LOCKING DOWN WORDPRESS

WORDPRESS PROS ON MAKING AND
KEEPING YOUR WORDPRESS
SITES SECURE

A CODEPOET.COM BOOK

CONTENTS

01

PREFACE

It's easy to blame WordPress when your client's site gets hacked and you're trying to talk them down from a ledge because the home of their beloved online business is now hawking Viagra on every single page. Likewise, when that just shipped site goes down entirely, and you're left holding the bag. Your clients start to question you, and to question this WordPress thing you told them would be so easy to use and maintain.

The reality of the situation is that you *can* take control of security for your WordPress installations, and while there's no 100% pure fix or safeguard, taking the right precautions and knowing what to do if things do go pear-shaped is priceless when you're shipping WordPress installations out in the wild.

In ***Locking Down WordPress***, seasoned WordPress pros Rachel Baker, Brad Williams, and John Ford take you through everything you need to know to make sure you have WordPress security under control.

RACHEL BAKER

RACHELBAKER.ME

RACHEL BAKER IS A FREELANCE WEB DEVELOPER LIVING IN CHICAGO, IL. RACHEL IS AN OCCASIONAL WORDCAMP SPEAKER AND PROJECT MANAGEMENT ADVOCATE

Her current pet project is a WordPress theme that ports Twitter's Bootstrap framework called BootstrapWP.

You can follow Rachel on Twitter at @rachelbaker or on Github.

What's the one, overriding security essential that goes into every project you work on?

Quality web hosting is a must for any type of website. Nothing is more frustrating than developing a beautiful custom WordPress site and cringing while migrating the site to the client's $5-$10.00/month shared hosting account that they maintain they've "never had a problem with." It's the equivalent of putting the engine of a Yugo into a brand new BMW. You are just asking for problems.

IT'S THE EQUIVALENT OF PUTTING THE ENGINE OF A YUGO INTO A BRAND NEW BMW. YOU ARE JUST ASKING FOR PROBLEMS

What do you look for in a web host?

Obviously, I look for a hosting company that can and hopefully has experience serving sites on WordPress. When I have a few options to choose from I call a few hosting companies within the budget and requirements of the client. Calling a company and asking questions about how they do business gives you great insight into how large or small the company is and how their culture operates.

My first question is, "What version are you currently running for the server's operating system, Apache web server, MySQL databases, and PHP?" If you need to be transferred more than twice for an answer to this question, don't use the hosting company. When I do get a response, I check it against the version release dates (easily found via Google, if I don't already know them) to get a general idea of how often they run updates and patches on their systems.

Finally, I ask for a written document(s) containing their server data backup, failover, and update or maintenance policy. If they don't have a written policy on what data they do back up on their servers and how long they keep that data, then I immediately look somewhere else.

IF THEY DON'T HAVE A WRITTEN POLICY ON WHAT DATA THEY DO BACK UP ON THEIR SERVERS AND HOW LONG THEY KEEP THAT DATA, THEN I IMMEDIATELY LOOK SOMEWHERE ELSE

What tips, suggestions, and guidelines can you share on hardening your WordPress setup against security vulnerabilities right after the five-minute install?

Instantly I move the `wp-config` file to the directory above the WordPress root folder. Using an FTP program, I check the folder permissions and file permissions and add rewrite rules to the `.htaccess` file to protect the `wp-includes` folder.

Are there specific instructions on how to do this?

Of course! You'll find instructions in the Security Bible Hardening WordPress from the WordPress Codex:

- http://codex.wordpress.org/Hardening_WordPress#Securing_wp-config.php
- http://codex.wordpress.org/Hardening_WordPress#FTP
- http://codex.wordpress.org/Hardening_WordPress#Securing_wp-admin

I STRESS THE IMPORTANCE OF BASIC MAINTENANCE SUCH AS KEEPING WORDPRESS AND ANY PLUGINS UP TO DATE

What guidelines would you give to a client on how to maintain a secure site after your work with them has finished?

I stress the importance of basic maintenance such as keeping WordPress and any installed plugins up to date, deleting any unused plugins or themes, disabling unused user accounts, and limiting permissions on new user accounts.

What plugins or third-party services do you recommend, if any, to your clients, and why?

For WordPress hosting I recommend WPEngine or ZippyKid. The piece of mind you get with proactive malware monitoring and removal along with automatic WordPress security updates is priceless.

If a specialized WordPress host is not an option I recommend Sucuri's yearly plan for proactive monitoring and blacklist removals.

How do you determine whether a plugin or theme are good fits for your project, and what caveats do you keep in mind when checking them out?

I don't use pre-built themes for any of my client projects. Developing custom themes allows me to have absolute knowledge and control over the code quality and overall site performance. There are a few plugins I use in every project: Akismet, BackupBuddy, Gravity Forms, WordPress SEO, and WYSIWYG Widgets. These plugins are stable, well coded, and they improve the client's overall experience using WordPress.

THERE ARE A FEW PLUGINS I USE IN EVERY PROJECT: AKISMET, BACKUPBUDDY, GRAVITY FORMS, WORDPRESS SEO, AND WYSIWYG WIDGETS

When searching for the right plugin, what security criteria do you use in making a choice?

If the client requests a plugin that I have never used before I review the plugin files and the plugin developer(s). When I review the plugin files I specifically look for WordPress Plugin API hooks, actions, and filters, properly sanitized data and MySQL statements, unique namespace items, use of the Settings API for any plugin settings or options, and nonces instead of browser cookies. I review the developer to verify reasonable response times to support items and that the plugin is actively developed.

What's the right and wrong way to set up user accounts for a new WordPress installation?

When creating user accounts for anything (server, accounting software or WordPress site) grant users the minimum privilege needed to do their job. Don't use "admin" as an account username and require strong passwords.

What's the biggest cause of security issues in your experience?

Outside of super cheap, shared hosting accounts, client website neglect is the biggest cause of security issues. Websites are built and forgotten about months later.

GRANT USERS THE MINIMUM PRIVILEGE NEEDED TO DO THEIR JOB

Which online resources do you turn to to keep up on best practices in WordPress security? Which would you recommend to others?

Hardening WordPress: it's the security bible.

Can you share a time you encountered a security-focused problem with WordPress and what you did to overcome it?

Recently, a volunteer organization I belong to had their WordPress site hacked. The site is hosted on Dreamhost and was compromised, which resulted in a malicious iframe being added to the footer to serve up spam. I followed the steps in the Codex FAQ My site was hacked. I changed passwords, replaced WordPress files with a newly downloaded .zip, reviewed log files, etc. I also reviewed the entire `wp-content` folder for contaminated plugins and theme files. I found several hacked themes that were not current active theme. I removed all the unused themes and plugins, and checked the database for any entries containing the iframe tag. After I was confident the site was clean, I checked it with the Sucuri Site Checker tool and opened a support ticket with Dreamhost asking them to verify the site was clean.

THE FAULT DOESN'T LIE WITH WORDPRESS, IT LIES WITH US

What's the one piece of WordPress security advice you'd like to share?

I believe as a developer community we have to get better about setting expections. We sell WordPress as "easy" and it is easy to a point. In five minutes you can be up and running with a dynamic website with zero coding knowledge. There are a wide variety of pre-built themes and plugins, where with a few clicks, customizing that website is a matter of visiting an "options" page. The expectation is that everything is that simple.

However, behind the WordPress dashboard are PHP, CSS, and JavaScript code files that connect to a MySQL database. To our clients and customers it's complicated, and they don't understand how WordPress works or the purpose of various files/folders. We are giving our clients fish, not teaching them how to fish or even what goes into fishing.

When a site gets hacked it's WordPress that gets the blame. The fault doesn't lie with WordPress, it lies with us. Having a website is a responsibility that doesn't stop once the site launches. We have to do a better job of conveying that ongoing attention and upkeep is a minimal requirement.

09

BRAD WILLIAMS

WEBDEVSTUDIOS.COM

BRAD HAS BEEN DEVELOPING WEBSITES FOR OVER 15 YEARS—DURING THE LAST FIVE, HE HAS FOCUSED ON OPEN-SOURCE TECHNOLOGIES LIKE WORDPRESS

Brad Williams is the co-founder of WebDevStudios.com, a co-host on WP Late Night, and the co-author of Professional WordPress and Professional WordPress Plugin Development.

What's the one, overriding security essential that goes into every project you work on?

I love to lock down the WordPress admin dashboard (`/wp-admin`) using an `.htaccess` file. This prevents anyone from even loading WordPress admin URLs unless they're from an IP specified in the `.htaccess` file. It's such a simple tip to implement. Just create an `.htaccess` file in your `/wp-admin` folder and add the following lines to it:

```
AuthUserFile /dev/null
AuthGroupFile /dev/null
AuthName "Access Control"
AuthType Basic
order deny,allow
deny from all
#IP address to Whitelist
allow from 123.123.123.123
```

This prevents anyone from accessing http://example.com/wp-admin unless their IP address is 123.123.123.123

What tips, suggestions, and guidelines can you share on hardening your WordPress setup against security vulnerabilities right after the five-minute install?

Stay secure locally. When accessing your web host use SFTP or SSH instead of FTP. Standard FTP passes your credentials unsecured, meaning anyone could sniff those out and steal them. SFTP and SSH pass data encrypted so there's no need to worry about someone stealing them. Most hosts have SFTP available, so if you aren't sure just ask your host about it.

Use SSL if possible on your website. Accessing the WordPress dashboard using SSL (https://) will encrypt all data passed to and from WordPress. This is especially important on the login screen. To enable SSL in WordPress just add the following options to your `wp-config.php` file:

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

If you aren't sure if your website has SSL, simply visit your website using https:// instead of http:// Most hosting companies can purchase and configure an SSL certificate if you ask for one.

It's also important to use strong passwords. This is an obvious tip, but you'd be surprised at how many people don't actually follow this rule. Passwords should also be changed on a schedule. Set a reminder in your calendar to change your passwords every month for added security.

The Codex has a great article on security tips.

What guidelines would you give to a client about maintaining a secure site after your work with them has finished?

Update, update, update. A good majority of WordPress sites get hacked because WordPress, themes, and/or plugins are out of date. It's so important to update your software to avoid being hacked.

What plugins or third-party services do you recommend, if any, to your clients, and why?

Login Lockdown is a really good security-related plugin. This plugin limits the number of failed log in attempts you can have while trying to log in to WordPress. If someone is trying to guess your password, it will stop them from doing so.

BulletProof Security is also a really good security plugin. This plugin has a ton of security-related features including `.htaccess` directory lockdowns, file/folder permission scanning, and a lot more. It also has very good documentation explaining the various features available in the plugin.

Sucuri.net is hands down the best malware scanning and cleanup service out there. They offer automated daily scans of your website to check for hacks and malicious code. If a hack is found they have automated scripts and a very knowledgeable staff to help clean up the infection.

BACKUPS SHOULD ALSO BE A VERY IMPORTANT PART OF YOUR WEBSITE. HAVING A SOLID BACKUP CAN MAKE CLEANING UP A HACK MUCH EASIER

Backups should also be a very important part of your website. Having a solid backup can make cleaning up a hack much easier. For a plugin I highly recommend BackupBuddy from PluginBuddy and iThemes. This plugin provides hands-off, scheduled backups of your entire WordPress install that you can push to Amazon S3, Dropbox, email, and other places. For a service I love VaultPress. This service takes real-time snapshots of your WordPress install making it very easy to restore your website should it get hacked.

How do you determine whether a plugin or theme are good fits for your project, and what caveats do you keep in mind when checking them out?

The first thing I check out is who created the plugin or theme. Are they a known member of the community with an established reputation? Download count is also a good gauge. If you're comparing two plugins that add a similar feature to WordPress, such as a Facebook like button, and one plugin has 100,000 downloads and the other has 100 downloads, I would go for the plugin with the higher download count. It's safe to say that plugin has been used and tested in more environments and is probably a more stable and secure plugin.

GO WITH THE PLUGIN WITH THE HIGHER DOWNLOAD COUNT

Also look in the support forum for the plugin on WordPress.org. Reading some of the forum threads can also help determine how well the plugin has been coded and if it's actively supported.

When searching for the right plugin, what security criteria do you use in making a choice?

Similar to the previous question, I generally go by the plugin author. I look at their WordPress.org profile and see how many plugins they've released, how many downloads it has, whether they're active in the support forum, and whether they're active in the WordPress community. As a developer I can skim through the source code to see how they built the plugin, but I know most people who use WordPress aren't developers and have no idea what things like escaping and sanitizing mean.

What's the right and wrong way to set up user accounts for a new WordPress installation?

When you first install WordPress you will be asked to create a default admin account. Be sure to use a unique username for this account. Prior to WordPress 3.0, the default WordPress account was always named "admin." Hackers know this and have bots that look for WordPress installations and use a dictionary attack to try and login under the admin account. If that account doesn't exist they won't have a shot. Knowing your username is half the battle, now all they have to guess is your password.

> **KNOWING YOUR USERNAME IS HALF THE BATTLE, NOW ALL THEY HAVE TO GUESS IS YOUR PASSWORD**

What's the biggest cause of security issues in your experience?

Websites running old versions of WordPress. If an incremental WordPress update is released (3.4.x), and it's announced that it's a security update, it is very easy to compare the new and previous version of WordPress to determine what that security vulnerability is. The hackers can do this too, so they will know what to exploit to hack your site. Staying up-to-date is the single most important thing you can do to protect your WordPress website.

Can you share a time you encountered a security-focused problem with WordPress and what you did to overcome it?

We generally encounter security-focused problems having to do with the setup on the hosting account. For example many hosts used to require the

`/wp-content/uploads` folder to be set to 777, i.e., a very loose folder permission that could allow a hacker to upload any file they want to your uploads directory. A good rule of thumb is to set file and folder permissions at 644 for files and 755 for folders. Here's where you can learn more about file permissions.

WE ALWAYS TALK TO THE CLIENT AND MAKE THEM AWARE THAT IF THEY AREN'T FAMILIAR WITH WHAT THEY'RE DOING THEY SHOULD ASK US FOR HELP

What's your take on permissions/access levels for new users? How much power do you give to your clients in this respect, and if at all, how much do you hold back for the good of both of you?

Generally speaking we give our clients full access to their website and hosting account. We also always talk to the client and make them very aware that if they aren't familiar with what they're doing they should ask us for help. Most clients understand their technical limits and when they should ask for help.

Which online resources do you turn to to keep up on best practices in WordPress security? Which would you recommend to others?

Sucuri.net has a great security focused blog. They write about security hacks they've encountered, cleanup processes, and overall good security-related news to follow. Google also has a very nice security related blog.

If your site gets hacked, what are the steps you should take to minimize the damage, pinpoint the vulnerability, and repair it?

Immediately enable some type of maintenance mode to take the website offline from the public. If your site has been hacked you'll want to limit the exposure your site has to the public to decrease the chance of a negative rating from search engines and antivirus programs.

IF YOUR SITE HAS BEEN HACKED YOU'LL WANT TO LIMIT THE EXPOSURE YOUR SITE HAS TO THE PUBLIC TO DECREASE THE CHANCE OF A NEGATIVE RATING FROM SEARCH ENGINES AND ANTIVIRUS PROGRAMS

If you plan to clean the hack yourself I recommend the Exploit Scanner plugin. This plugin searches your WordPress files, plugins, themes, and data in your database for suspicious looking code. This is a more advanced plugin because it doesn't actually fix anything, but rather, it reports suspicious findings to you so you can determine if it is in fact a hacked file or not.

The Codex also has a great article on cleaning up a hacked site.
If you want to hire a company to clean your infected site, I always recommend Sucuri.net. Their prices are so justifiable for the services they offer. There really is no comparison when it comes to a security service like this.

What's the one thing you found out about securing your WordPress site(s) after it was too late?

File and folder permissions being set too loose. You'll want to verify your files and folders are set with the proper permissions before it's too late or a hacker may be able to upload a malicious file to your server.

IF YOU AREN'T COMFORTABLE UPDATING YOUR WORDPRESS WEBSITE THERE ARE PLENTY OF FREELANCERS AND COMPANIES OUT THERE TO DO IT DAILY

What's the one piece of WordPress security advice you'd like to share?

Update! Have I said that already? :) It really is that important. If you aren't comfortable updating your WordPress website there are plenty of freelancers and companies out there that do it daily and can help keep your website running the most current versions of WordPress, your theme, and all plugins. It really is the most important thing you can do to keep your website safe from hacks.

Is there any advice you can offer or a specific process you follow when clicking on the dreaded update button? What tips and tricks have helped you avoid the white screen on updating WordPress?

Always backup before hitting that update button. Worst case scenario: you can always roll back to your backup. I generally go through each one of my plugins and update them individually prior to updating WordPress.

Most plugins authors will release an update if their plugin isn't compatible with the newest version. You can also check the plugin's changelog tab on WordPress.org to see what items are contained in the newest version. If you stick with more popular plugins, the chance of your website exploding after a WordPress update is very slim.

THERE ARE ACTUALLY VIRUSES IN THE WILD THAT WILL INFECT YOUR LOCAL COMPUTER, AND THEN LOOK FOR OPEN FTP CONNECTIONS AND AUTOMATICALLY UPLOAD A HACK FILE TO YOUR WEB HOST USING THAT CONNECTION

Were there any important questions we didn't ask or questions you wished we'd asked?

One security tip that many people don't think about is making sure your local computer is clean from viruses and malware. There are actually viruses in the wild that will infect your local computer, and then look for open FTP connections and automatically upload a hack file to your web host using that connection. This is pretty scary stuff, so it's very important that your local computer is also protected using a strong antivirus program with scheduled scans.

...oh, and UPDATE! :)

JOHN FORD

JOHNFORD.IS

JOHN FORD, A RECENTLY-GRADUATED VAULTPRESS DEVELOPER, THRIVES ON HELPING OTHERS DEMYSTIFY THE SOMETIMES COMPLEX AND OFTEN MISUNDERSTOOD, “BACKSTAGE” OF THE INTERNET.

Ensuring the safety of WordPress users everywhere just adds fuel to his happy meter.

You can find him on the web at JohnFord.Is

What's the one, overriding security essential that goes into every project you work on?

Strong passwords. I use 1Password to create difficult passwords and log in to WordPress sites automatically for me. That way all of the passwords I use are different for each site, extremely hard to guess, and I don't have to remember each one. KeePass is a similar open source tool for creating and storing passwords.

ALL OF THE PASSWORDS I USE ARE DIFFERENT FOR EACH SITE, EXTREMELY HARD TO GUESS, AND I DON'T HAVE TO REMEMBER EACH ONE

What tips, suggestions, and guidelines can you share on hardening your WordPress setup against security vulnerabilities right after the five-minute install?

You should always make sure the permissions on `wp-config.php` are not world readable especially in a shared hosting environment. If someone on the server gets access to your database settings or authentication keys they can get access to your WordPress admin and cause trouble. Each server configuration requires different file permissions but most of the time 600 should work for the `wp-config.php`.

For extra hardening, consider adding HTTP authentication to your `/wp-admin/` area. By password protecting the admin area it's harder to brute-force access. You'll need to make sure to allow `/wp-admin/admin-ajax` or things such as uploads may not work. Here is an example of what your `.htaccess` should look like after password protecting `/wp-admin/`:

```
AuthUserFile /path/to/your/htpasswd
AuthType basic
AuthName “Restricted”
require valid-user
<Files admin-ajax.php>
   Order allow,deny
   Allow from all
   Satisfy any
</Files>
```

What guidelines would you give to a client about maintaining a secure site after your work with them has finished?

- The first step is always brief education on why using strong and unique passwords for every site is important. This goes for WordPress, FTP, web hosting control panel, email accounts, or anything that needs a password.

- WordPress, themes, plugins, and any other software on the server need to be kept up to date. This goes for all sites on your web hosting account.

- Remove unused themes and plugins. Even when not activated, a vulnerable plugin or theme can be used to attack a site.

What plugins or third-party services do you recommend, if any, to your clients, and why?

I’m a bit biased since I worked on the project, but when it comes to security I always recommend VaultPress. VaultPress hotfixes known security threats, regularly scans for malicious code on your server, provides notifications, automated fixes, and you have access to the team if your site is ever attacked and you need help cleaning it up. Along with the security features, it provides real-time backups of your site. Every time you add a new post or upload a photo in WordPress the individual change is synced.

> **I USUALLY LEAN TOWARD SIMPLISTIC PLUGINS IF I'M NOT BUILDING SOMETHING MYSELF. I LIKE A PLUGIN THAT CAN DO ONE OR TWO TASKS REALLY WELL**

Although, not security related, I install WP Super Cache on all WordPress sites that I work on. It's great at caching pages, reducing the load on the server, and it's really easy to set up.

How do you determine whether a plugin or theme are good fits for your project, and what caveats do you keep in mind when checking them out?

I usually lean toward simplistic plugins if I'm not building something myself. I like a plugin that can do one or two tasks really well. It makes it easier to evaluate and use the code in the way that I want. If I think a plugin is useful for the project and will save time and money for the client, without compromising quality, then I'll use it.

I also take a look at the plugin page in the Plugin Directory. Do I know the author? How often do they update the plugin? When was it last updated?

How many people use the plugin? You can get a good sense if the plugin is actively developed which usually means the developer(s) will update the plugin quickly if any problems are found.

I ALSO TAKE A LOOK AT THE PLUGIN PAGE IN THE PLUGIN DIRECTORY. DO I KNOW THE AUTHOR? HOW OFTEN DO THEY UPDATE THE PLUGIN? WHEN WAS IT LAST UPDATED? HOW MANY PEOPLE USE THE PLUGIN?

When searching for the right plugin, what security criteria do you use in making a choice?

It may not be practical for everyone, but I like to review the code. I typically take a quick look to make sure the plugin can only be executed with the proper WordPress capabilities, that SQL queries are done through the appropriate `$wpdb` functions and escaped, and that data is sanitized with the proper functions before being printed to the screen.

I also take a look at the plugin page in the Plugin Directory. Do I know the author? How often do they update the plugin? When was it last updated? How many people use the plugin? You can get a good sense if the plugin is actively developed which usually means the developer(s) will update the plugin quickly if any problems are found.

What's the right and wrong way to set up user accounts for a new WordPress installation?

- Right way—don't use the username 'admin' and use strong passwords
- Wrong way—weak passwords

SO MANY PEOPLE USE SIMPLE PASSWORDS AND/OR THE SAME PASSWORD FOR ALL OF THEIR LOGINS

What's the biggest cause of security issues in your experience?

Old vulnerable versions of TimThumb seem to be a common entry point for attacks these days but I would normally say compromised passwords. So many people use simple passwords and/or the same password for all of their log ins. If an attacker guesses the password or sniffs it on an insecure wireless network they are in. If it's the same password you use for your email account watch out—an attacker can get into all of your accounts by having "reset password" emails sent.

Can you share a time you encountered a security-focused problem with WordPress and what you did to overcome it?

My most painful experience was due to a shared hosting server configuration. By default, the server allowed read access to other files on the server (an extremely bad practice in my view). An attacker somehow gained access to an account on the server, read the `wp-config.php` on the account I managed, and used the authentication keys to spoof a login to the admin area. From there, they edited theme files and inserted malicious JavaScript that tried to serve PDF files infected with malware. Sneaky bastards.

To fix things, I updated the permissions on all files so none of them were world readable, changed all passwords (FTP, hosting control panel, database, WordPress, etc.), and actually switched providers soon after.

Another good step would have been to disable the theme and plugin editor by adding the following to `wp-config.php`:

```
define( ‘DISALLOW_FILE_EDIT’, true);
```

WHEN CHOOSING A HOSTING PROVIDER THE PRIMARY QUALITY I LOOK FOR IS SOLID SUPPORT

What qualities do you look for in a hosting provider?

When choosing a hosting provider the primary quality I look for is solid support. Computers have issues, networks go down, and people make mistakes. No matter which host you choose your site won’t be up 100% of the time. Most of them offer the same type of hardware, software, and specifications that will run 99% of the sites out there so looking for the fanciest specs usually isn’t that important (but do make sure they make regular backups that you can access).

If something does go wrong or you need support are they there for you? Are they speedy and helpful? Are they transparent and post notifications online immediately when something happens? That peace of mind and knowing someone is there to help goes a long way when your lolcats knitting site goes down and you have an emotional breakdown. I’ve been there and have felt the pain.

What's your take on permissions/access levels for new users? How much power do you give to your clients in this respect, and if at all, how much do you hold back for the good of both of you?

Most clients get administrator privileges. We always have a discussion about uploading plugins and changing code so they understand what it means. I've worked with really great clients and I want them to have full control over their sites. If someone on their team only needs to update content we'll make them an Editor.

WE ALWAYS HAVE A DISCUSSION ABOUT UPLOADING PLUGINS AND CHANGING CODE SO THEY UNDERSTAND WHAT IT MEANS

Which online resources do you turn to to keep up on best practices in WordPress security? Which would you recommend to others?

- Hardening WordPress
- Data Validation

If your site gets hacked, what are the steps you should take to minimize the damage, pinpoint the vulnerability, and repair it?

- Let your web host know what happened. They may have other sites that are infected on their servers and be able to provide helpful information.

- Make a full backup of the infected site. It's helpful for reviewing what happened and in case you mess up something during the repair.

- Change all of your passwords and the authentication keys in the `wp-config.php`
- Remove any old themes, plugins, and unused code from your server.

IF YOU DON'T HAVE THE ABILITY TO FIX THE INFECTED FILES THE BEST THING TO DO IS RESTORE FROM A RECENT CLEAN BACKUP

- Update all code on your server. I even like to do a re-install of WordPress from the Updates page in the admin so all of the WordPress files are overwritten with fresh copies. You may also want to reinstall themes or plugins with fresh copies to make sure no malicious code was inserted.
- Check that the file permissions on your files are correct, especially `wp-config.php` and uploads.
- Remove the rogue code and make sure you check all sites on your hosting account. There are tools that can help scan and clean the infection such as VaultPress. Exploit Scanner also scans for certain exploits.
- If you don't have the ability to fix the infected files the best thing to do is restore from a recent clean backup. If you keep regular backups of your site then you should have the peace of mind that the site can always be fixed.

The common areas of entry tend to be:

- Compromised passwords
- Exploitable themes/plugins/code

IF AN ATTACKER CAN'T GUESS YOUR PASSWORD OR FIND BAD CODE TO EXPLOIT THAT TAKES AWAY THE MAIN WAYS THEY LIKE TO ENTER

From there, you may want to take a look at the server access logs. Search for any bad file names that you found on your server, patterns passed as query strings, or dates/times that may clue you in to when the attack happened. You may be able to find the point of entry from there and see the IP address and which files the attacker used to wreak havoc on the site. Many attacks are more clever these days and use the POST method to send data to the server which most access logs don't record. Finding POST requests on files that shouldn't be posted to is a good sign that something is funny.

Here's some additional info on what to do if your site is hacked.

What's the one piece of WordPress security advice you'd like to share?

Since I've said use strong passwords over and over the next most important advice is keeping WordPress, themes, plugins, and any other software on the server up to date. If an attacker can't guess your password or find bad code to exploit that takes away the main ways they like to enter a site. Most of the automated scripts they use look for those weaknesses.

TL;DR

OUR COLLABORATORS' ADVICE IN SHORT SHOTS

You need not read the entire book to refresh your memory on the tip that changed the way you work. We've pulled out the best bits of advice from the narrative and have chunked 'em up to make it easy for you to find the information you need, fast.

This handy legend tells you who said what*:*

- Rachel Baker (RB)
- Brad Williams (BW)
- John Ford (JF)

HOSTING

- Beware cheap ($5-$10/month) shared hosting accounts. (RB)
- Look for hosts with experience hosting WordPress sites. (RB)
- Look for hosts with solid support. (JF)
- Look for hosts that are transparent: who communicate quickly and post issues online. (JF)
- Make sure your host does regular backups that you can access. (JF)
- Call your potential host to find out which versions of Apache web server, MySQL, and PHP they're running. Check the version release dates with a Google search. (RB)

- Ask your host for written documents containing their server data backup, failover, and update or maintenance policy. If they don't have them, find another host. (RB)
- Recommended hosts: WP Engine and ZippyKid (RB)

HARDENING & PROTECTING WORDPRESS

- To harden your WordPress install, follow these steps.
- Keep WordPress, themes, and plugins up to date. Always. Period. (BW)
- If you're unsure about how to update WordPress, themes, and plugins, hire someone to do it for you. (BW)
- Backup your site before you update WordPress, themes, and/or plugins. (BW)
- Disable unused user accounts. (RB)
- Never use "Admin" as your username. Ever. (BW)
- Grant users the minimum privilege they need to do their jobs. (RB)
- Require strong passwords. (RB)
- Use 1Password or KeePass to create strong passwords. (JF)
- Use a different, strong password for every site log in. (JF)
- Lock down the WordPress admin dashboard (`/wp-admin`) using an `.htaccess` file. (BW)
- Use SFTP to access your web host. (BW)
- Enable SSL on your WP install. (BW)
- Change your passwords once a month. Set a reminder in your calendar if you have to. (BW)
- Do backups. Recommended: BackupBuddy, VaultPress (BW)
- Set file permissions at 644 and 755 for folders. (BW)
- Ensure that the permissions on `wp-config.php` are not world readable especially in a shared hosting environment. (JF)
- Consider adding HTTP authentication to your /wp-admin/ area. (JF)
- Read Sucuri.net's blog. (BW)
- Read Google's security blog. (BW)

CHOOSING THE RIGHT PLUGIN

- Look for WordPress Plugin API hooks, actions, and filters. (RB)
- Look for properly sanitized data and MySQL statements, unique namespace items, use of the Settings API for any plugin settings or options. (RB)
- Look for plugins that use nonces instead of browser cookies. (RB)
- Check out how quickly the developer responds to support requests. (RB)
- Check out forum threads to see how well the plugin is supported. (BW)
- Is the developer a known and respected member of the community? (BW)
- Look for a plugin that does one or two tasks really well. (JF)
- If two plugins do similar things, choose the one with the higher download count. (BW)

YOU'VE BEEN HACKED. NOW WHAT?

- Take the site offline. Now. That way you avoid getting a bad rap from search engines and antivirus programs. (BW)
- Let your web host know what happened. (JF)
- Make a full backup of the infected site. It's helpful for reviewing what happened and in case you mess up something during the repair. (JF)
- Change all of your passwords and the authentication keys in the `wp-config.php`. (JF)
- Remove any old themes, plugins, and unused code from your server. (JF)
- Update all code on your server. Re-install WordPress so all of the WordPress files are overwritten with fresh copies. (JF)
- Reinstall themes or plugins with fresh copies to make sure no malicious code was inserted. (JF)

- Check that the file permissions on your files are correct, especially `wp-config.php` and uploads. (JF)
- Remove the rogue code and make sure you check all sites on your hosting account. There are tools that can help scan and clean the infection such as VaultPress. Exploit Scanner also scans for certain exploits. (JF)
- If you don’t have the ability to fix the infected files the best thing to do is restore from a recent clean backup. (JF)
- Check your server access logs. Search for any bad file names that you found on your server, patterns passed as query strings, or dates/times that may clue you in to when the attack happened. (JF)

RESOURCES

Here's a handy list of all the resources our collaborators cited in *Locking Down WordPress*.

HARDENING YOUR WORDPRESS INSTALL

- WordPress Codex
- Hardening WordPress
- Securing `wp-config.php`
- FTP
- Strong passwords
- WP Codex: My site was hacked (FAQ)
- Setting file permissions
- Data validation

GRACIOUS HOSTS

- WP Engine
- ZippyKid

RESOURCES

MONITORING, BACKUP, AND MALWARE BEWARE

- Sucuri.net
- BackupBuddy
- VaultPress

STRONG PASSWORDS

- 1Password
- KeePass

PLUGINS WE LOVE

- Akismet
- BackupBuddy
- Gravity Forms
- WordPress SEO
- WYSIWYG Widgets
- LoginLockdown
- Bulletproof Security
- Exploit Scanner
- WP Super Cache

RESOURCES

FURTHER READING

- Sucuri.net’s blog
- Google’s security blog

A CODE POET BOOK

Locking Down WordPress is the third in a series of free books geared toward, and focused on, the needs, strategies and field tactics of people who work with WordPress in the real world to build sites for clients, friends, and family.

Visit codepoet.com to see additional Code Poet resources, sign up to receive updates, or let us know what you think.

We'd love to hear your ideas. Let us know what we should be focusing on next to better serve your needs via our quick Code Poet survey.