Website Security: This Excites me!

Sitting trying to find my php.ini for my local WordPress multi-install, and getting frustrated that I know I found it, and I changed the value I needed to change, but it isn't show up as changed, I get an en email. It only contains one thing, but a beautiful thing:

> *Dear Site Admin,*
>
> *A host, **198.154.227.219**, has been locked out of the WordPress site at http://pureheartcenter.com due to **too many attempts to access a file that does not exist**.*

Then I sit back and reflect a little on why I am busting my ass doing this work. All the training, all the classes, and all the reading. On top of that trying to find new clients. All whist dealing with being at the end of a horrendous Chemo and Radiation treatment for Cancer, (did I get the medal yet?) Then the Universe shows up with this. It may not mean a lot to most of you readers, but it means the world to me. It means that I am learning a little about website security, and the things I am implementing are paying off. Happy days.

I had two such emails yesterday for a client site, and I had no problems sharing it with them. I enjoyed letting them know that they are now protected. This particular client had been hacked badly, her site had been down for 2 months, and she was losing money before she found us. So we fixed her up, and now she can rest assured that things are working on her behalf, and she can get on with focussing on her own stuff, and leave the running of the website to us.

The client in question is hosting with a notoriously bad host that a lot of people use because they appear to be cheap up front, and they are a popular domain registration website as well. So heck, why not do everything in the one place, right? This host has been getting some real bad press lately about it's inability to stop spammers and hackers, but why would that be an issue for them since they have a product they can sell you for that should such an event occur, mmmmmmm.

There are a few ‘too big to fail’ companies out there doing the very same thing. That is why small personal touch companies such as BarbApple Studios need to band together, and work a little harder at getting through to these clients to show them that there is a better, smarter way to take care of their website.

This hacker was thwarted by two plug-ins, two not so measly plug-ins with I will cover in a minute. A plugin that was correctly installed and configured. Hey that’s what you pay us for, and this is proof that your money is well spent right? It is the desire to do something well, and to keep at it that should drive us. If what you are doing sucks, then do something else. If you can’t stop doing what you are doing, then do that something else at the same time until you can transition over to it.

iThemes Security

WordFence Security

The plug-ins in question are *Wordfence, and iThemes Security,* and these are in my ‘recommended plug-ins’ article. These are a must install in my humble opinion on every website. They match all 5 of my 5 Step Criteria as to when to install a plug-in. I will post the 5 step below so that you don’t have go to another article to read them.

There are other things I look for, but these are my top 5. Don’t be shy about leaving a comment on what you think is important for a plug-in. I am open to new things.

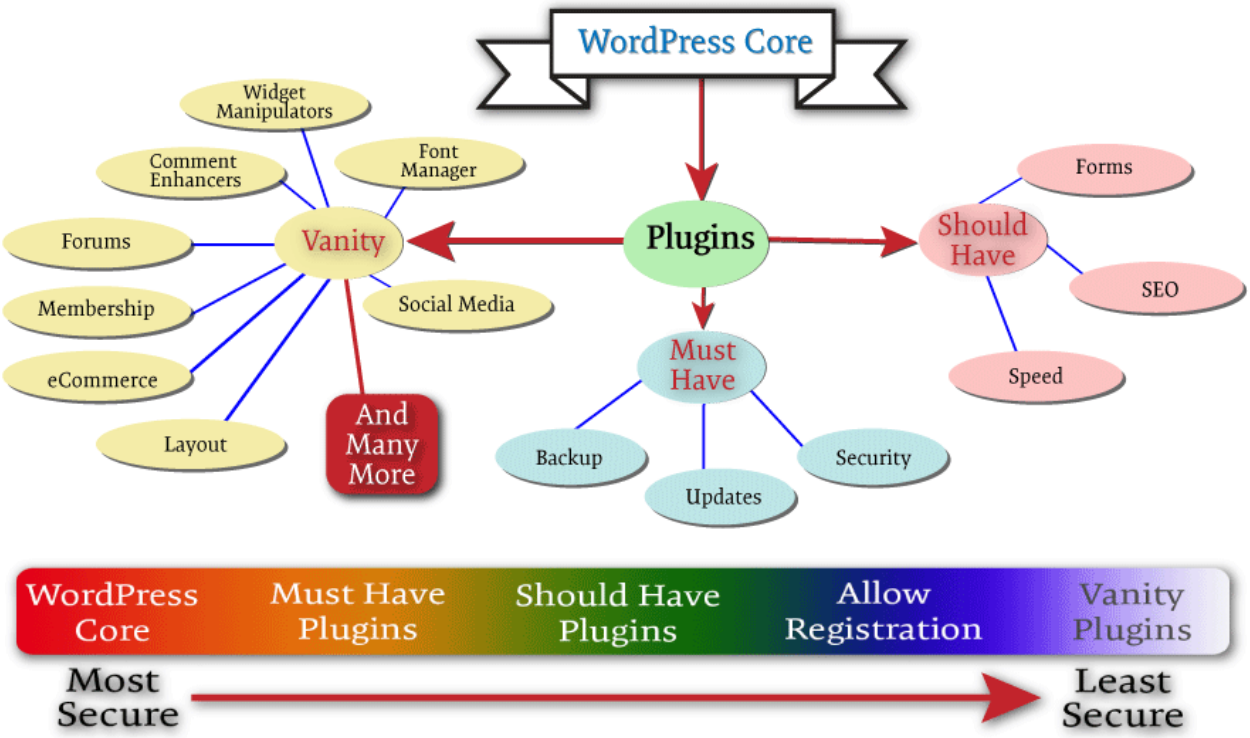
BarbApple Studios 5 Step Criteria for the Installation of a Plug-in

1. **Do you really need it**
    1. Sometimes we do install plugins for a reason other than necessity. That reason, and we all do it, is just because it's cool. I have nothing against have these cool plug-ins on a website as long as they don't break my 5 rules. Even a plug-in that I feel my site really needs is not implemented unless it passes the tests.
2. **Does it rate high**
    1. This doesn't help newer plug-ins.
    2. Those ones that have just been born and look like they are going to grow up into something really useful.
    3. This is where you make a choice as to whether or not you think it is worth.
    4. If it works then go and rate it so you can contribute to the rating portion of the 5 Step Criteria.
3. **Is it updated on a regular basis**
    1. Does it say "Not tested with your particular version of WordPress" when you look at the details portion of the plugin?
4. **Do they offer a decent free version and a paid version**
    1. Does the free version actually have enough features turned on to check out what it can do properly?
    2. Does the paid version offer enough of a change, and add something you can use that would enhance your site even more?
5. **How fast is their technical support**
    1. Send an email to support and see how fast the get back to you
    2. Sometimes this can go back to number 4. Maybe the fast technical support is only in the paid version. I have seen that in some plugins.

But even the basic configuration of these plug-ins will help you slow down any attempt at malicious entry into your website. Nothing is perfect, and I am sure there are those of you out there that could do a better job, but what we do here at BarbApple Studios works, and works well. It doesn't take long to read their installation and configuration documentation anyway if you wanted to tweak

them further. So take the time with these plug-ins an you won't be disappointed with the results.

Types of WordPress Plugins I Should Use



WordPress plugins tree

As you can see from the above chart, it is more like the family tree of plugins off the main WordPress core. The explanation and the presentation of it is my interpretation of the WordPress plugin hierarchy. I know some of you may not agree, some of you will, and even more of you will think it is over simplified, but that's the kind of thing I meant to convey.

The WordPress core itself is extremely secure, and by that I mean as secure

as any content management system, CMS out there can be. Since it is written and updated by developers, and has a whole community behind it helping its validity, it is one of the most secure CMS's out there today. It has checks and balances because if it.

The WordPress core, (red,) is the most secure version of your site. As it moves to the right and you keep adding more and more things, such as plugins, it gets less secure, (white.) Coming off of the green into the blue area denotes a website that is more vulnerable to breaking and/ or getting hacked. My best advice is to make sure security is in place, and research your vanity plugins thoroughly before installing them.

Must have plug-ins: These are the plugins in my book that I feel no WordPress website should be without. This will definitely vary from person to person, and from developer to developer. These are the plugins that I recommend, and I am totally open to this changing as I learn more or hear better arguments. That can happen a lot in this business, and one of the coolest thing about WordPress. In this area I have the following categories: **Backups, Updating, Security, and Anti-spam.**

Should have WordPress plugins: These are the plugins that you will install after you have finished installing and testing the plugins on the "Must have" list. This section, plus the previous section will give you a fully functioning interactive site, with the bare minimum of headache when you are trying to keep your site secure. I have included the following categories in this area: **SEO, Caching, Responsiveness, and Forms.** Personally I don't think you can do without any of the plug-ins from either of the above areas. This, to me, is a full site if you are looking to have a functional, interactive site, that also has the chance to be discovered in the web.

Vanity WordPress plugins: Believe it or not, this is a favourite section of mine. I do like my Vanity plugins, because some of them are really cool, add value, and most are very well supported. I am not one of those developer that will poo-poo you because you want to add vanity plugins to your website. If I am designing your website you just have to abide by my rules when it comes to any plugins in this category. You just have to be careful how you choose a Vanity plugin, and what purpose it is supposed to serve on your site.

I have created a table for you to look at with specific examples of plugins I use that fall into each of the areas. Also when adding a new plugin directly from the list below, I have outlined the procedure below, and this procedure should work most of the time, but otherwise it is very easy to figure out:

1. Click the link to the plugin
2. Download the plugin to your hard-drive
3. Go back into your "Admin" section of your site
4. Select "Plugins"
5. Select "Add New"
6. Select "Upload Plugin" at the top of the page
7. Cling the "Choose file" button
8. Find the plugin on your heard-drive – highlight file and select Open, (usually in your downloads folder.)
9. Click the "Install Now"
10. Activate plugin
11. Re-read documentation on the plugin to know how it sets itself up on your computer
12. Check that plugin is there and configure it

Video coming soon on how to download and install a plugin

Area	Category	Specific plugin (* = Best in my book)
Must Have	**Backup**	Backup Buddy * No free version BackWPUp * – Free
	Updating	iThemes Sync * Free – on-line service JetPack Monitor Free – on-line service ManageWP * Monthly subscription – on-line service
	Security	iThemes Security * Free and paid version Sucuri * No free version – on-line CloudFlare * Free and paid version – on-line service Really Simple CAPTCHA – Free
	Anti-Spam	Akismet – * Free and comes with WordPress
Should Have	**SEO**	WordPress SEO by Yoast * Free and paid version
	Caching	W3 Total Cache * – Free and paid version P3 (Plugin Performance Profiler) – Free

Area	Category	Specific plugin (* = Best in my book)
	Responsiveness	WP Touch * – Paid version JetPack Mobile theme – Free
	Forms	Gravity Forms * – No free version Contact Forms 7 * Free
Vanity	**Editor**	WPEdit * Free
	Social buttons	Floating Social Bar * Free SumoMe – Free and paid version – On-line service with plugin
	Widgets	Display Widgets – Free
	Media Library	Enhanced Media Library – Free
	Typogrphy	Google Font Manager – Free Hide Title – Free No Page Comment – Free Yet Another Related Posts Plugin – Free

There are definitely tons more plugins than this, but this will give you a basic idea of the areas that you will most likely need to fill first. Whatever you are looking for can be found by following the steps above the table for finding a plugin or a type of plugin. Let's say you have an idea and you want to see if there is a plugin exists that might help, then type it in.

Remember that a bad plugin has the potential of crashing your site. So when you install a plugin, always check that your site is working after **EACH** install. Don't install 5 or 6 plugins, and then check your site. If it isn't working, then there is no way to tell which plugin was responsible. So take your time and test, test, test as much as you can. Try and limit the number of plugins you install, and delete the plugins that you are not using. Also delete any themes that you aren't using as well. This can help the possible chances that a hacker can get to your website, but all of this is discussed in another article with this site, when I talk about how to tighten up, or lock down your site.

Wanna Find a Plug-in?

I re-worked this wonderful compilation of plugins I have come across. Some of them will be old, so let me know, and I will try to keep an updated list. My favourites are among these, but I have probably test-driven all of them at some point. I have also left out some of the more obvious ones, and it's fine to bring my attention to those as well.

So if you have a plug-in you would like to see on the list feel free to post it in the comments section below along with anything else you might have to say. This list will be changing from week to week and I will be adding new information as I get ideas of what to include, and I will be tweeting the changes so make sure you are following me on twitter.

I am also not rating which I think are best at the moment, but it is on the cards when I review this list for plugin additions, so if you see an asterisk, or other form of rating mechanism, then that means I have started doing just that. So check your twitter feed under @barbapplestudio

A really nice resource for searching for plugins based on category, downloads, votes, etc is:

http://wpplugindirectory.org/

"Google Trends for .org Plugins" – Simple tool to compare free WordPress.org plugins side-by-side:

https://bestfreewpplugin.com/

Custom Post Types

- http://www.wp-types.com
- http://wordpress.org/plugins/cpt-onomies/
- http://pods.io/
- http://wordpress.org/plugins/my-content-management/ — Lesser known, not great for clients, but still powerful for developers and free.

Custom Fields

- http://www.advancedcustomfields.com/

OPTIMIZATION

For Images

- http://jetpack.me/support/photon/
- http://wordpress.org/plugins/ewww-image-optimizer/
- http://wordpress.org/extend/plugins/wp-smushit/
- https://wordpress.org/plugins/imsanity/

For Managing When Plugins or Scripts Load

- http://wordpress.org/plugins/css-javascript-toolbox/
- http://wordpress.org/plugins/plugin-organizer/

For Caching

- http://wordpress.org/plugins/w3-total-cache/
- http://wordpress.org/plugins/wp-super-cache/
- http://wordpress.org/plugins/hyper-cache/
- http://wordpress.org/plugins/cloudflare/
- http://wordpress.org/plugins/em-object-cache/
- http://wp-rocket.me/ (Premium — free version on it's way soon)

SEO

- http://www.prelovac.com/vladimir/wordpress-plugins/seo-friendly-images
- http://www.vretoolbar.com/news/seo-slugs-wordpress-plugin
- http://yoast.com/wordpress/seo/
- http://www.weberz.com/plugins/404-redirected/

Google Analytics Dashboard

- https://wordpress.org/plugins/google-analytics-dashboard-for-wp/

Sliders

- http://soliloquywp.com
- http://codecanyon.net/item/slider-pro-wordpress-premium-slider-plugin/253501
- http://shouldiuseacarousel.com/

- http://codecanyon.net/item/layerslider-responsive-wordpress-slider-plugin-/1362246
- http://dimsemenov.com/plugins/royal-slider/wordpress/
- http://wordpress.org/plugins/infinite-slider/

Full Screen Background Sliders

- http://wordpress.org/plugins/wp-supersized/

Social Sharing

- Social Sharing Toolkit http://www.blogaid.net/social-media-widget-plugin-injecting-spam Video tutorial to help folks switch from the Social Media Widget plugin over to Social Sharing Toolkit and configure it.

Security

- iThemes Security (formerly Better WP Security) http://wordpress.org/plugins/better-wp-security/
- BruteProtect http://wordpress.org/plugins/bruteprotect/
- Wordfence Security http://wordpress.org/plugins/wordfence/
- All In One WP Security and Firewall http://wordpress.org/plugins/all-in-one-wp-security-and-firewall/

Spam

- http://bad-behavior.ioerror.us/
- http://www.itquad.com/wordpress/plugins/wp-email-guard

Event

- http://wp-events-plugin.com/
- http://wordpress.org/plugins/the-events-calendar/
- https://wordpress.org/plugins/all-in-one-event-calendar/

RSS Aggregation / Feed to Post Import

- http://www.wprssaggregator.com

Frontend Post/Registration

- http://wedevs.com/plugin/wp-user-frontend-pro/

Forms

- http://www.gravityforms.com/
- http://contactform7.com/
- http://formidablepro.com
- http://ninjaforms.com

Backup/clone

- https://wordpress.org/plugins/duplicator/

Newsletter

- https://wordpress.org/plugins/wysija-newsletters/

Sidebar

- http://wordpress.org/plugins/content-aware-sidebars/
- http://wordpress.org/plugins/woosidebars/

This is by no means a definitive list but it will be growing and I will be posting it on twitter for sure.

Limit Logins

This is a great plugin and does exactly what it says it will do. When you go to install it, you will most definitely notice that it hasn't been updated in a while but don't worry about that in this plugins particular case. It really doesn't do anything that requires updating. I have a warning with this plugin though, if you forget your password, and login the number of times that you specify in its settings, it will lock you out. Even if yoiu use the "change password" option, you will still have to wait the allotted time before it will allow you to log back in again. So bookmark this post if you must because the following solution is the only way to reopen your site.

You will need to be able to FTP to your server, go into the wp-content folder and rename the limit-login-attempts folder. Now go to your wp-admin and login with the new password, or the old one if you finally remembered it, and log back in.

In it's own words:

"This plugin will limit the number of login attempts possible both through normal login as well as using auth cookies.

By default WordPress allows unlimited login attempts either through the login page or by sending special cookies. This allows passwords (or hashes) to be brute-force cracked with relative ease.

Limit Login Attempts blocks an Internet address from making further attempts after a specified limit on retries is reached, making a brute-force attack difficult or impossible."

My favorite plugins

These are just a few of my favorites that I put on most of my sites. This changes from time to time as new ones come out or old ones get better, and that's the fun of it. If you have a professional site, do not play with the plugins. Get them working, and leave them alone. Update them when they need to be updated and get familiar with their tech support. Install a localhost web-server on a local computer, easy to do these days, and play around there. Or you can get another domain just for playing and testing your plugins before you deploy them to your regular site. As a developer, that's what I do. I have a few online sites and a localhost server that I have broken quite a few times with lame plugins. Just have fun!

Must Installs

These are the plugins that I install right off the bat on client websites. Most of them are security plugins, but some will be ones that allow me to do things faster when I am called to update or repair a client site. The plugins below will have "*a*

must install" right after the plugin title

WordPress SEO – By Team Yoast – *a must install*

Love this plugin and it is a must have, but there is a learning curve with this, and this is where my yerly subscription to lynda.com comes in handy. I can learn from the best in there.

The first true all-in-one SEO solution for WordPress, including on-page content analysis, XML sitemaps and much more.

iThemes Security – by iThemes

Maybe it is because I know the developer, maybe it's because it's a great plugin or a combination of both, but I love this plugin. It covers a lot of bases when it comes to WordPress website security, and gives me peace of mind for my website. It isn't the only thing I have installed but it is a must and a first security install for me on a clients site. **In their own words:**

> *iThemes Security shows you a list of things to do to make your site more secure with a simple way to turn options on or off. We've simplified these steps and provided descriptions of each action so you know exactly what's happening on your site. You shouldn't have to be a security pro to use a security plugin. And isn't that the point?*

iThemes Sync – by iThemes

This is an awesome unobtrusive plugin to help you keep track of all of your theme and plugin updates. Easy to install and configure which is a plus for me. **In their own words:**

> ***It's important to keep your WordPress sites updated**, both for the security of your site and to take advantage of the latest features and improvements of your themes and plugins.*
>
> ***Updates to WordPress core** and any plugins or themes installed on your sites can happen pretty frequently. And if you're managing multiple WordPress sites, keeping them all updated can take up a lot of your valuable time.*

> ***iThemes Sync is an easy way to manage*** *updates for all your WordPress sites from one place. Instead of logging in to each site individually, you have one place to view and install available updates.*

NOT Must installs

WP Google Authenticator – By Google

Like the World of Warcraft authenticator from Blizzard. You will need to install the app for you phone so that you can generate the auth code. This might not be a good idea if you are allow user registration because many client smay not have the savvy to be able to use the phone authenticator. There is a lot t it. I locked myself out attempting to set it up on my live test site. As a matter of fact I am locked out as we speak for half hour. Hence i decided to update this article

Dynamic Widgets – By Qurl

Dynamic Widgets gives you full control on which pages a widget will display. It lets you dynamically show or hide widgets on WordPress pages.

No Page Comment – By Seth Alling

A plugin that uses javascript to disable comments by default on posts, pages and/or custom post types, but leave them enabled on others, while still giving you the ability to individually set them on a page or post basis.

Hide Title – By Randall Runnels

Allows authors to hide the title tag on single pages and posts via the edit post screen.

AddThis Follow Widget – By The AddThis Team

Generate followers for your social networks and track what pages are generating the most followers

Share Buttons by AddToAny – By AddToAny

Share buttons for your pages, including AddToAny's universal sharing button, Facebook, Twitter, Google+, Pinterest, WhatsApp and many more.

Limit Login Attempts – By Johan Eenfeldt – *a must install*

This plugin will limit the number of login attempts possible both through normal login as well as using auth cookies. By default WordPress allows unlimited login attempts either through the login page or by sending special cookies. This allows passwords (or hashes) to be brute-force cracked with relative ease. Limit Login Attempts blocks an Internet address from making further attempts after a specified limit on retries is reached, making a brute-force attack difficult or impossible.

Editors note: I disabled this plugin. Maybe it was just me, but it was a pain logging in to some of the websites I manage. As soon as I added other security plugins, this became obsolete, believe it or not there is such a thing as too much security.