Guide

WordPress. The most hacked CMS in the world and how not to become a part of the statistic.

Paweł Wałuszko 10.06.2019

Without a doubt, WordPress is our favorite Content Management System (CMS) in recent years. According to most recent statistics of W3Techs, WordPress accounts for roughly 60% of entire CMS market share in the first quarter of 2019. Other CMS platforms, such as Joomla and Drupal account for less than 7 per-cent together.[1]

Given its ergonomic interface, thousands of pre-made templates and even more funcitonality-extending plugins, it's no wonder that many SMBs choose WordPress as their default CMS of choice. Moreover, the default out-of-the-box install of WordPress is quite secure in itself.

However, millions of active users also means millions of developers tinkering with the code. This is a double-edged sword: on one hand, the open-source nature of WordPress allows anyone to inspect, build upon, or improve the code. If a security issue is found, it can be quickly patched. On the other hand, the open-source nature allows the black hats to closely examine the code for potential exploits—and create mischief. Moreover, given that WordPress enjoys such outstanding market success, it cannot benefit from the model of "security by obscurity" – which perhaps works in favor of other CMS platforms out there.

The numbers

Despite (perhaps because of) its market success, year after year WordPress ranks as the top security-compromised CMS.

According to a 2017 study on more than 34,000 websites and subsequently published on the *Hacked Website Report 2018* by Sucuri – a subsidiary of Go Daddy Operating Company – WordPress accounted for 83% of compromised CMS platforms.[2] What's worrisome is the the fact that this is a continuing, noticeably upward trend. In the 2019 report, for example, this number already reached 90%.[3]

The issues

One may be quick to jump to conclusion, that perhaps WordPress is security-deficient in itself. Nothing is farther from the truth, however. WordPress is an open-source project, inspected and improved upon version-by-version by hundreds of developers and security experts.

However, there are a few security considerations to keep in mind, when rolling out a WordPress-based website.

First of all, it's important to notice that in the 2018 study, nearly 40% of compromised WordPress installations were outdated.

Year after year, one of the leading causes of WordPress security compromises is a direct result of running outdated software. For some administrators, this might be a simple fact of negligence. After all, "don't fix what isn't broken" philosophy certainly chimes well with many of us. However, there might be technological reasons which prevent running WordPress updates – such as plugin incompatibility – which brings us to the second point.

Extensions are often the problem.

Running too many plugins on WordPress not only negatively impacts the resource use on our servers and slows our website rendering time, but also is responsible for the bulk of security breaches. Unfortunately, this is an intrinsic characteristic of plugins to begin with – after all, they are pieces of code made by developers world-wide with radically different development philosophies. As the plugins hook into our WordPress installation, they can have their way with out data. The rule of thumb is that if a plugin is compromised, WordPress is compromised.

Last but not least, is lack of security-conscious installation and administration.

The model "set it and forget it" perhaps better suits operating a thermostat, rather than running a corporate website. Unfortunately, one of the main reasons for security compromises in WordPress is the lack of security hardening during and after install. This includes setting weak passwords, mis-configuring the back-end infrastructure, lack of SSL certificates on login pages and numerous other offenses.

Takeaway

Once again, the staggering numbers of compromised WordPress installations is not an indicator of inherent insecurity of the platform. Investing a little bit of time into running our WordPress-based site will definitely push our website outside of the 90% statistic.

1. **Whenever possible, update your plugins and WordPress to the latest version.**

While there may be compatibility issues to be resolved, it's always best to be running the latest version of WordPress. Even though minor updates might not bring any visual changes (such as bringing Gutenberg editor), the changes in the back-end are nonetheless there and should not be ignored.

2. **Minimize your reliance on extensions.**

Although the WordPress team takes plugin security very seriously by manually reviewing each plugin before accepting it to the WordPress Plugin Directory, new security holes arise each day.

Even after acceptance into the Plugin Directory, users can find and report plugin security issues, which are promptly dealt with by the WordPress Security Team.[4]

With this level of attention to security, one might feel completely safe installing numerous plugins. However, no level of security consciousness can account for thousands of plugins and a plethora of configuration or mis-configuration options out there. As such, it's best to keep your website running as low on plugins as possible. First of all, your SEO ranking will definitely improve, as search engines prefer quick, responsive websites. Second of all, you minimize the risk of running into plugin incompatibility issues, which would prevent you from upgrading your WordPress instance.

3. **When installing in production environment, consider your security options.**

From using strong passwords to moving your /wp-admin URL to a different location, options are endless. If you are unsure about WordPress security hardening, there are numerous well-written tutorials online, starting with *Hardening WordPress* on WordPress.org. There are, of course, security-hardening plugins as well, which help you proactively block scripts and attacks. As mentioned above, it's best to use caution. Last, but not least, consider looking into outside protection from DoS and other attacks by using blacklisting and reverse-proxy services, which examine the incoming traffic before passing it onto your servers.

If you got some questions or you're unsure of how to implement the steps mentioned above? Contact us!

1. https://w3techs.com/technologies/history_overview/content_management
2. https://sucuri.net/reports/Sucuri-Hacked-Report-2017.pdf
3. https://blog.sucuri.net/2019/03/hacked-website-trend-report-2018.html
4. https://developer.wordpress.org/plugins/wordpress-org/plugin-security/