David Olliver

Political news, Tech news and much more

15 effective ways to secure your WordPress site

Miljan Zujić · Saturday, March 25th, 2017

No one wants to have the experience of hacked website and losing many years of work and adding content on it, but it actually happens to many people. Research shows that every day 37,000 websites get hacked, of which 25.4% are based on the **WordPress** system.

WordPress security is a special topic; after you install WordPress, choosing a difficult to remember user names and easy passwords, really are not the only things about which you should care. The poorly made theme, wrong installed plugin, incorrectly or incompletely protected files may cause hacking your site overnight.

Whether you are a WordPress novice, or to use the CMS from the very beginning of its existence, this article can help you to improve the security of your website using WordPress. These tips you will not find on popular articles "how to protect your website", but be sure that these will save your WordPress website one day.

1. **Regular update to the latest version**

It often happens that WordPress offers a new version – do not ignore it! It's vital that the website is up to date in terms of version, plugins, and themes which safety is raised at a higher level with a new version. WordPress will notify you when a new version is available and you can easily perform an update.

In order to enable the automatic update of WordPress version in the *wp-config.php* file, add the following line of code:

1. Enable all core updates, including minor and major:
2. define ('WP_AUTO_UPDATE_CORE', true);

There is also the option to set the automatic updating of themes and plug-ins, but our advice is to do it manually.

2. **Hide WordPress Version**

As usual, **WordPress** displays the version of the system you have currently installed.

This helps to establish the exact number of sites worldwide which use a particular version of **WordPress** worldwide. However, it can be useful for WordPress, but not for a user of WordPress. Bots can scan your code and identify which version you have at the moment, and use it against you, using known weaknesses and failures of that version.

To hide the number of the current version of WordPress, add this code to your functions.php file:

```
add_filter ( 'the_generator', '__return_null');
```

3. **Turn off plugin and theme editor**

WordPress allows its users to edit the structure of the code, on themes and plugins, directly through the admin panel. However, as far as this benefit seems excellent, just one mistake can cost you a lock from the entire administration and loss of your website. Also, hackers can infiltrate infected content in your theme or plugin to allow themselves the backdoor access.

You can protect yourself by disabling editor of plugins and themes and leave the option to edit files – only those with FTP access.

You can do this by adding the following code to your *wp-config.php* file:

```
Define ( 'DISALLOW_FILE_EDIT', true);
```

4. **Test themes and plugins**

Themes and plugins can contain certain security vulnerabilities that hackers can exploit. Use only verified themes and plugins that meet all the rules of the WordPress codex.

We suggest these two plugins for testing themes and plugins:

- Theme Check
- Plugin Check

5. **Delete inactive/old themes and plugins**

WordPress themes and plugins that are installed but not in use can be a potential security risk, and in case they are not up to date, they may have security vulnerabilities that hackers can exploit.

It would be the best to remove all themes and plugins that are not in use and keep only those that are necessary.

6. **Enable Two-Factor Authentication**

Two-factor authentication is becoming one of the most popular ways to protect online accounts, and soon, we believe, almost all the websites will ask from their customers to add this type of security.

Given that WordPress has no built-in Two-Factor Authentication, you can install one of these plugins, to enable it:

- Google Authenticator
- Authy
- Clef
- Rublon

7. **Limit the failed login attempts**

There are many ways in which hackers try to take control of your website, and one of the most common technique is called bruteforce attack; when a hacker tries different combinations of user names and passwords – over and over again until he enters the right combination and gains administrator access.

By default, WordPress does not have any kind of protection against such attacks, but if you install the plugin WP Limit Login Attempts, which limits the number of logins with a single IP address, hackers will much harder be able to take control of your website in this way.

8. **Scan your code occasionally**

Files, themes, plugins, links and similar elements that are harmless at first glance, can be used to take control of your website. Do not wait for hackers to exploit the weaknesses of your site, to take safety measures. Install the plugin to regularly scan your code, which will promptly notify you if there are unknown file changes.

One of the quality plugins for this purpose is Wordfence. It allows you to manually or automatically scan your website and also automatically notifies you if there are any suspicious activity on your site.

It also sends information about suspicious comments and compares your themes and plugins with the WordPress repository to alert you if there are changes of versions of themes or plugins you have installed, and which could be used for the backdoor approach mentioned before.

Other plugins with which you can scan your site are:

- Sucuri Security Scanner
- Acunetix WP Security
- iThemes Security (known as “Better WP Security”)

9. **Change hosting provider**

Although this might sound like simple advice, it has a lot of weight. Research shows that 41% of hacked WordPress websites are hacked because of the security flaws of hosting platform on which they were located. The disturbing information is that the

more sites that are on WordPress, gets hacked due to the weaknesses of hosting, than due to the use of weak passwords for access to the administration.

Your hosting provider can play a key role in whether your site will be hacked or not. We recommend you to choose hosting providers who dedicate a lot of time to improve the security of their servers. Some of them offer unlimited space and traffic, as unlimited e-mail addresses and databases, and some of them offer a free renewal of your domain every year, as long as you pay for the hosting service, which can about cost $4/month. When ordering, you can use promotional coupons to get a lower price.

10. **Disconnect PHP reporting errors**

When a theme or plugin on your site creates a specific problem, the PHP error reporting can help by showing you a message that explains the reason for errors or incompatibilities. However, this convenience has one disadvantage; when PHP errors are reported, the report displays the full connection of files from the server to the end user or a visitor, releasing the information that hackers can use against you.

You can protect yourself by turning off the PHP error reporting. Simply add the following code to your wp-config.php file:

error_reporting (0);

@ini_set ('display_errors', 0);

11. **Work on licenses of WordPress files**

When it comes to increasing the security of your site, one of the key things is to make sure that your WordPress files have adequate permission or server permission. This will make it harder for hackers to manipulate with files of your themes, plugins, and CMS.

It's very important that permissions of the WordPress folder to be set to 755 or 750; permission of files should be set to 640 or 644; and permission of files wp-config.php should be set to 600.

12. **Make regular backups**

Even big corporate websites, with teams of security experts – are being hacked. Even if you are sure that your website is more secure than 99.9% of other sites, things can still go wrong. The best security you can have against hackers is a quality backup. Make sure you make backups of your site often, and if possible, on a daily basis. By this way, if your website is hacked, you have saved the files and you may easy bring back all to where it was.

Here are some of the best backup plugin for WordPress:

- BackUpWordpress
- BackUp Guard
- VaultPress

- BackUpBuddy

13. **Restrict access to login page**

One of the best ways to protect your WordPress website is to completely block the access to the wp-admin folder, and wp-login.php page. This is recommended only if you sign in on administration using a single IP address that does not change (you do not want to restrict the access to yourself). It's possible to grant access to multiple IP addresses but it's necessary to have IP address recorded.

To restrict access to your login page, add this code to your .htaccess file:

```
<IfModule mod_rewrite.c>

RewriteEngine on

RewriteCond% {REQUEST_URI} ^ (. *)? Wp-login \ .php (. *) $ [OR]

RewriteCond% {REQUEST_URI} ^ (. *)? Wp-admin $

RewriteCond% {REMOTE_ADDR}! ^ Your IP address $ 1

RewriteCond% {REMOTE_ADDR}! ^ Your IP address $ 2

RewriteCond% {REMOTE_ADDR}! ^ Your IP address $ 3

RewriteCond% {REMOTE_ADDR}! ^ Your IP address $ 4

RewriteCond% {REMOTE_ADDR}! ^ Your IP address $ 5

RewriteRule ^ (. *) $ – [R = 403, L]

</ IfModule>
```

Note that in the code is the phrase "Your IP address" with numbers from 1 to 5. Instead of these sentences add the IP address of your choice. You can remove existing lines, or add more lines depending on how many IP addresses you want to allow access.

14. **Prevent access to files with .exe extension**

Executable files can create problems, as they often contain malicious code that can install viruses to your computer. They could be blocked, of course, the use of .htaccess.

Add the following code to your .htaccess file:

```
# deny all the .exe files
```

> <files ” *. Exe “>
>
> order deny, allow
>
> deny from all
>
> </files>

This prevents any .exe files to access the server raising security to a higher level.

15. **iThemes security – currently the best security solution**

Almost all the items we mentioned above can be solved with the help of iThemes Security plugin. This plugin really combines all the most important segments of protection WordPress website with over 30 different ways of protection from hackers. All settings are made directly from the WP dashboard so that users with less experience may find it easier to cope.

This entry was posted on Saturday, March 25th, 2017 at 9:00 am and is filed under Tech
You can follow any responses to this entry through the Comments (RSS) feed. Responses are currently closed, but you can trackback from your own site.