WEEBLOGGER

The Ultimate WordPress Security Guide – Step by Step

WordPress security is a topic of huge importance for every website owner. Each week, Google blacklists around 20,000 websites for malware and around 50,000 for phishing. If you are serious about your website, then you need to pay attention to the WordPress security best practices. In this guide, we will share all the top WordPress security tips to help you protect your website against hackers and malware.

While WordPress core software is very secure, and it's audited regularly by hundreds of developers, there is a lot that can be done to harden your WordPress website.

At Weeblogger, we believe that security is not just about risk elimination. It's also about risk reduction. As a website owner, there's a lot that you can do to improve your WordPress security (even if you're not tech savvy).

We have a number of actionable steps that you can take to improve your WordPress security.

To make it easy, we have created a table of content to help you easily navigate through our ultimate WordPress security guide.

Why Website Security is Important?

A hacked WordPress site can cause serious damage to your business revenue and reputation. Hackers can steal user information, passwords, install malicious software, and can even distribute malware to your users.

Worst, you may find yourself paying ransomware to hackers just to regain access to your website.

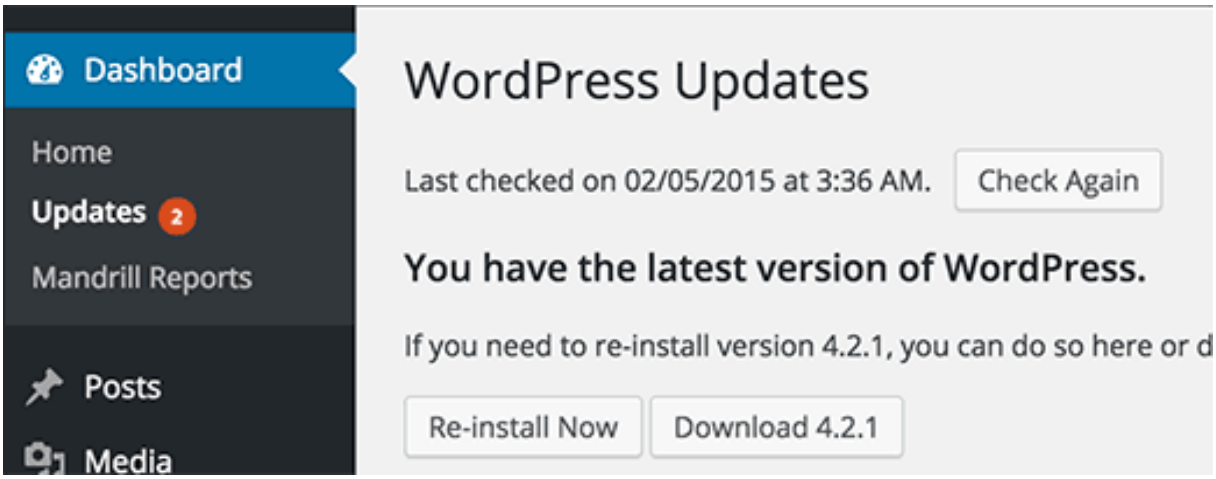
In March 2016, Google reported that more than 50 million website users have been warned about a website they're visiting may contain malware or steal information.

Furthermore, Google blacklists around 20,000 websites for malware and around 50,000 for phishing each week.

If your website is a business, then you need to pay extra attention to your WordPress security.

Similar to how it's the business owners responsibility to protect their physical store building, as an online business owner it is your responsibility to protect your business website.

Keeping WordPress Updated



WordPress is an open source software which is regularly maintained and updated. By default, WordPress automatically installs minor updates. For major releases, you need to manually initiate the update.

WordPress also comes with thousands of plugins and themes that you can install on your website. These plugins and themes are maintained by third-party developers which regularly release updates as well.

These WordPress updates are crucial for the security and stability of your WordPress site. You need to make sure that your WordPress core, plugins, and theme are up to date.

Strong Passwords and User Permissions

The most common WordPress hacking attempts use stolen passwords. You can make that difficult by using stronger passwords that are unique for your website. Not just for WordPress admin area, but also for FTP accounts, database, WordPress hosting account, and your professional email address.

The top reason why beginners don't like using strong passwords is because they're hard to remember. The good thing is you don't need to remember passwords anymore. You can use a password manager.

Another way to reduce the risk is to not give any one access to your WordPress admin account unless you absolutely have to. If you have a large team or guest authors, then make sure that you understand user roles and capabilities in WordPress before you add new user and authors to your WordPress site.

The Role of WordPress Hosting

Your WordPress hosting service plays the most important role in the security of your WordPress site. A good shared hosting provider like Siteground take the extra measures to protect their servers against common threats.

However, on shared hosting you share the server resources with many other customers. This opens the risk of cross-site contamination where a hacker can use a neighboring site to attack your website.

Using a managed WordPress hosting service provides a more secure platform for your website. Managed WordPress hosting companies offer automatic backups, automatic WordPress updates, and more advanced security configurations to protect your website.

WordPress Security in Easy Steps (No Coding)

We know that improving WordPress security can be a terrifying thought for beginners. Specially if you're not techy. Guess what – you're not alone.

We have helped thousands of WordPress users in hardening their WordPress security.

We will show you how you can improve your WordPress security with just a few clicks (no coding required).

If you can point-and-click, you can do this!

Install a WordPress Backup Solution

Backups are your first defense against any WordPress attack. Remember, nothing is 100% secure. If government websites can be hacked, then so can yours.

Backups allow you to quickly restore your WordPress site in case something bad was to happen.

There are many free and paid WordPress backup plugins that you can use. The most important thing you need to know when it comes to backups is that you must regularly save full-site backups to a remote location (not your hosting account).

We recommend storing it on a cloud service like Amazon, Dropbox, or private clouds like Stash.

Based on how frequently you update your website, the ideal setting might be either once a day or real-time backups.

Thankfully this can be easily done by using plugins like VaultPress or BackupBuddy. They are both reliable and most importantly easy to use (no coding needed).

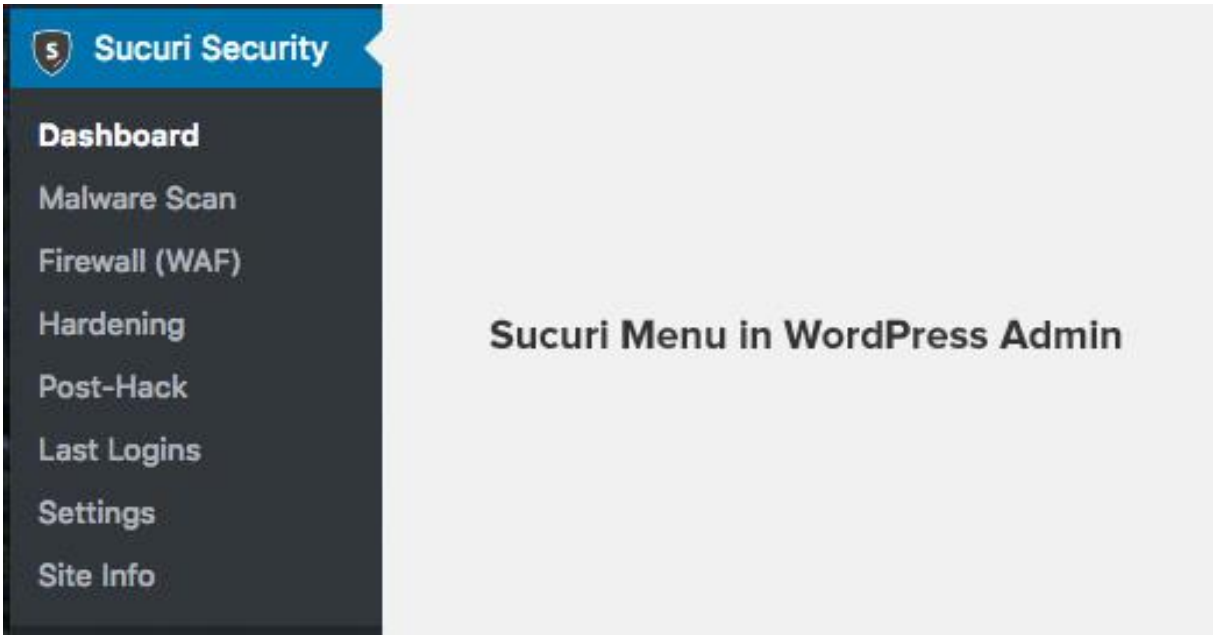
Best WordPress Security Plugin

After backups, the next thing we need to do is setup an auditing and monitoring system that keeps track of everything that happens on your website.

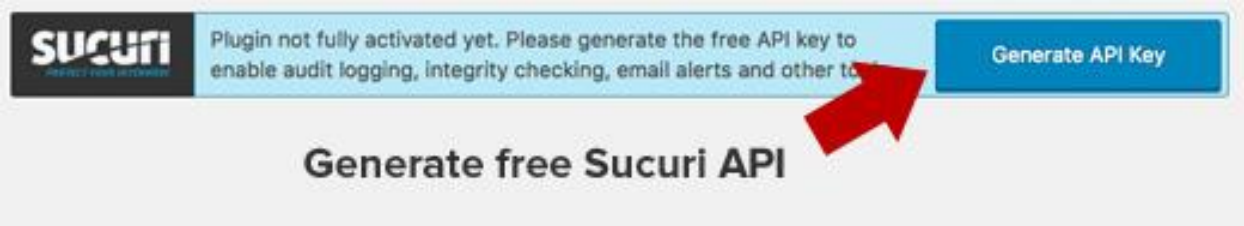
This includes file integrity monitoring, failed login attempts, malware scanning, etc.

Thankfully, this can be all taken care by the best free WordPress security plugin, Sucuri Scanner.

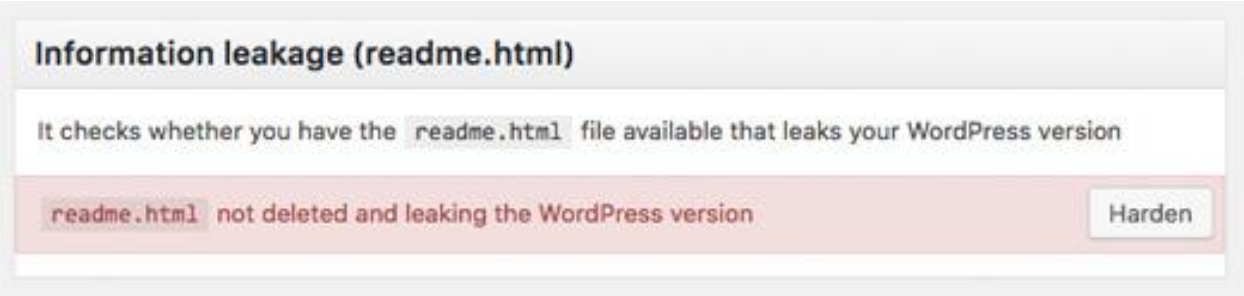
You need to install and activate the free Sucuri Security plugin. Upon activation, you need to go to the Sucuri menu in your WordPress admin.



The first thing you will be asked to do is Generate a free API key. This enables audit logging, integrity checking, email alerts, and other important features.



The next thing, you need to do is click on the Hardening tab from the Sucuri Menu. Go through every option and click on the “Harden” button.



These options help you lock down the key areas that hackers often use in their attacks. The only hardening option that’s a paid upgrade is the Web Application Firewall which we will explain in the next step, so skip it for now.

We have also covered a lot of these “Hardening” options later in this article for those who want to do it without using a plugin or the ones that require additional steps such as “Database Prefix change” or “Changing the Admin Username”.

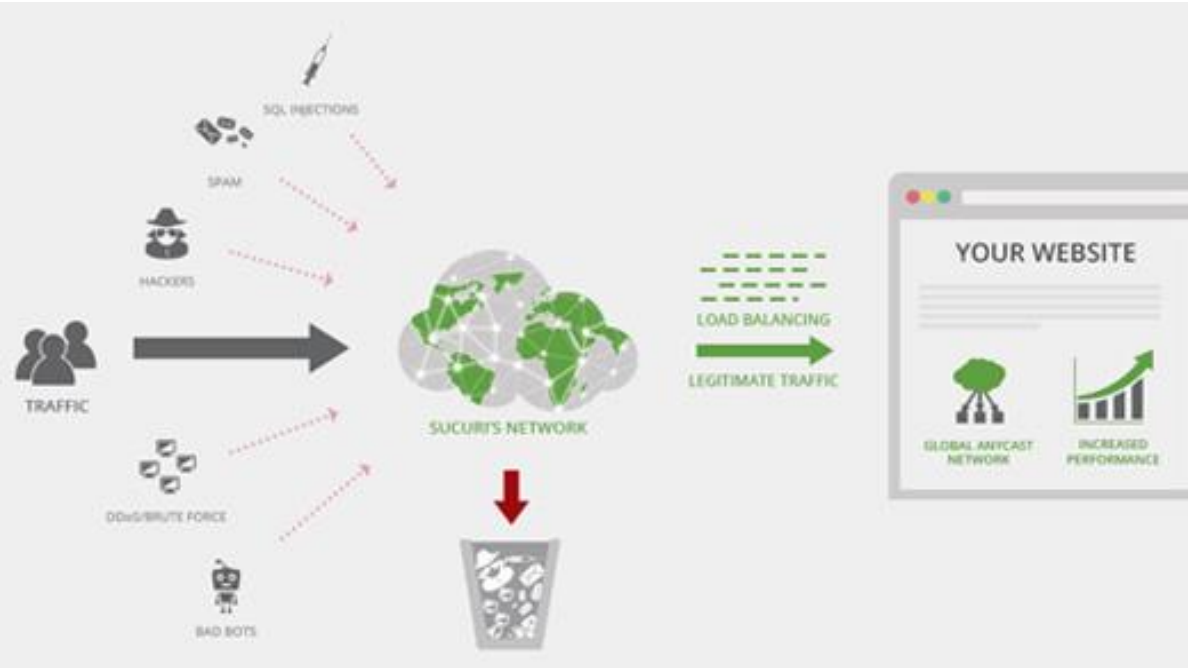
After the hardening part, most default settings of this plugin are good and doesn’t need changing. The only thing we recommend customizing is the Email Alerts.

The default alert settings can clutter your inbox with emails. We recommend receiving alerts for key actions like changes in plugins, new user registration, etc. You can configure the alerts by going to Sucuri Settings » Alerts.

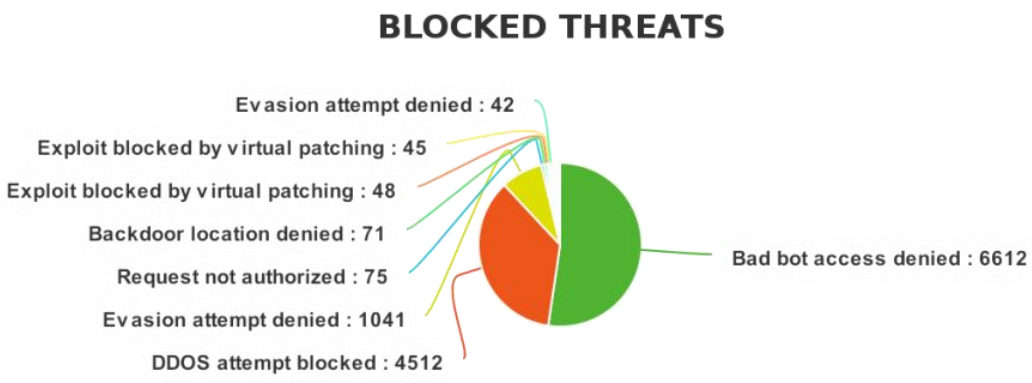
This WordPress security plugin is very powerful, so browse through all the tabs and settings to see all that it does such as Malware scanning, Audit logs, Failed Login Attempt tracking, etc.

Enable Web Application Firewall (WAF)

The easiest way to protect your website and be confident about your WordPress security is by using a web application firewall (WAF). The firewall blocks all malicious traffic before it even reaches your website.



We **use and recommend** Sucuri as the best web-application firewall for WordPress. You can read about how Sucuri helped us block 450,000 WordPress attacks in a month.



The best part about Sucuri's firewall is that it also comes with a malware cleanup and blacklist removal guarantee. Basically if you were to be hacked under their watch, they guarantee that they will fix your website (no matter how many pages you have).

This is a pretty strong warranty because repairing hacked websites is expensive. Security experts normally charge $250 per hour. Whereas you can get the entire Sucuri security stack for $199 per year.

WordPress Security for DIY Users

If you do everything that we have mentioned thus far, then you're in a pretty good shape.

But as always, there's more that you can do to harden your WordPress security.

Some of these steps may require coding knowledge.

Change the Default "admin" username

In the old days, the default WordPress admin username was "admin". Since usernames make up half of login credentials, this made it easier for hackers to do brute-force attacks.

Thankfully, WordPress has since changed this and now requires you to select a custom username at the time of installing WordPress.

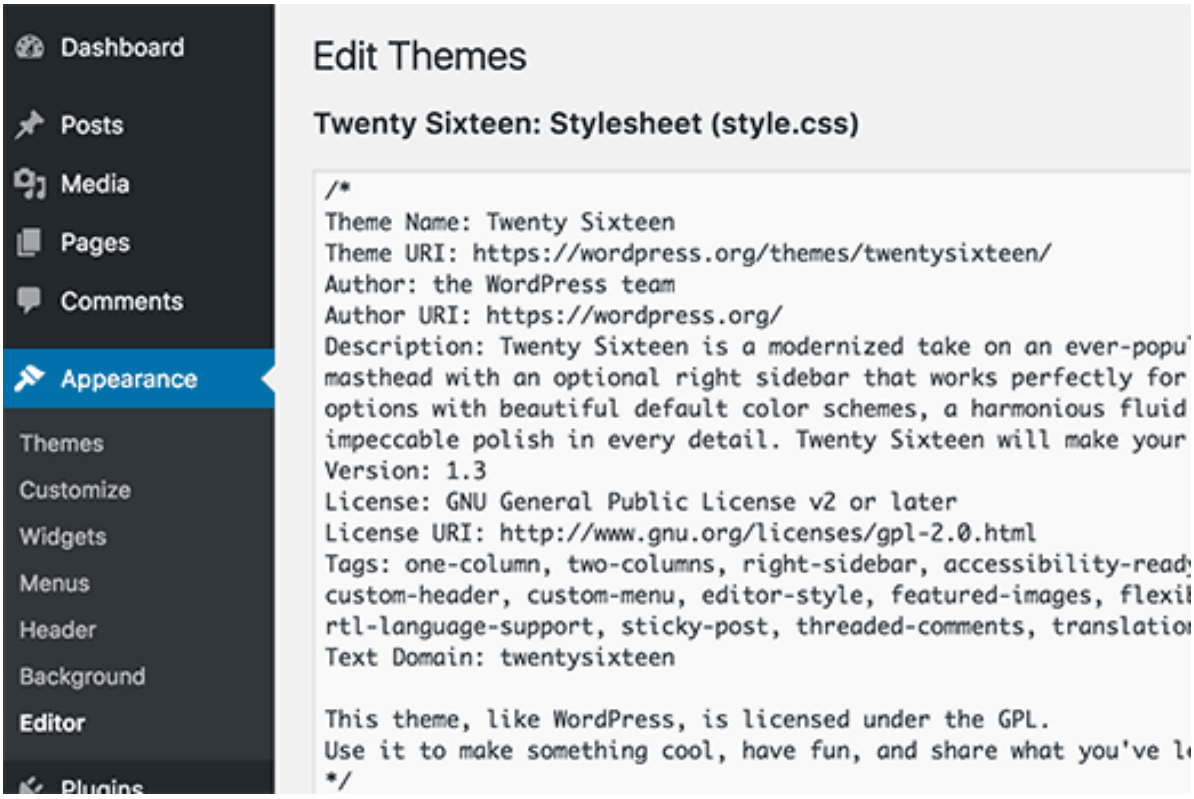
However, some 1-click WordPress installers, still set the default admin username to "admin". If you notice that to be the case, then it's probably a good idea to switch your web hosting.

Since WordPress doesn't allow you to change usernames by default, there are three methods you can use to change the username.

1. Create a new admin username and delete the old one.
2. Use the Username Changer plugin
3. Update username from phpMyAdmin

Disable File Editing

WordPress comes with a built-in code editor which allows you to edit your theme and plugin files right from your WordPress admin area. In the wrong hands, this feature can be a security risk which is why we recommend turning it off.



You can easily do this by adding the following code in your wp-config.php file.

```
// Disallow file editdefine( 'DISALLOW_FILE_EDIT', true );
```

Alternatively, you can do this with 1-click using the Hardening feature in the free Sucuri plugin that we mentioned above.

Disable PHP File Execution in Certain WordPress Directories

Another way to harden your WordPress security is by disabling PHP file execution in directories where it's not needed such as /wp-content/uploads/.

You can do this by opening a text editor like Notepad and paste this code:

```
<Files *.php>deny from all</Files>
```

Next, you need to save this file as **.htaccess** and upload it to /wp-content/uploads/ folders on your website using an FTP client.

Limit Login Attempts

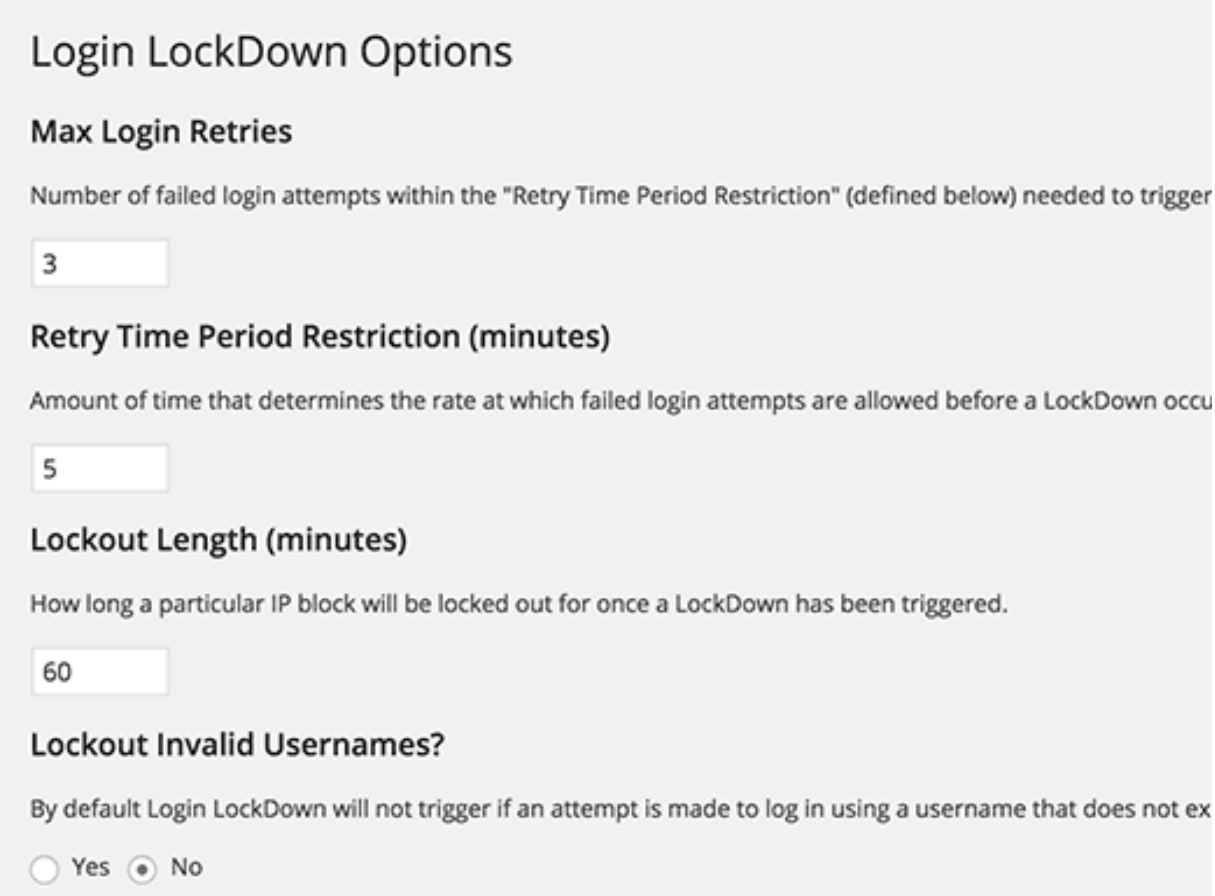
By default, WordPress allows users to try to login as many time as they want. This leaves your WordPress site vulnerable to brute force attacks. Hackers try to crack passwords by trying to login with different combinations.

This can be easily fixed by limiting the failed login attempts a user can make. If you're using the web application firewall mentioned earlier, then this is automatically take care of.

However, if you don't have the firewall setup, then proceed with the steps below.

First, you need to install and activate the Login LockDown plugin.

Upon activation, visit **Settings » Login LockDown** page to setup the plugin.

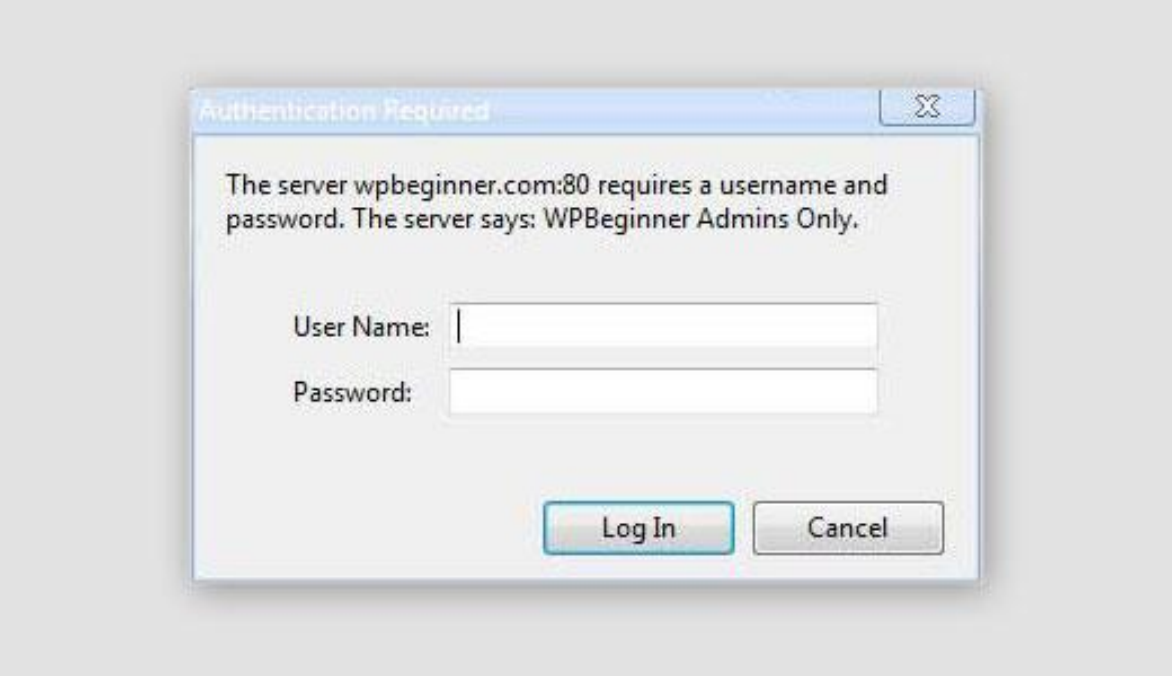


Change WordPress Database Prefix

By default, WordPress uses wp_ as the prefix for all tables in your WordPress database. If your WordPress site is using the default database prefix, then it makes it easier for hackers to guess what your table name is. This is why we recommend changing it.

Note: This can break your site if it's not done properly. Only proceed, if you feel comfortable with your coding skills.

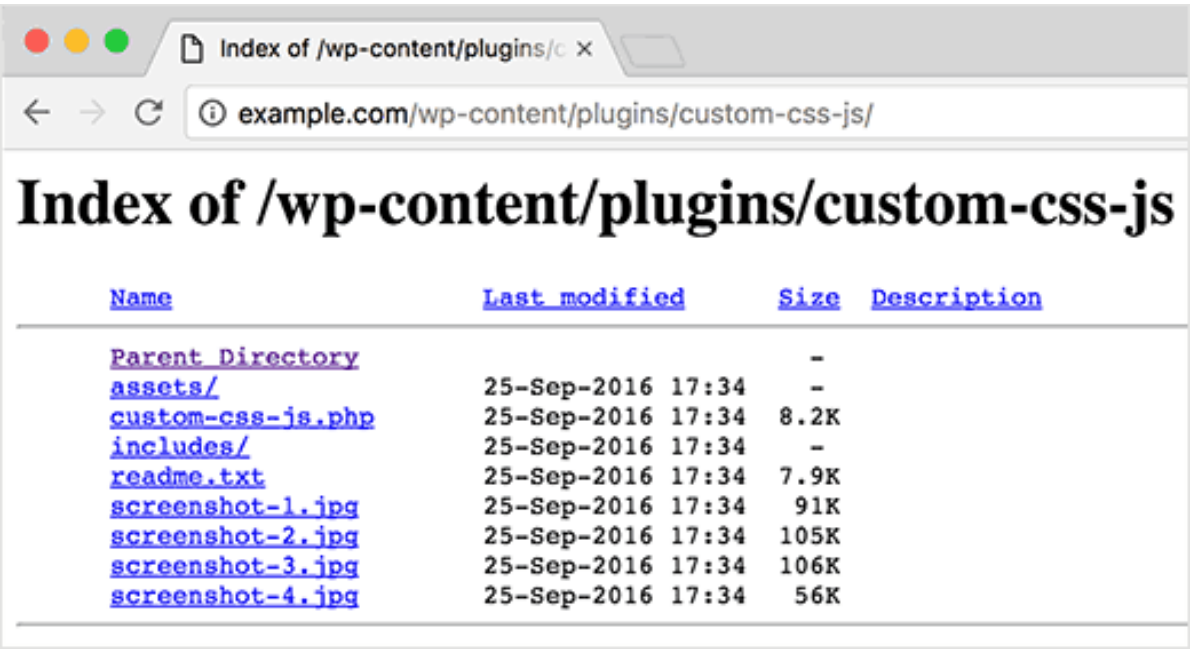
Password Protect WordPress Admin and Login Page



Normally, hackers can request your wp-admin folder and login page without any restriction. This allows hackers to try their hacking tricks or run DDoS attacks.

You can add additional password protection on a server side which will effectively block those requests.

Disable Directory Indexing and 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.

You need to connect to your website using FTP or cPanel's file manager. Next, locate the .htaccess file in your website's root directory. If you cannot see it there, then refer to our guide on why you can't see .htaccess file in WordPress.

After that, you need to add the following line at the end of the .htaccess file:

```
Options -Indexes
```

Don't forget to save and upload .htaccess file back to your site.

Disable XML-RPC in WordPress

XML-RPC was enabled by default in WordPress 3.5 because it helps connecting your WordPress site with web and mobile apps.

However because of it's powerful nature, XML-RPC can significantly amplify the brute-force attacks.

For example, traditionally if a hacker wanted to try 500 different passwords on your website, they would have to make 500 separate login attempts which will be caught and blocked by the login lockdown plugin.

But with XML-RPC, a hacker can use the **system.multicall** function to try thousands of password with say 20 or 50 requests.

This is why if you're not using XML-RPC, we recommend that you disable it.

Tip: The .htaccess method is the best one because it's the least resource intensive.

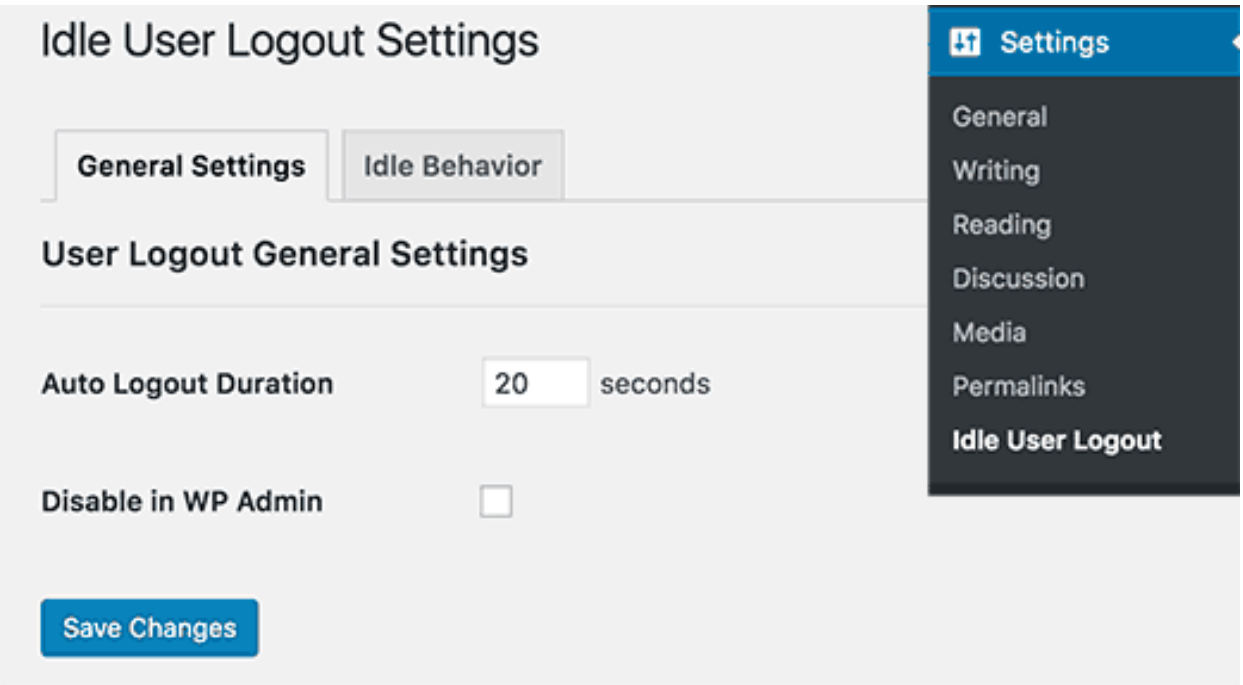
If you're using the web-application firewall mentioned earlier, then this can be taken care of by the firewall.

Automatically log out Idle Users in WordPress

Logged in users can sometimes wander away from screen, and this poses a security risk. Someone can hijack their session, change passwords, or make changes to their account.

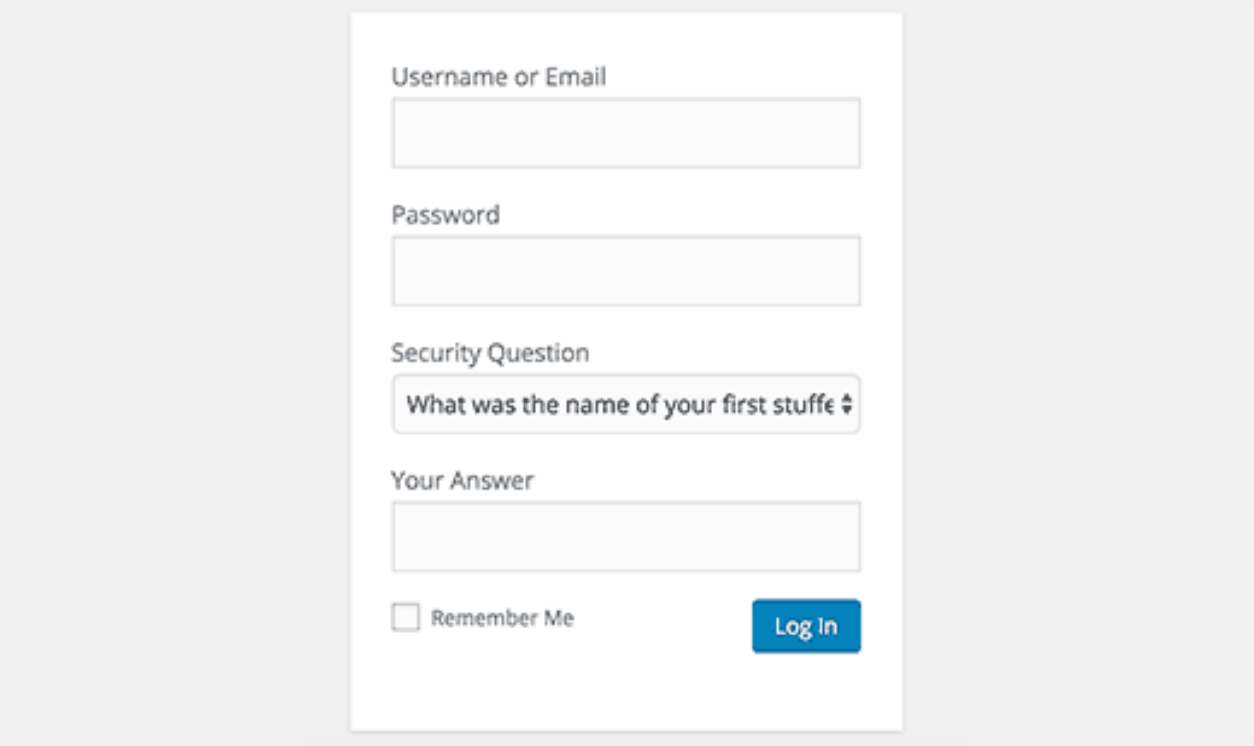
This is why many banking and financial sites automatically log out an inactive user. You can implement similar functionality on your WordPress site as well.

You will need to install and activate the Idle User Logout plugin. Upon activation, visit **Settings » Idle User Logout** page to configure plugin settings.



Simply set the time duration and uncheck the box next to ‘Disable in wp admin’ option for better security. Don’t forget to click on the save changes button to store your settings.

Add Security Questions to WordPress Login Screen



Adding a security question to your WordPress login screen makes it even harder for someone to get unauthorized access.

You can add security questions by installing the WP Security Questions plugin. Upon activation, you need to visit Settings » Security Questions page to configure the plugin settings.

Fixing a Hacked WordPress Site

Many WordPress users don't realize the importance of backups and website security until their website is hacked.

Cleaning up a WordPress site can be very difficult and time consuming. Our first advice would be to let a professional take care of it.

Hackers install backdoors on affected sites, and if these backdoors are not fixed properly, then your website will likely get hacked again.

Allowing a professional security company like Sucuri to fix your website will ensure that your site is safe to use again. It will also protect you against any future attacks.

That’s all, we hope this article helped you learn the top WordPress security best practices as well as discover the best WordPress security plugins for your website.