WP Security Ninja

By

Paul Okeeffe
Global Marketing Ninja

Disclaimer
All the material contained in this book is provided for educational and informational purposes only. No responsibility can be taken for any results or outcomes resulting from the use of this material.
While every attempt has been made to provide information that is both accurate and effective, the author does not assume any responsibility for the accuracy or use/misuse of this information.

- Table of Contents -

How to Think About WordPress Security – Covering the Basics

When it comes to WordPress security, it can be easy to feel a little scared and overwhelmed. If you don't consider yourself to be particularly tech savvy, then you might not fully grasp where the security risks lie in a WordPress site and you may not know where to *start* when it comes to fixing them. You might hear people throwing words like 'zero hour threats' and 'brute force attacks' around and just feel lost. So what do you do? Give up? Pay a security team?

And Breathe…

For the most part, the latter won't be necessary. If you are dealing with payments and transactions then you might want to consider consulting with a company about security services but if your small business website is more of an online advert, or a blog, then you likely won't need any highly advanced security measures.

In this case, the main threat to your security will be from 'bots' designed to try and hack websites on scale and in security flaws that exist within WordPress and the plugins you install (this is what zero hour means).

This means it's relatively simple and easy to protect yourself and your blog using the following simple steps:

- Add some security plugins such as CAPTCHAs for your log in forms
- Change your passwords to something hard to guess
- Avoid installing plugins that you haven't heard of without checking reviews first
- Avoid installing *too many* plugins
- Run updates on WordPress itself and on all plugins

If you do just these basic things, then you will be protected against the large majority of threats and should find that you experience minimal issues.

Your Own Security

One last thing to consider is your own personal and physical security. This means avoiding malware on your computer and avoiding logging into your

WordPress account on public machines. While hackers rarely target individuals so much as using software en-masse, when they *do,* they will often do so by first planting malware on the user's computer.

For instance, some malware works by recording the key strokes that you make on your keyword, which makes it very easy to record things like passwords. You can avoid this by using your mouse to move the cursor around when typing passwords (the cursor can't be recorded) but of course it's just easier to maintain security on your computer and to avoid using machines that you aren't familiar with.

WordPress security isn't rocket science – most often it comes down to common sense!

How to Stop People From Logging Into Your WP-Admin Panel

WordPress is designed to make everything simple and straightforward for new users and offers perhaps the quickest way that anyone can go about setting up their own website.

Unfortunately, in a bid to keep things simple, WordPress *also* introduces unique risks and dangers. One example of this is the WP-Admin panel, where you will likely log in and make your changes to the site. As the site administrator, all you need to do by default is go to your address/wp-admin and enter your password and you can start making changes.

The problem is, anyone who knows anything about WordPress will suspect this, meaning they now know how to locate your log-in page. This means they can now start attempting to log in – which puts you at risk.

Some Changes You Can Make

Many people don't realize just how vulnerable their website is right from the start if they've kept the default settings on WordPress.

Prior to the 4.1.2 update of WordPress, the CMS would actually go so far as to tell you whether it was the password or the username that you got wrong. This means that a would-be hacker could potentially only have to guess at one of those fields rather than both, drastically reducing the amount of time it would take them to be successful logging in. The first thing to do then if you haven't already, is to update to the latest version of WordPress.

Another tip is to move your WordPress login page URL. This won't make a gigantic difference to a 'bot' which can easily find the page still but it could deter human attempts to log in to your site.

What's a bot? That's essentially a program that attempts to log in to your WordPress by using thousands of password combinations until it finds the right one. This is the main thing you'll have to defend yourself against if you hope to keep your site safe from unauthorized logins, so make sure that you add a spam filter to your login which asks you to solve a maths sum or to identify some letters. This will prevent all but the most advanced bots from trying to log into your account.

Finally, think carefully when choosing your password. Pick something memorable but at the same time, make sure that it is long and seemingly random. Think both in terms of how you can defend yourself from machines *and* how you can defend yourself against human hacks.

How to Protect Yourself From Brute Force Attacks

One of the most straightforward types of attack you will have to deal with as a blogger, is the 'brute force' attack. This is a type of attack on your security that utilizes a 'bot' or computer script, designed to try and break your username and password combinations by using sheer *volume* of attempts. Here we will look at why this is a threat and at what you can do to solve the problem.

What is Brute Force?

So how does this work? Essentially a brute force attack occurs when a computer program attempts to log into your control panel, post spam or sign up as a user simply by entering a huge volume of username and password combinations. Eventually, the hope is that it will land on the correct combo by chance and thus gain access to your site's backend, or be able to make changes/post spam.

So how do you prevent this from posing a risk to your own security?

The Right Username and Password Combination

One of the most straightforward ways to defend yourself against brute force attacks is to use a smart username and password combination that will be hard for a machine to guess – even after millions of attempts.

If your username is currently 'Admin' (the default) then you should change that *immediately*. Likewise, it's a good idea to avoid having a password that is the same as your username when you post on the site, or that is the same as your website name. Ideally, your username should be long and random and involve varying cases and numbers – just like a good password. This way, the chances of it getting entered are slim.

With passwords you need to be even more careful as this is where the software will enter the most attempts. The single best tip here is to make your password *long*. Great examples of long passwords include the first few words of a song for instance.

CAPTCHA

Another tip is to use plugins that add captcha to your site. This is a small test that will involve identifying letters in an image or performing basic math – no

doubt you will have encountered this yourself online. The reason this is useful is that it prevents brute force programs from making even a few attempts to hack your site. Unless the software is very advanced – enough to include OCR (optical character recognition) – then basic captcha will protect you from the majority of these kinds of attacks.

How to Get Rid of Analytics Spam

If you have a WordPress blog, then you're probably keen to get seen by as many people as possible. To this end, you likely have some form of analytics set up to allow you to keep an eye on how many people are visiting your site and what its most popular content is. Popular options include Jetpack stats and Google Analytics.

Either way, this means you will be likely to have encountered the very annoying 'analytics spam' that plagues these areas of your site. This spam can be found when you look at the 'referers' to your website and find that sites including 'Semalt.com' and 'buttons-for-websites.com' are sending people to your page. This is exciting until you realize that it's a lie and that these are in fact just spam bots, destroying dreams and messing up your data. And some of them are malicious.

What is Referral Spam?

This referral spam is created by scripts designed to ping your site and make it look like you had a visitor. Some of these bots are almost like 'digital graffiti' and don't really do anything negative. Others though are malicious and are trying to do things like set up fake accounts – you're just seeing the trail.

Fixing the Problem

So how do you fix this problem?

The first step is to use Google Analytics rather than other platforms. This gives you the most control and the most flexibility to alter your analytics. Here for instance there's a checkbox that says 'Filter Known Bots & Spiders'. If you tick this, you can remove some of the most common 'bots' from your data. It's still there but at least your data will be accurate.

For the rest, you need to create 'filters' on your data sets. These will show you the information you're looking for only, while removing bots and spam. Go to Audience -> Technology and then Network and choose 'Hostname' as the 'primary dimension' for filtering. Now you should put down valid hostnames like translate.google.com, web.archive.org and add the rest to a regex expression.

You can also filter by Network Domain – which will normally be a brand such as Comcast, Verizon or .edu. This is the ISP that your visitors use when visiting you. Non-human users meanwhile use things like cloud service providers and

Tier 1 telecoms. Another trick is to sort your list by the bounce rate, which will expose fake network domains like Googlebot that don't spend any time reading your content.

Put these in a regex expression and you'll have much cleaner – if not perfect – data.

Common and Recent WordPress Security Threats

If you use WordPress to provide the backbone of your website, then you will be using the same platform as many of the biggest websites on the net, meaning that you can rely on its capability to help you become very successful. There are countless people working on WordPress security around the clock and the whole system was built with security in mind from the start.

But that said, no website is completely impervious to attack and even WordPress proves vulnerable from time to time. Here we will look at some examples of things that can go wrong…

WordPress SEO by Yoast

WordPress SEO is a plugin design by Yoast which many bloggers use to promote their sites on search engines. A while back, a security flaw was discovered that left websites open to a type of attack called a 'Blind SQL Injection'. This essentially would ask the system 'true or false' questions and use this as a way to insert SQL queries into the database. This could result in malware and spam appearing on a webstie.

Luckily, Ryan Dewhurst of WPScan found the problem before the hackers did and let Yoast know. This in turn led to an update being issued rapidly that fixed the problem. If you have been updating Yoast regularly then you shouldn't be at any risk of this problem – but this does highlight the importance for regularly updating plugins and of being careful not to use too many.

XSS Vulnerability

Many WordPress plugins were recently open to Cross-Site Scripting via add_query_arg() and remove_query_arg(). You don't really need to know what that means, except that it affected a *lot* of big plugins including Jetpack, WordPress SEO, Ninja Forms and more. Again, recent updates have mostly fixed this problem.

Other Risks

Many other risks face users of WordPress sites. For instance, many sites let you see which version of WordPress they use by simply looking at the page header meta tag or readme.html file. Likewise, there's an inherent risk in allowing vis-

itors to sign up as users even when there's no community aspect to your site. This feature is on by default, so make sure you remove it!

As you can see then, WordPress is far from being flawless which means it falls to *you* to be vigilant in looking after your security. No platform is perfect, so ultimately the responsibility always belongs to the site owner.