5 WordPress Security Best Practices

WordPress being the most popular web publishing platform with 59% market share, their websites are constantly under attack. Yet sadly, they lack notoriously when it comes to security. More than fifty thousand WordPress websites are getting hacked everyday. As a **website owner**, be a **blogger** or a **developer**, it is your prime concern to secure your WordPress website. You may contemplate as to why should a hacker would be interested in your website. Well, not all hackers are interested in your data or the site content. Let us find out what's in it for them, how the websites are being hacked and top practices to protect your website from vulnerabilities in the upcoming year, 2018.

Why and How would your website be hacked?

Hackers do not follow a defined logic to hack into a website. Irrespective of how small or large your traffic is, they see you as a target. These are the possible benefits they consider out of their attack attempts.

5 WordPress Security Best Practices

1. Hackers would want **to redirect your website visitors** to other websites which may pay them for helping generate traffic to these other websites.
2. In order to obtain information to their benefits, hackers may use your website to further **infect your visitor computers** with malicious software like key loggers, ransom-demanding malware, etc.
3. Hackers can also completely take charge of the your website's server and perform brute force or DOS / DDOS attacks, **send spamming emails**, etc. This would further lead your website to be **blacklisted** for use.

Most of the attacks done by the hackers are automated. Specific human attacks are only performed on websites which deal with confidential or financially critical data. While these attacks are rare,

5 WordPress Security Best Practices

these attacks are sensibly planned and hence perilous. Hackers usually use programs called **bots and botnets** to find vulnerabilities in the websites and further compromise their security. While bots are used to target smaller number of websites, botnets are used for attacks on a larger number of websites at the same time. Hacks on most of the WordPress websites are performed via botnets.

The top security issues or common entry points for a hacker, has been depicted in the infographic shown below.

As per the statistics illustrated above, the highest percentage of hacks happen via vulnerabilities in the **hosting platform**. Ill-protected plugins and unsafe themes constitute another major security loophole in the WordPress websites, followed by login issues like weak passwords.

5 WordPress Security Best Practices

So how to keep your website safe from these vulnerabilities?

Analysis of the above information led us to formulate the ultimate security best practices, you would need to follow, to ensure that your website is secure in the upcoming year.

Practice 1. Ensure your website is hosted securely

Given this being the leading cause of security violations for the WordPress platform, this is the first most critical step to be considered. If a shared hosting provider does not maintain effective isolation between accounts, there are chances that your account will be compromised, should there be any attack on the shared server. Hence **choosing a reputable and trusted web-hosting service provider** is required who understands the risks of cross-contamination, segregates the website accounts and configures the security permissions of each account present in their WordPress-optimised environment. If dedicated hosting is not an option, then make sure you use **SiteGround** or **BlueHost**, as these providers are known to have security-focused features.

5 WordPress Security Best Practices

Practice 2. Update and maintain your core WordPress platform and the associated themes and plugins

Security gaps in WordPress' themes and plugins together constitute to a whopping 51% of the reasons of compromises to WordPress websites. This makes it obvious to ensure that this aspect is critically dealt with, using the suggestions as below:

5 WordPress Security Best Practices

(i) Update your WordPress core

While updating the core WordPress installation is the most obvious activity to perform to fortify your website, an enormous eighty-six percent of WordPress installations still run on outdated versions. Post the 3.7 release, WordPress provides automatic update features and hence maintenance at your end becomes far simpler. All you have to do is to configure the wp-config.php file to include the following line.

```
define( 'WP_AUTO_UPDATE_CORE', true
);
```

However, remember to perform an automated testing in advance to ensure the auto-updates do not break your website, in which case, continue with the standard settings and manually update the core website.

(ii) Hide the WordPress version number

Uncovering the WordPress version is an easy task for the hackers, as the tag in your website's head section shows off the current running version of your CMS. In cases of use of an outdated version, hackers

will leave no stone unturned to exploit this find of theirs. To disable this feature, you need to update the functions.php file to reflect the following:

```
1define( remove_action('wp_head', 'wp_generator');
```

(iii) Maintain your WordPress plugins and themes

With over half of attacks happening through ill-protected plugins and themes, them being an opening to obtain administrator access for the website, security needs to be extended to these as well. Auto-updates for these are easy to be performed, requiring the insertion of the following lines of code to your wp-config.php file:

For plugins:

```
1add_filter( ‘auto_update_plugin’, ‘__return_true’ )
```

For themes:

```
1add_filter( ‘auto_update_theme’, ‘__return_true’ )
```

To further **reduce the possibilities of vulnerabilities** and hacker attempts, a few other aspects need to be kept in mind while dealing with themes and plugins as below:

- Eliminate unused or old plugins and themes
- Check before installation of plugins / themes from untrusted sources
- Do not download paid or premium plugins and themes for free

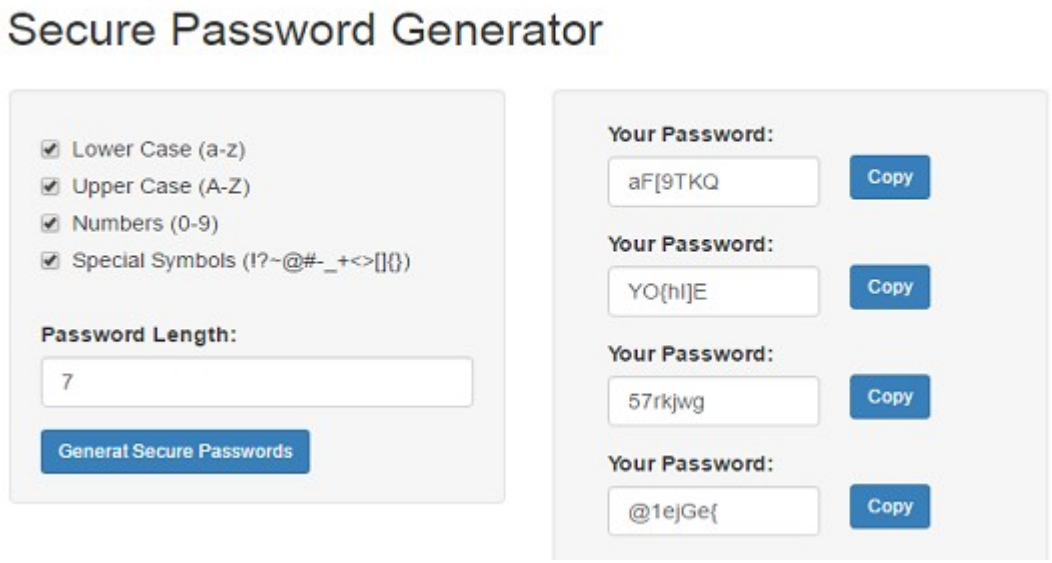
Practice 3. Secure your user / admin login to prevent brute force attacks

To ensure minimum viable security, you need to secure your login page. With your WordPress URL being public, hackers may try to brute force their way in into the **backend** of the website. As a first line of defence, you would need to adhere to the below mentioned practices

5 WordPress Security Best Practices

to enable login protection and save your private data from unwanted hacker attempts.

(i) **Use strong passwords for logging into your website**. You can check your password strength and generate a complex one using a secure password generator. WordPress also helps generate a strong password in its account management section. Also, the passwords need to be changed at periodic intervals (quarterly at a minimum).



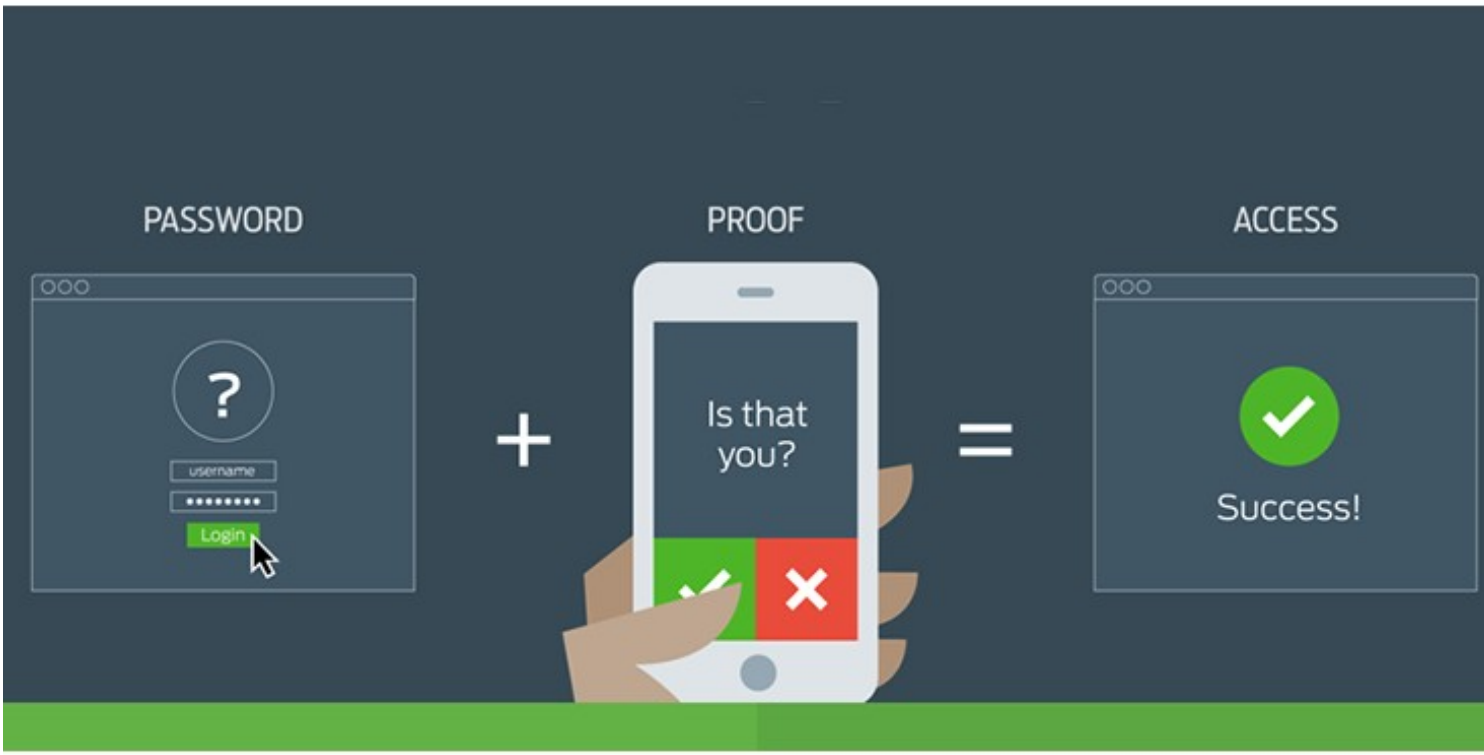
(ii) **Using the default username “Admin” for logging in is completely prohibited**. It is suggested to register another user and provide this new user with all administrator privileges. The previous user can be either locked, deleted or assigned to a Subscriber role.

(iii) **Using an email ID to log in** is a more safer approach than following the traditional method of having usernames to log in. This is based on the general assumption that usernames are easily guessable, or can be hacked into, in comparison to email IDs which are a little more trickier to predict.

(iv) **Incorporate two-factor authentication for increased security**. The two-steps shall ensure that along with your password, the unique token / OTP received only by you (as an SMS to your

5 WordPress Security Best Practices

phone) will be your combination for logging in. The best option is to use the **Google Authenticator plugin**, provided by WordPress.



(v) **Remove the default setting of unlimited logins** using limited login attempt functionalities, provided by plugins like Cerber Security and LockDown. The iThemes security plugin is also a recommended solution to this problem. In cases of failed login attempts, it immediately bans the attacker’s IP address, locks the site and notifies you of this unauthorised activity.

(vi) **An additional security question** during login (the more personal it is, the more trickier it is to hack), is an effective method to enhance your login.

(vii) **Customize your login URL** to restrict access to the login page via wp-admin and wp-login PHP files. Along with securing the login credentials (as in the above steps) and now with the changed login

5 WordPress Security Best Practices

URL, almost all brute-force attacks can be prevented. Plugins like iThemes Security can help achieve these settings. Examples of modified URLs can be as follows.

- Change `wp-login.php` to something unique; e.g. `my_new_login`
- Change `/wp-admin/` to something unique; e.g. `my_new_admin`
- Change `/wp-login.php?action=register` to something unique; e.g. `my_new_registeration`

Practice 4. Harden your WordPress database

Even if you have taken the above points into consideration and no matter how secure your website is, enhancing the protection of your database will ensure greater security in times of any unwanted attacks. WordPress uses mySQL as its database management system, and the below-mentioned practices will boost up your overall website’s security.

(i) Backup your website on a regular defined periodicity

In reality, inspite of taking all the requisite security measures, it is difficult to ascertain that your WordPress website will never be prone

to attacks. Hence, the best way to mitigate this explicit risk and reduce the impact of a disaster is to periodically backup your website. This gives you assurance that your data is not lost and can be recovered in case of any emergency. **Real-time backup of data** is always the best, which if not, data should be backed up at least daily. While there are several premium and paid plugins serving as backup solutions of your website, choosing a secure cloud offering like Google Drive or Dropbox might also be a wise consideration. In most cases, your hosting provider could also help keep your site's copy in a safe location.

(ii) Make your WordPress database table prefix unique

Default database table prefixes eases the conduct of SQL injection attacks to your website and hence it is important to **modify them** to something **difficult to decipher by a hacker**. As you would have observed, 'wp-' serves as the default table prefix for any WordPress website. Examples of changed prefixes could be 'wp007AS-' or 'wpnew1-'etc. However, please refrain from choosing the name of your domain as your new prefix. To customize your table prefix, you would need to update it in your wp-config.php file. An alternative to this could be using an effective plugin to perform the same activity, like iThemes Security or WP-DBManager.

Practice 5. Fortify your WordPress Administrator and Control panels

The most targeted attacks also spread to users having admin or super user privileges, and to the associated administrative files. Hence strengthening their security cannot be ignored. The key security measures in this domain are listed below:

5 WordPress Security Best Practices

(i) Secure access to the wp-admin directory

Since this directory is the heart of your website, it is one of the prime targets for attacks. An additional layer of HTTPS authentication (HTTPS providing stronger encryption than HTTP) will password-protect your wp-admin directory. In this method, you will need to **provide two passwords** for accessing the WordPress dashboard – one to restrict access to the login page and another to the admin panel. To do this, you need to have a .htpasswd file created for your website. This can be done manually via a set of directives, or via the AskApache Password Protect plugin.

(ii) Secure the wp-config.php file

While the admin directory is the most crucial for your website, the config file is similarly important, and hence access to this has to be restricted. To achieve this, all you need to do is to move your wp-config.php file from the root directory to a level higher up, thereby hiding this file yet being accessible to your web server.

5 WordPress Security Best Practices

(iii) Enforce HTTPS (SSL encapsulation in HTTP) for login and admin activities

To enable encryption during data transmission and increasing authenticity of login hosts, it is required to secure your WordPress site with HTTPS. Not all areas are needed to be safeguarded. The admin area page (wp-admin) for the sensitive data in transit and the login form page (wp-login) for authorised login credentials, need to have SSL via HTTP implemented. This can be accomplished by defining the boolean states for the two constants in the wp.config file.

```
1add_filter(define('FORCE_SSL_LOGIN', true))
```

```
1add_filter( define('FORCE_SSL_ADMIN', true))
```

(iv) Disable / remove user primitive user accounts

Remove users who are inactive in the system for a long period, especially the ones who had write access / administrator access to your WordPress website. In cases where removal is not an option, reducing their privileges to a ‘Subscriber’ role, with only read / display access could be considered.

It is recommended to implement a wide array of additional key file and directory level security configurations to fortify your WordPress security.

Final Words

Having a WordPress hack is one of the most dreaded scenarios for any website owner, and we have emphasised how important it is be proactive in maintaining the security of your website. The above list, if followed carefully, is aimed at delivering a website with heightened security. However, to a user’s delight who finds manual configurations difficult, there exists **multiple one-stop solutions** which implement the same safety features. The most recommended and security-

5 WordPress Security Best Practices

centric platforms and plugins are – **iThemes Security**, **Sucuri Security** and **Wordfence**. With this kind of protection in place, not only are you better prepared for any attack, but also ready to combat attacks to cause lesser harmful impacts to your website.