A GUIDE TO BRUTE FORCE ATTACKS
FOR WORDPRESS SITE OWNERS

+ TIPS TO PROTECT YOUR WEBSITE
Introduction

Are you in danger of brute force attacks? If you have a WordPress website, you are. Whether you are a giant corporation, a neighborhood shop, or a personal blogger, if you have a website, the bad guys will attack.

WordPress brute force attacks are a very real danger for every WordPress site owner. In fact, **brute force attacks are the most common type of attack on WordPress sites.**

In this guide, you'll learn what a brute force attack is and the dangers that come with them. You'll also learn what you need to do to secure your site against brute force login attempts.

The good news is that by taking a few actions to secure your website, you can reduce the chance of a successful brute force attack by up to 99%. Let's take a look.
What is a Brute Force Attack?

The brute force attack process is often referred to as exhaustive search. As you know, every website running WordPress as its content management system has its own login page where you enter a username and password to access the admin panel.

Hackers are fully aware of how the login works for WordPress sites, so it's simple for them to locate the login page of any site running on WordPress. Then an attacker will systematically check unlimited passwords until the correct one is found.

In a nutshell, brute force attacks refer to a trial and error method used by hackers and bots to discover the right username and password combinations in order to gain unauthorized entry into a website. Brute force attacks are the most common type of attack on WordPress sites.

Even more concerning: software has been developed to aid an attacker in the password guessing process. The success of a brute force attack depends on computing power, the number of combinations attempted, and the level of site security a website owner has in place.
After a hacker has accessed your site's admin dashboard, they will use their access to engage in any number of malicious activities.

These malicious activities can include:

- Stealing your data
- Storing malicious files
- Launching attacks on other sites
- Defacing your site
- Sending spam emails from your site
- Cluttering your site with spam links
- Injecting your site with scripts that make it difficult to regain control of your site

But that's only the beginning. When Google realizes that your site's been hacked, it throws up a warning. This warning message will appear to everyone who lands on your URL that your website may be hacked. Google may even blacklist your site so it no longer appears in search results, and your site host may suspend it altogether.

So it goes without saying that it's important to stop brute force attacks to maintain your business's success. If your customers can't get to your website, then your business can't keep going.

From the list above, preventing brute force attacks means preventing a long list of headaches and stress. We never want anyone to have to experience a hack or security breach, so we're dedicated to providing an easy-to-use but powerful solution for securing every single WordPress site on the planet.
Why Do Hackers Target WordPress Websites with Brute Force Attacks?

WordPress currently powers over 40% of all websites, so it has become an attractive target for hackers with malicious intent. Many WordPress site owners aren’t taking the right precautions or have poor security measures in place.

There are three main reasons that WordPress is such a popular target for attackers:

1. The WordPress login URL is the same for every WordPress site. Anyone with experience working with WordPress knows the default login URL for WordPress is located on the /wp-login.php page. Keep in mind that even if you use a plugin to change the URL of where you keep your login form, it will not change how you would log in using the command line. Most attacks on the WordPress login will use a terminal and not a web browser.

2. WordPress doesn’t limit the number of invalid login attempts. By default, there isn’t anything built into WordPress to limit the number of failed login attempts someone can make. Without a limit on the number of failed login attempts an attacker can make, they can keep trying an endless amount of usernames and passwords until they are successful.
3. **Brute force attacks require no skill.** Brute force attacks refer to a trial and error method used to discover username and password combinations to hack into a website. Any beginner-level hacker can create a bot that scours the internet looking for WordPress login pages. Or you can just use one of the many open-source brute force applications that have already been created.

**Should I Hide My Login Page?**

For some of the reasons listed in the previous section, you may hear you should try to hide or obscure your WordPress login URL. The truth is the problem isn't with the WordPress login itself, but with the way users secure their logins.

Think of your WordPress login as the front door of your house. Without a lock on your front door, it would be easy for anyone to just walk right into your home, start moving your furniture around, smashing your stuff, and stealing your TV. It only makes sense to add a lock to your front door to make it harder for a would-be thief to break into your home.

In the rest of this guide, we'll cover better security measures than hiding your WordPress login page.
3 Reasons WordPress Websites are At Risk for Brute Force Attacks

1. WordPress does not automatically limit the number of failed login attempts, which can be a big vulnerability for brute force attacks.

2. Early versions of WordPress defaulted to the username ‘admin’ and many people either forget or neglect to change it.

3. No matter your domain, all WordPress sites have the same admin login URL.
   - /wp-admin
   - /wp-login
   - /wp-login.php
How Do Brute Force Attacks Work?

Hackers program bad bots to locate vulnerable WordPress sites, automatically open the login page, and begin an all-out brute force attack. Bots will attempt many different combinations of common passwords and usernames in hopes of gaining admin access.

An attacker will systematically check unlimited passwords until the correct one is found. Depending on your server settings, an attacker can go through 1000 different password variations in a minute.

The bots will continue to make hundreds, and even sometimes thousands, of login attempts every minute.

But that's only part of the problem.

Even if the bad bot cannot properly guess your login credentials, the attack can still damage your WordPress site. The sheer number of login attempts that it makes within a few minutes can overwhelm your server and cause major slowdowns or crashes.

This is why it's extremely important to use the strongest login credentials that hackers aren't able to crack. But that alone isn't enough. To fully stop brute force attacks, you'll need to take additional security steps.
Are You Inviting Brute Force Attacks?

This year alone, grim statistics point to the urgent need for website owners to take active security measures to defend their sites against cyberattacks such as brute force attacks.

Simply put: If you or any other admin user on your WordPress site has a weak password, you are welcoming brute force attacks. You should change your password ASAP and implement all of the tips in this guide.

Unfortunately, some WordPress site owners use simple usernames and passwords that are easy to crack. And hackers keep huge databases of the most commonly used passwords and usernames for WordPress accounts, such as password4321.

Using strong passwords for all your logins is one of the best online security practices you can develop.

The best practice to follow is to create a different password for every single website you are registered on. Definitely don’t use the password you use for your bank account on another site.
Why Your Passwords Matter – A Lot

It has never taken long for a hacker to brute force their way past a weak password into a website. Now that hackers are leveraging computer graphics cards in their attacks, the time it takes to crack a password has never been lower.

For example, in a recent report created by Terahash, a high-performance password-cracking company, an 8-character password can be cracked INSTANTLY. That is not only impressive but also really scary.

In addition, even though 91% of people know reusing passwords is poor practice, 59% of people still reuse their passwords everywhere!

Why is the habit of reusing passwords so risky? Let’s say you have an account on some website and you’re not too worried if someone gains access to your password because this particular account doesn’t have any useful information.

Imagine that “useless” site gets hacked and now the attacker has your password to that account. Even though that specific site may be useless to a hacker, your password isn’t.

Let’s say you use that same password on another online shopping site. The hacker now has your password to that account, which stores your payment information. Now you have a big problem you have to deal with.
Attackers often use compromised passwords as a starting point for cracking accounts. If your password is exposed and you’re reusing your credentials across multiple websites, attackers could compromise your account in just one or two attempts instead of millions.

Hackers can use a form of a brute force attack called a dictionary attack. A dictionary attack is a method of breaking into a WordPress website with commonly used passwords that have appeared in database dumps.

For example, the “Collection #1” Data Breach that was hosted on MEGA included 1,160,253,228 unique combinations of email addresses and passwords. That is billion with a $B$.

That kind of score will really help a dictionary attack narrow the most commonly used WordPress passwords. This is why it is important to have different passwords for each website you are registered on.

If you are reusing this password for other accounts, you should choose a new unique password for each of them. We recommend using a password manager like LastPass or 1Password to generate and store strong, random passwords for all your online accounts.
It has never taken long for a hacker to brute force their way past a weak password into a website. Now that hackers are leveraging computer graphics cards in their attacks, the time it takes to crack a password has never been lower.

**TOP 10 MOST COMMON PASSWORDS**

1. 123456
2. 123456789
3. qwerty
4. password
5. 111111
6. 12345678
7. abc123
8. 1234567
9. password1
10. 12345

**SOURCE:** UK’S NATIONAL CYBER SECURITY CENTRE (NCSC)

Every single one of these 1,160,253,228 accounts are vulnerable to hackers if they have reused the same email address and password for multiple online accounts.

**70% of people are reusing passwords for work-related accounts.**

70% of people are reusing passwords for work-related accounts.

**10% of people have used at least one of the 25 worst well-known passwords.**

10% of people have used at least one of the 25 worst well-known passwords.

The “Collection #1” Data Breach included 1,160,253,228 unique combinations of email addresses and passwords. That is billion with a B.

**SOURCE:** SPLASHDATA

70% of people are reusing passwords for work-related accounts.

10% of people have used at least one of the 25 worst well-known passwords.
How to Protect Against Brute Force Attacks

WordPress brute force attack prevention and keeping hackers at bay involves seven specific security protocols that you should put into practice on your website as soon as possible.

1. Use Strong, Complex, and UNIQUE Passwords and Usernames

Long, unique, and random usernames and passwords are always the best way to avoid successful brute force login attempts.

As a rule, always use a random combination of special characters, uppercase, and lowercase. An uncrackable password should look something like this:

```
Z{&egQ"!%Q^KH}6V
```

Use the WordPress random password generator or a different password generator to craft a password someone won’t easily find online to secure your login.

Invest in a password manager service like LastPass or 1Password to generate and store your passwords from prying eyes and determined hackers.
2. Never Reuse or Share Passwords

When it comes to password security, you need a different strong password for each of your online accounts. If you use the same password for every site and one of those sites is compromised, you are now using a compromised password on every website.

Hackers can use data dumps of compromised passwords paired with your email address or username to gain access to your accounts. It’s best not to even take the risk.

Attackers often use compromised passwords as a starting point for cracking accounts because it is faster than brute-forcing all possible password combinations. If your password is exposed and you’re reusing your credentials across multiple websites, attackers could compromise your account in just one or two attempts instead of millions.

The **Password Requirement** feature in the iThemes Security Pro plugin is not only your password policy, but it is also your enforcement tool.

You can force users of your website to use a strong password, choose a time of password expiration, refuse passwords that have been found in a database breach, and force a site-wide passwords change to make everyone comply with your new strong password policy.
3. Set a Limit on Login Attempts

The bad bots that initiate brute force attacks on your WordPress suite are programmed to attempt a seemingly infinite number of username and password combinations to gain access to the WordPress dashboard. They also make thousands of attempts within a few minutes.

As we mentioned earlier, WordPress doesn’t limit the number of invalid login attempts someone can make. This means that a bot can spend all of eternity guessing random combinations of usernames and passwords until they finally brute force their way into the backend of your website.

But what if you were able to stop the bad bot before it was able to do any damage at all?

A great way to do this is by limiting the number of login attempts for site users. After a user makes more than, for example, five login attempts with incorrect credentials, they’re locked out from making any more attempts until their account is unlocked.

The iThemes Security Pro plugin allows you to limit the number of login attempts on your WordPress site. The Local Brute Force Protection feature keeps tracks of invalid login attempts made for a username or from an IP address. Once an IP or username has made too many consecutive invalid login attempts, they will get locked out and will be prevented from making any more attempts for a set period of time.
4. Use Two-Factor Authentication

No doubt you've noticed how many of the popular websites you frequent that require you to take two different steps in order to log in.

Facebook and Gmail are just two examples. Think of it as knowing the password and the secret knock.

In step one of the process, you enter a username and your password. After that, the site you’re using will text message you a numeric code to your phone that you need to enter in order to access the site and your personal account.

This simple two-step method helps ensure that the real user is the one logging into the site because it verifies their identity in real-time.

The simple way to implement a two-step validation method on your WordPress site is by downloading and installing a plugin like iThemes Security Pro that provides two-factor authentication. After you enable the plugin, when you first log into your site, you'll need to enter a unique verification code to your smartphone or email. Only after you enter the code, will you be able to access the WordPress admin dashboard.

The iThemes Security Pro plugin's Two-Factor Authentication feature integrates with common 2FA apps like Google Authenticator and Authy so you can easily add two-factor authentication to your website without the need for any code or an additional plugin.

Google shared that using two-factor authentication can stop 100% of automated bot attacks.
5. Add ReCAPTCHA to Login Forms

reCAPTCHA is a powerful tool that will help you win your website’s battle against bad bots. On a more technical level, reCAPTCHA is a type of technology that uses advanced risk analysis techniques to tell humans and bots apart.

By adding reCAPTCHA to your website's login forms, you can block bots that may be attempting brute force attacks. reCAPTCHA helps keep bad bots from engaging in abusive activities on your website such as attempting to break into your website using compromised passwords, posting spam, or even scraping your content.

Legitimate users, however, will be able to login, make purchases, view pages, or create accounts. reCAPTCHA uses advanced risk analysis techniques to tell humans and bots apart.

The iThemes Security Pro plugin's reCAPTCHA feature allows you to enable reCAPTCHA to protect your site from bots by verifying that the person submitting comments or logging in is indeed human. You can add reCAPTCHA to your login page, password reset, comments, and new user registration.
5. Activate Brute Force Protection at the Network and Local Level

A solid approach to blocking brute force attacks includes activating protection at both the local and network level. The iThemes Security plugin offers both types:

- **Local Brute Force Protection** looks only at attempts to access your site and bans users per the lockout rules specified in your security settings. Once an IP or username has made too many consecutive invalid login attempts on your website, they will get locked out and will be prevented from making any more attempts for a set period of time.

- **Network Brute Force Protection** takes the level of protection a step further. The network is the iThemes Security community and is over a million websites strong. If an IP is identified as trying to break into websites in the iThemes Security community, the IP will get added to the Network Bruce Force banned list.

The iThemes Security Pro [Local and Network Brute Force Protection](#) and Banned Users settings work in tandem to secure and protect the most attacked part of your website, the WordPress login.

When you activate the iThemes Brute Force Protection Network, you join over 1 million other websites to unite against malicious IPs that are attacking WordPress sites around the world.
6. Ban Bad Bots and User Agents

Once a bot or hacker has been caught attempting brute force attacks, it's important to ban them from being able to access your site. Bots and hackers will have an IP address that you can use to identify them and ban them.

The iThemes Security Pro Banned Users feature allows you to ban the IP addresses of known bad actors. You can also ban repeat offenders permanently with too many invalid login attempts.

7. Monitor Brute Force Attacks

Every day, lots of activity is happening on your site that you may not be aware of. Many of these activities can be related to your site's security, so monitoring these events is vital to keeping your site secure.

The iThemes Security Pro plugin provides a real-time WordPress Security Dashboard that monitors security-related events on your site 24 hours a day, 7 days a week.

From your security dashboard, you can see a graph of the number of brute force attacks happening on your site. You'll probably be amazed by how often your site is under attack.
Wrapping Up: To a Safer Web, Together!

For WordPress site owners, WordPress brute force attacks are the most common type of cyberattack. In fact, you may not even realize they're happening on your site until you activate a plugin like iThemes Security Pro to help monitor the types of activity that indicate an attack.

Unfortunately, brute force attacks have a high rate of success due to so many site owners using weak login credentials.

That said, by implementing the strategies we've covered in this guide, and running a powerful WordPress security plugin like iThemes Security Pro, you'll be able to thwart hackers and bad bots from running these brute force attacks.

And when you do, you'll keep your site safe and running smoothly for your users to enjoy.
Install a trusted WordPress security plugin to help defend your website against brute force attacks. The iThemes Security plugin offers WordPress brute force protection in addition to multiple other WordPress security features to secure and harden WordPress.

GET ITHEMES SECURITY PRO NOW