8 in 1 tips for WORDPRESS SECURITY

Their Issues & Their Solutions

CHETAN SONI

Cyber Security Expert & Penetration Tester

chetansoni@live.com, www.chetansonisecurityspecialist.com

1. Securing the htaccess file

The Security Issue: Hackers can use the ***.htaccess*** file to redirect the malicious sites from the URL. They will also try to hide their secret code at the bottom of the file generally called as footer. They may also change the permissions of the .htaccess file to stop editing the file. With the help of this file, hacker can easily redirect the whole site to any other malicious URL and the site will be blacklisted by some domain providers like Yandex, Google and MacAfee.

The Security Solution: Normally for WordPress sites, there are two types of servers are there: Apache and Nginx. For Apache, it uses htaccess to prevent unauthorized access to certain parts of the website. And the file **wp-config.php** should never be accessed directly and it contains the confidential database details, it should block it from htaccess file too. This can be done by adding the some lines to your htaccess file.

```
<Files .htaccess>
order allow,deny
deny from all
</Files>
```

.htaccess is a configuration file that allows you to override your server's global settings for the directory that it's in, by limiting file access.

While you can install various security plugins, monitoring services and CDN services (Content Delivery Networks) which filter the traffic, configuring .htaccess file so it strengthens the WordPress security is a good step toward that **peace of mind** every website owner needs.

2. Disabling the Theme/Plugin Editor

The Security Issue: In the WordPress Dashboard, there is an option to edit the theme/plugins files. This option is not to be used by normal users under any circumstances. However, for hackers it can be extremely dangerous.

For example, suppose a hacker is able to login to your site using some exploit or rootkit, then one of the easiest mechanisms for them to add malware to the site will be by editing existing files. So disabling the ability to edit **PHP** files in the WordPress themes and plugins is one way to keep a persistent hacker from making significant changes to the WordPress website without your permission. Also, the files can be edit via FTP and completely eliminate using the WordPress admin dashboard to make changes to PHP files.

The Security Solution: By disabling the option to edit these files, wp-config.php is the best method for it; well you can also use some security plugins to disable same things.

To accomplish locking down the edit ability of PHP files in the WordPress admin area:

1. First, navigate to the ***wp-config.php*** file. To edit this file, there are so many editors are there like Filezilla or SmartFTP. After successfully logged in, navigate to the WordPress root directory. The **wp-config.php** file will be in the main WordPress directory.
2. Now add the following line of code to the wp-config.php file: `define('DISALLOW_FILE_EDIT', true);` and save it.

3. Protect the wp-config file

The Security Issue: The single most important file in the entire WordPress Installation is ***wp-config.php***. The WordPress website is made up of two elements: a WordPress database, and its files. Wp-config.php is the one element that links the database and files together. Hackers try to access this file to destroy the whole website using some methods called as **Symlinking**.

The Security Solution: Change the permissions of the file, so that only a Web server can access it. Further this file should not be modifiable/writable by anybody. Hence the preferred permission here would be to use: **400 or 600** depending on your server. Permissions can typically be changed by using FTP or cPanel.

This file can also be secured by using some codes in htaccess file,

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```

We can also move the wp-config.php file up one directory where **wp-includes** are to further tighten security. This method should probably only be used by those of you that know the implications.

4. Change Table Prefix:

The Security Issue: WordPress Database is like a brain for the entire WordPress site because every single information is stored in there thus making it hacker's favorite target. Spammers can run automated codes for SQL injections and Cross site scripting. Well, unfortunately many people forget to change the database prefix while they install WordPress.

This makes it easier for hackers to plan a mass attack by targeting the default prefix **wp_**. The WordPress database consists of many tables to store posts, links, comments, users etc. Now these tables by default have standard names like wp_users, wp_options, wp_posts etc. Now a hacker knows that the user details are stored in the table wp_users, and will try and exploit this.

The Security Solution: The smartest way to protect the database is by changing the database prefix which is really easy to do on a site that is setting up. But it takes a few steps to change the WordPress database prefix properly for the established site without completely messing it up. To do this, open your ***wp-config.php*** file which is located in the WordPress root directory.

Change the table prefix line from **wp_** to something else like this **wp_chetansoni123_**

```
$table_prefix  = 'wp_chetansoni123_';
```

5. Use WordPress Security Plugins

The Security Issue: Currently, the numbers of WordPress security plugins are available that address many of the common security issues that most WordPress website owners face (e.g. preventing hackers from accessing your site, protecting your site from malicious software, etc.)

The Security Solution: There are so many different plugins available for the WordPress security such as:

1) **Bulletproof**: The Bulletproof Security WordPress plugin is designed to be a fast, simple and convenient one click way for you to switch between different levels of ***.htaccess*** website security and ***.htaccess*** maintenance modes (503 Website Under Maintenance) from within your WordPress Dashboard.

   BPS plugin blocks ALL **XSS and SQL Injection** hacking attempts.

2) **All in One WP Security & Firewall:** This plugin is one of the best security plugin to secure the website. This plugin give option to check the login attempts from different IP's and can ping back if someone is performing ping action on website. We can Block the IP's who can do multiple attempt.

3) **Sucuri Security - Site Check Malware Scanner**: This Plugin is also used to secure the website. It checks any malware, JavaScript, iframes that may infect the website and remove it.

6. Change Security Keys

The Security Issues: When a user logs into the Admin panel, WordPress generates cookies to keep the status of the users. To ensure that the cookies are safe and not guessable, it adds salt keys while generating the cookie which is very much secured. This salt should ideally be long and difficult to guess. The salt is picked from 8 parameters in wp-config.php i.e. **Auth Key**, **Secure Auth Key**, **Logged In Key**, **Nonce Key**, **Auth Salt**, **Secure Auth Salt**, **Logged In Salt and Nonce Salt.**

The Security Solution: WordPress provides an excellent tool to generate these randomly. For more info, please go through this link: https://api.wordpress.org/secret-key/1.1/salt/

Also, in case if the site gets hacked, it is highly advisable to change these keys with fresh ones. This will force all users to login again, and hence the hacker cannot use old cookies.

```
/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {
 * @link https://api.wordpress.org/secret-key/1.1/salt/
 * WordPress.org secret-key service}
 * You can change these at any point in time to invalid
 * This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define('AUTH_KEY',         '_jOnZYD%rNd)H0sWgTU6');
define('SECURE_AUTH_KEY',  'c=c7_7x_(&@$5mUaARNF');
define('LOGGED_IN_KEY',    'Ij7Pm$nP$JyQmSQ!xnbp');
define('NONCE_KEY',        'IPgx_x!g0bCZ648IR G-');
define('AUTH_SALT',        'Z$AmUw5vWz5WSGGc_1kx');
define('SECURE_AUTH_SALT', 'Pb$#Sb=Vd8OHx-=$XOqS');
define('LOGGED_IN_SALT',   'Q4D6UT/prSTRfnx62Db@');
define('NONCE_SALT',       'wmTBOSh=6BnOrX!fQ$*n');
```

7. Always Update WordPress Themes and Plugins

The Security Issue: WordPress is open source, making it an easier target for hackers. Nearly 80 million sites use WordPress in today's time. WordPress updates are often issued for the purposes of fixing potential security issues.

If you do not update them frequently, you are just about guaranteed to get hacked at some point.

Wordpress site has three important updates:

a) The Actual WP Installation
b) Themes
c) Plugins

The Security Solution: It doesn't take long to update your WordPress installation, according to WordPress it takes less than 5 minutes to complete. Before you begin updating any of these items, you should make sure that you have a current backup. This is important because sometimes these updates don't go as well as planned and you need to restore a previous version of your site. Additionally, you might have made some modifications to the theme or plugin and forgot about the changes you made.

8. Prevent Directory Browsing

The Security Issue: If you create a new directory on your website, and do not put an "**index.html**" or "**index.php**" file in it, you may be surprised to find that your visitors can get a directory listing of all the files in that directory.

For example, if you create a folder called "download", you can see everything in that directory simply by typing "**http://www.example.com/download**" in your browser. No password or anything is needed.

Prerequisites – The Website must be on an APACHE Server and Your webhost must have enabled .htaccess overrides.

The Security Solution: Protecting your directories from being listed by your website's visitors does not, in and of itself, make your website very much secure. Add the following line to your **.htaccess** file.

```
Options -indexes
```

Make sure you hit the ENTER key (or RETURN key if you use a Mac) after entering the "***options -indexes***" words so that the file ends with a blank line.