

How To Increase Security On Your WordPress Site

1. Restrict Access (.htaccess)

- a. Installing a plugin to help rate limit login attempts is a step in the right direction.
- b. However a .htaccess file limiting directory/file access is likely one of the best.

An example snippet of code is shown here:

```
<FilesMatch wp-login.php>
Order Allow,Deny
Allow from xx.xx.xx.xx
Deny from all
</FilesMatch>
```

2. Do not look like a “new” Wordpress installation

- a. Remove default posts, etc.
- b. Remove Version information in default files. This is done in two places:
 - i. The first is the meta generator tag in your template.
That is found in wp-content/{name of your WordPress theme}/header.php.
 - ii. The other element is in your RSS feed. Open up wp-includes/general-template.php and look around line 1858. Find:

```
function the_generator( $type ) {
    echo apply_filters('the_generator', get_the_generator($type), $type) . "\n";
}
```
 - iii. Make sure a hash is applied next to the “echo” command so that it looks like this:

```
function the_generator( $type ) {
    #echo apply_filters('the_generator', get_the_generator($type), $type) . "\n";
}
```
- c. Remove “Powered by Wordpress” footers.
- d. Remove install or upgrade files
 - i. Be sure to delete /wp-admin/install.php and /wp-admin/upgrade.php after every WordPress installation or upgrade!
You don't need them for day to day WordPress functionality.
- e. Change some of the miscellaneous default settings
 - i. Go to Settings > Miscellaneous in your admin console and change the names of wp-content/directory and wp-comments-post.php.
 - ii. Make sure to change the template URL within the template and wp-comments-post.php accordingly, to maintain the function of your site.

3. Disable custom HTML when possible

- a. If it's not necessary for the form and function of your site, disable it. You can add the following to your wp-config.php file:

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

4. Hide Indexes or limit access

- a. In a .htaccess file, add:

```
Options -Indexes
```
- b. Make sure PHP source code is never revealed:
 - i. Your site's wp-includes/ directory is the most important one to block. Find the .htaccess file there and insert:

```
RewriteRule ^(wp-includes)V.*$ ./[NC,R=301,L]
```
 - ii. If there are or will be subdirectories of wp-includes/, insert the following code for each one in the same .htaccess configuration file:

```
RewriteRule ^(wp-includes)subdirectory-name-here)V.*$ ./[NC,R=301,L]
```

More Information:

http://codex.wordpress.org/FAQ_Security

http://codex.wordpress.org/Hardening_WordPress

<http://wordpress.org/extend/plugins/limit-login-attempts/>

Related articles

Content by label

There is no content with the specified labels

