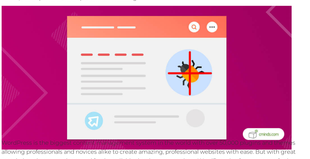
7 Types of WordPress Attacks (And How To Avoid Them)

Feb 13, 2023 | WordPress | Matthias Treuberg



allowing professionals and novices alike to create amazing, professional websites with ease. But with great popularity, a huge user base, and freely available development options, WordPress is often a target of cyber criminals who exploit vulnerabilities to cause harm.

Here are 7 of the most notable attack types affecting WordPress pages today and how to secure your site:

1. Brute Force Attacks

The simplest form of attack that targets one of the potentially weakest links in security – your password! A Brute Force Attack involves a cyber criminal attempting a gigantic number of password combinations over and over again until the correct combination is found.

This form of attack is far from elegant but has proven to be very effective against weak passwords and usernames like '123', 'password', and 'admin'.

However, a simple attack has a simple defence. Be aware of the WordPress password strength meter and try the following:

- Long Passwords
- A good mixture of numeric and alphabet characters
- Avoid dictionary words and words relating to your site or company
- Avoid obvious substitutions like "f1at*f1gh"
- Add **Two-Factor Authentication** as an additional layer of security

A rule of thumb is that if you appear to be receiving a large number of random login requests, then you are most likely under a brute force attack.

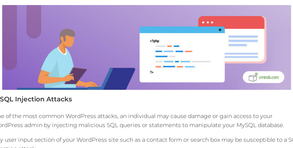
2. WordPress Core Vulnerabilities

WordPress is open source, allowing your business to reduce cost and provides extensive innovation opportunities.

But since the source code is easily obtainable, potential cyber criminals can identify core vulnerabilities and exploit them.

One of the easiest ways of exposing your WordPress site to attack is to continue to use updated WordPress versions as well as running older versions of WordPress's scripting language, PHP.
Thankfully there are developers who identify those same exploits and create fixes to maintain the security of your WordPress site.

To protect your site from new and existing threats always ensure you have installed the latest updates. Do this by simply logging into your WordPress admin account and go to Dashboard >> Updates.



3. SQL Injection Attacks

One of the most common WordPress attacks, an individual may cause damage or gain access to your WordPress admin by injecting malicious SQL queries or statements to manipulate your MySQL database.

Any user input section of your WordPress site such as a contact form or search box may be susceptible to a SQL Injection attack.

Themes and PLugins may be your weak link to SQL Injection attacks so make sure anything installed comes from a reliable and trusted developer.

As your MySQL Database software is vulnerable to this form of attack it is important to make sure you keep up with software updates and never allow access to your MySQL credentials.

One of the simplest tricks to beat basic hackers is to change the default WordPress database name. Using a more unique database name will make it far more difficult for cyber criminals to identify your database details and aid in keeping the back-end of your site neat.

4. Plugin and Theme Vulnerabilities

Plugin and Themes are a fantastic way to add functionality into your WordPress pages or create a unique look. But plugins are a frequent point of WordPress attacks owing to their reliance on developers to keep up to date with security weaknesses and exploits.

A dated plugin may become susceptible to an attack so here are a few tips to protect your page:

- Always update your plugins from the WordPress dashboard
- Use the Plugin Security Scanner found in Dashboard > Tools to detect potential issues with your current plugins

If a plugin has not been updated in over 6 months, the developer may have abandoned it. These plugins are most vulnerable to exploits and it is best to avoid them entirely.

5. Cross Site Scripting

Another very regularly seen attack type and often referred to as an XSS attack.

An XSS attack is the silent uploading of malicious JavaScript code by a cyber criminal aimed at either collecting data without the user's knowledge or redirecting to another site.

Phishing style methods such as newsletter subscriptions or forum posts are common types of XSS attacks.

The best way to avoid this attack is by ensuring proper data validation practices across the entirety of your WordPress site. Validation is an important skill required for proper security and basically means checking that all data your website matches what you expect it to be.

WordPress has several fantastic developer functions to sanitize data but for those starting out in scripting there are a few WordPress XSS plugins that help protect against code injections. Some WordPress plugins are able to assist in preventing XSS attacks by providing security functions to block and prevent vulnerabilities.

6. DDoS Attacks

DDoS attacks are one of the most talked about attacks today having crippled hospitals, banks, and high profile organizations around the world such as Sony, Netflix, and Amazon.

A Distributed Denial of Service (DDoS) attack occurs when a web server is bombarded with such a large volume of requests that the server eventually crashes.
DDoS attacks are highly organised and exploit both small and large websites.

While DDoS attacks are often well disguised and difficult to handle there are various tools available to prevent and stop an attack. A powerful attack but there are ways to defend yourself such as:

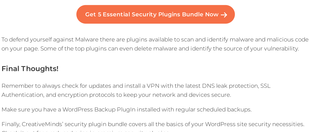
- You can try disabling exploited API's during an attack to reduce the number of requests
- Disabling third-party applications to interact with your WordPress page may help too
- Using plugins that automatically block IPs which perform suspicious activities

But to prevent an attack, activating a Website Application Firewall can identify suspicious requests and prevent them from accessing your website.

Search Improvement Console

Among other features, the **Search Improvement Console WordPress plugin** blocks IPs that search certain queries you set.

This creates a great first line of defense when dealing with attacks coming from specific machines.



7. Malware

One of the most routine goals of a cyber attacker is to upload malware on a user's device and the popularity of WordPress makes it a popular target.

Cyber criminals aiming to upload malware will often scan for WordPress pages using outdated versions as they can exploit the unprotected vulnerabilities. Just another reason to maintain updates.

To defend yourself against Malware there are plugins available to scan and identify malware and malicious code on your page. Some of the top plugins can even delete malware and identify the source of your vulnerability.

Final Thoughts!

Remember to always check for updates and install a VPN with the latest DNS leak protection, SSL Authentication, and encryption protocols to keep your network and devices secure.

Make sure you have a WordPress Backup Plugin installed with regular scheduled backups.

Finally, CreativeMinds' security plugin bundle covers all the basics of your WordPress site security necessities. Check it out for a reduced price in premium security plugins.

Continuing to learn about current trends in security will go a long way to ensure the security of your WordPress site and you can always check out **cminds.com** for information in WordPress trends.

Matthias Treuberg

UPDATED ON: Feb 13, 2023

About the Author

Matthias Treuberg is a Professional and have been part in 2020. CreativeMinds have been creating WordPress products since 2006, and cminds.com has become a good resource of WordPress premium plugins.