



Lesson #46

Securing WordPress

By

Lynette Chandler
Tech Based Training

<http://TechBasedTraining.com/>

**NOTICE: You Do NOT Have the Right
to Reprint or Resell this Report!**

You Also MAY NOT Give Away, Sell or Share the Content Herein

If you obtained this report from anywhere other than **Tech Based Training.com** , you have a pirated copy.

Help stop internet piracy by letting me know. Send email to
customerservice@techbasedsupport.com

© 2010 Copyright Lynette Chandler

Legal Disclaimer: Keeping things simple here, I have to say that I cannot promise you success. I can give you direction and advice based on my experiences and good internet marketing practices. What you do with this information is up to you. As a Tech Based Training member you agree to not hold me responsible for your results.

Background

Whenever a software becomes popular and is able to reach the masses, there you will also find the 'bad people'. The hackers, the script kiddies and everything else in between. There is little we can do in our spot to stop this but we do certain things to reduce and make it a lot harder for these people to mess with our sites and our clients' sites.

There's also a selfish reason for us to secure client sites. So that we can create added value to our services or use it as an add on package to increase our prices. Either way you will be seen as a step above the average blog designer.

The following are some of the things we can do to secure client blogs.

Protecting The Admin Folder

There are many ways to protect this folder. The reason is so you can add a 2nd layer of protection to the admin area, so anyone who is trying to access the admin area needs to first get past the gatekeeper before asked to log in.

Password Protection

Some prefer to protect the admin folder by adding another login. This is perhaps the better method. The down side is, you'll be forced to log in twice. Once to get past the folder protection, another time the actual admin login. Some people don't like this, but it really depends how concerned they are about security. If you client complains you can always suggest [Roboform](#) or [1Password](#) using your affiliate link of course ;-)

To password protect this folder, go to cPanel, click on Password Protect Directories, select the folder you want to protect. Give it a username and password.

IP Filtering

This method denies access to the admin folder for anyone who is not logging in from a certain IP address. Since IP addresses change – even broadband users' IP addresses change, this may not be feasible. Besides, if the client travels, they may be locked out of the admin area.

However it can be helpful if the place they are logging in to is consistent and they have a static IP address. To do that, you enter the following code into the wp-admin folder's htaccess file.

```
AuthUserFile /dev/null
AuthGroupFile /dev/null
AuthName "Access Control"
AuthType Basic
order deny,allow
deny from all
# whitelist home IP address
allow from XXX.XXX.XXX.XXX
# whitelist work IP address
allow from XXX.XXX.XXX.XXX
allow from XXX.XXX.XXX.XXX
```

For those who are ambitious, you can also use both at the same time :)

Changing Admin Username

Unless WordPress was installed using Fantastico or another one-click installation program, the default username for admins is admin. Most people won't change that and it makes it easier for anyone trying to hack into the admin area. They only have to figure out part of the combination – the password.

Changing the admin password forces the hacker to try to figure out two parts of the combination. If you're going to change the admin username, don't make it easy either. Don't use names like 'God', your name, administrator, moderator, super user or anything like that.

How do you change the admin username since you can't change usernames inside WordPress? In lesson 88, we learned how to interact with the database using

phpMyAdmin. We also touched about how to use it to change the admin username. Follow those directions.

Disallowing Folder Listing

Most web hosts already disallow folder listing. But some don't – you'd be surprised how many don't and it's easy to overlook too especially after moving web hosts, you don't think of checking for things like these. Better to err on the side of caution.

What is folder listing? Sometimes you click on a link and instead of a web page that you expect to see, you find a complete list of files and folders. This is because an index.php file is missing from a folder.

Some of the older WordPress sites don't have an index.php file in the wp-content folder which means you can browse all the plugins and themes that are being used or used as a gateway for attack. This is true for any site not just WordPress.

To fix that you can simply create a blank index.php or index.html file and put it in the folder. But that can be tiring when you have a ton of folders, sub-folder and sub-sub-folders. There is an easier way. Pop the following code into your .htaccess (the one in public_html)

```
# prevent directory browsing
Options -Indexes
```

Hiding/Forbidding Wp-Config.php

The wp-config file stores the most crucial data for your blog. It only makes sense to protect it. The wp-config.php is only to be used by WordPress internally. Nobody should be able to access that file – not even you. If you need to access it, you can always access it via FTP or PsPad.

So, you deny everyone from loading that file in their browser. Using the following code, inside the blog's .htaccess file (the same folder as your WordPress files, e.g wp-content, wp-config.php)

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

Also, make sure the wp-config.php file permissions are at least 644 it would usually be, just one more step to make sure.

Disallowing .htaccess

Same as the above for wp-config.php, you want to deny people access to your htaccess files. You can always access it through FTP or PsPad – that's how you'd work with it anyway. Put this in the htaccess file that is in the root of your site (in the public_html folder)

```
# protect the htaccess file
<files .htaccess>
order allow,deny
deny from all
</files>
```

Changing Database Prefix

Almost everyone who installs WordPress doesn't change this which means your WordPress and my WordPress database tables look alike. They all start with wp_ - take a look in your database using phpMyAdmin. You'll see what I mean.

WordPress can work with a different pre-fix. This helps reduce database attacks. To do this, when installing WordPress, when you edit wp-config.php, find this line.

```
$table_prefix = 'wp_'; // Only numbers,
letters, and underscores please!
```

Change wp_ to something else. Example btb_ must include the underscore. Please do this BEFORE you run the 3 minute installation process, at the same time you enter the database information.

This is great for new blogs but what about established blogs? There are ways to do this on an established blog. It is a lot more involved, requiring familiarity and confidence managing databases. I know most of you here are in this to be a designer not a developer. So the best thing, outsource it.

Scanning Source Code Daily

Another thing I do for my blog and for clients who pay an extra monthly fee is to scan their source code daily. Every morning, I get an email with the web site's source code. This is different from viewing the source code from the browser. I have a little trick that makes the site think I am Google bot and present me with source code as Google bots see it.

Why? Because at one time in the past, smart hackers have hacked WordPress sites so that when you view the source code all looks nice and clean but when Google or any search engine robot checks out the site, they see something else including links to their sites – basically, hijacking your rank or traffic.

I've written an extensive tutorial [here](#), how to set this up. Scanning is still a manual process. But don't worry you won't have to spend all your time doing it. Every morning when the email comes in, I just check the code above the <body> and after the </body> tag. This is usually where malicious code if any is found.

Create Strong Passwords

While your client can always change the passwords you supply them, many don't. I can't tell you how many times I have worked with clients who still used the temporary password e.g. temp123 that was set by the original designer and they've been using it for years.

Set the example for the client. When creating passwords for their admin account, give them a strong password. If you use [Roboform](#) or [1Password](#) (you should be using them anyway! Don't trust the browser or your memory), there is a password generator included. Use it.

Be Careful Of What Plugins & Themes You Use

Whenever a plugin asks you to change a folder's permissions to 777, be wary! I personally do not like plugins or themes that require that and will rather choose an alternative if any.

At the moment, the plugins and themes in WordPress.org directories are pretty clean – they did a massive theme clean out too so that helps but you should always be wary of those you get outside of WordPress.org especially the free ones and in forums and sites you don't know about.

Sometimes clients may request or insist on it. What I do it is warn and advise them of the risks. If they insist you execute their wish but since you've advised them, the risk is squarely on their shoulders.

Keep Your Computer Clean

Believe it or not, if your computer is infected, all your precautions above could go to waste! Keeping your computer clean is not only for your own good – so that you have a tool to keep making money for you, but also a responsibility to your clients.

This may sound so out of the world but it is something I have experienced myself so you can trust the information is true and very valid. A client of mine continually had their web site hacked. Despite my best efforts of securing the site they would never fail to get in after a while.

It was then I knew the attack didn't come from the web but from someone's computer. The client has many people working on their sites, an average of 3-4 people – they have a big team and that's not including me.

I at once advised the client to check all computers and tell everyone on their team to clean the computers. Sure enough someone found a key logger on their computer. Sure enough, not long after they log in the attacks occur.

When I advised the staff to use [Roboform](#) or [1Password](#), they refused, mistakenly thinking that keeping the logins on paper, out of their computers is safer. **Not so!**

In fact, you can also reduce the risk by using these programs. First, the data is encrypted. Second, when you use these programs, you are not using your keyboard. The software logs in for you. Therefore the keylogger won't be able to detect what the password is. Wise up, stay safe.

Next Lesson...

Our final lesson! I'll share some final thoughts and as a reward for making it to this far, a special invitation. Don't miss it.

Lynette Chandler

Lynette Chandler

Tech Based Training