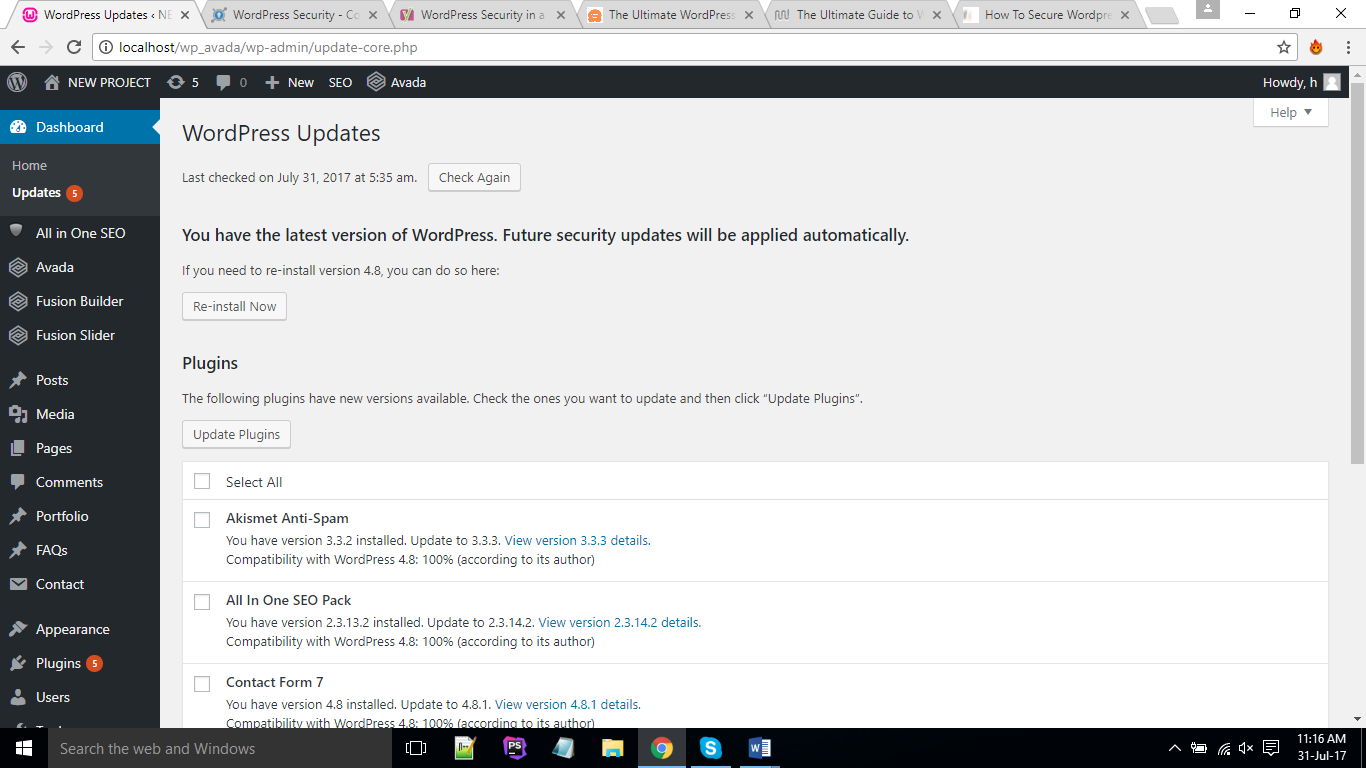
**WORDPRESS SECURITY**

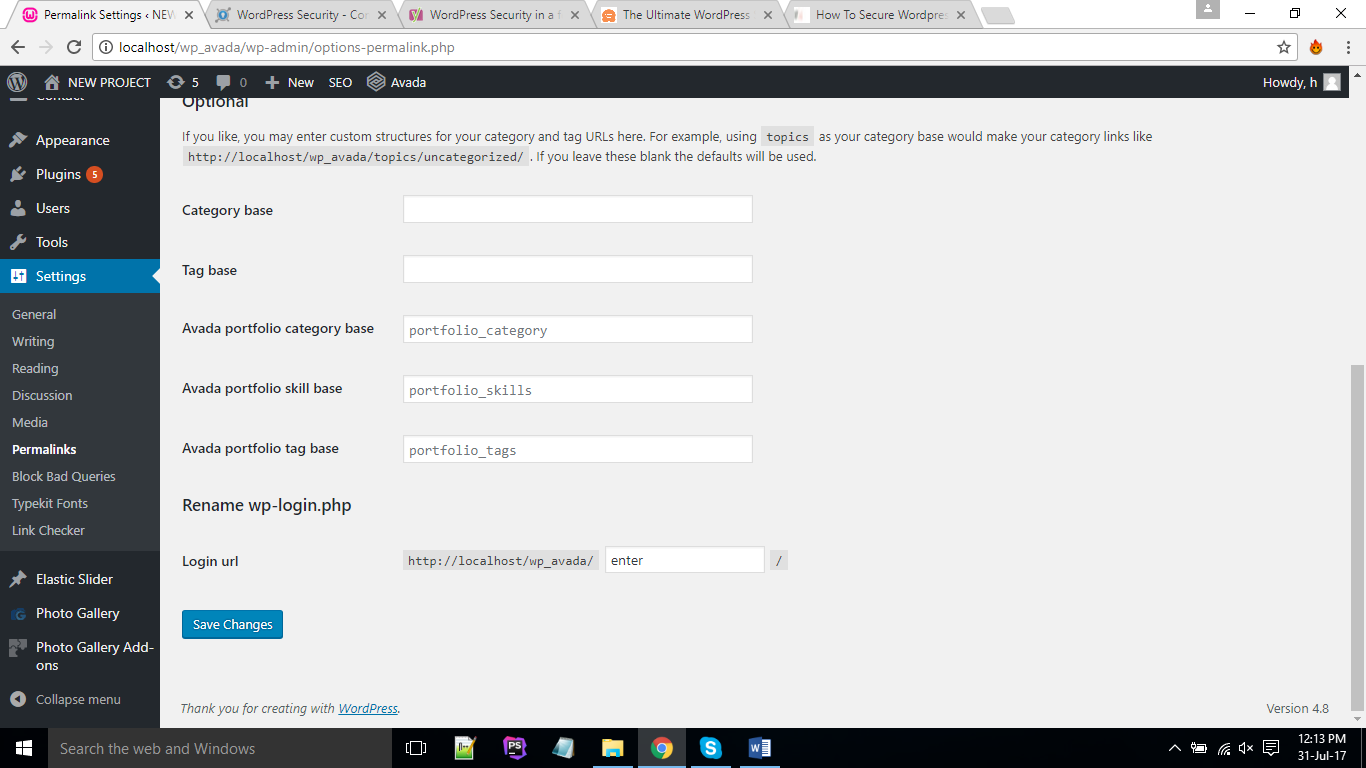
1. Keep WordPress up to date:



You should **always keep your version of**[WordPress up to date](http://codex.wordpress.org/Updating_WordPress)**as well as all of your plugins**. If you don’t do so you will fall too far behind and then there will be more chances of vulnerabilities, as hackers generally target older versions. So you should always download the latest version of WordPress from [wordpress.org](https://wordpress.org/). Since WordPress 3.7, WordPress has added automatic updates, which means you will most likely see the update in your dashboard and you can simply click to update.

1. Rename wp-login.php: You should rename your **wp-login.php** because majority of today’s attacks target your **wp-admin / wp-login** access points using a combination of admin and some password in what is known as [Brute Force attacks](http://en.wikipedia.org/wiki/Brute-force_attack). If you rename **wp-login**, anyone trying to access your login panel using brute force attacks cannot access it. There are many plugins to do so. some of them are:

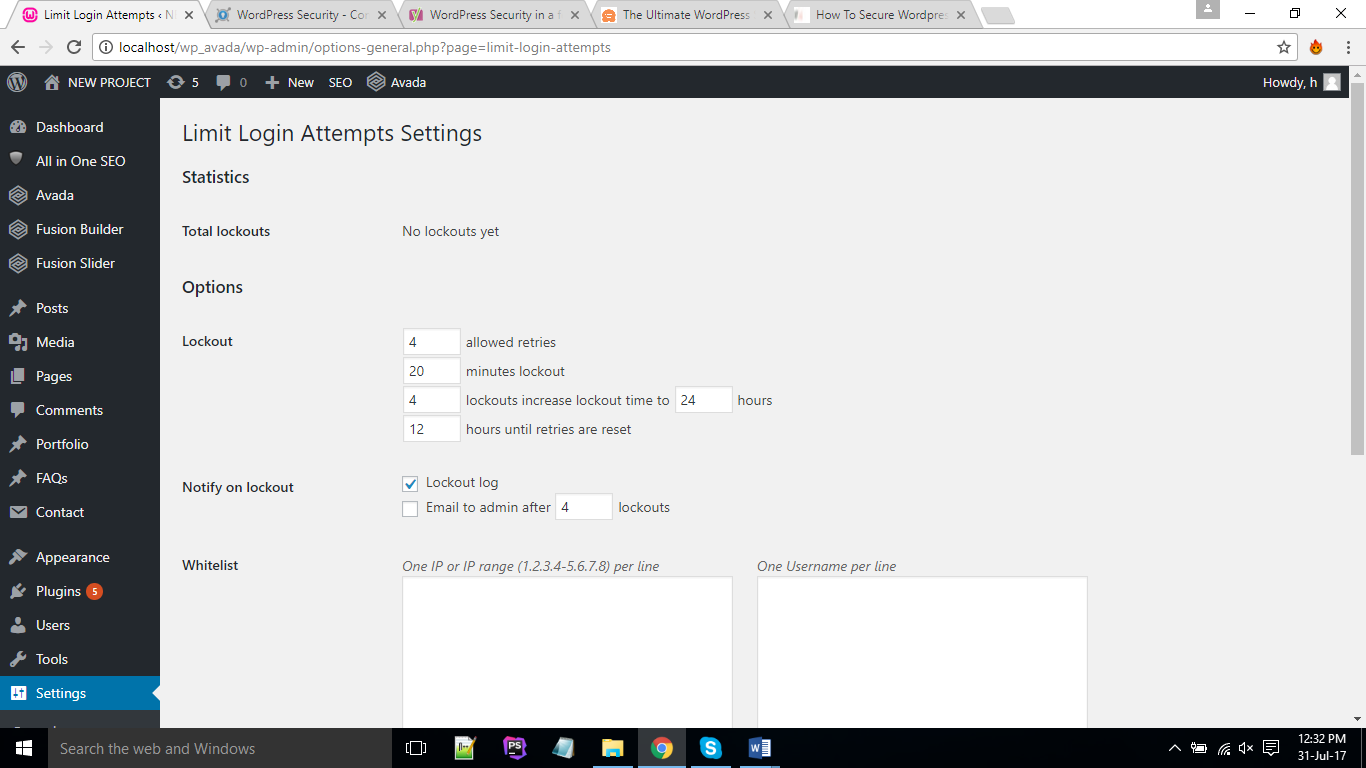
* [Rename wp-login.php](http://localhost/wp_avada/wp-admin/plugin-install.php?tab=plugin-information&plugin=rename-wp-login&TB_iframe=true&width=600&height=550)
* Rename wp-login.php to anything you want



Rename here

1. Use smart username and passwords: Be smart with your usernames and password in WordPress. **Don’t use “admin” as your username and choose a complex password.**This is probably one of the best ways to harden your WordPress security, and ironically it is one of the easiest. However many people use something they can easily remember such as “1234567” and end up regretting later when they are caught with a brute-force attack. Remember there are bots constantly crawling the internet and as your site grows they will always be trying to spoof your login.
2. Lock down wordpress login page: Locking down your **‘/wp-admin**’ login page is by far the easiest security precaution you can implement. On most websites there are thousands of failed login attempts per day that you probably never even realized. There are many of the security plugins that allow you to **limit the login attempts allowed** in their configuration pages. Some of these are:

* Wp limit login attempts.
* Limit login attempts.
* Cyber security and login attempts.
* Limit login attempts reloaded.



1. Hide wp-config.php and .htaccess files: Your **wp-config.php** contains all the necessary information for an intruder to gain access to your database. **This is the most important file in your entire WordPress install. So it is better to hide these files from intruders.** You just have to write some lines of code in your .**htaccess** file. This is relatively easy to do, but doing it wrong might make your site inaccessible. Recommended make a backup before doing so.

To hide **wp-config.php** file add following code to your **.htaccess** file.

/------------------/

<Files wp-config.php>

order deny,allow

deny from all

allow from 122.173.29.221

</Files>

/------------------/

This code will hide the **wp-config.php** file from everyone expect from the IP address 122.173.29.221(ip of pc to which you want to give access to wp-config.php file).

Similar code can be used to hide .**htaccess** file or any other file from everyone or from a particular ip and to give access to a particular ip, just replace the file name with “**wp-config.php**” and write ip address you want to give or take access to file.

1. Disable file editor in dashboard: If a hacker gets in, the easiest way to change your files would be to go to **Appearance > Editor** in WordPress. To lift your WordPress security, you could [disable](http://codex.wordpress.org/Editing_wp-config.php#Disable_the_Plugin_and_Theme_Editor) writing of these files via that editor. Open **wp-config.php** and add this line of code:

define('DISALLOW\_FILE\_EDIT', true);

1. Block bad queries: There are always bad bots, scrapers, and crawlers hitting your WordPress sites and stealing your bandwidth. To stop this install “**block bad queries**” plugin.
2. Always use secure connections: No matter where you are you should always trying to ensure the connections you are using are secure. **You should use SFTP encryption if your web host provides it**, or SSH instead of FTP. If you are using an FTP client the default port for SFTP is usually 22.
3. Disable directory indexing or browsing: Directory browsing can be used by hackers to find out if you have any files with known vulnerabilities, so they can take advantage of these files to gain access.

Directory browsing can also be used by other people to look into your files, copy images, find out your directory structure, and other information. This is why it is highly recommended that you turn off directory indexing and browsing. To disable directory browsing you have to insert the following line of code at the end of your “.**htaccess**” file.

Options All -Indexes

1. Database security: To secure database the first thing we recommend is using a different table prefix. By default WordPress uses “**wp\_”**. If you change this to something like “x3sdf\_” it will make it much harder to guess by an intruder.

You can change your table prefix on the setup screen when you are installing WordPress.



If you already have WordPress installed, you can use the following WordPress plugins to change the [database prefix](http://www.wpbeginner.com/wp-tutorials/how-to-change-the-wordpress-database-prefix-to-improve-security/).

* [Sucuri Security](https://wordpress.org/plugins/sucuri-scanner/)
* [iThemes Security](https://wordpress.org/plugins/better-wp-security/)

1. Use wordpress security plugins: There are a lot of good WordPress security plugins which will lock down your site and help protect you from brute-force attacks. These plugins allow you to block malicious networks, view WHOIS reports on visitors, rate limit or block security threats, enforce strong passwords, scan for vulnerabilities, see which files have changed, implement a firewall to block common security threats, monitor DNS changes, view real-time traffic and much more.

* Sucuri security
* iThemes security
* Wordfence security
* Simple security firewall