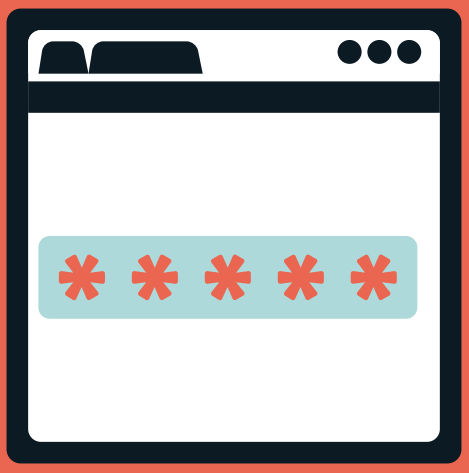
ITHEMES PRESENTS

A GUIDE TO WORDPRESS BRUTE FORCE ATTACKS

+ TIPS TO PROTECT YOUR WEBSITE

WHAT ARE BRUTE FORCE ATTACKS?



Brute force attacks refer to a trial and error method used by hackers and bots to discover username and password combinations in order to gain entry into a website.

HOW DO BRUTE FORCE ATTACKS WORK?

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.

1000X / MINUTE

ARE YOU INVITING BRUTE FORCE ATTACKS?

If you have a weak password, you are welcoming brute force attacks. You should change your password ASAP.

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), 2019

10% of people have used at least one of the 25 worst passwords. Are you one of them?

SOURCE: SPLASHDATA, 2017

3 REASONS WHY WORDPRESS WEBSITES ARE AT RISK

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

NO FAILED LOGIN LIMITS

ADMIN

DEFAULT USERNAME

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

KNOWN LOGIN URL

5 WAYS TO PREVENT BRUTE FORCE ATTACKS

1. USE STRONG, COMPLEX PASSWORDS

2. DON'T REUSE PASSWORDS FOR MULTIPLE ACCOUNTS

3. NEVER USE 'ADMIN' AS YOUR WORDPRESS USERNAME

4. LIMIT FAILED LOGIN ATTEMPTS

5. ADD TWO-FACTOR AUTHENTICATION TO WORDPRESS

+ TIPS TO PROTECT YOUR WEBSITE

FOR WORDPRESS USERS

- Make a habit of using a different password for every website you use.
- Use a password with a combination of lower and uppercase letters, symbols and numbers.
- Change your passwords often.

FOR WORDPRESS ADMINS

- Do not use ‘admin’ as your username.
- Install a WordPress security plugin such as iThemes Security to activate network & local WordPress brute force protection.

FOR WORDPRESS DEVELOPERS

- Limit the number of failed login attempts on /wp-admin & /wp-login.php
- Add a captcha for logins.
- Offer a two-factor authentication login option for users.

HOW A WORDPRESS SECURITY PLUGIN CAN HELP

- NETWORK & LOCAL BRUTE FORCE PROTECTION
- LIMIT FAILED LOGIN ATTEMPTS
- SCHEDULED MALWARE SCANS
- ENFORCE STRONG PASSWORDS
- 30+ WAYS SECURE, PROTECT & HARDEN WORDPRESS

iThemes Security

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.

PROTECT YOUR WEBSITE NOW →

GET MORE WORDPRESS SECURITY RESOURCES AT ITHEMES.COM/PUBLISHING