# 11 security tips for WordPress blogs

In terms of technical nature, the need to do immediately after configuration, setting up WordPress blog is to ensure the level of security and security needed. In the following article, we will introduce you to 11 basic tips that can be applied in many situations to accomplish this ...

**TipsMake.com - When considering the technical nature, the need to do immediately after configuration, set up WordPress blog is to ensure the level of security and security needed.** In the following article, we will introduce you to 11 basic tips that can be applied in many situations to accomplish this.

>>>Assign SSL security mechanism to WordPress blog

## 1. Encrypt login information:

This is our first point of concern here that every time you log in, the password will not be encrypted, but transmitted directly to the database. If you visit in public, the opportunity for hackers to 'stare' and steal this information is huge thanks to **Keylogger** software or other applications. However, we can completely overcome this problem with the plug - in Chap Secure Login with the main function of assigning random hash codes to the password character string, then proceeding to validate the match. method of account with CHAP protocol.

## 2. Prevent Brute Force Attack:

In fact, hackers can completely break the login password and user credentials using the Brute Force Attack mechanism. To reduce this risk, please use Login LockDown plug-in for **WordPress** . This utility will record all information whenever required to access from a certain IP address to log in to **WordPress** system after a certain number of failed login attempts, the system will block access, as well as all other requests from that address.

## 3. Use the password according to the standard:

This is very basic, but it seems that many people still do not apply correctly, it is to choose and use complex passwords but still easy to remember, others are difficult to guess, do not use familiar information strings such as relative name, phone number, address . that must combine characters and numbers, special characters, lowercase letters .

## 4. 'Protection' folder wp-admin:

In essence, the **wp-admin** directory contains all the important and necessary information that can directly affect the stability of the system. And one solution to use here is to install AskApache Password Protect plug-in for **WordPress** to set a password to protect that folder, grant access to the person or account you trust.

## 5. Remove information about WordPress version:

In fact, there are many **WordPress** themes that contain version information in the meta tag, and based on that, hackers can rely on this to find a suitable attack plan. To fix it, please access the main control panel of **WordPress** , then open **Design> Theme Editor.** On the right side, we select the **Header** file and search for the code line that looks like this:

/ /

Please delete this line and click the **Update File** button. Please note that with **WordPress 2.6** or later, the system automatically attaches version information in the Wp_head section. And to fix it, we just need to install the WP Security Scan plug-in.

## 6. 'Hide' the plugins folder:

If you access the directory or **http://yourwebsite.com/wp-content/plugins link** , you will see the entire list of system plug-ins used. If you want to hide this folder, you only need to upload an empty **index.html** file to this plugin directory. Simply open an application to edit any text, then save it as **index.html,** use the ftp program and download this **index.html** file into the **/ wp-content / plugins directory.**

## 7. Change username:


The default **Username** name is **admin** , but we can still change it to prevent hacker attacks on simple systems. In the main **WordPress** control panel, open the **Users** and create a new account, then assign the **administrator** and log back in with the account you just created.

Go to the **Users** section, this time check the box next to **admin** and select **Delete** . When the system displays the notification confirmation window, we select **Attribute all posts and links to:** and select the account we just created in the above dropdown list. This process will transfer all articles to a new account. Then you click **Confirm Deletion.**

## 8. Always update the latest version of WordPress and plug - in:

Technically, the latest version of **WordPress is** always updated with security patches, so users should pay attention to this process. At the time of this article, WordPress has released version 3.3, and you can download it directly here.

## 9. Perform a regular scan process:

As mentioned above, you need to install the WP Security Scan utility and perform regular scans to detect security holes in the system. Another point to apply here is to change **wp_ to** a custom prefix, to avoid hacker snooping.

## 10. Backup database:

To do this, please install and use the utility that supports WP-DB-Backup with the main function of backing up the entire database of the system according to the time and schedule of the administrator. .

## 11. Set the appropriate decentralization level:

In case there are more than one Author - Author in your system, use the Role Manager plug-in to create, manage, and monitor authorization levels for users or groups in the system.

Good luck!