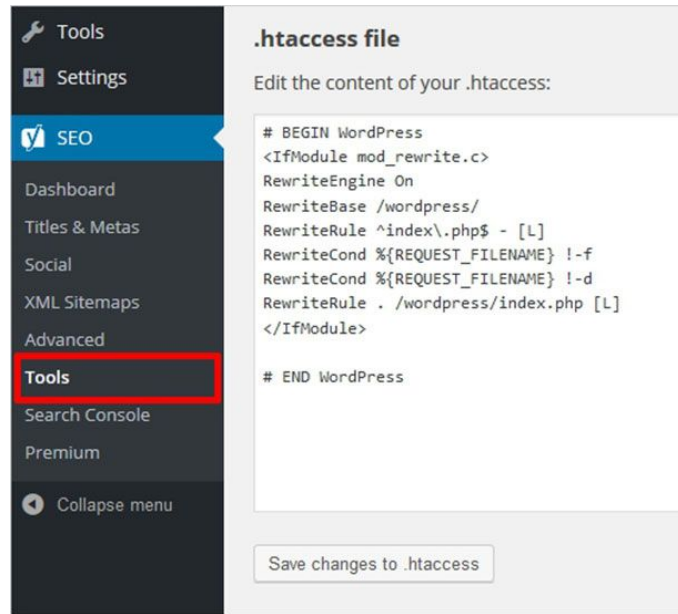
2. Archivo *.htaccess*

Una buena alternativa si se usa un servidor web *Apache*, es agregar una directiva que evite que se desplieguen los archivos de los directorios de publicación web. Esto se logra creando un archivo *.htaccess* en la raíz del sitio web o agregando, si ya se cuenta con uno, la siguiente directiva:

Options -Indexes

De esta forma se evita mostrar el listado en cualquier directorio del sitio.

Si se está utilizando un administrador de contenidos como *Drupal* o *Wordpress*, por lo regular no hay que preocuparse de esta situación, ya que éstos contemplan cuestiones básicas de seguridad. En todo caso, bastaría con incluir la directiva arriba mencionada al final del archivo *.htaccess*, como ya se mencionó.



Configuración típica del archivo .htaccess de wordpress

3. Archivo de configuración de Apache

También se puede modificar el archivo de configuración del servidor web Apache (*httpd.conf*).

Hay que localizar la línea:

The option directive is both complicated and important. Please see

<http://httpd.apache.org/docs/2.2/mode/core.html#options>

for more information.

#

Option Indexes FollowSymLinks

Y sustituirla por:

Option -Indexes FollowSymLinks

Créditos

Coordinación del proyecto

Dra. Marcela Peñaloza Báez

Directora de Colaboración y Vinculación

MATIE. Juan Manuel Castillejos Reyes

Subdirector de Visibilidad Web

L.C. Irene G. Sánchez García

Enlace Institucional de Iniciativas de Visibilidad

Equipo de trabajo

Ing. Mario Alberto Arredondo Guzmán

Autor del documento

L.C. Irene G. Sánchez García

MATIE. Juan Manuel Castillejos Reyes

Revisores del documento