Learn WordPress Security

March 23, 2022
This book is the result of a collaborative effort of a community of people like you, who believe that knowledge only grows if shared. We are waiting for you!

Get in touch with the rest of the team by visiting http://join.wikitolearn.org

You are free to copy, share, remix and reproduce this book, provided that you properly give credit to original authors and you give readers the same freedom you enjoy. Read the full terms at https://creativecommons.org/licenses/by-sa/3.0/
Chapter 1

Importance of Secure WordPress

1.1 Tips To Improve Security Of WordPress Site

WordPress security – 13 simple steps for improved security  WordPress sites are often attacked by vulnerabilities and security threats. The question about its safety is always elevated. Here in this post, we are discussing simple steps to attain maximum security.

It is a myth among the developers that by installing a security plugin, the WordPress site can be maintained. To some extent, it does so but you can’t take it for guarantee. Even a security plugin designed to deal with advanced security breaches might also give you a false sense of security. It might produce sluggish and unexpected results.

It is a well-accepted fact that WordPress website is always prone to cyber-attacks and vulnerabilities. Companies expecting higher outcomes from businesses can no more rely on the plugin’s false sense of security. For a WordPress website, security is its weakest link.

In this course, we are discussing various tips that can improve your Wordpress site security. Simple 13 steps to ensure security is elaborated here.

Table of content:
1) How is Word Press secure?
   i) Update WordPress, plugins and themes
   ii) Uninstall inactive plugins and themes
   iii) Use the right (restrictive) file permissions
   iv) Disable the built-in file editor
   v) Set a custom database prefix
   vi) Use strong usernames and passwords
   vii) Change security keys in wp-config.php
   viii) Disable XML-RPC
ix) Hide what WordPress version you are using
x) Use SSL and HTTPS
xi) Change WP-Admin URL
xii) Make sure to take daily backups
xiii) Choose a partner for taking security measures

How Secure is WordPress? All the languages at their core including WordPress are secure but much depends on the coders how well they incorporate the inherited features of a language. The best feature of WordPress is that it can rigorously deal with the common [wordpress vulnerabilities](https://en.wikipedia.org/wiki/Wordpress_vulnerabilities) and other security issues.

This means that if you can keep your WordPress installation updated there is a miniature risk that your website will be blemished by hackers. In most of the intrusion case, the most common reason is a loophole from the administrator’s side. The little negligence has opened the door for hackers. To avoid this, you must do the following:

Update WordPress, plugins and themes The new types of vulnerabilities and viruses are continuously getting introduced perhaps the most important security measure you can take is to keep your WordPress, plugins and themes up to date.

Since WordPress is an open-source platform, reading the code is easy. It is a great benefit to the dev community to improve coding skills. But at the same time, proves out to be the most dangerous feature as the hackers and others with malicious intent can read the code. They can plant vulnerabilities and use these to take control of other people’s websites.

Keeping this in mind, it becomes the moral responsibility of the WordPress developer to keep track of new vulnerabilities and make sure that he scans wordpress site periodically and remove any malicious code or malware in wordpress website. Every time a new one arrives, the site requires immediate update. To implement this, first of all, you must work with the updated version of WordPress. The latest version is under observation and any new vulnerability becomes easy to track. Therefore, build a habit to update WordPress, themes and plugins as often as you can.

Every time updating the site especially with the eCommerce application running on it becomes a tedious task. Moreover, you might land up increasing the load time of your website after updates. Therefore, keeping a backup before the update will keep you in safe mode.

A developer must always remember that WordPress core, plugin and themes are all up-to-date. It is important to do a periodic scanning of wordpress themes to detect malware so that our site doesn’t gets compromised. Otherwise it could lead to various kind of hacks such as Japanese keyword hack which is a spam-related hack that creates new pages with autogenerated Japanese text on your WordPress website. It may also lead to [suspension of google ads account](https://support.google.com/ads/answer/144837?hl=en) , run into issues with Google’s unwanted software policy and you may get a notice that
your google ads have been rejected due to Malicious or Unwanted Software on your wordpress site.

**Automatic updates** The automatic updates got introduced in WordPress 3.7, providing minor updates and security plugin and themes aches of WordPress that can be automatically installed on your website.

Adding the below-written code in functions.php file will activate automatic updates of themes and plugins on your site:

```php
add_filter( 'auto_update_plugin', '__return_true' );
add_filter( 'auto_update_theme', '__return_true' );
```

**Verify updates in a staging environment first**

For the safer side, it is recommended to always update on a staging site first and verify that updates work correctly. This would be a hassle-free action to ensure no surprise problems arise when updating your live website.

**Uninstall inactive plugins and themes** Intruders all the time look for the unused data, inactive plugins and themes. Hackers can exploit known vulnerabilities in inactive plugins and themes. The inactive plugins always keep getting alerts for an update which is even riskier for the working site.

From now onwards, we strongly urge to keep removing inactive plugin and themes.

**Use the right (restrictive) file permissions** In the Word Press, the administrator can provide the file permissions to read, write and modify the pages. He has the right to restrict the access to make use of the internal security provided by Word Press. The strict way of allocating file permissions is an indication to the hackers that modifying your site is not easy. any easy technique will not work.

3 numeric digits specify file permissions such as where each digit represents a user group and what that group has the permission to do.

The first group from the left is “user” (or “owner”) rights, the second is “group” rights and the third group is “others” rights.

Simply explained, one can say that the higher the number the more rights the user has. For the interested, here is an explanation of what the different numbers actually mean:

- 4 = read (r)
- 2 = write (w)
- 1 = execute (x)
- 0 = no permission (-)
- Read + write + execute = 7
- Read + write = 6
- Read + execute = 5

All folders should have 755 or 750.
All files should have 644 or 640, except wp-config.php that should have either 440 or 400 to prevent anyone else from access it.

No folders should ever be set to 777, giving all users full rights. It should never be necessary as the PHP process is run by the file owner, and thus it can write in folders with 755.

Unyielding file permissions are essential in a “shared hosting” environment, where you share a server with other websites. You have to be sure of protecting your files from other users who are sharing web space with you.

**How to change file permissions?** The FTP client interface helps to change the file permissions. The FTP like FileZilla can be used for this purpose. Just right-click on the file or folder you want to set the permissions for and press “File permissions…”

**Instruction to change file permissions in FileZilla**

**Disable the built-in file editor**

Word Press comes with own built-in editor for themes and plugins. The convenience to edit files on your website directly in WP-Admin is bliss, but it can also pose some risks.

When the built-in file editor is enabled, administrators and developers can edit the code in the themes and plugins directly in the browser. It poses a potential security risk because it is prone to mistakes. The consequences can be dangerous as the entire page might stop working after making changes. Besides, it also gives hackers quick access to all files of your website.

The experts recommend to completely disable this built-in file editor and instead edit via files over SFTP. The built-in file editor can be easily disabled in wp-config.php by adding the following code snippet:

```php
define('DISALLOW_FILE_EDIT',true);
```

**Set a custom database prefix**

WordPress files start with a prefix ” wp” in front of all the database tables. The hackers aware of the same try to attack files with the wp prefix. However, if you change the prefix, you can protect your file from hackers.

In this way, no doubt you will increase the protection level, but changing the prefix especially for the existing files is not risk-free. Thus, we recommend that changing prefix for the new installation of WordPress is a wise decision. but don’t try doing it for the old database prefix.

**Use strong usernames and passwords** Intruders entry to a WordPress site by cracking passwords is the most tried out process. Simple and common password setting is like having a house with the main gate open. There are chances for unauthorized persons to easily access your website through a so-called brute-force attack. The attacker submits a large number of different passwords until they crack it. A stronger password will fail the hacker’s attempts to access the site.

People with the technical knowledge understand the need for it but the common
users keep traceable passwords. The companies list common passwords that can be easily cracked. Some of them are:

- 123456
- 123456789
- qwerty
- password
- 1234567

However, keeping a long and complex password is the first security measure that will prevent an attack. It is also quite common for people to use the username “admin” for their administrator account. Instead, for extra security, it is recommended to use a different username, making it even more difficult for a hacker to guess the correct username and password.

Passwords are security keys that should be unique and unbreakable.

**Change security keys in wp-config.php**

WordPress security keys are a collection of randomly generated variables to improve the encryption of data stored in visitors and administrators cookies.

Four special security keys are AUTH_KEY, SECURE_AUTH_KEY, LOGGED_IN_KEY, and NONCE_KEY.

At the time of the WordPress installation process, these keys are generated randomly for your website. In case, you move from one web host to another, or if you have taken over your website after another owner, then generating new security keys would be a good idea.

The keys can easily be replaced at any time. Their main purpose is to provide login and logout facility to your website. A smart tool can be used to generate security keys on WordPress.org and then paste them into wp-config.php.

Replacing the security keys in wp-config.php after moving to a new host is a smart choice.

**Disable XML-RPC**

To communicate with other systems WordPress used XML-RPC feature. In recent years, the fuse of this feature has been steadily declining. In future, it can be completely removed and replaced with WordPress’s API instead.

Today, XML-RPC has become a popular “tool” for hackers, thus its use is minimized. As it allows testing hundreds of password combinations with a single command.

You can either disable XML-RPC using a plugin or by pasting some code into one’s theme’s functions.php file:

```
add_filter( 'xmlrpc_enabled', '__return_false' );
```

.. or even better is to disable it using .htaccess:

```
<Files xmlrpc.php>
order deny, allow
```

```
deny from all
</Files>

**Hide what WordPress version you are using**  Another gateway for the hackers to get the information of the Word Press version you are using on your website by incorporating in the site’s HTML code, The older version are already having many vulnerabilities so try to install the latest version of WordPress.

However, maintaining the WordPress security is purely the developer’s job but we recommend to hide the version number. It will prevent direct attacks that can destroy your website’s working.

The following code will hide WordPress version in functions.php:

```php
function wp_version_remove_version() {
    return ";
}
add_filter(‘the_generator’, ‘wp_version_remove_version’);
```

The outcome of the above discussion is that you must hide the version of Word-Press.

**Use SSL and HTTPS**  The web administrators are aware of the fact that using SSL, you can use the encrypted protocol HTTPS instead of old and un-encrypted HTTP. The benefit is when you log in on a page with HTTPS, the information is encrypted, including passwords and other sensitive information. The encryption techniques make it impossible for anyone else to snoop. The use of SSL has an advantage in SEO as the search engines prefer HTTPS requests over HTTP.

An SSL certificate for your WordPress website is a necessity especially if the site is providing eCommerce services. An initial expenditure cud is fruitful in the long run.

**Change WP-Admin URL**  All WordPress sites initially use the same URL for WP Admin, for example, secure.wphackedhelp.com/ /wp-admin. One budding issue with this is that everyone knows of this address, including bots and hackers. if you modify the URL to WP-Admin, your site will be less vulnerable to attacks.

However, it is not a long run and effective solution. However, it will make it more difficult for hackers to access your site.

The URL of WP-Admin is easy to change. Try doing it or contact our team to help you!

**Make sure to take daily backups,**  Backing up is an administrative action that comes under the site maintenance plan. It will not protect your website from hackers but can act as a resource to restore your website if an attack takes place.

There are no hard and fast rules to follow while taking backup. It entirely depends on the administrator/ developer to plan it regularly especially before installing a
plug-in or updating the theme.

No matter what action or security measures you take, your website will never be 100% secure. Thus, one should always make sure that backups of one’s website are taken regularly.

We strappingly suggest taking regular backups of your WordPress site.

**Choose a partner for taking security measures**  
When it comes to security and WordPress, numerous factors sit deeper than the website itself. Several security measures need to be taken at the server level, of which your web host is responsible. At WP Hacked Help, they take security very seriously and always have a safety mind in everything we do.

It is vital to tie up with a company that you can trust. They provide a WordPress malware scanner tool that can quickly clean your WordPress website. Regular cleaning can prevent the site from malware.

**WP Hacked help** is one of the best wordpress malware scanners out there. Besides, we are a top-end WP security and Management service company leveraging security services to Word press Websites.

Our WP malware scanner not only cleans your site but helps you in a situation where your site can be shut at any moment. We facilitate rescue hacked websites.

**Final Closing Remarks**

In the closing remarks, it will be worth mentioning again that WordPress is the most popular platform for building websites despite having vulnerabilities and security threats.

The above-mentioned steps prove that maintaining site security is not a tedious task in WordPress. However, web critics forget to mention that the security of a website depends on many factors. The server involvement, network, web hosting company are some of the most common ones. Therefore, it is important that you either have a very good understanding of IT security yourself or that you choose a company that takes security seriously.

Daily backups of one’s website are also an absolute must so that you have something to fall back on. The proactive action also helps to prevent your website.

If you have any questions about WordPress security then you are welcome to approach us at WP Hacked Help website.

**Further Reading:**

- [https://wordpress-security.glitch.me/](https://wordpress-security.glitch.me/)
- [https://worksheets.codalab.org/worksheets/0xa1f19cd13b3e4b0a8b12ebf5644b2922](https://worksheets.codalab.org/worksheets/0xa1f19cd13b3e4b0a8b12ebf5644b2922)
Chapter 2

Text and image sources, contributors, and licenses

2.1 Text


2.2 Images


2.3 Content license

- [Project:Copyright Creative Commons Attribution Share Alike 3.0 & GNU FDL]
- Creative Commons Attribution-Share Alike 3.0