

# 3.7 DESIGNS

## WORDPRESS SECURITY TIPS

### HOW TEACH THOSE HACKERS A LESSON

THIS DOCUMENT PROVIDED BY

**37DESIGNS.com & StylizedWeb.com**

306 South Main, Suite LLA

Ann Arbor, MI 48104

734-231-3369

# INTRODUCTION

## WHY YOU SHOULD READ THIS DOCUMENT

It is hard to argue with the value of using open source software. The low cost, large talent pool and huge capabilities of open source software have proven how valuable it can be to businesses of all sizes. Like all things the concept is not perfect.

There is nothing that makes breaking through a barricade easier than being able to see everything behind it. Because the source code of the software is literally open to the public, hackers with malicious intent can see everything behind the scenes making it easier to break into your software.

Now that isn't to say that open source software isn't secure (typically it is extremely secure). Just that extra steps can and should be taken to prevent that poorly coded plugin or misconfigured server from opening up a security hole.

In this document we will cover some easy and common steps to ensure that your Wordpress site is secure and hacker proof.

# SERVER CONFIGURATIONS

## CONFIGURE YOUR SERVER FOR MAXIMUM SECURITY

### 1. Disallow bots from scanning the important Wordpress directories

By using the `Robots.txt` file it is always a good idea to block the `wp-content`, `wp-admin`, etc... directories. This can be done by adding the following line:

```
Disallow: /wp-*
```

### 2. Turn off directory browsing.

Many servers by default allow you to browse the listing of files with in a given directory. You may have come across this before when a page is missing or there is no index to a directory. The server outputs a listing of the files in the directory instead. This is particularly important in regards to plug-ins. If someone can see which plugins you have on your site they might be able to see which ones are venerable.

**This can be done through your `.htaccess` be using the code below:**

```
Options All -Indexes
```

### 3. Protect your WP-ADMIN folder

The `wp-admin` folder is a critical security point with in Wordpress. Denying access to this folder (as well as the `wp-config.php` file) goes a long way to ensuring that your Wordpress site is secure.

This can be done in several ways and you may want to do all of them.

#### 3.1 Limit access to your `wp-admin` folder by IP Address

If you know that you are on an IP Address that doesn't change you can prevent any intruders by blocking every IP but your own. The drawback here is that if you are traveling, are off site or trying to update the site from a location that is not your typical one you will be denied access as well.

This can be done through your `.htaccess` by using the example code below:

```
<Limit GET POST PUT>
order deny,allow
deny from all
allow from 12.345.67.890
allow from 890.67.345.12
</Limit>
```

#### 3.2 Limit access to your `wp-admin` folder through password protection

While not as secure as the IP Address method, it can be extremely effective to simply password protect your folder on the server level. This can also build upon the security enhancement of 3.1. For example if someone is able to spoof your IP address they still would need to hack your password to break in.

The easiest way to setup password protection is through the [Wordpress htaccess Password Protect Plugin](#).

#### 3.2 Limit access to your `wp-admin` folder by hiding it

There is no reason that your `wp-admin` folder has to be called `wp-admin`. Hackers look for this administration folder in this location. One easy way to eliminate hacking of your site and administration area is simply rename the folder to something else. Simple enough?

### 4. Protect your `wp-config.php` file

The password to your database is stored in plain, readable text in your configuration file (`wp-config.php`). Access to your database gives hackers control over your complete site, so to say you need to protect it is an understatement. The first and most obvious step is to ensure the permissions are set correctly.

Some servers set the wrong permissions by default which allows anyone who wants to the ability to read the contents of that file.

The permission should be set using SSH or through an FTP client to `640`

```
chmod 640 wp-config.php
```

Additionally you can actually move the wp-config.php out of the main Wordpress directory and still have everything function properly. This way hackers don't know where to look for the file. For example if your wp-config.php is located in /public\_html/blog/wp-config.php you could move it to /public\_html.

## 5. Install the 3G Blacklist

A lot of Wordpress installations are hosted on an Apache server. If your site is on an Apache server then you can improve the security (not just Wordpress) by installing the 3G Blacklist. The 3G Blacklist is:

*“a concise, lightweight security strategy for Apache-powered websites...the 3G Blacklist serves as an extremely effective security strategy for preventing a vast majority of common exploits. The list consists of four distinct parts, providing multiple layers of protection while synergizing into a comprehensive defense mechanism.”*

[Find instructions and usage information on the 3G Blacklist here.](#)

# WORDPRESS CONFIGURATION

## TURN WORDPRESS ITSELF INTO AN ARMORED FORTRESS

### 1. Remove the Wordpress version number from the META tags

Some hackers target specific versions of Wordpress because of known open vulnerability's. An easy way to prevent your site from coming up as a target is to simply remove any indicators of the software version.

**In older version of wordpress your theme file would hav the following code in the header.php that generates a simple tag that outputs the current version:**

```
<meta content="WordPress &lt;?php bloginfo('version'); ? /&gt;" name="generator" />
```

You can prevent this from being an issue by simply deleting that line of code.

**Newer versions of Wordpress output the version automatically through the wp\_head() ; function. You can remove these by installing the [Secure Wordpress plugin](#).**

### 2. Disable the “Admin” account

By default Wordpress creates an “admin” account every time you install it. While the passwords are generated randomly it is never a good idea to let people know the login of your most powerful account. Because all Wordpress installations have the same username for the master account you are doing just that.

Simply changing the username from admin to something less obvious will improve the security of your site.

This will have to be done through the database as Wordpress won't let you change or remove the account through the administration interface. The account is located in the wp\_users table, and you can simply change the account name, display name, etc... to that of your choosing.

### 3. Change the Wordpress table prefix

All installations of Wordpress use the same name for all of the tables on the database. The problem with this is that if a hacker is able to use a SQL injection exploit they know exactly which tables to change data on. If you use an alternative prefix when you install the software this is prevented.

Already have a Wordpress installation? The [WP Security Scan plugin](#) can help you switch.

### 4. Use secure connections when connecting to the ADMIN pages

To prevent data being intercepted between your computer and the server hosting your website you can actually force a secure connection to all of the administration panels. This will require that you purchase and implement a SSL certificate from your host first, but once you have done this you can add the following code to your wp-config.php file to activate secure administration:

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

### 5. Use Security Keys

Wordpress doesn't require that you take advantage of their "security key" tool that better encrypts cookies, there by better protecting your passwords. Using security keys is a simple process where you generate a key and make some simple modifications to the wp-config.php file.

You can generate [Wordpress security keys on this website](#).

## WORDPRESS PLUGINS

### ADDITIONAL FUNCTIONALITY TO IMPROVE SECURITY

#### 1. Login Lockdown Plugin

This simple plugin will record the IP address of every failed login attempt. If there are too many failed attempts from one IP address the login function will be disabled for that IP range. This prevents brute force password break-ins.

[You can download the plugin here.](#)

## 2. Invisible Defender Plugin

This plugin protects registration, login and comment forms from spambots by adding two extra fields hidden by CSS. The idea behind Invisible Defender is simple: SPAMBOTS either fill every form field they find (generic spambots) or fill WordPress-specific fields only (spambots which will recognise WP or are targeting WP only).

[You can download the plugin here.](#)

## 3. Maximum Security

You can perform and identify a lot of the problems outlined in this document automatically through this full featured and robust plugin. It can identify permission issues and has an intrusion protection system.

[You can download the plugin here.](#)

## 4. Secure Wordpress

Little help to secure your WordPress installation: Remove Error information on login page; adds index.html to plugin directory; removes the wp-version, except in admin area.

[You can download the plugin here.](#)

## 5. Secure Admin

Secures Login and Admin pages using Private or Shared SSL.

[You can download the plugin here.](#)

# BEST PRACTICES

## NOT WORDPRESS SPECIFIC, BUT ALWAYS A GOOD IDEA

There are plenty of good security practices that you should follow that are not specific to Wordpress.

### 1. Pick your passwords wisely

The first step to being secure is to ensure your passwords are well formed. A strong password contains upper and lowercase letters, numbers, punctuation marks and are not a common dictionary word. This should be tested on every aspect of your website from your SFTP / FTP account, database password and user accounts.

[You can test your passwords using this handy website.](#)

### 2. Only use secure connections

Most website owners and developers use FTP connections to access the files on their server. This is all good and fine except that the transmission is not secure and is open to security holes. Instead setup an SFTP account which will encrypt your connection and prevent stolen information.

### 3. Keep your software up-to-date

Any software should be updated as frequently as possible. Updates often fix security holes among other things (performance enhancements, new functionality, etc...) This certainly is the case with Wordpress. Now that the system has automatic upgrades there is no excuse to have out of date software.

This is not limited to the Wordpress core software either, you should also upgrade your plugins as often as possible as well.

### 4. Backup often

While it is not going to directly improve the security of your site, the only thing worse than getting your site hacked is getting it hacked with no way of restoring it. You should not only backup the actual files of the site but the database as well.

With the WP-DB-Backup plugin you can automate this process and even have it e-mail a copy of the backup to you on a regular schedule.

[You can download the plugin here.](#)

Have a hard core an intensive Wordpress site? You can even backup the important parts of your Wordpress installation to Amazon S3 servers through the WP S3 Backups.

[You can download the plugin here.](#)

### 5. Secure your MySQL Database

Not specific to Wordpress but you can make a lot of strides to improving the security of your MySQL database server. I won't go into the specific details in this document but you can get more than enough information [from this detailed website.](#)

# ABOUT 3.7 DESIGNS

## A LITTLE BIT ABOUT US AND HOW WE WORK

***We design interfaces, websites and dream up marketing plans that create big results.***

We've solved problems for some incredible clients— from large multinational companies and local governments to small businesses and school districts. We're widely known for our planning and strategy skills, as well as our overriding focus on improving conversion.

We're a web design and web strategy firm based in Ann Arbor, MI. We believe that small inputs can lead to large growth — and we work hard to bring that idea to life. 3.7 is not your typical, oversized, all-you-can-eat interactive agency. Rather, we focus on doing our ***favorite things very well***. What does this mean for you? Higher quality work. Expert advice. A good working relationship. Sparkles and cupcakes.

## Services & Skills

- Web Design
- Web Strategy
- Internet Marketing
- Wordpress & Silverstripe Consulting

## Awards & Extracurriculars

- Co-founders: Refresh Detroit
- Co-host: Web Axe Web Accessibility Podcast and Blog
- Community Chair: Ann Arbor Ad Club
- Certified: Google Search Marketing Professionals
- CEO is an instructor of the Internet Professionals program at Washtenaw Community College
- 3.7 team are frequent speakers at industry conferences and events