Lock Down Your WordPress Site

Dustin Hartzler (@DustinHartzler)

Twitter Hashtag: #YWE

Your WEBSITE Engineer.com

About Me

- ✓ My Name is Dustin Hartzler
- ✓ Full-time WordPress developer
- ✓ I have had my share of hacks and I know what works!

Overview

- ✓ Initial Set Up
- ✓ Make your Website Harder to Hack
- ✓ Restore from a Hack

Your WEBSITE Engineer.com

Why Worry About Security?

- ✓ Getting hacked is a complete pain to recover from.
- ✓ Lots of wasted time
- ✓ Unnecessary hair pulling :)

WordPress Quick Install

- ✓ Most hosting providers give you the ability to quickly install WordPress
- ✓ Take the following precautions for secure installation:
  - ✓ Install WordPress in a directory
  - ✓ Change the Table Prefix
  - ✓ Choose a specific database name
  - ✓ Select a username other than admin
  - ✓ Create a difficult (7 or 14) password

Your WEBSITE Engineer.com

Live Demo

Your WEBSITE Engineer.com

Overview

- ✓ Initial Set Up
- ✓ Make your Website Harder to Hack

Your WEBSITE Engineer.com

Manually Modify Code

- ✓ If you are comfortable with FTP, then there are more changes that you can make

Your WEBSITE Engineer.com

Step #1 - Change WordPress Keys

- ✓ Changes the cookies within WordPress
- ✓ If someone is logged into your site, they will have to reauthenticate
- ✓ Paste in wp-config.php file
- ✓ https://api.wordpress.org/secret-key/1.1/salt/

Your WEBSITE Engineer .com

Step #1 - Change WordPress Keys

```
define('AUTH_KEY',         'eWMG^B7;Xor`CZf{v-,BHCA4U(>}q+C@o<fA>-`#>+|lqZ,Cs;7l-z;@wmtV#&I>');
define('SECURE_AUTH_KEY',  '/Mo+-EyxF=la8dl5~|UDx>HhL7laswrJoq4^6?Al&CPjlaMrCk]3G,L|@S>ztov$');
define('LOGGED_IN_KEY',    'ph;y+68a^%u@]@_GZ0ksNpQ G|7{j>-~`a?hk[q?$-rg4!KEl@oBMN;9]qMG^)&.');
define('NONCE_KEY',        'Pz<Re%xK.zcm|SSSluiDc3k%rvy{}MGeN4UP=T:nmxu+_sPa^OCpa)bW5EQ$&MMI');
define('AUTH_SALT',        'b6na0dWi)EWa%YU2T_Vakyx,+A]~^/2Xm[(aF!*Il_>XkTU+|qVk-9&J.%]_bp3!');
define('SECURE_AUTH_SALT', 'o/XU|8cJA;s)K<!R{6jwcf##RUc#*hq lqda.#d`c,gYkyX_O|]s7)C#AOi_9m_u');
define('LOGGED_IN_SALT',   'I6ocPQbHk{:C:S?5y1{zL3lQMc&m{xYM<MX]$2A|=g{3.pjsfHyL$fS-/(+/[$])');
define('NONCE_SALT',       'yM`Na 0q>{ %vJ]%IX:hYDm=eiby5m/Ci+^7`iUAfv,p@k#8<n9f0xpU&^Oqx:M7');
```

```
/**#@+
 * 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 invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define('AUTH_KEY',         'RVdibU1T ^7^Y]Ty$KAX@}{zPrslp`)~y%C(-J4D{[=}A:N 12W|NsXk0&q@_g__');
define('SECURE_AUTH_KEY',  'pwNMd-|w%mAsnd,Zk}!#mD#W[bZ-$;`Q>q)wV)YXi?@`YDge1QbJFf(-+DQ>os,f');
define('LOGGED_IN_KEY',    'pNQ!t((+<m>1V@;L>:korPh1 -Ki[&`k :IB91u/JHYRLUx|])#mJrI?wmTgHE_?');
define('NONCE_KEY',        '6_R;]J,S_U0_ m]8}+iZG|_j?OO][CZtmw~#pW|y^oE7nV aGJ :?;>;A`XrrTW}');
define('AUTH_SALT',        't,.cYR;-dUKGC^c?-p1&R@1BB^/0-TIy=iI!pos)fdU+ Eb[7tF;gH|F*WIn,g^~');
define('SECURE_AUTH_SALT', 'A~Sr0i8B-)8ocCwl+5?HEX^pAPKV~#{>gI|-A|;=g}%ZIqQ-W2xmLkY@(8pcZ a*');
define('LOGGED_IN_SALT',   ':u|]{|N9uI@KtrI59MVRyg>(l7pTxs[~LeQX-|K2?4+LjTi))B+DR()$l[p C5!7');
define('NONCE_SALT',       '(aH9;z]e7)AB.N &7hI-6P%/uj9F5DY6fni3I|HJg2,X<%Sn$!4sL]FW>8mY][+Y');
```

Your WEBSITE Engineer.com

Step #2 - Block Search Engine Spiders

- ✓ Spiders crawl your blog and index everything unless they are told not to.
- ✓ Place this code in a robots.txt file

```
#
User-agent: *
Disallow: /cgi-bin
Disallow: /wp-admin
Disallow: /wp-includes
Disallow: /wp-content/plugins/
Disallow: /wp-content/cache/
Disallow: /wp-content/themes/
Disallow: */trackback/
Disallow: */feed/
Disallow: /*/feed/rss/$
Disallow: /category/*
```

Your WEBSITE Engineer.com

Step #3 - Protect .htaccess

- ✓ .htaccess is the root level configuration file
- ✓ It is used to specify security restrictions throughout your site
- ✓ Add this code to prevent external access to this file

```
# STRONG HTACCESS PROTECTION</code>
<Files ~ "^.*\.([Hh][Tt][Aa])">
order allow,deny
deny from all
satisfy all
</Files>
```

Your WEBSITE Engineer.com

Step #4 - No Directory Browsing

- ✓ Don’t let visitors browse through your website directory
- ✓ Add the following code to .htaccess directory

```
# disable directory browsing
Options All -Indexes
```

Your WEBSITE Engineer.com

Step #5 - Secure wp-config.php

- ✓ wp-config.php contains your database username & password

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

Your WEBSITE Engineer.com

Step #6 - Protect Admin Files

- ✓ wp-admin should only be access by you (and fellow bloggers)
- ✓ You can use .htaccess to allow specific IP addresses to the directory

```
# deny access to wp admin
order deny,allow
allow from xx.xx.xx.xx #
This is your static IP
deny from all
```

Your WEBSITE Engineer.com

Step #7 - Prevent Script Injection

- ✓ Protect your site from script injections and modifications of _REQUEST and / or GLOBALS

```
# protect from sql injection
Options +FollowSymLinks
RewriteEngine On
RewriteCond %{QUERY_STRING} (\<|%3C).*script.*(\>|%3E) [NC,OR]
RewriteCond %{QUERY_STRING} GLOBALS(=|\[|\%[0-9A-Z]{0,2}) [OR]
RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})
RewriteRule ^(.*)$ index.php [F,L]
```

Your WEBSITE Engineer.com

Step #8 - Remove WordPress Version Number

- ✓ Add this line of code to functions.php folder

```
function wpbeginner_remove_version() {
return '';
}
add_filter('the_generator', 'wpbeginner_remove_version');
```

Your WEBSITE Engineer.com

Step #9 - Move WordPress Folder

- ✓ Move from the main directory
- ✓ http://codex.wordpress.org/Giving_WordPress_Its_Own_Directory

Your WEBSITE Engineer.com

Security Plugins

- ✓ If you aren't comfortable with FTP
- ✓ For WordPress beginners, adding these plugins will help you tremendously

Limit Login Attempts

- ✓ Limit number of login attempts possible (per IP address)
- ✓ Email Notifications
- ✓ http://wordpress.org/extend/plugins/limit-login-attempts/

Your WEBSITE Engineer .com

Sucuri Sitecheck Malware Scanner

- ✓ Scans for malware
- ✓ It will produce some false positives
- ✓ http://wordpress.org/extend/plugins/sucuri-scanner/

Your WEBSITE Engineer.com

Better WP Security

- ✓ Best Security Plugin
- ✓ Perfect for incorrect WordPress installations
- ✓ http://wordpress.org/extend/plugins/better-wp-security/

Better W

System Status

1. You are not enforcing strong passwords. Click here to fix.
2. Your Wordpress header is showing too much information to users. Click here to fix.
3. Non-administrators can see all updates. Click here to fix.
4. The *admin* user has been removed.
5. Your table prefix is fvqdkj_
6. You are not scheduling regular backups of your WordPress database. Click here to fix.
7. Your Wordpress admin area is available 24/7. Do you really update 24 hours a day? Click here to fix.
8. Your login area is not protected from brute force attacks. Click here to fix.
9. Your Wordpress admin area is hidden.
10. Your .htaccess file is NOT secured. Click here to fix.
11. Your installation is not actively blocking attackers trying to scan your site for vulnerabilities. Click here to fix.
12. Your installation accepts long (over 255 character) URLS. This can lead to vulnerabilities. Click here to fix.
13. You are allowing users to edit theme and plugin files from the Wordpress backend. Click here to fix.
14. Users may still be able to get version information from various plugins and themes. Click here to fix.
15. You have renamed the wp-content directory of your site.
16. You are not requiring a secure connection for logins or for the admin area. Click here to fix.

- Items in green are fully secured. Good Job!
- Items in orange are partially secured. Turn on more options to fully secure these areas.
- Items in red are not secured. You should secure these items immediately
- Items in blue are not fully secured but may conflict with other themes, plugins, or the other operation of your site. Secure them on if you can but if you cannot do not worry about them.

Your WP Engineer

Live Demo

Your WEBSITE Engineer.com

Backup Your Site

- ✓ BackupBuddy
- ✓ WordPress Backup to Dropbox
- ✓ WP-DBManager

Your WEBSITE Engineer.com

Backup Your Site

- ✓ It doesn't matter which of these tools you use, you need to be using one.
- ✓ Weekly: Database
- ✓ Monthly: All contents

Your WEBSITE Engineer.com

Overview

- ✓ The Initial Set Up
- ✓ Make your Website Harder to Hack
- ✓ Restore from a Hack

Step #1 - Don't Panic

- ✓ Even if something is terribly wrong, it can be fixed

Step #2 - Duplicate Everything

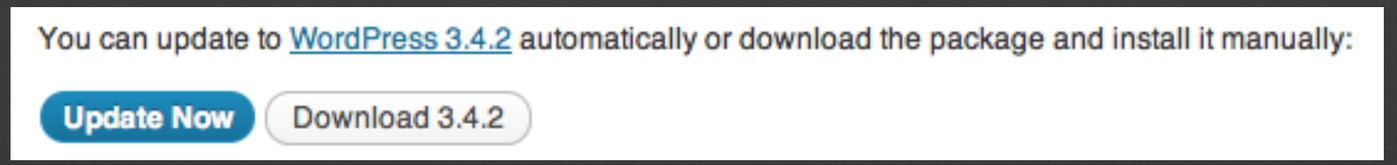
- ✓ Make a copy of all of your files and store on your computer
  - ✓ public_html folder on server
  - ✓ copy of your database

Your WEBSITE Engineer.com

Step #3 - Install a Fresh Version of WordPress

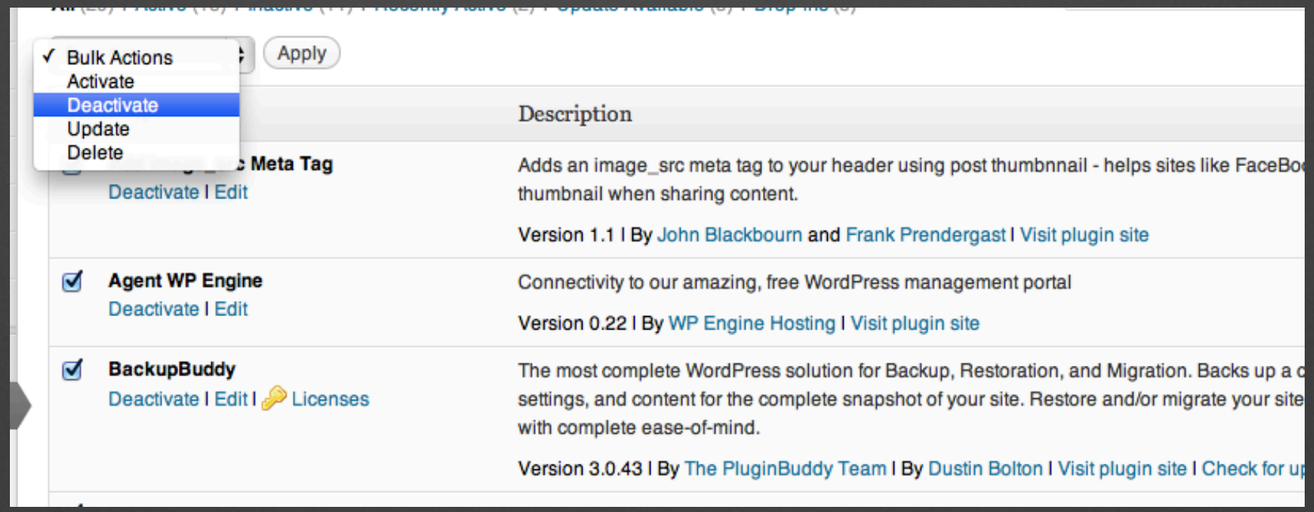
- ✓ Download a fresh copy of WordPress
- ✓ Copy all files except wp-content folder to server
- ✓ Or you can reinstall WordPress inside dashboard
- ✓ This will see if the hack is inside of WordPress

Your WEBSITE Engineer.com



Step #4 - Start Digging

- ✓ Disable all of your plugins
- ✓ Turn them on one at a time
- ✓ Try enabling twenty eleven or twenty ten theme



Your WEBSITE Engineer.com

Step #5 - Restore the Database

- ✓ Remember those backups that we set up?
- ✓ If you have blog posts that have published since your last backup, save those

Your WEBSITE Engineer.com

Site is Malware Free

- ✓ Are you done now?

Your WEBSITE Engineer.com

Step #6 - Change Passwords

- ✓ WordPress Passwords (I'd recommend usernames too!)
- ✓ FTP Passwords (even if you don't use them)
- ✓ Change the WordPress Salts in the wp-config.php file.

Your WEBSITE Engineer.com

Step #7 - Relax

- ✓ Go back to creating awesome new content!

Your WEBSITE Engineer.com

Good Practices

- ✓ Keep WordPress and plugs up-to-date
- ✓ Use plugins sparingly
- ✓ Use a reputable web host
- ✓ ALWAYS BACKUP

Your WEBSITE Engineer.com

Thank you!

- ✓ For more free WordPress information:
  - ✓ Listen to Your Website Engineer Podcast
  - ✓ Go to YourWebsiteEngineer.com
  - ✓ What do you want to learn?
    Email: Dustin@YourWebsiteEngineer.com

Your WEBSITE Engineer .com

Any Questions?

Your WEBSITE Engineer.com