5 Security Codes to Protect Your WordPress files from Hackers

by Amberd Design Studio

3. Protecting .htaccess file itself

We have been adding security codes to the *.htaccess* file and it is a no-brainer that we have to protect this file too in case hackers access this file and remove all the security configurations we have just added.

Put the following code in your .htaccess file to secure it.

```
# Securing .htaccess file

<files ~ "^.*\.([Hh][Tt][Aa])">
order allow,deny
deny from all
satisfy all
</files>
```

4. Disabling directory browsing

Directory browsing can be very dangerous, hackers can get access to it and find files that are less secure and use those files to get access to your site. We have to disable the directory browsing in WordPress to make sure all your files are secure.

All you need to do is put this very small code in your *.htaccess* file.

```
#Disable directory browsing

Options -Indexes
```

AMBERD

1. Protect your wp-includes folder

Put this code in your website's *.htaccess* file, this code blocks web access to your wp-includes folder which is a very common target for hackers.

```
# Blocking web access to the wp-includes folder

<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^wp-admin/includes/ - [F,L]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/[^/]+\.php$ - [F,L]
RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F,L]
RewriteRule ^wp-includes/theme-compat/ - [F,L]
</IfModule>
```

2. Protect wp-config.php file

wp-config.php file is another critical file that needs to be protected. This file holds your website's username, password and database information, protecting this file should be a high priority.

Put the below code in your website's .htaccess file.

```
# Blocking web access to the wp-config.php file

<files wp-config.php>
order allow,deny
deny from all
</files>
```

5. Remove the default file editor

WordPress comes with a default file editor in its dashboard, which can be very dangerous. If someone gets access to your website they have full control over your files and they can damage your entire website.

It is very important to disable this file editor and access your site over FTP if you need to.

All you have to do is open your *wp-config.php* file and copy-paste the below code right before the text *"That's all, stop editing! Happy blogging."*

```
#Disable WP file editor

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

Using these 5 security patches on your website will make your WordPress site very secure and will keep the hackers away!

Bonus Security Tips:

3 Easy Ways to Protect Your WordPress Installation Files

How to Protect your Configuration File From Hackers

Introduction to SSL Certificates. What Is an SSL Certificate?