Advanced WordPress Security

This article is a continuation of our Protecting WordPress article, and contains other more advanced steps.

1. Control sensitive information

1. Permissions on files are configurable for a reason. Control what files are visible to the world, and limit particulars about your account functionality.
2. For example, disable world read permissions on the readme.html file to avoid letting outsiders see what version of WordPress you're using.
3. Make sure you don't have phpinfo.php or i.php files accessible to everyone.
4. DO NOT leave .sql backup files in your web directory - your usernames and passwords are saved in those files along with all your posts and comments.

2. Restrict Access (.htaccess file)

Installing a plugin to help rate limit login attempts is a step in the right direction. However a .htaccess file limiting directory/file access is likely one of the best. <FilesMatch wp-login.php> Order Allow,Deny Allow from xx.xx.xx.xx Deny from all </FilesMatch>

3. Remove Version information in default files

This is done in two places. The first is the meta generator tag in your template. That's found in wp-content/{name of your WordPress theme} /header.php. Look for something like “” and remove it. The other element is in your RSS feed. Open up wp-includes/general-template.php and look around line 1858. Find: function the_generator($type) { echo apply_filters('the_generator', get_the_generator($type), $type) . "\n"; } Make sure a hash is applied next to the “echo” command so that it looks like this: function the_generator($type) { #echo apply_filters ('the_generator', get_the_generator($type), $type) . "\n"; }

4. Disable custom HTML when possible

If it's not necessary for the form and function of your site, disable it. You can add the following to your wp-config.php file: define('DISALLOW_UNFILTERED_HTML', true);

5. Hide Indexes or limit access

1. In a .htaccess file, add: Options –Indexes

2. Make sure PHP source code is never revealed:

    a. Your site's wp-includes/ directory is the most important one to block. Find the .htaccess file there and insert: RewriteRule ^ (wp-includes)\/.*$ ./ [NC,R=301,L]

    b. If there are or will be subdirectories of wp-includes/, insert the following code for each one in the same .htaccess configuration file: RewriteRule ^(wp-includes|subdirectory-name-here)\/.*$ ./ [NC,R=301,L]

6. Install Security Plugins

1. Remember to only install plug-ins offered through the WordPress control panel since external plug-ins may not be secure. Most plugins offered from WordPress.org are regularly audited for the benefit of your security.

2. Guard against brute force attacks Thousands of failed login attempts happen on servers every day. While we do provide firewall protection to help defend against attacks like this, there are steps you can take as well!

    a. Programs like Limit Login Attempts can help you defend your account from brute force attacks.

b. http://wordpress.org/extend/plugins/limit-login-attempts/

c. http://wordpress.org/extend/plugins/si-captcha-for-wordpress/

3. Exploit scanner http://wordpress.org/extend/plugins/exploit-scanner/

4. Install other useful plugins Bad Behavior and User Spam Remover

7. Protect Against Malware

1. Monitor for malware every day http://www.sitelock.com/ http://sucuri.net/introducing-server-side-scanning.html

2. Do something about it The tools above will actually help you resolve the issues that come up. Make sure that you are proactive in taking care of possible infections **immediately**.

8. Clean your site

1. Just like you complete daily chores around the house, you should regularly clean up your site and files that you do not need.

2. Having old files on your account can leave you vulnerable, even if you've deactivated the old plugin or kept a backup of an old version in your web folder.

3. Stay clean and keep things organized - you should know all the files on your account well enough to identify when something is there that shouldn't be.

9. Back up your website

1. A good plugin that can be used here is WP-DB Manager (note that it may consume excessive resources in a shared environment). This plugin can be useful for reporting other vulnerabilities as well, when it detects accessibility issues. http://wordpress.org/extend/plugins/wp-dbmanager/

2. Remote backups are also good options, if you haven't already, check out ComCure: https://www.comcure.com/

10. Report bugs and vulnerabilities – WordPress or plugins

1. You can send anything you discover to security@wordpress.org for the main software.
2. Any plugins that you want to report issues with can be reported through plugins@wordpress.org
3. It's best to avoid discussing the vulnerabilites in Social Media, since hackers may be able to pick up on and exploit users before patches can be implemented.

11. Stay vigilant

1. Security is not a one-time task. You cannot just set it and forget it, you must be aware that it is an ever changing and continuous job.
2. Set up a schedule for scanning. Make sure you analyze your logs and keep copies of them off-site.
3. Find and follow WordPress bloggers or security Twitter accounts to stay ahead of the game.
4. Protecting your site will help prevent harm to your account, your content, your users, and other machines that connect to you throughout the Internet.