SECURITY HARDENING

A technical document describing security measures to enhance security on WordPress websites

Produced by Alex Whyatt

27 November 2013

This document explains at a technical level how to carry out the 9 recommended steps for hardening WordPress. If further explanation on the motivation or reasoning behind a change is required, please get in touch (email link on front page).

Each of the changes is independent, with the possible exception of backup. It is **highly recommended** to take a backup of the site before attempting any changes, **especially #5 and #7.** No responsibility can be taken for loss resulting from implementing any of these changes.

This document covers the following 9 security hardening steps:

1. Admin username
2. Password strength
3. robots.txt
4. File and folder permission
5. WordPress database table prefix
6. Login attempt limiter
7. Importance of updates
8. Backup planning
9. Version hiding

1. Admin Username

The admin username cannot be renamed. Rather a new username with administration permission must be created, ideally with a special character e.g. @dmin or admin!. Only when there is a new administrative user I place, can the admin user be deleted.

2. Password

Passwords should be at least 8 characters long and contain (at least) a capital letter, a number and a special character such as #, $, % or @. Use the website www.howsecureismypassword.net to get a sense of the crack-ability of your password. Ideally your password result should 100s of days or even years to crack.

Compare the password john@1234 with John@1234 – just the capitalization of the 'J' has a huge effect!

3. Disable search bots

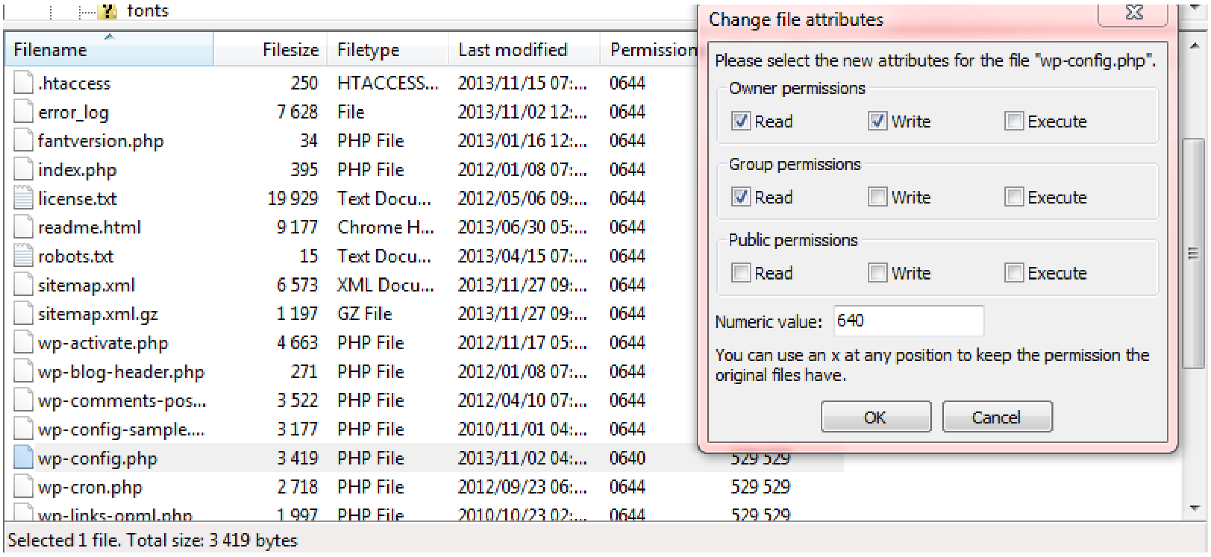
When search engines catalogue and index the site, it's possible that they can publish details of system files. This is not desirable, so we indicate a preference for these folders not to be scanned by adding the following line to a file called **robots.txt** in the website root.

```
Disallow: /wp-*
```

4. Check folder permissions

WordPress folders can be another area where hacking and other attacks can occur. This step involves checking and if necessary changing the permission of folders and files to a level that allows WordPress to continue to function correctly, but prevents the internet gaining unwanted control. The desired permission for all folders is 755, while for files is it 644. The exception is the wp-config.php file which is particularly sensitive, and is set to 640.

In the screen shot on the next page, you can see the permission shown, when using a simple FTP program such as FileZilla. Right-clicking will allow you select a “File Permission” option which opens the dialog box visible. The change can be made in this dialog, and then saved.



fonts

Filename	Filesize	Filetype	Last modified	Permission	
.htaccess	250	HTACCESS...	2013/11/15 07:...	0644	
error_log	7 628	File	2013/11/02 12:...	0644	
fantversion.php	34	PHP File	2013/01/16 12:...	0644	
index.php	395	PHP File	2012/01/08 07:...	0644	
license.txt	19 929	Text Docu...	2012/05/06 09:...	0644	
readme.html	9 177	Chrome H...	2013/06/30 05:...	0644	
robots.txt	15	Text Docu...	2013/04/15 07:...	0644	
sitemap.xml	6 573	XML Docu...	2013/11/27 09:...	0644	
sitemap.xml.gz	1 197	GZ File	2013/11/27 09:...	0644	
wp-activate.php	4 663	PHP File	2012/11/17 05:...	0644	
wp-blog-header.php	271	PHP File	2012/01/08 07:...	0644	
wp-comments-pos...	3 522	PHP File	2012/04/10 07:...	0644	
wp-config-sample....	3 177	PHP File	2010/11/01 04:...	0644	
wp-config.php	3 419	PHP File	2013/11/02 04:...	0640	529 529
wp-cron.php	2 718	PHP File	2012/09/23 06:...	0644	529 529
wp-links-opml.php	1 997	PHP File	2010/10/23 02:...	0644	529 529

Selected 1 file. Total size: 3 419 bytes

Change file attributes

Please select the new attributes for the file "wp-config.php".

Owner permissions

☑ Read ☑ Write □ Execute

Group permissions

☑ Read □ Write □ Execute

Public permissions

□ Read □ Write □ Execute

Numeric value: 640

You can use an x at any position to keep the permission the original files have.

Figure 1 File Permission edited in FTP program

Turn off directory browsing

When you browse to one of the WordPress sub-folders it is possible to see the contents of that folder. This can allow hackers to see weaknesses or opportunities to attack the site (for example evidence of a weak plugin). This change prevents the contents of a folder being listed. The change is to the .htaccess file in the root of the website, and the following line is added:

Options All –Indexes

5. **Change table prefix**

The tables in the WordPress database start with the prefix wp_. Would-be hackers know this and can configure attacks using this prefix, accessing WordPress database tables.

Note that carrying out these steps may make the website unavailable – so it should be attempted hen traqffic is lowest. Also, make a backup of the site before attempting in case something goes wrong!

Follow these steps to implement:

Wp-config.php edit

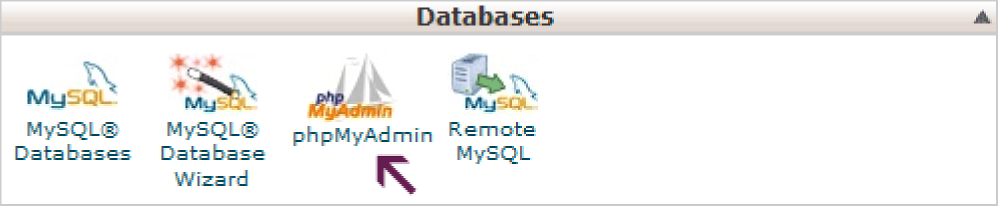
Open your wp-config.php file which is located in your WordPress root directory. Change the table prefix line from **wp_** to something else like this **wp_a123456_**

So the line would look like this:

$table_prefix = ‘’wp_123_’;

Change all Database Tables Name

You need to access your database (most likely through phpMyAdmin), and then change the table names to the one we specified in wp-config.php file. If you are using the cPanel WordPress hosting, then you can find the phpMyAdmin link in your cPanel. Look at the image below:



There are a total of 11 default WordPress tables:

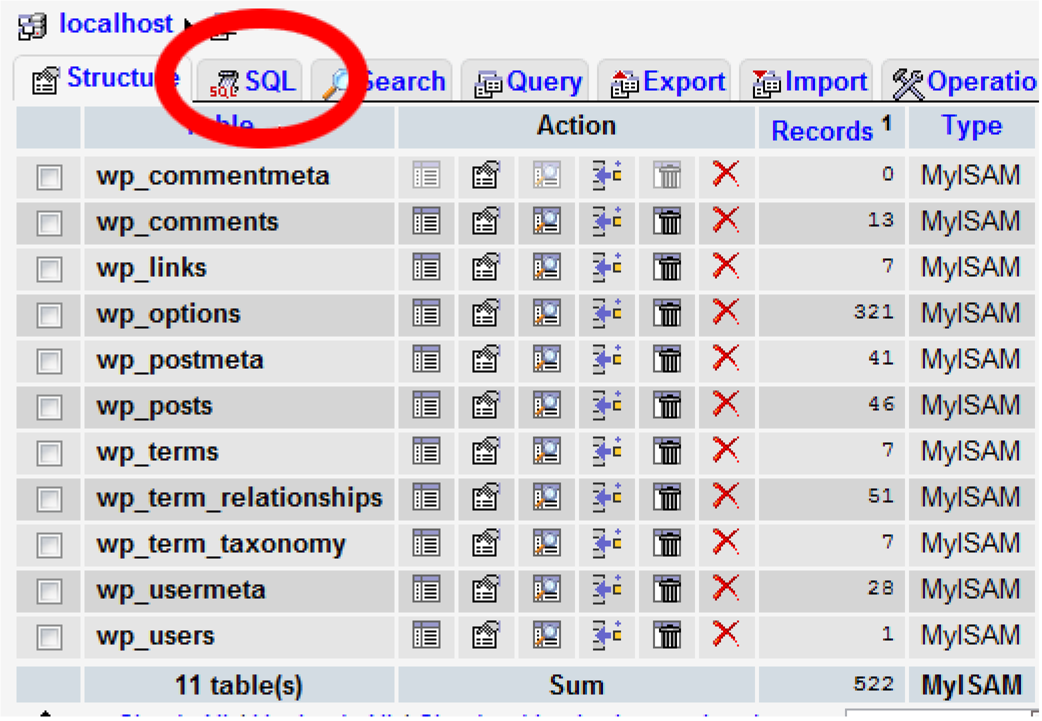


	Table	Action	Records 1	Type
□	wp_commentmeta		0	MyISAM
□	wp_comments		13	MyISAM
□	wp_links		7	MyISAM
□	wp_options		321	MyISAM
□	wp_postmeta		41	MyISAM
□	wp_posts		46	MyISAM
□	wp_terms		7	MyISAM
□	wp_term_relationships		51	MyISAM
□	wp_term_taxonomy		7	MyISAM
□	wp_usermeta		28	MyISAM
□	wp_users		1	MyISAM
	11 table(s)	Sum	522	MyISAM

Each table prefix must be changes, and this SQL code below will accomplish this:

```
RENAME table `wp_commentmeta` TO `wp_123_commentmeta`;
RENAME table `wp_comments` TO `wp_123_comments`;
RENAME table `wp_links` TO `wp_123_links`;
RENAME table `wp_options` TO `wp_123_options`;
RENAME table `wp_postmeta` TO `wp_123_postmeta`;
RENAME table `wp_posts` TO `wp_123_posts`;
RENAME table `wp_terms` TO `wp_123_terms`;
RENAME table `wp_term_relationships` TO `wp_123_term_relationships`;
RENAME table `wp_term_taxonomy` TO `wp_123_term_taxonomy`;
RENAME table `wp_usermeta` TO `wp_123_usermeta`;
RENAME table `wp_users` TO `wp_123_users`;
```

You may have to add lines for other plugins that may add their own tables in the WordPress database. The idea is that you change all tables prefix to the one that you want.

The Options Table

We need to search the options table for any other fields that is using wp_ as a prefix, so we can replace them. To ease up the process, use this query:

```
SELECT * FROM `wp_a123456_options` WHERE `option_name` LIKE'%wp_%'
```

This will return a lot of results, and you need to go one by one to change these lines.

UserMeta Table

Next, we need to search the usermeta for all fields that is using wp_ as a prefix, so we can replace it. Use this SQL query for that:

```
SELECT * FROM `wp_a123456_usermeta` WHERE `meta_key` LIKE'%wp_%'
```

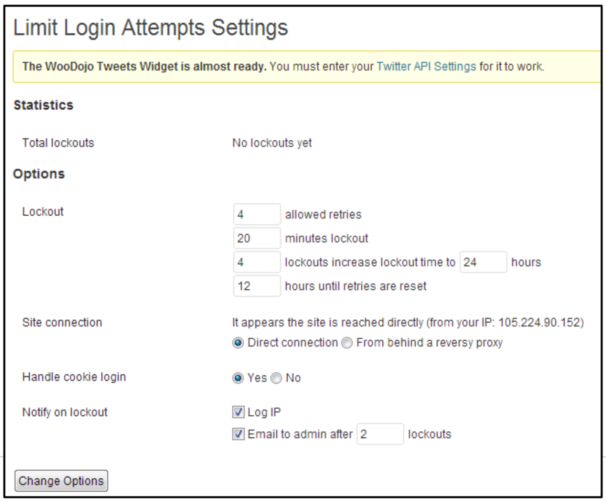
Number of entries may vary on how many plugins you are using and such. Just change everything that has wp_ to the new prefix.

You are now ready to test the site. If you followed the above steps, then everything should be working fine.

6. Install Limit Logins

By default WordPress allows an unlimited number of login attempts. This means that hackers and their automated password cracking robots have no restrictions on the number of passwords they can try while trying to crack your site. Using the Limit Logins plugs we set a cap on the number of failed attempts, and enforce a waiting period before further attempts are permitted.

In the plugin menu, search for the Limit Login plugin, and install. Below is a recommended configuration.



Limit Login Attempts Settings

The WooDojo Tweets Widget is almost ready. You must enter your Twitter API Settings for it to work.

Statistics

Total lockouts: No lockouts yet

Options

Lockout:
4 allowed retries
20 minutes lockout
4 lockouts increase lockout time to 24 hours
12 hours until retries are reset

Site connection: It appears the site is reached directly (from your IP: 105.224.90.152)
● Direct connection ○ From behind a reversy proxy

Handle cookie login: ● Yes ○ No

Notify on lockout:
☑ Log IP
☑ Email to admin after 2 lockouts

Figure 2 Limit Login suggested setup

I took a quick look at WordFence, and it does appear to have a function to block brute force attacks. I am not sure how configurable it is. If you choose to use Limit Logins, then it would be advisable to disable that feature on WordFence so the two mechanisms are not in competition.

7. **Importance of updates**

There is nothing extra or special I can recommend in connection with updates. Their importance stems from the security holes they fix based on user community involvement. Very important prior to carrying out the upgrade is to take a backup of the site.

8. **Version Hiding**

Hiding the WordPress version can help with security as it means would-be hackers don't know you version, and cannot take advantage of any known weaknesses inherent with that version. The same goes for the version of themes and plugins. In the theme's functions.php file add the following:

```
// remove version info from head and feeds

function complete_version_removal() {

   return '';

}

add_filter('the_generator', 'complete_version_removal');
```

9. **Backup Strategy**

Backup Strategy can be determined by your perception of risk, as well as the frequency and volume of updates to the sites. If you are updating daily with lots of content, then a daily backup would minimise the risk of loss of data should the site crash or be hacked.

A backup plugin I have used and recommend would be BackUpWordPress. Using this simple plug in you can setup either content-only backups daily or weekly, or full database backup. The resulting backup file can be saved on the server, or (assuming it's not too large) can be emailed out.