Is Your WordPress Site at Risk of Attack?

January 22, 2021 6 min read

Opinions expressed by *Entrepreneur* contributors are their own.

This past October, the WordPress security team used an internal feature to push a security update to a popular plugin. The ability to forcibly push an update was unknown to many, even among experienced developers.

The bug found in the Loginizer plugin, used by more than a million sites, was categorized as one of the worst security issues affecting a WordPress plugin in recent memory, which is why the security team at WordPress felt the action was necessary.

Not everyone appreciated WordPress's proactive approach, users complained on Loginzer's forum and the WordPress.org site. Some were surprised to learn it was even possible to update a plugin with disabled automatic updates. Users complained in 2015 as well, after WordPress first used the forced update feature.

Related: Give Your WordPress Site a Makeover with 80 Premium Marketing Upgrades

WordPress decided to push a security fix to thwart a dangerous SQL injection bug found in the plugin. The vulnerability could have enabled hackers to take over WordPress sites using outdated versions of Loginizer, which ironically provides security enhancements for the WordPress login page.

WordPress update

About two weeks later, WordPress rolled out the WordPress 5.5.2 security and maintenance release for WordPress core. This update contains ten security fixes, and WordPress recommends all users update their sites immediately.

As of 2016, WordPress powered about 34% of the 1.2 billion websites on the internet. A content management system (CMS), WordPress is preferred by web developers of basic and advanced skill levels, primarily due to its ease of use. With so many installs, it is a constant target for cybercriminals, and site owners around the world have fallen prey to a continual string of brute force and other types of attacks. These regular security updates from WordPress are critical to keeping these sites safe and available.

WordPress ecosystem

Not only does WordPress attract nefarious hackers, but it also attracts entrepreneurs. Companies such as Astra, iThemes, Sucuri, and Bullet have built their businesses on solving security issues for WordPress website owners.

Along with the ease of use of this popular CMS comes simple customization. No matter what type of site you wish to build, there is a plugin to provide ready-made customization. At last count, WordPress.org listed more than 58,000 solutions, but these plugins and themes are often the entry point for attacks.

WordPress, plugins, and themes are most often vulnerable to:

- Brute Force Attacks – entering different username and password combinations until gaining entry.
- Cross-Site Scripting – hackers entice victims to a site that contains malicious JavaScript codes.

- File Inclusions – exploitation of vulnerabilities in the WordPress PHP code.
- Malware – code injected into the site to facilitate, for example, unauthorized redirects or allow high-level access to your hosting account.
- SQL Injections – attackers look for unsecured databases and access them using MySQL injections, which gives them control over all the data and enables them to create admin accounts or insert content into the database such as links to other sites that contain malware.

Related: This Expert Guide to Building a Professional-Quality WordPress Site

Why is your WordPress website at risk?

Most WordPress websites (all websites) are vulnerable because website developers and owners do not exercise best practices when it comes to security. Poor passwords are a primary point of vulnerability and quickly addressed, yet thousands of sites every day are breached because of weak, easy-to-guess passwords.

Simple passwords

To impede brute force attacks, create complicated passwords by using 12 or more characters, mixing symbols, letters, and numbers, and ensuring the password is unique to your WordPress site. Password vault applications such as LastPass and 1Password make this easy.

No authentication

Multi-factor authentication provides an additional layer of

security that, when added to other best practices, will help keep hackers from accessing your website. There are several applications, such as Google Authenticator for your mobile device to authenticate authorized access attempts.

Unused plugins and themes

Other points of entry for WordPress websites are outdated plugins and themes. Though sites run faster with fewer plugins, many website owners install plugins, try them, and then choose not to use the feature they provide. The abandoned plugins are left behind and updates ignored. Over time, websites may accumulate dozens of unused plugins and themes.

Exercise caution when installing new plugins and themes. Always download from trustworthy websites such as ThemeForest, CodeCanyon, and WordPress.org. Use fewer plugins by choosing those with multiple functions rather than several single-function plugins.

Delete themes by logging in to your hosting account or using FTP software. Also, check the database for table orphans created by plugins you're no longer using.

No security plugin

Every site should have a security plugin, and there are many good ones. These are your first line of defense should hackers attempt to access your site. You will often find Sucuri, iThemes Security, All In One WP Security & Firewall, BulletProof Security, Jetpack, SecuPress, Cerber Security, and Wordfence on top-ten lists along with other lesser-known options.

No hosting security

Many hosting companies have security features included or available as an add-on service. Configure the software (and

your WordPress security plugin) for regular scans—daily is not too often—and to alert you of any anomalies.

A backup plan

While every website owner should follow security best practices, the chance of having a site hacked still exists. Backup plans are the fail-safe when all that can go wrong does. Enable regular backups based upon how often you make changes to the site. If it’s a daily task, create daily backups. Store them off-site and keep a week’s worth in case you don’t discover an attack right away and need to go back several days to find a clean backup.

The developers behind WordPress work tirelessly to keep websites safe, but owners must take responsibility for ensuring their software is up to date, and passwords are secure. In the same way WordPress has made developing sites easy, it has also made security as easy. Install updates, use complicated passwords, add authentication, and schedule backups to keep your site running and earning money.

https://www.entrepreneur.com/article/359906