WordPress Security Guide

WordPress security is a topic of huge importance for every website owner. Google blacklists around 10,000+ websites every day for malware and around 50,000 for phishing every week.

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 keep your site secure.

At WPBeginner, 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 protect your website against security vulnerabilities.

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

WordPress Security Guide

Table of Contents

Basics of WordPress Security

WordPress Security in Easy Steps (No Coding)

WordPress Security for DIY Users

Ready? Let’s get started.

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.

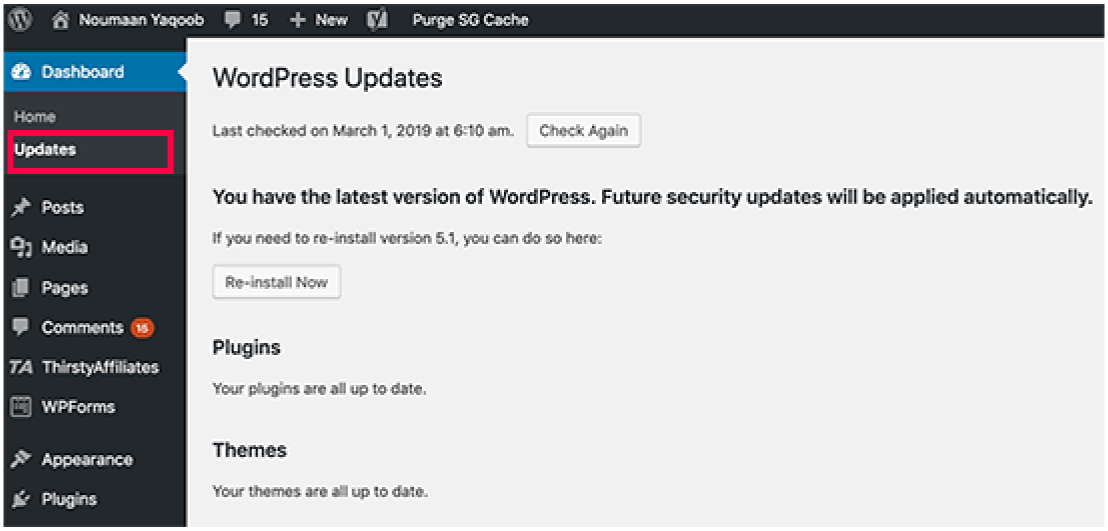
If your website is a business, then you need to pay extra attention to your WordPress security.

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.

[Back to Top ↑]

WordPress Security Guide

Keeping WordPress Updated



WordPress Updates

Last checked on March 1, 2019 at 6:10 am.

You have the latest version of WordPress. Future security updates will be applied automatically.

If you need to re-install version 5.1, you can do so here:

Plugins

Your plugins are all up to date.

Themes

Your themes are all up to date.

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.

[Back to Top ↑]

WordPress Security Guide

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 custom email addresses which use your site’s domain name.

Many beginners don’t like using strong passwords because they’re hard to remember. The good thing is that you don’t need to remember passwords anymore. You can use a password manager. See our guide on how to manage WordPress passwords.

Another way to reduce the risk is to not give anyone 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 accounts and authors to your WordPress site.

[Back to Top ↑]

WordPress Security Guide

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 Bluehost or Siteground take the extra measures to protect their servers against common threats.

Here is how a good web hosting company works in the background to protect your websites and data.

- They continuously monitor their network for suspicious activity.
- All good hosting companies have tools in place to prevent large scale DDOS attacks
- They keep their server software and hardware up to date to prevent hackers from exploiting a known security vulnerability in an old version.
- They have ready to deploy disaster recovery and accidents plans which allows them to protect your data in case of major accident.

On a shared hosting plan, 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

We recommend WPEngine as our preferred managed WordPress hosting provider. They’re also the most popular one in the industry. (See our special WPEngine coupon).

[Back to Top ↑]

WordPress Security Guide

WordPress Security in Easy Steps (No Coding)

We know that improving WordPress security can be a terrifying thought for beginners. Especially 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.

WordPress Security Guide

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 UpdraftPlus. They are both reliable and most importantly easy to use (no coding needed).

[Back to Top ↑]

Best WordPress Security Plugin

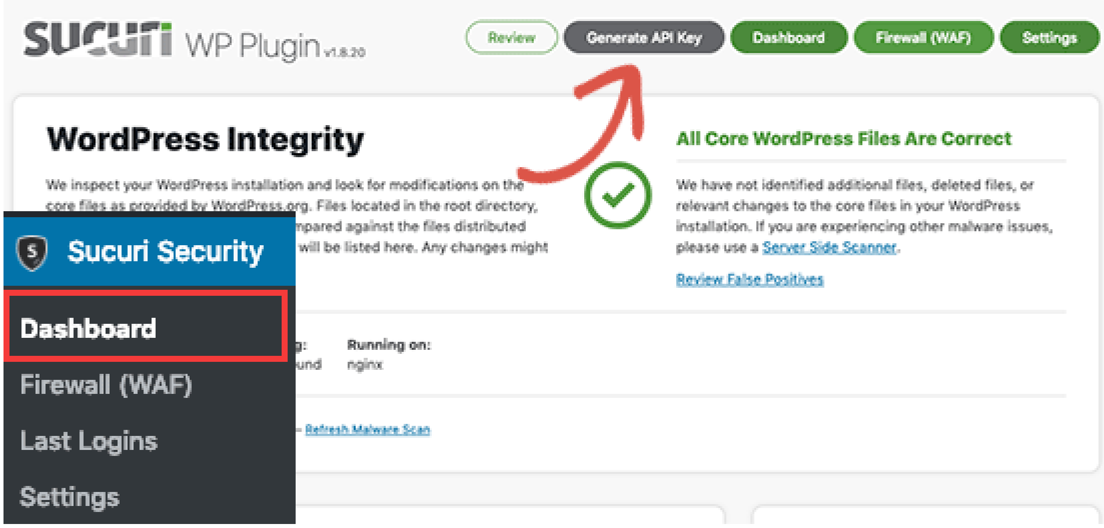
After backups, the next thing we need to do is setup an auditing and monitoring system that keeps track of everything that happens on your website.

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. For more details, please see our step by step guide on how to install a WordPress 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.



WordPress Integrity

We inspect your WordPress installation and look for modifications on the core files as provided by WordPress.org. Files located in the root directory, mpared against the files distributed will be listed here. Any changes might

All Core WordPress Files Are Correct

We have not identified additional files, deleted files, or relevant changes to the core files in your WordPress installation. If you are experiencing other malware issues, please use a Server Side Scanner.

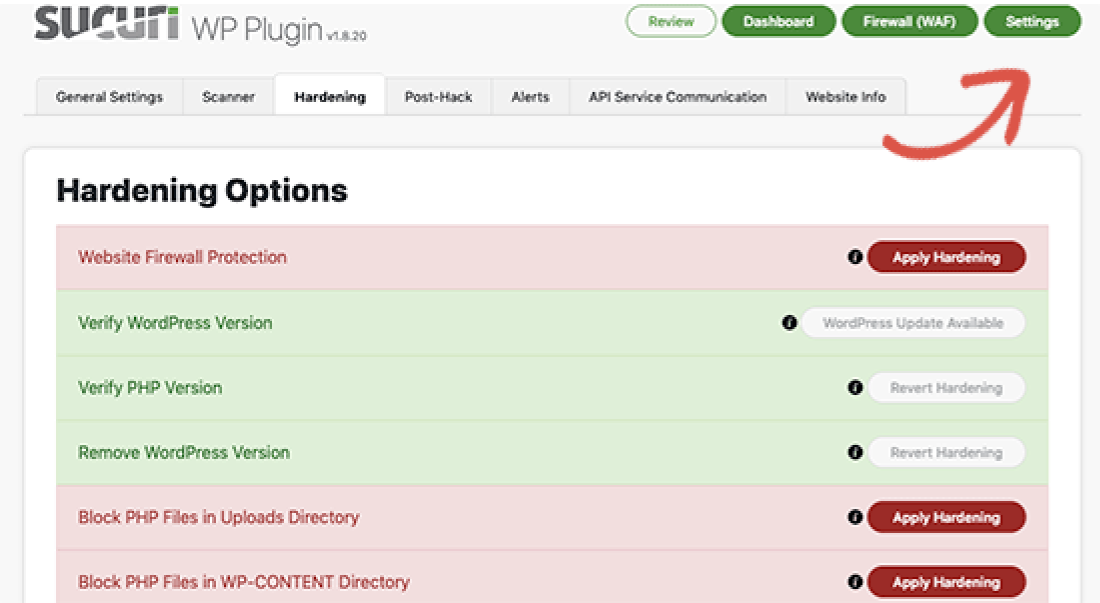
Review False Positives

g: und

Running on: nginx

- Refresh Malware Scan

The next thing, you need to do is click on the ‘Hardening’ tab from the settings menu. Go through every option and click on the “Apply Hardening” button.



Hardening Options

Website Firewall Protection — Apply Hardening

Verify WordPress Version — WordPress Update Available

Verify PHP Version — Revert Hardening

Remove WordPress Version — Revert Hardening

Block PHP Files in Uploads Directory — Apply Hardening

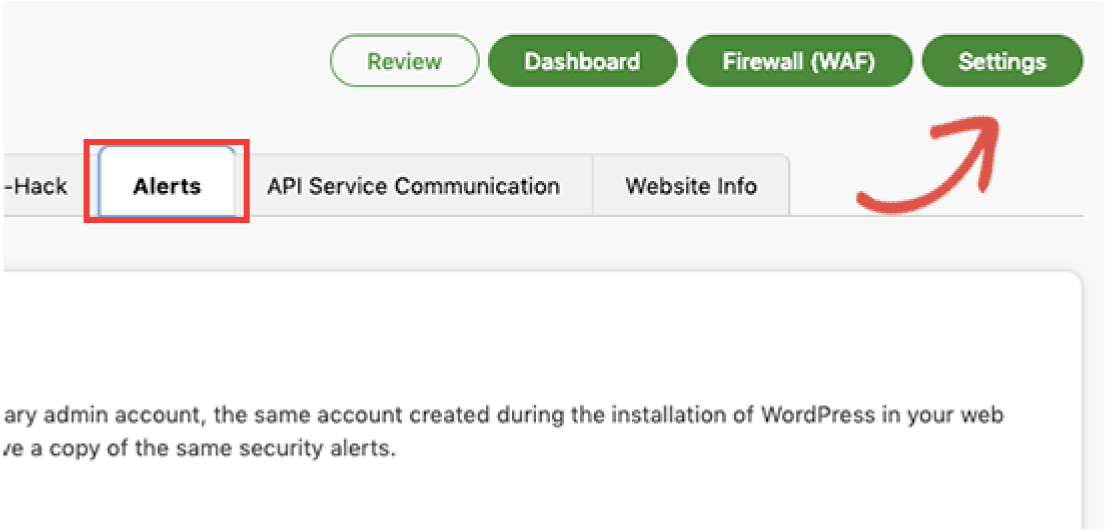
Block PHP Files in WP-CONTENT Directory — Apply Hardening

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, the default plugin settings are good enough for most websites and don’t need any changes. The only thing we recommend customizing is ‘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.



ary admin account, the same account created during the installation of WordPress in your web
/e a copy of the same security 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 site and be confident about your WordPress security is by using a web application firewall (WAF).

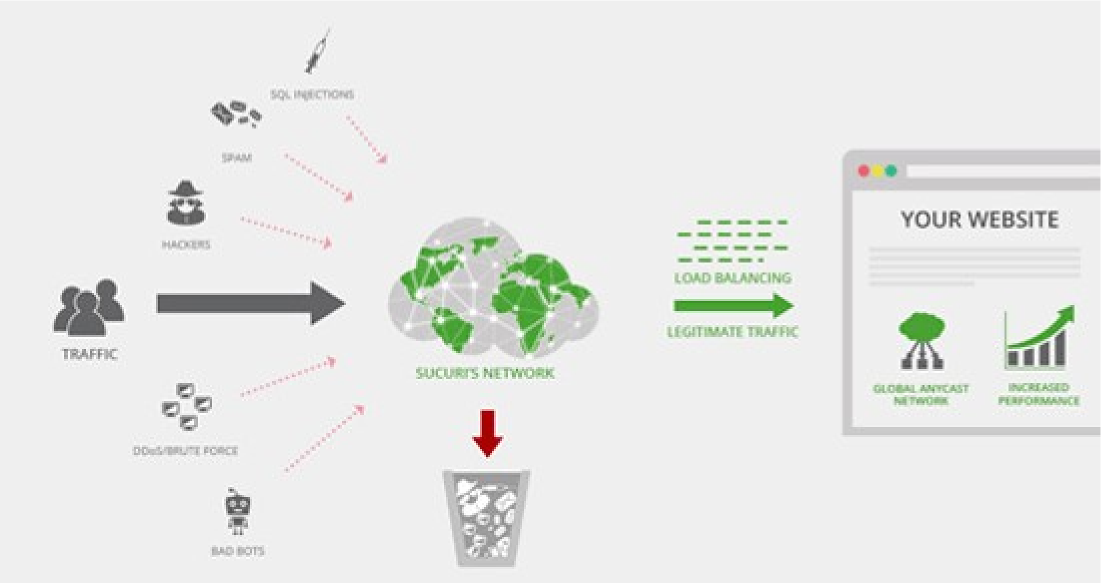
A website firewall blocks all malicious traffic before it even reaches your website.

WordPress Security Guide

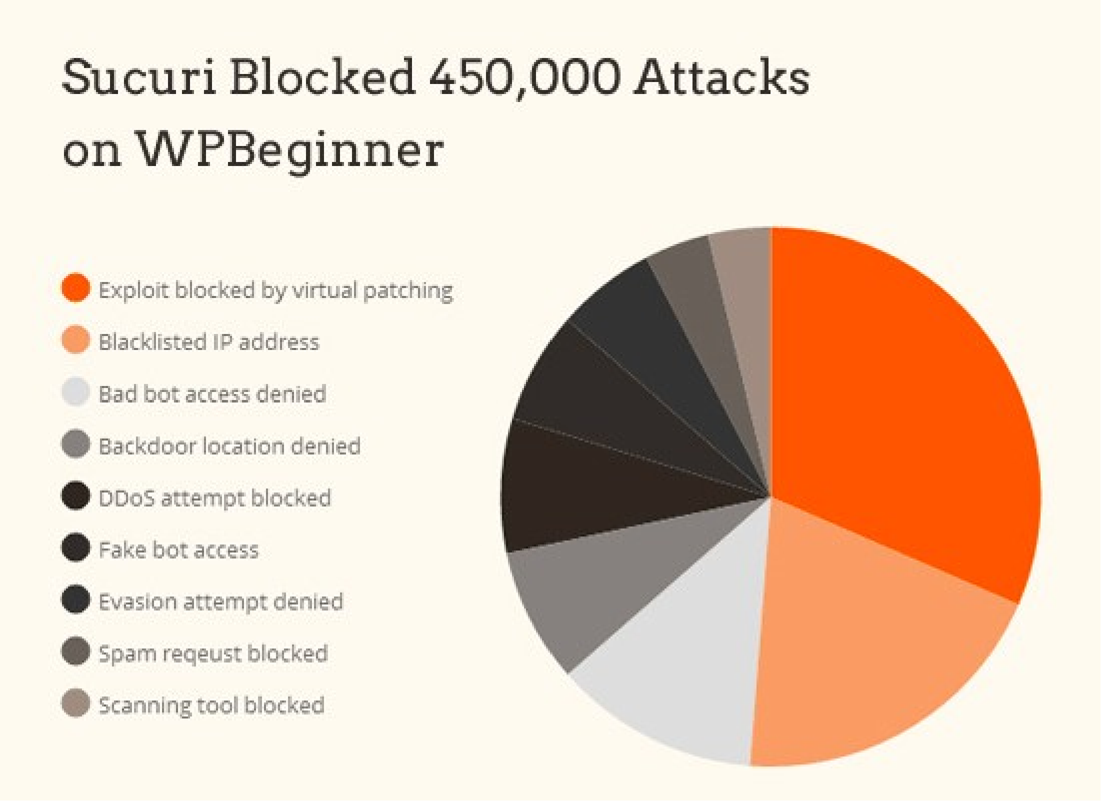
DNS Level Website Firewall – These firewall route your website traffic through their cloud proxy servers. This allows them to only send genuine traffic to your web server.

Application Level Firewall – These firewall plugins examine the traffic once it reaches your server but before loading most WordPress scripts. This method is not as efficient as the DNS level firewall in reducing the server load.

To learn more, see our list of the best WordPress firewall plugins.



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.

Improve your WordPress Security with the Sucuri Firewall »

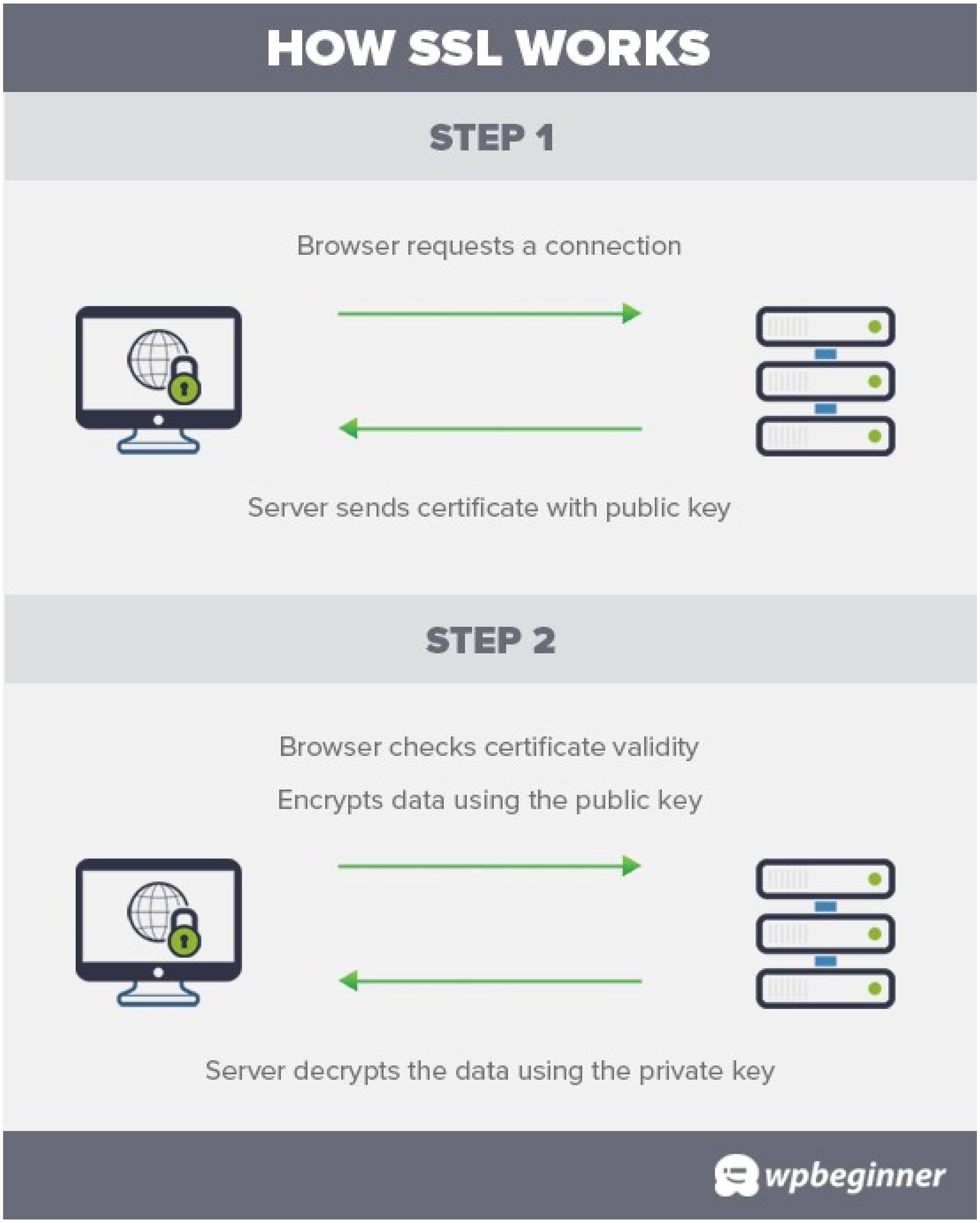
Sucuri is not the only DNS level firewall provider out there. The other popular competitor is Cloudflare. See our comparison of Sucuri vs Cloudflare (Pros and Cons).

[Back to Top ↑]

WordPress Security Guide

Move Your WordPress Site to SSL/HTTPS

SSL (Secure Sockets Layer) is a protocol which encrypts data transfer between your website and users browser. This encryption makes it harder for someone to sniff around and steal information.


HOW SSL WORKS
STEP 1
Browser requests a connection
Server sends certificate with public key
STEP 2
Browser checks certificate validity
Encrypts data using the public key
Server decrypts the data using the private key
wpbeginner

Once you enable SSL, your website will use HTTPS instead of HTTP, you will also see a padlock sign next to your website address in the browser.

SSL certificates were typically issued by certificate authorities and their prices start from $80 to hundreds of dollars each year. Due to added cost, most website owners opted to keep using the insecure protocol.

To fix this, a non-profit organization called Let’s Encrypt decided to offer free SSL Certificates to website owners. Their project is supported by Google Chrome, Facebook, Mozilla, and many more companies.

Due to this, it is now easier than ever to start using SSL for all your WordPress websites. For step by step instructions, see our article on how to get a free SSL certificate for your WordPress website.

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

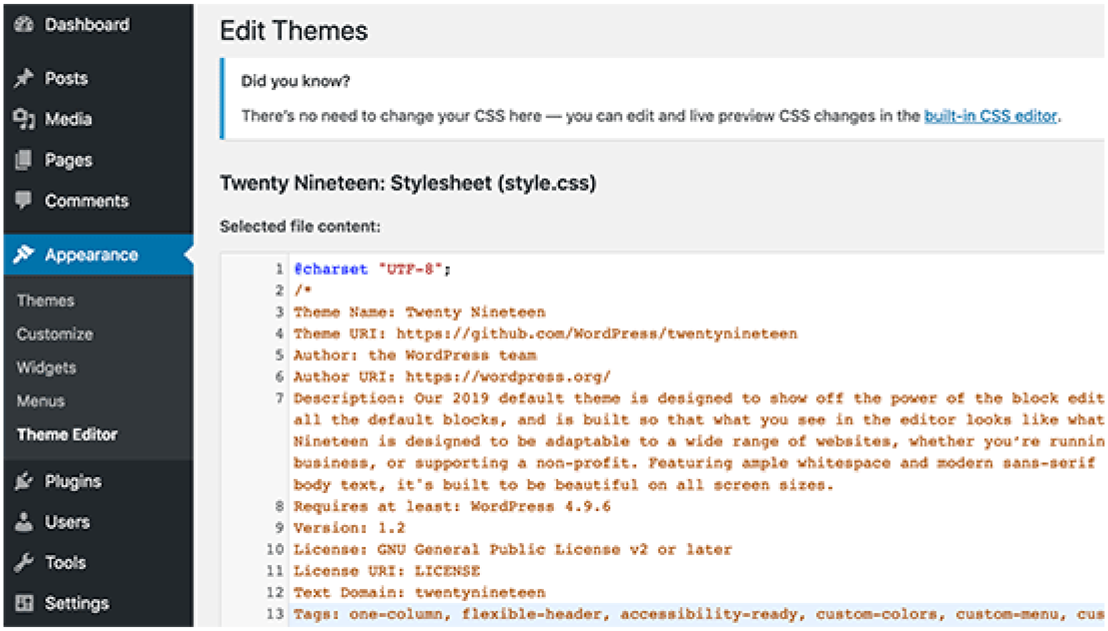
We have covered all three of these in our detailed guide on how to properly change your WordPress username (step by step).

Note: We’re talking about the username called “admin”, not the administrator role.

[Back to Top ↑]

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.



Edit Themes

Did you know?

There's no need to change your CSS here — you can edit and live preview CSS changes in the built-in CSS editor.

Twenty Nineteen: Stylesheet (style.css)

Selected file content:

```
@charset "UTF-8";
/*
Theme Name: Twenty Nineteen
Theme URI: https://github.com/WordPress/twentynineteen
Author: the WordPress team
Author URI: https://wordpress.org/
Description: Our 2019 default theme is designed to show off the power of the block edit
all the default blocks, and is built so that what you see in the editor looks like what
Nineteen is designed to be adaptable to a wide range of websites, whether you're runnin
business, or supporting a non-profit. Featuring ample whitespace and modern sans-serif
body text, it's built to be beautiful on all screen sizes.
Requires at least: WordPress 4.9.6
Version: 1.2
License: GNU General Public License v2 or later
License URI: LICENSE
Text Domain: twentynineteen
Tags: one-column, flexible-header, accessibility-ready, custom-colors, custom-menu, cus
```

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

```
// Disallow file edit
define( '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.

[Back to Top ↑]

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:

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

For more detailed explanation, see our guide on how to disable PHP execution in certain WordPress directories

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

[Back to Top ↑]

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.

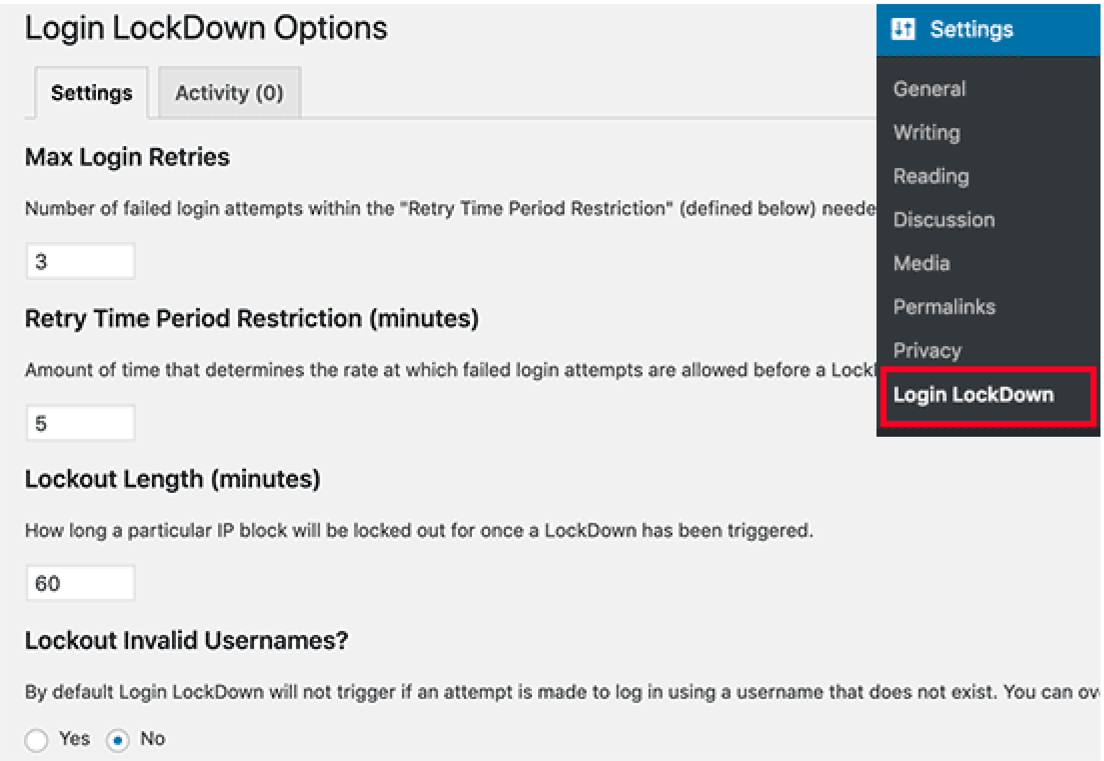
This can be easily fixed by limiting the failed login attempts a user can make. If you’re using the web application firewall mentioned earlier, then this is automatically taken care of.

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. For more details, see our step by step guide on how to install a WordPress plugin.

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

WordPress Security Guide



Login LockDown Options

Max Login Retries

Number of failed login attempts within the "Retry Time Period Restriction" (defined below) neede

3

Retry Time Period Restriction (minutes)

Amount of time that determines the rate at which failed login attempts are allowed before a Lockl

5

Lockout Length (minutes)

How long a particular IP block will be locked out for once a LockDown has been triggered.

60

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 ov

○ Yes ● No

For detailed instructions, take a look at our guide on how and why you should limit login attempts in WordPress.

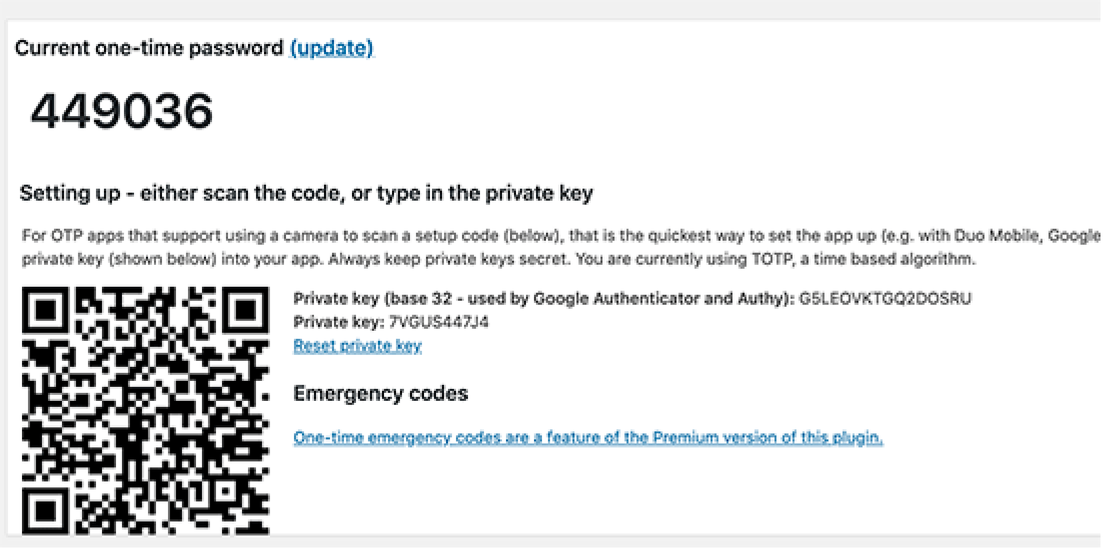
[Back to Top ↑]

Add Two Factor Authentication

Two-factor authentication technique requires users to log in by using a two-step authentication method. The first one is the username and password, and the second step requires you to authenticate using a separate device or app.

Most top online websites like Google, Facebook, Twitter, allow you to enable it for your accounts. You can also add the same functionality to your WordPress site.

First, you need to install and activate the Two Factor Authentication plugin. Upon activation, you need to click on the ‘Two Factor Auth’ link in WordPress admin sidebar.



Current one-time password (update)

449036

Setting up - either scan the code, or type in the private key

For OTP apps that support using a camera to scan a setup code (below), that is the quickest way to set the app up (e.g. with Duo Mobile, Google
private key (shown below) into your app. Always keep private keys secret. You are currently using TOTP, a time based algorithm.

Private key (base 32 - used by Google Authenticator and Authy): G5LEOVKTGQ2DOSRU
Private key: 7VGUS447J4
Reset private key

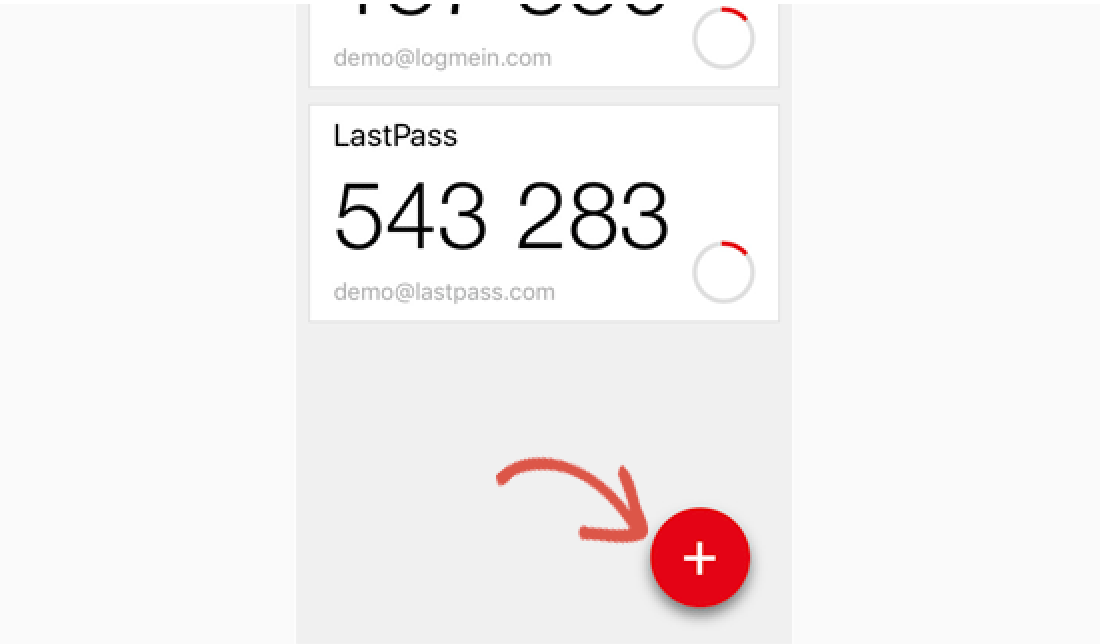
Emergency codes

One-time emergency codes are a feature of the Premium version of this plugin.

Next, you need to install and open an authenticator app on your phone. There are several of them available like Google Authenticator, Authy, and LastPass Authenticator.

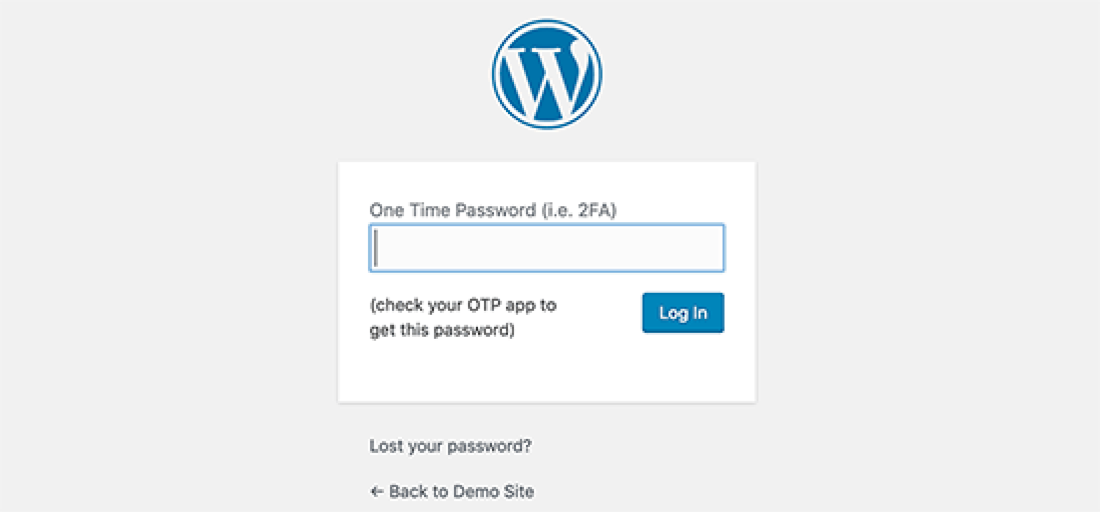
We recommend using LastPass Authenticator or Authy because they both allow you to back up your accounts to the cloud. This is very useful in case your phone is lost, reset, or you buy a new phone. All your account logins will be easily restored.

We will be using the LastPass Authenticator for the tutorial. However, instructions are similar for all auth apps. Open your authenticator app, and then click on the Add button.



You will be asked if you’d like to scan a site manually or scan the bar code. Select the scan bar code option and then point your phone’s camera on the QRcode shown on the plugin’s settings page.

That’s all, your authentication app will now save it. Next time you log in to your website, you will be asked for the two-factor auth code after you enter your password.


One Time Password (i.e. 2FA)
(check your OTP app to get this password)
Log In
Lost your password?
← Back to Demo Site

Simply open the authenticator app on your phone and enter the code you see on it.

[Back to Top ↑]

Change WordPress Database Prefix

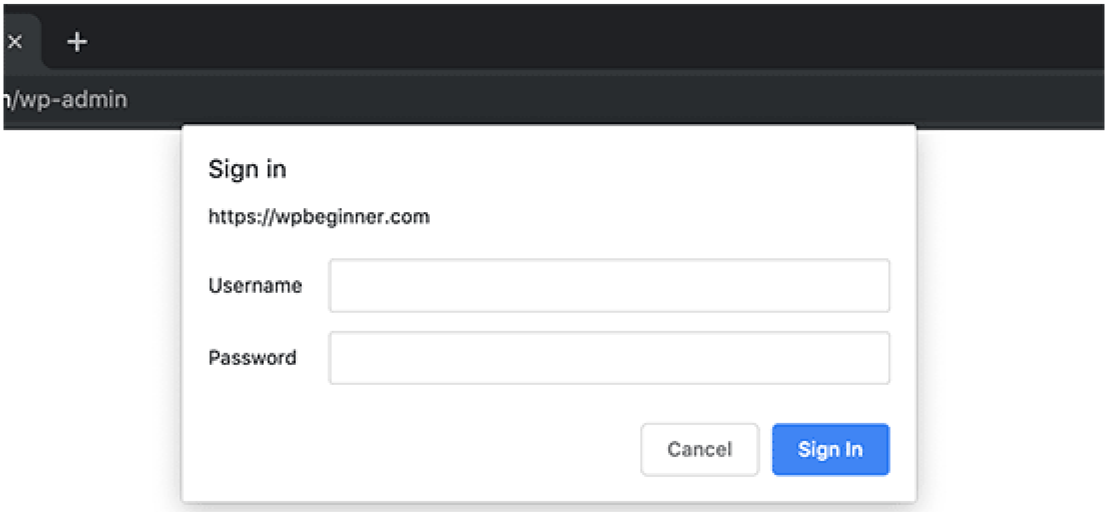
By default, WordPress uses wp_ as the prefix for all tables in your WordPress database. If your WordPress site is using the default database prefix, then it makes it easier for hackers to guess what your table name is. This is why we recommend changing it.

You can change your database prefix by following our step by step tutorial on how to change WordPress database prefix to improve security.

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

[Back to Top ↑]

Password Protect WordPress Admin and Login Page



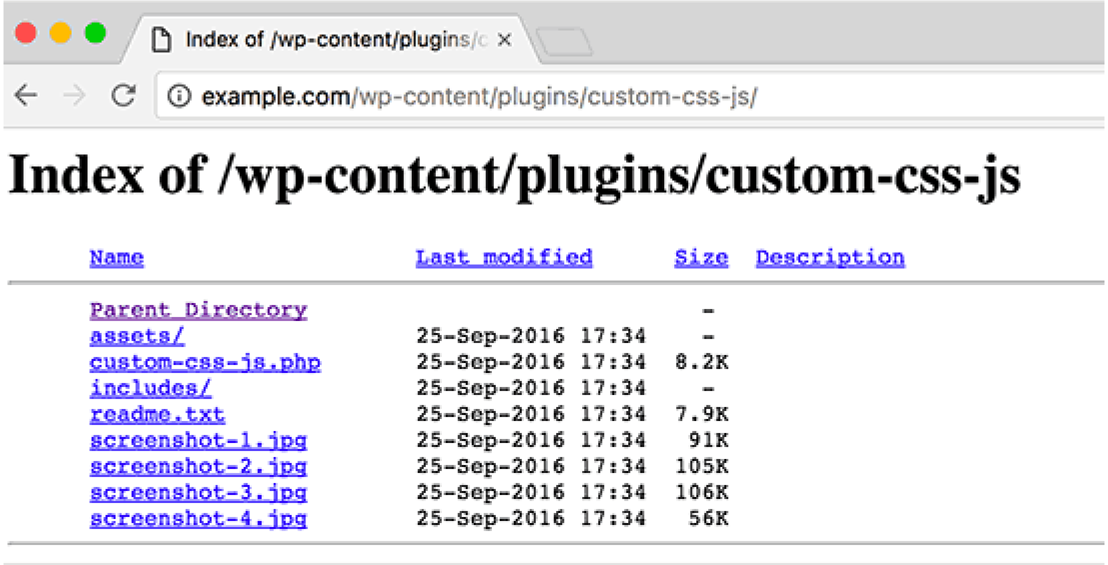
Normally, hackers can request your wp-admin folder and login page without any restriction. This allows them to try their hacking tricks or run DDoS attacks.

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

Follow our step-by-step instructions on how to password protect your WordPress admin (wp-admin) directory.

[Back to Top ↑]

Disable Directory Indexing and Browsing


Index of /wp-content/plugins/c ×
example.com/wp-content/plugins/custom-css-js/

Index of /wp-content/plugins/custom-css-js

```
Name                    Last modified      Size  Description

Parent Directory                              -
assets/                 25-Sep-2016 17:34     -
custom-css-js.php       25-Sep-2016 17:34  8.2K
includes/               25-Sep-2016 17:34     -
readme.txt              25-Sep-2016 17:34  7.9K
screenshot-1.jpg        25-Sep-2016 17:34   91K
screenshot-2.jpg        25-Sep-2016 17:34  105K
screenshot-3.jpg        25-Sep-2016 17:34  106K
screenshot-4.jpg        25-Sep-2016 17:34   56K
```

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. For more on this topic, see our article on how to disable directory browsing in WordPress.

[Back to Top ↑]

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.

Because of its 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, then we recommend that you disable it.

There are 3 ways to disable XML-RPC in WordPress, and we have covered all of them in our step by step tutorial on how to disable XML-RPC in WordPress.

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.

[Back to Top ↑]

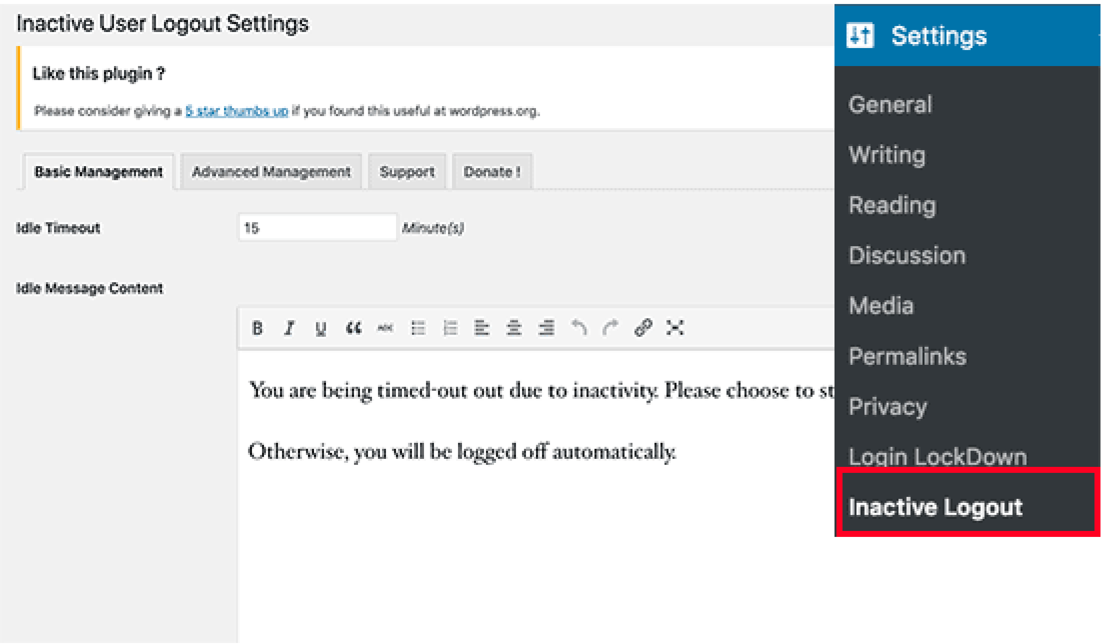
WordPress Security Guide

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 [Inactive Logout]() plugin. Upon activation, visit **Settings » Inactive Logout** page to configure plugin settings.



Inactive User Logout Settings

Like this plugin ?

Please consider giving a 5 star thumbs up if you found this useful at wordpress.org.

Idle Timeout: 15 Minute(s)

Idle Message Content

You are being timed-out out due to inactivity. Please choose to st

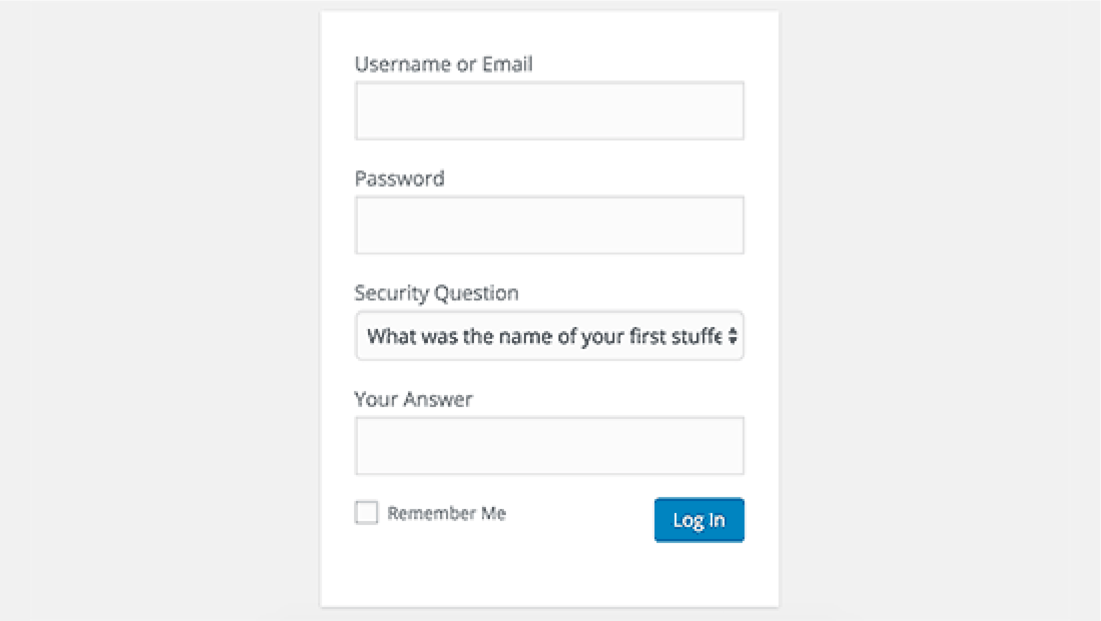
Otherwise, you will be logged off automatically.

Simply set the time duration and add a logout message. Don’t forget to click on the save changes button to store your settings.

[[Back to Top ↑]()]

WordPress Security Guide

Add Security Questions to WordPress Login Screen



Username or Email

Password

Security Question

What was the name of your first stuffe

Your Answer

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.

For more detailed instructions, see our tutorial on how to add security questions to WordPress login screen.

[Back to Top ↑]

WordPress Security Guide

Scanning WordPress for Malware and Vulnerabilies

If you have a WordPress security plugin installed, then those plugins will routinely check for malware and signs of security breaches.

However, if you see a sudden drop in website traffic or search rankings, then you may want to manually run a scan. You can use your WordPress security plugin, or use one of these malware and security scanners.

Running these online scans is quite straight forward, you just enter your website URLs and their crawlers go through your website to look for known malware and malicious code.

Now keep in mind that most WordPress security scanners can just scan your website. They cannot remove the malware or clean a hacked WordPress site.

This brings us to the next section, cleaning up malware and hacked WordPress sites.

[Back to Top ↑]

WordPress Security Guide

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.

For the adventurous and DIY users, we have compiled a step by step guide on fixing a hacked WordPress site.