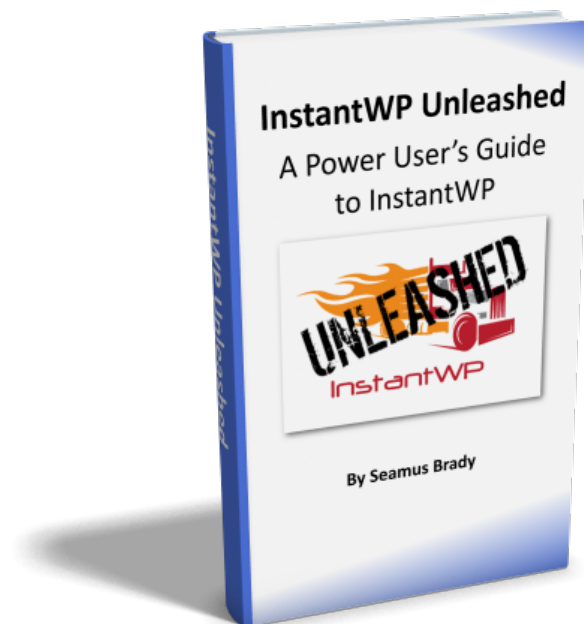


Welcome to your free chapter of InstantWP Unleashed

Don't forget you can get your own copy of InstantWP
Unleashed below:

<https://instantwp.com/unleashed/>



InstantWP Unleashed

A Power User's Guide to InstantWP



<http://www.instantwp.com>

email: support@instantwp.com

Copyright, Legal Notice and Disclaimer

This publication is protected under the Irish Copyright and Related Rights Act of 2000 and all other applicable international, state and local laws, and all rights are reserved, including resale rights: you are not allowed to give or sell this ebook to anyone else without permission.

Please note that much of this publication is based on personal experience and anecdotal evidence. Although the author and publisher have made every reasonable attempt to achieve complete accuracy of the content in this ebook, they assume no responsibility for errors or omissions. Also, you should use this information as you see fit, and at your own risk.

The author or publisher of this ebook may have a marketing connection to any brand, topic or product mentioned in this ebook. Through the use of affiliate links contained in this ebook the author or publisher may collect fees from purchases made.

Any trademarks, service marks, product names or named features are assumed to be the property of their respective owners, and are used only for reference. There is no implied endorsement if we use one of these terms.

Nothing in this ebook is intended to replace common sense, legal, medical or other professional advice, and is meant to inform and entertain the reader.

Copyright © 2019 Webtools LLC

Table of Contents

1. Tools and Tips for a WordPress Professional	7
1.1. Overview.....	7
1.2. Basic Tools.....	7
1.3. Portable Tools	9
1.4. Get a Dropbox Account.....	10
1.5. Useful Documentation.....	11
1.6. Tips on Designing and Developing within InstantWP	11
1.7. The Importance of WordPress Backups.....	13
1.8. Advanced Server Config with InstantWP	14
1.9. Summary.....	14
2. How To Use InstantWP Like A Power User	15
2.1. Overview.....	15
2.2. Typical InstantWP Setups.....	16
2.3. Basic WordPress Development.....	17
2.4. Site Testing.....	18
2.5. Rolling Out Multiple WordPress Websites	19
2.6. Soliciting Client Feedback	20
2.7. Exhibitions and Presentations	21
2.8. Client Sandbox Training	22
2.9. Courses and Coaching.....	23
2.10. Summary.....	24
3. How to Create an InstantWP Duplicate of an Existing WordPress Website	25
3.1. Overview.....	26
3.2. Step by Step Guide	27
3.3. Summary.....	44
4. How to move an InstantWP installation onto the Web.....	45
4.1. Overview.....	46
4.2. Step by Step Guide	47
4.3. Summary.....	71
5. How to Secure an InstantWP Installation after Moving it onto the Web	72
5.1. Overview.....	72
5.2. Note on Installing Plugins	73
5.3. Step by Step Guide	75
5.4. Summary.....	87
6. Troubleshooting Your InstantWP Migrations.....	88
6.1. Troubleshooting the Duplicator Plugin	88
6.2. An Alternative Way To Do WordPress Migrations.....	89
6.3. Housekeeping	103
6.4. Summary.....	104
7. Conclusion	105

We hope that InstantWP brings you the same freedom and creativity in your work with WordPress.

Regards

Webtools LLC

Foreword

This ebook is broken into the following six sections:

- Tools and Tips for a WordPress Professional.
- How To Use InstantWP Like A Power User.
- How to create an InstantWP duplicate of an existing WordPress Website.
- How to move an InstantWP installation onto the Web.
- How to Secure an InstantWP installation after moving it onto the Web.
- Troubleshooting Your InstantWP Migrations.

The first two chapters deal with background and setup and the rest of the chapters deal in detail with step by step guides to each topic.

5. How to Secure an InstantWP Installation after Moving it onto the Web

5.1. Overview

InstantWP is great for running a WordPress website on your local computer but it is inherently insecure. Any website based on InstantWP needs to be hardened and secured once it is moved onto the web. This chapter outlines a few housekeeping tasks you should carry out to secure and optimise your WordPress installation once you have transferred your InstantWP installation onto your web server. This will set a good basic level of security for any website.

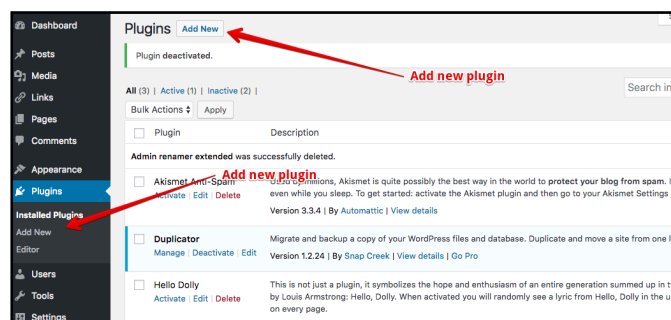
Most of the tips here involve installing and configuring simple WordPress plugins. There are many more sophisticated security plugins that do multiple security tasks. You should take a look at some of these [security plugins available for WordPress](#) after reading this chapter, just to see what is available.

Please note that some of the changes suggested below can sometimes go wrong. You may lose Internet access halfway through a step, for instance. Your WordPress installation could get broken. Always have a backup! If you are following this ebook, then you still have the Duplicator package as a backup. But in other situations, make a backup before making these changes.

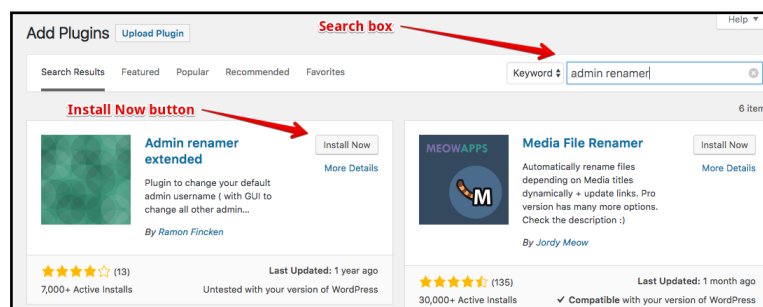
5.2. Note on Installing Plugins

Installing plugins in WordPress is easy, as you have seen from installing the Duplicator plugin. The steps for installing all the plugins in this section are the same, so rather than repeat them, here is a simple overview of WordPress plugin installation.

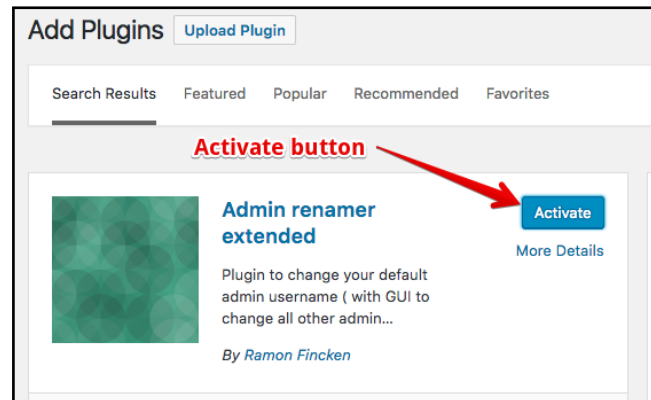
- You must go to the **Plugins→Add New** menu or the **Add New** button at the top of the Plugins page.



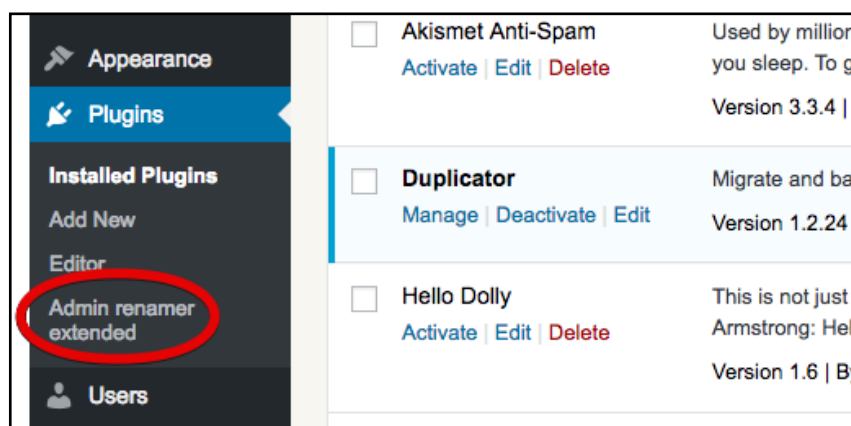
- Type the plugin name into the search box on the top right of the page.
- The Search Results screen will be shown - select the plugin you want to install by clicking the **Install Now** button.



- The plugin will be downloaded from the WordPress website and once it has finished installing you can click the **Activate** button to turn on the plugin.



- If the plugin has any adjustable settings, they are normally available from within the **Settings** or **Plugin** menu (though occasionally some plugins use the **Tools** menu too or a link from the **Plugins** page. See the specific plugin documentation for details).

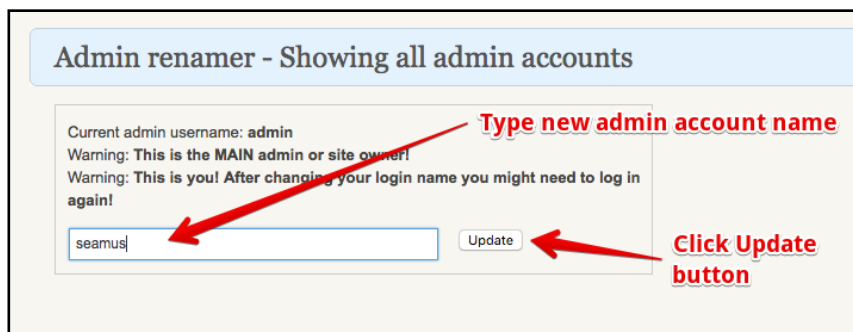


5.3. Step by Step Guide

Step 1 - Change Administrator Account Name.

Leaving 'admin' as the username for the administrator account can be a security risk. You can now change this to something different using the **Admin Renamer Extended** plugin.

Once you have installed and activated this plugin the standard way, click on the the **Admin Renamer Extended** link menu item on the **Plugins** menu. The plugin will then show all administrator accounts - there should generally only be one listing for your WordPress installation.



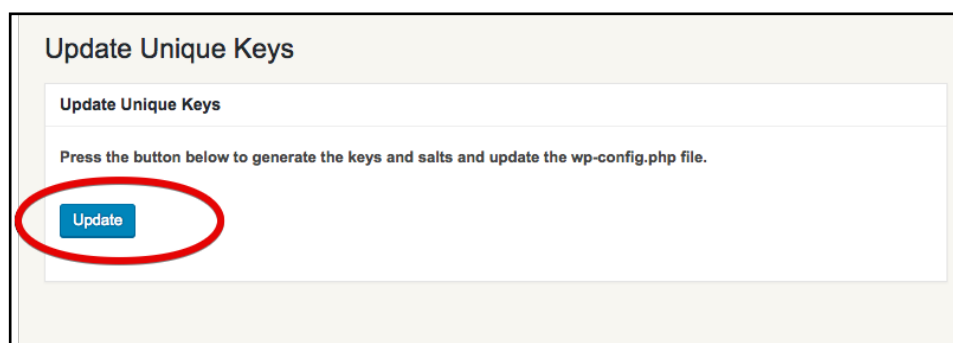
The screenshot shows the 'Admin renamer - Showing all admin accounts' interface. It displays the current admin username as 'admin' and includes two warnings: 'Warning: This is the MAIN admin or site owner!' and 'Warning: This is you! After changing your login name you might need to log in again!'. A text input field contains the new username 'seamus'. A red arrow points from the text 'Type new admin account name' to this input field. To the right of the input field is an 'Update' button, with a red arrow pointing from the text 'Click Update button' to it.

- Type in a new name for the administrator account (I have chosen 'seamus' as shown above).
- Click the Update button.
- You should log out and log back in with this new administrator account (the password will still be the same).

Step 2 - Update Unique Keys in your wp-config.php file.

The **Update Unique Keys** plugin makes your site harder to hack by adding random elements to password encryption. These secret keys are stored in the WordPress settings file wp-config.php. This is an older plugin but it still works very well.

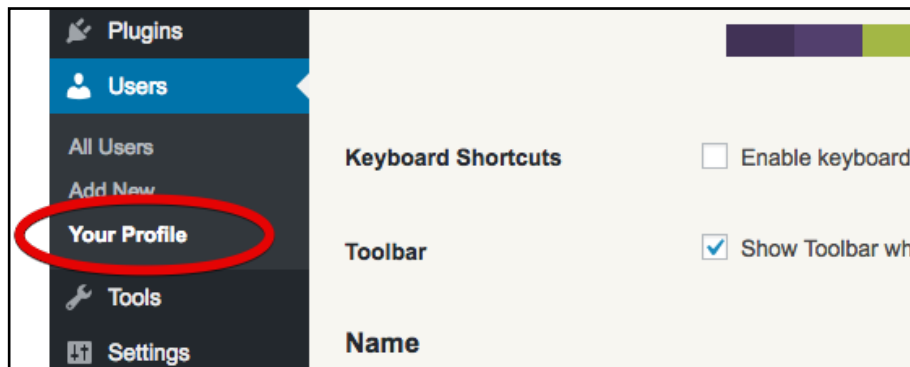
You can begin by installing the **Update Unique Keys** plugin in the standard way. The settings page for the plugin is available on the Settings menu. You just have to click on the Update button.



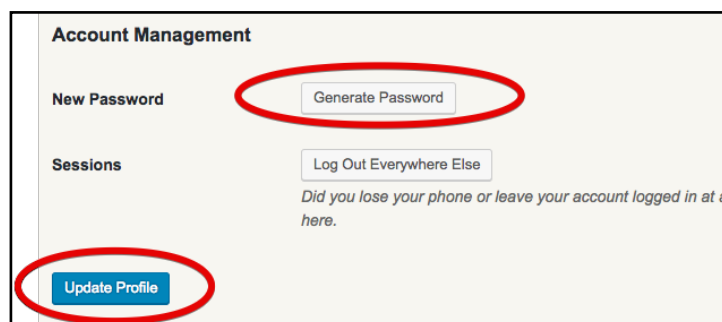
This plugin will automatically set and update the WordPress hosted Unique Key generator by adding new random values in the wp-config.php file. You must log out and log back in after this update.

Step 3 - Change Administrator Account Password.

You should now change the administrator account password to something more secure. Go to your profile by using the **Users→Your Profile** menu.



You can update your password at the base of this screen by clicking on the **Generate Password** button. WordPress will suggest a new password, you can use this or add your own.

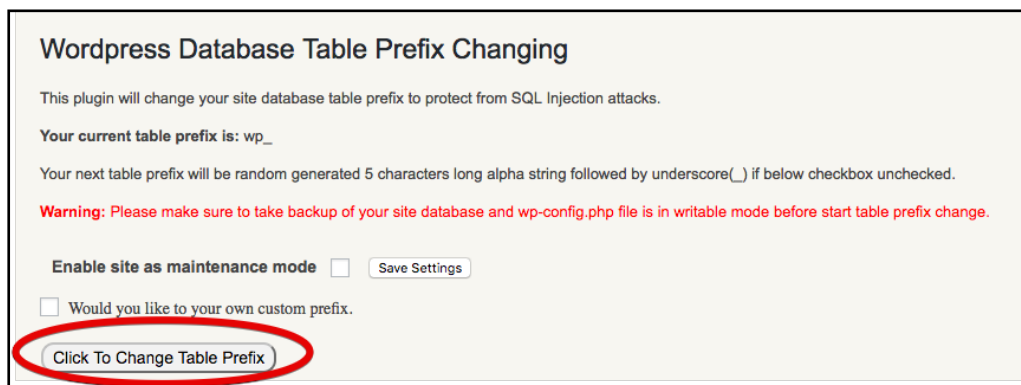


Click on the **Update Profile** button to save. You should memorise or make a copy of the password before this of course! You should also log out and log back in with this new password before continuing.

Step 4 - Change WordPress Database Prefix in your WordPress database.

In some installations of WordPress, all the tables in the WordPress database have the prefix 'wp' in the table name. This is a security risk as it allows hackers to guess the names of the tables in your site more easily.

You can rename the default WordPress tables in the database from having the prefix 'wp' by using the **Change Table Prefix** plugin. Simply install the plugin in the standard way and go to the **Settings-->Click to Change Table Prefix** menu item.



Wordpress Database Table Prefix Changing

This plugin will change your site database table prefix to protect from SQL Injection attacks.

Your current table prefix is: wp_

Your next table prefix will be random generated 5 characters long alpha string followed by underscore(_) if below checkbox unchecked.

Warning: Please make sure to take backup of your site database and wp-config.php file is in writable mode before start table prefix change.

Enable site as maintenance mode ☐

☐ Would you like to your own custom prefix.

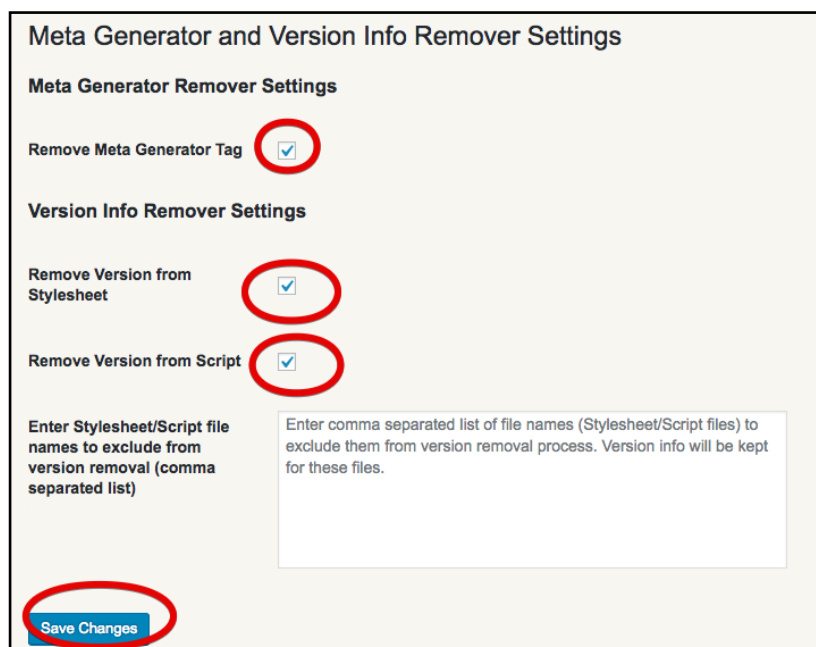
On the resulting page just click on the **Change Database Table Prefix** button. This will fix the database prefix issue.

Step 5 - Prevent the WordPress version from being displayed.

The version of WordPress in your installation gets appended to various style and script web addresses automatically. This can be a security risk as it allows hackers to identify what attacks might penetrate the specific version of WordPress you are running. In order to stop this, you should install the **Meta Generator and Version Info Remover** plugin.

Once installed, you can access the plugin settings via the **Settings-->Meta Generator and Version Info Remover Settings** menu item.

You can then make sure that the **Remove Meta Generator Tag**, **Remove Version from Stylesheet** and **Remove Version from Script** checkboxes are ticked (this should be done by default).



Meta Generator and Version Info Remover Settings

Meta Generator Remover Settings

Remove Meta Generator Tag ☒

Version Info Remover Settings

Remove Version from Stylesheet ☒

Remove Version from Script ☒

Enter Stylesheet/Script file names to exclude from version removal (comma separated list)

Enter comma separated list of file names (Stylesheet/Script files) to exclude them from version removal process. Version info will be kept for these files.

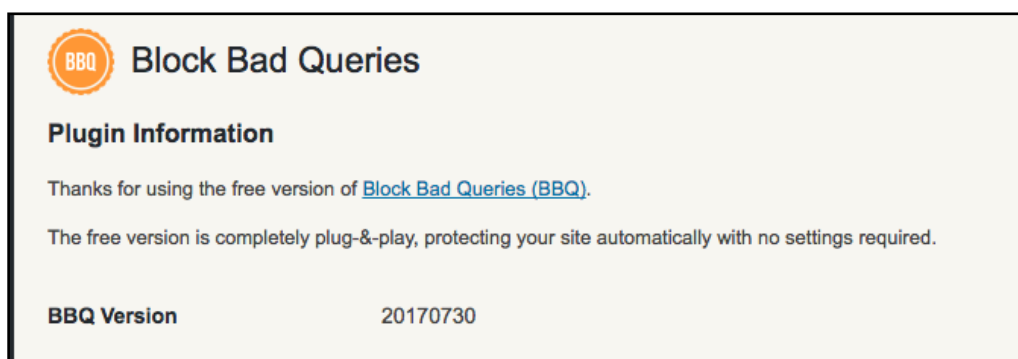
Save Changes

Just click on the **Save Changes** button afterwards.

Step 6 - Stop SQL Injection and Bad Query Attacks.

SQL injection is a hacking technique that exploits security vulnerabilities occurring in the database layer of a web site. Bad queries are specially formulated malicious URL requests that can open security holes in a web application. Both are bad news and both should be stopped.

Install the **BBQ: Block Bad Queries** plugin to identify and stop the most obvious hacking attempts against WordPress. This plugin is very simple and needs no manual adjustment, it just works.

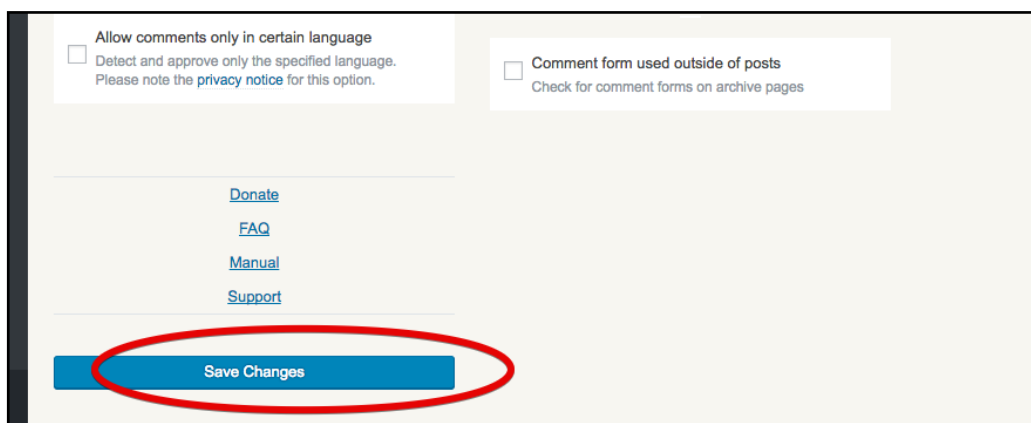


Once installed and activated, there is nothing further to do.

Step 7 - Stop Comment Spam.

Comment spam is endemic on the Internet. You should install a plugin to filter the spam comments from the real comments.

Antispam Bee is a free WordPress antispam plugin that comes highly recommended. Once installed and activated, you can find the Antispam Bee plugin menu under the **Settings** menu. The default options are a pretty good start but you can customise them if you wish.



Simply click on the **Save Changes** button here to stop comment spam.

Step 8 - Disable the WordPress File Editor.

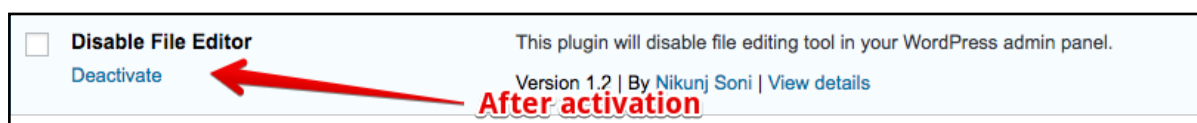
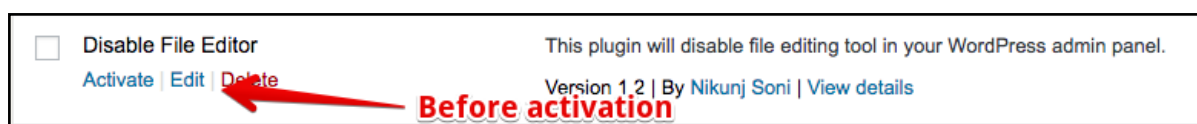
WordPress comes with a built-in file editor that is quite useful for local development (for instance when using InstantWP) but it can be exploited by hackers. This tool is accessed via the **Edit** menu item under each plugin on the plugins page for instance.

It is recommended that you disable file editing within the WordPress dashboard. You can do this in two ways:

- WordPress has a constant that disabled this editing via the wp-config.php file. Append the following two lines to the end of your wp-config file:

```
## Disable Editing in Dashboard  
define('DISALLOW_FILE_EDIT', true);
```

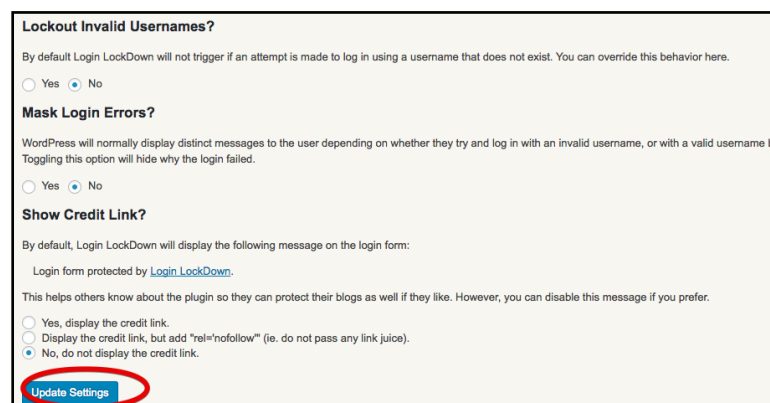
- Or the easier option - just install the Disable File Editor plugin and activate it. You will see that the **Edit** menu item disappears.



Step 9 - Limit Login attempts.

Your WordPress installation allows users to attempt login as many times as they want. This can lead to hackers trying different usernames and password combinations until they get one that works. This is called a brute force attack.

The simplest way to stop this is to limit the amount of times a user can login in a specified time period. You can install the **Login Lockdown** plugin to take care of this for you.



Lockout Invalid Usernames?

By default Login LockDown will not trigger if an attempt is made to log in using a username that does not exist. You can override this behavior here.

☐ Yes ☒ No

Mask Login Errors?

WordPress will normally display distinct messages to the user depending on whether they try and log in with an invalid username, or with a valid username but a wrong password. Toggling this option will hide why the login failed.

☐ Yes ☒ No

Show Credit Link?

By default, Login LockDown will display the following message on the login form:

Login form protected by [Login LockDown](#).

This helps others know about the plugin so they can protect their blogs as well if they like. However, you can disable this message if you prefer.

☐ Yes, display the credit link.
☐ Display the credit link, but add "rel=nofollow" (ie. do not pass any link juice).
☒ No, do not display the credit link.

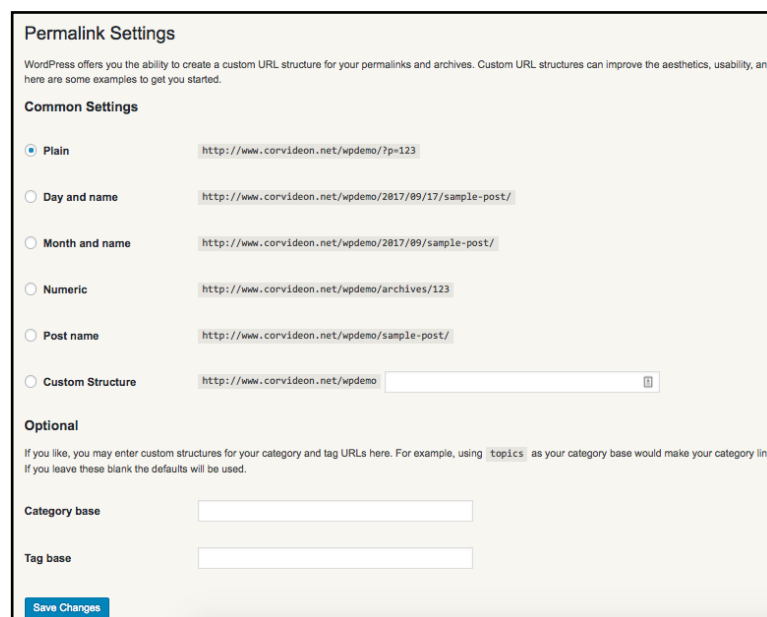
[Update Settings](#)

Once you install and activate the plugin, you can access the Settings-->Login Lockdown menu item and then check the plugin settings. The default values are generally OK and you can just click the **Update Settings** button.

Step 10 - Check your permalink settings.

The next two steps are more housekeeping steps than a security issues, but they are important nonetheless for WordPress to function correctly.

By default, WordPress uses URLs which have question marks and numbers in them which look ugly. However WordPress offers you the ability to create a custom URL structure for your permalinks (short for "permanent link"). Go to the Settings **Permalinks Screen** using the **Settings→Permalink** menu item.



Permalink Settings

WordPress offers you the ability to create a custom URL structure for your permalinks and archives. Custom URL structures can improve the aesthetics, usability, and here are some examples to get you started.

Common Settings

☒ Plain http://www.corvideon.net/wpdemo/?p=123

☐ Day and name http://www.corvideon.net/wpdemo/2017/09/17/sample-post/

☐ Month and name http://www.corvideon.net/wpdemo/2017/09/sample-post/

☐ Numeric http://www.corvideon.net/wpdemo/archives/123

☐ Post name http://www.corvideon.net/wpdemo/sample-post/

☐ Custom Structure http://www.corvideon.net/wpdemo/

Optional

If you like, you may enter custom structures for your category and tag URLs here. For example, using `topics` as your category base would make your category link `http://www.corvideon.net/topics/`. If you leave these blank the defaults will be used.

Category base

Tag base

[Save Changes](#)

Make your changes and click the 'Save Changes' button.

Tip: A simple and useful permalink structure is

`%post_id%/%postname%/`

This will provide good SEO benefits and performs well.

Step 11 - Update your URLs

After you move a WordPress website, some of your posts or pages may still have the old website address listed in their contents or as links. If you install and activate the **Velvet Blues Update URLs** plugin you can fix this problem. Go to the **Tools→Update URLs** menu item to get to the plugin settings page.

These settings let you update your permalinks and any old URLs embedded in content or excerpts. It will replace all occurrences of the old URL with the new URL. Simply put the old website address in the top box (normally something like `http://127.0.0.1:10080/wordpress/` for InstantWP) and your new website address in the lower box.

Velvet Blues Update URLs

After moving a website, Update URLs lets you fix old URLs in content, excerpts, links, and custom fields.

WE RECOMMEND THAT YOU BACKUP YOUR WEBSITE.
You may need to restore it if incorrect URLs are entered in the fields below.

Step 1: Enter your URLs in the fields below

Old URL
Old Site Address

New URL
New Site Address

Step 2: Choose which URLs should be updated

- ☒ URLs in page content (posts, pages, custom post types, revisions)
- ☐ URLs in excerpts
- ☐ URLs in links
- ☐ URLs for attachments (images, documents, general media)
- ☐ URLs in custom fields and meta boxes
- ☐ Update ALL GUIDs *GUIDs for posts should only be changed on development sites. [Learn More.](#)*

Then click the **Update URLs** button.

Step 12 - Review Your Backup Strategy.

Every website needs backups, but what sort of backups and how often depends on the specific website. At the very least it is a good idea to take time out to consider what your website needs.

- You just need to think about what would happen if your website was hacked or if there was a hardware failure in your hosting company. Would you lose money, time or customers? Is there a potential legal issue looming?
- How often should you do a backup? Every day? Every week?
- Do you need an offsite backup to a separate service like Dropbox?
- Is the security of your data in your backups important?

To start, take a look through the various backup plugins available for WordPress and see what looks useful. There are many useful free plugins available and you really owe it to yourself to take a look, *before* you need to:

<https://wordpress.org/plugins/search/backup/>

5.4. Summary

You should now have a more secure WordPress installation. You should have carried the following tasks:

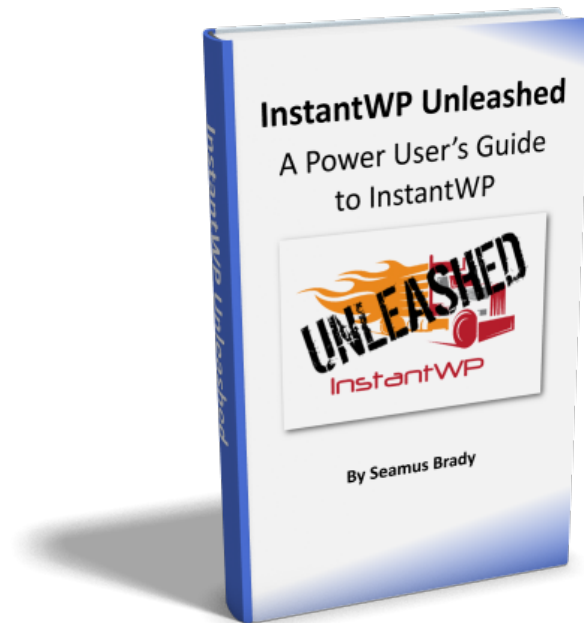
- Changed the administrator account name.
- Changed the administrator account password.
- Updated the unique keys in your wp-config.php file.
- Changed the WordPress database prefix in your WordPress database.
- Prevented the WordPress version from being displayed.
- Stopped sql injection and bad query attacks.
- Stopped comment spam.
- Disabled the wordpress file editor.
- Limited login attempts.
- Checked your permalink settings.
- Updated your URLs.
- Reviewed your backup strategy.

If you are interested in learning more about securing WordPress, check out the **Hardening WordPress** topic in the **WordPress Codex**:

http://codex.wordpress.org/Hardening_WordPress

If you found this free chapter of InstantWP Unleashed useful, get your full copy of InstantWP Unleashed now!

<https://instantwp.com/unleashed/>



InstantWP Unleashed Testimonials

"Thank you so much for this really excellent software - and for your generosity in making it freeware. It is so simple to use and the fact that it runs so easily from a usb stick makes it especially useful. The addition of InstantWP Unleashed makes working with WordPress on localhost and then going live a doddle!"

- Charle C. (UK)

"After reading through the Ebook and checking out the videos, I am very impressed with how well the topics are explained. You include the most basic details, but also smoothly move into the more advanced areas with easy to follow instructions. "

- Christie H. (Colorado, USA)

"I purchased InstantWP Unleashed yesterday and had a chance to go through the manual last night. I was really impressed with the step-by-step instructions and how thorough they were. ... If you have a WordPress Blog then you need this even if you only use it to backup and restore your websites."

- Lewis S. (Northern Ireland)

"After reading through the manual, it was a step by step guide with lots of illustrations. There was a bunch of plug-ins he showed that I've never seen before which I will be using to change out config files and vulnerable areas of the security. Seamus has it laid out pretty easy so anyone can follow along. I thought I had a pretty good knowledge of WP. I guess I've just been schooled!"

- Jack L. (New York)

Get Your Copy of InstantWP Unleashed Now:

<https://instantwp.com/unleashed/>

