WordPromise
Expert Website Maintenance & Support™

Handle Brute Force Attacks, A Journey to safety

Email us at info@wordpromise.com

Brute force attack is one of the traditional forms of cybercrime, and still, they are extremely popular with hackers. In fact, they are likely to become even more and more disastrous with evil mind technology and plugins.

Through this guide we will let you aware of what a brute force attack is, how dangerous it can be, and what to do to minimize and nullify the attacks.

In this guide we will explore the followings:

- What is WordPress Brute Force Attack?
- How do Brute Force Attacks work?
- Types of Brute Force Attacks.
- Are you inviting Brute Force Attacks?
- Why WordPress sites are at risk?
- What to do in case of Brute Force Attacks?
- Useful WordPress security plugins that can help.

Seems Interesting?

Let’s Start

What is WordPress Brute Force Attack?

Brute Force Attack is a type of cyberattack in which an attacker systematically attempts to gain unauthorized access to a WordPress website by trying different username and password combinations until the correct combinations of username and password is found.

The term "brute force" refers to the strategical and repetitive nature of the attack, where the hacker uses automated tools to guess potential login credentials.

If the attack gets unauthorized access to your website, the hackers can deploy malicious scripts, get access to all confidential data, and redirect users to malicious pages that collect login credentials and other personal information.

How do Brute Force Attacks work?

In layman's term, a brute force attack means making numerous repetitive unsuccessful logins attempts until it gets the successful combination of correct username and password.

Now to make the things faster, hackers do follow strategically planned attempts in combination of various hacking software tools. Usually, the hackers have a list of usernames and a list containing of probable set of passwords, possibly in millions. They need to go through all these passwords one by one until they find the correct one. It’s not common for a human being to do it manually, that is why there are plenty of tools that automate the process.

Here's how a WordPress Brute Force Attack typically works:

- **Username Enumeration**:
  The attacker may start by identifying valid usernames associated with the WordPress site. This can be done by exploiting vulnerabilities or using information gathered from other sources.

- **Password Guessing**:
  Once the attacker has a list of valid usernames, automated tools are used to systematically try different passwords for each username. These tools often use dictionaries of commonly used passwords, as well as variations and combinations of words, numbers, and symbols.

- **Automated Tools**:
  Brute force attacks are usually carried out using specialized software or scripts that automate the process of trying numerous username and password combinations in a short amount of time. These tools can make thousands or even millions of login attempts per minute.

- **Credential Stuffing**:
  In some cases, attackers may use credentials obtained from other data breaches (where usernames and passwords were compromised) to attempt unauthorized access to WordPress sites. This is known as credential stuffing.

- **Lockout Avoidance**:
  To avoid detection and lockout mechanisms implemented by the WordPress site, attackers may use techniques like slow and steady login attempts, distributed attacks from multiple IP addresses, or rotating IP addresses.

Types of Brute Force Attacks

Brute force attacks come in various types, each with its own characteristics and targets. Depending on the mechanism used for login exploitation, attackers may use one of the following or combinations of the following:

Simple Brute Force Attack:
In this, an attacker systematically attempts all possible combinations of passwords until the correct one is found. This method is straightforward but can be time-consuming.

Dictionary Attack:
In a dictionary attack, attackers use a predefined list of words, phrases, or commonly used passwords to attempt unauthorized access. This method is more efficient than a simple brute force attack as it focuses on likely passwords.

Credential Stuffing:
Credential stuffing is a type of brute force attack where attackers use username-password pairs obtained from previous data breaches on other websites to gain unauthorized access to user accounts on a different platform.

Reverse Brute Force Attack:
In a reverse brute force attack, attackers use a single, commonly known password and attempt to gain access to multiple accounts by trying it with different usernames. This

approach relies on the assumption that at least one user is using the known password.

Hybrid Brute Force Attack:

Hybrid attacks combine elements of dictionary attacks and brute force attacks. They involve using a combination of known words, phrases, and patterns to increase the likelihood of success.

Online Brute Force Attack:

In an online brute force attack, the attacker attempts to gain access to a system or account directly, making repeated login attempts. This type of attack can be easier to detect, as it involves interacting directly with the target system.

Offline Brute Force Attack:

In an offline brute force attack, attackers have obtained a copy of the password database, usually through a data breach. They can then attempt to crack the password hashes at their own pace without interacting directly with the target system.

Rainbow Table Attack:

Rainbow table attacks involve using precomputed tables that map plaintext passwords to their hash values. These tables can significantly speed up the process of cracking hashed passwords by eliminating the need to compute hashes on the fly.

To defend against brute force attacks, organizations and individuals should implement strong security measures, including strong password policies, account lockout mechanisms, monitoring for unusual login activity, and the use of multi-factor authentication.

Are you inviting Brute Force Attacks?

Here are some common loopholes, weak practices which are very prone to brute force attacks on WordPress websites:

Weak Passwords:
Ensure that strong, unique passwords are used for all user accounts. Encourage users to use a combination of uppercase and lowercase letters, numbers, and special characters in their passwords. Having a weak password is like giving a free access to the attackers.

Default Admin Username:
Having a default "admin" username is again a big NO for a secure environment.

No extra layer of login authentication:
If you are relying only on the username and password for the login then you are taking all the risk which is not worth at all. It is always better to have an extra layer of login authentication such as Two-Factor Authentication (2FA) in the forms of email OTP/ mobile OTP, pre-generated backup codes, use of real authenticator APP like Google Authenticator etc.

Outdated version of WordPress Core and Plugins:
Having the older version of software and plugins, again gives

the leverage to the hackers for their advantage. It is always recommended to have the latest version of all the relevant software and plugins.

Running a Website with Web Application Firewall (WAF): No Firewall means, all sort of network traffic can consume your network bandwidth and exploit your digital infrastructure freely without restrictions. It is highly risky to ignore the Firewall shield and a task made easy for attackers for their benefit.

Remember that the security landscape is always evolving, and it's essential to stay informed about the latest security practices. Regularly review and update your security measures to protect your WordPress website from potential threats.

Why WordPress sites are at risk?

WordPress websites are often targeted by brute force attacks for several reasons such as:

- **Popularity**:
  WordPress is the one of the most popular content management systems (CMS) globally, powering a significant percentage of websites on the internet. As per recent survey in 2023, WordPress has a market share of 62.6% considering the websites whose CMS are well known in the industry. Its widespread use makes it an attractive target for attackers, as compromising a widely used platform can yield a large number of potential victims.

- **Standard Login URL**:
  The default login URL for WordPress sites is predictable and follows a standard format (e.g., yoursite.com/wp-admin). Attackers can easily locate the login page, making it easier to launch brute force attacks.

- **Common Usernames**:
  WordPress installations comes with default usernames such as "admin" which we should disable as the first thing. Additionally, users sometimes choose weak or easily guessable usernames, making it easier for attackers to

narrow down their targets and execute successful brute force attacks.

- **Weak Passwords**:
  Due to unawareness, some WordPress users keep weak passwords that are easy to crack by an automated tool. Since WordPress is user-friendly and caters to a diverse user base, not all users may think the importance of having strong password practices.

- **Outdated Software**:
  WordPress website is a combination of key elements such as core WordPress software, PHP platforms, themes, and plugins. To keep a website completely secure, all the software, themes and plugins must be up to date and compatible with each other.
  Failure to keep WordPress core, themes, and plugins updated can leave a site vulnerable to known security vulnerabilities. Even keeping the software versions publicly accessible is another clue, hackers look after, so that the outdated software can be targeted. Attackers can exploit these vulnerabilities to facilitate brute force attacks.

- **Lack of Two-Factor Authentication (2FA)**:
  Many WordPress sites do not have two-factor authentication enabled by default. Without 2FA, attackers only need to compromise the username and password to gain access, making brute force attacks more feasible.

- **Inadequate Security Measures**:
  Some WordPress site owners may not implement adequate security measures, such as IP blocking after a certain number of failed login attempts, which makes it easier for attackers to carry out brute force attacks without detection.

- **Plugin Vulnerabilities**:
  Since WordPress supports a vast ecosystem of plugins, vulnerabilities in poorly coded or outdated plugins can be exploited by attackers to facilitate brute force attacks.

To mitigate the risk of brute force attacks on WordPress sites, it is very crucial for website to have strong security features implemented.

What to do in case of Brute Force Attacks?

Important ways to prevent Brute Force Attacks in WordPress websites.

To protect against WordPress Brute Force Attacks, website owners should implement strong security measures, including:

- **Strong Password Policies**:
  Set/force strong passwords for high level user’s roles on your website such as admins, editors etc. Strong password enforcement is one of the best ways to lock down WordPress. We can define a password expiry as well, which normally require a collaboration to fix the expiry duration. Encourage or enforce the use of complex passwords for user accounts. Ensure that strong, unique passwords are used for all user accounts whether it is administrator type users, moderator, or authors. Encourage users to use a combination of uppercase and lowercase letters, numbers, and special characters in their passwords. It is always better to have a strong password policy in place and all the users must be sensitized to understand the importance of strong password.

- **Two-Factor Authentication (2FA)**:
  Enable 2FA to add an extra layer of security, requiring users to provide a second form of verification in addition to their password. With WordPress two-factor

authentication, users are required to enter both a password and a secondary code sent to a mobile device or email ID. Both the password and the code are required to successfully log in to a user account. Two-factor authentication adds an extra layer of WordPress security to verify it’s YOU who is trying logging in.

- **Login Attempt Monitoring**:
  Implement mechanisms to monitor and detect multiple failed logins attempts and consider implementing lockout policies. It is highly recommended to limit the number of logins attempts to prevent attackers from repeatedly trying different passwords. There are various tools and WordPress security plugins which can be very handy in implementing this feature.

- **Firewall Protection**:
  Use a web application firewall (WAF) to help block malicious traffic and prevent unauthorized access attempts. We can configure website security to block suspicious traffic and activities to keep hackers away from your site. This includes banning the bad hosts, preventing the brute force attacks, hitting multiple 404 error pages and setting up away mode so that there is no access to admin panel in non-business hours.

- **Regular Software Updates**:
  Remember to regularly update your WordPress

installation and all installed plugins to ensure you have the latest security patches. Any conflict or mismatch in versioning of the themes and plugins will expose the vulnerabilities which can be easily exploited by the attackers.

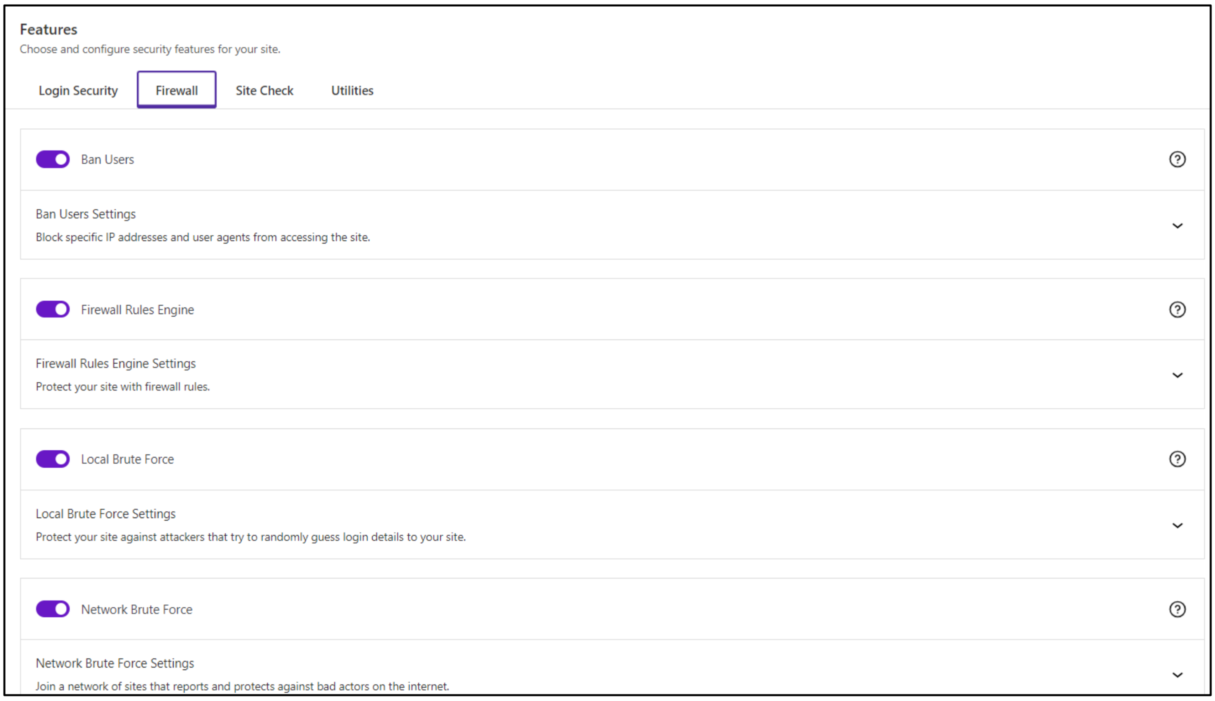
- **Use Security Plugins:**
  Consider using security plugins that provide additional protection against brute force attacks and other security threats, as explained below.

By implementing these security measures, website owners can significantly reduce the risk of successful brute force attacks on their WordPress sites.

Useful WordPress security plugins that can help

WordPress security is utmost important, and using plugins to restrict brute force attacks is a good practice. Some popularly known WordPress security plugins such as iThemes Security, Sucuri Security, Wordfence Security that can be handy in protecting your website:

- **Solid Security Pro (formerly Better WP Security)**: iThemes Security is a feature-rich plugin that helps in securing your WordPress site. It offers extensive security features such as limit login attempts, ban troublesome user agents, enforce SSL, and block specific IP addresses. It also offers other security features like file integrity checks and strong password enforcement.



Features

Choose and configure security features for your site.

Ban Users

Ban Users Settings

Block specific IP addresses and user agents from accessing the site.

Firewall Rules Engine

Firewall Rules Engine Settings

Protect your site with firewall rules.

Local Brute Force

Local Brute Force Settings

Protect your site against attackers that try to randomly guess login details to your site.

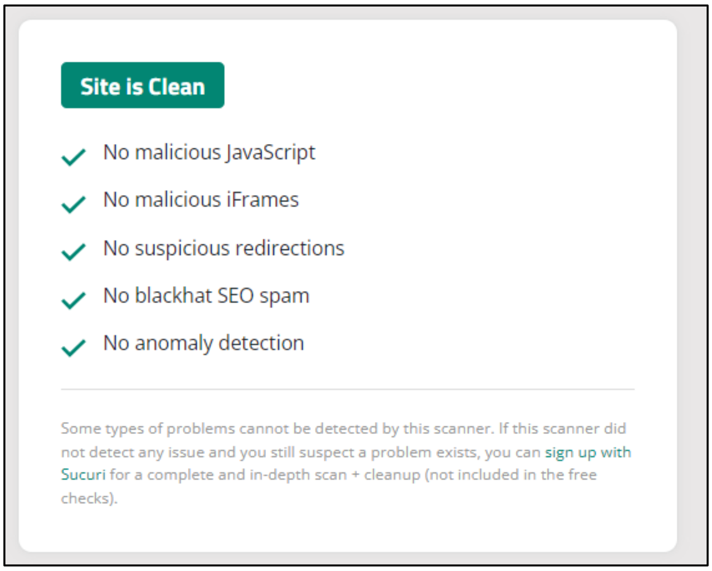
Network Brute Force

Network Brute Force Settings

Join a network of sites that reports and protects against bad actors on the internet.

- **Sucuri Security**:
  Sucuri is another comprehensive security plugin that offers website monitoring, malware scanning, and a firewall. It can also protect against brute force attacks by limiting login attempts and blocking suspicious IP addresses.

  This offers a powerful Web Application Firewall and Intrusion Detection System for any WordPress user and many other platforms. Once enabled, Sucuri firewall act as a shield, protecting your site from attacks and preventing malware infections and reinfections. It will block SQL injection attempts, brute force attacks, XSS, RFI, backdoors and many other threats against your site.



✓ No malicious JavaScript

✓ No malicious iFrames

✓ No suspicious redirections

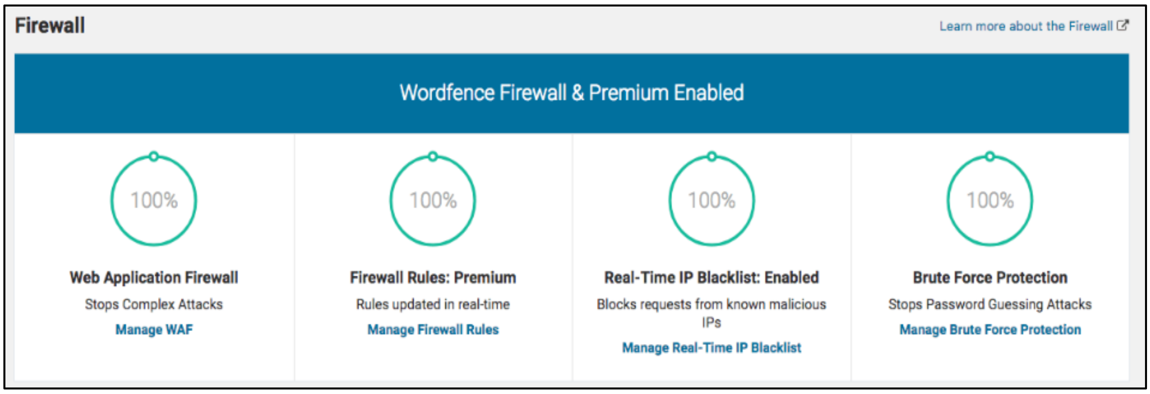
✓ No blackhat SEO spam

✓ No anomaly detection

Some types of problems cannot be detected by this scanner. If this scanner did not detect any issue and you still suspect a problem exists, you can sign up with Sucuri for a complete and in-depth scan + cleanup (not included in the free checks).

- **Wordfence Security**:
  Wordfence is also, one of the most widely used security plugins for WordPress. It includes a firewall, malware scanner, and options to limit login attempts. You can configure it to block IP addresses that have too many

failed login attempts. Wordfence Security includes an endpoint firewall, malware scanner, robust login security features, live traffic views, and more.



Firewall

Learn more about the Firewall

Wordfence Firewall & Premium Enabled

100%

Web Application Firewall

Stops Complex Attacks

Manage WAF

100%

Firewall Rules: Premium

Rules updated in real-time

Manage Firewall Rules

100%

Real-Time IP Blacklist: Enabled

Blocks requests from known malicious IPs

Manage Real-Time IP Blacklist

100%

Brute Force Protection

Stops Password Guessing Attacks

Manage Brute Force Protection

In addition to the above, it is also recommended to implement other security best practices, such as using strong passwords as per defined strong password policies, removing the unused themes and plugins, and regularly backing up your site.

Wrapping Up

Brute force attacks are used to break through security measures to target the vulnerable websites and datasets. If anyone has unlimited time and wanted to try an unlimited number of password combinations to get into your site, they eventually would, right?

While this may seem like something only hackers can use to their advantage, many security firms do use brute force attacks to test their clients’ systems in real environments.

Having said all this, technologies have its pros and cons. Going thru the nature of Brute Force Attacks, a website is under an automated attack all the time and it can be severe threat because it’s only a matter of time before the attack succeeds. By implementing remedial measures you can at least slow attackers down.

We at WordPromise do protect your site against attackers that try to randomly guess login details to your site. For more details and queries, you may reach out to us at info@wordpromise.com

Have a Happy Shield for your much deserving website !