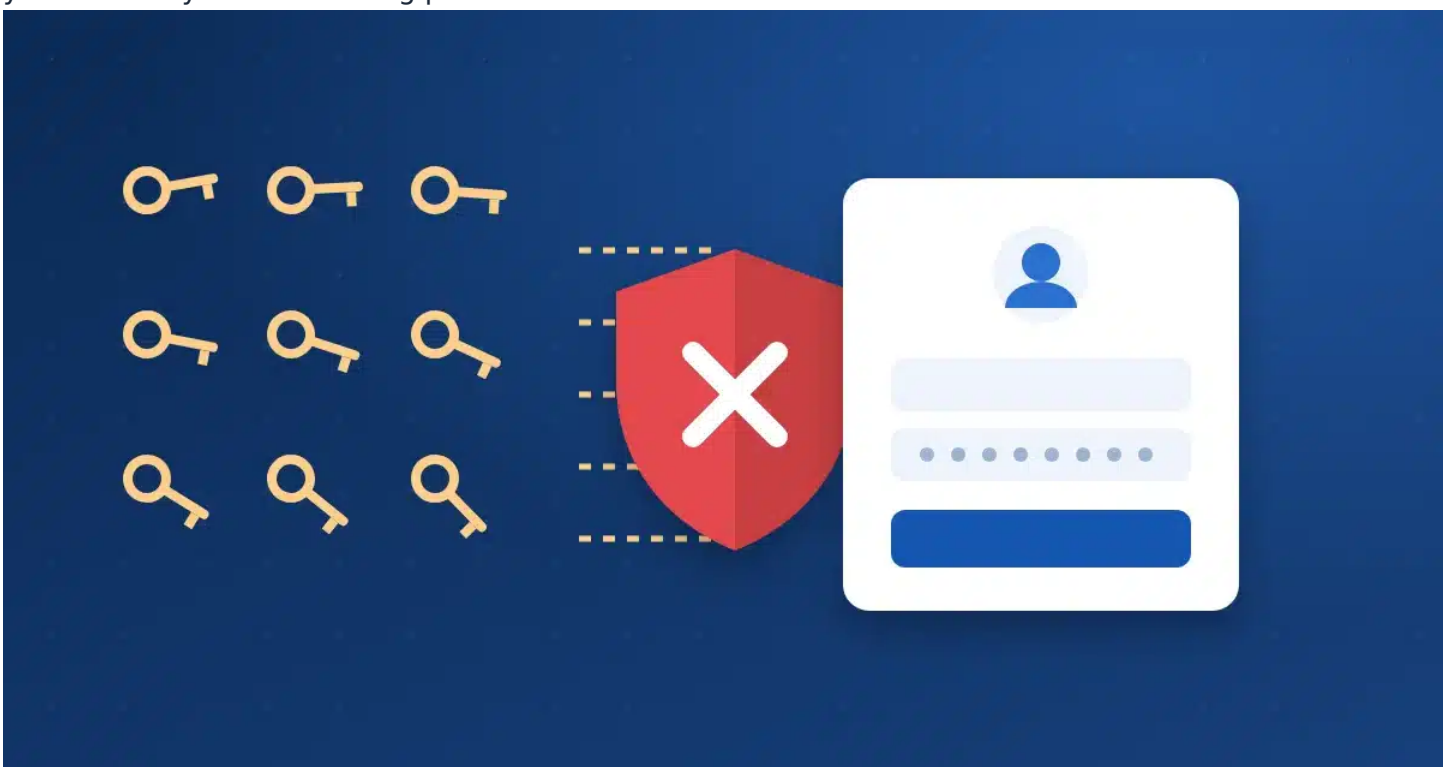
Brute Force Attacks: How They Work and How We Protect Your Site

Website Security · https://www.hyyat.com/en/knowledgebase/brute-force-protection/

In shortA brute force attack automatically tries thousands of passwords on a WordPress, cPanel, email or SSH login until one works. Hyyat Host servers log failed logins and block repeat offenders, and if you are blocked by mistake after forgetting your password, a CAPTCHA lets you unblock yourself. On your side: a long password and two-factor authentication.



How does the attack work?

The attacker uses software and a network of infected devices to send thousands of login attempts a minute, using common passwords or ones leaked from other sites. The attack rarely targets your site by name; it tries every site it can find.

*W***WordPress dashboard**wp-login.php and xmlrpc.php are among the most common targets.

C**cPanel and webmail**Logging in there means control of the whole site and email.

@**Email accounts**To send spam in your domain’s name.

>_**SSH and FTP**On private and cloud servers.

Why is it dangerous even when it fails?

Every login attempt uses CPU and memory. Thousands a minute slow your site down or stop it, before the attacker achieves anything. And if they succeed, they upload malicious files such as a C99 shell or send spam from your account.

How we protect your site at Hyyat Host

1. **We log every failed login:** The server records the IP address of each failed login on WordPress, Joomla, cPanel and email.
2. **We block repeat offenders:** When failures repeat from the same address, it is blocked from every login form on the server, so its attempts never reach your site or use its resources.
3. **We tell you apart from the attacker:** If you forget your password and get blocked by mistake, you see a CAPTCHA instead of an error. Solve it and the block is lifted.

This works together with the **CSF** firewall, **cPHulk** and **Imunify360** on the server, and needs no setup from you.

What you should do

- A long (15+ characters), unique password for every account.
- Two-factor authentication in cPanel, the client area and WordPress.
- Do not use the username admin for the administrator account.
- If you do not use xmlrpc.php, disable it with your security plugin. See the best WordPress security plugins.
- During a large attack you can turn on Cloudflare’s Under Attack mode.

Blocked and no CAPTCHA? Open a ticket from the client area with your IP address, and we will lift the block and tell you why.

Frequently asked questions

Why was I blocked from my own site?

Usually several wrong logins from your device, or an email app with an old saved password. Solve the CAPTCHA if it appears, or open a ticket with your IP address.

Is a WordPress security plugin enough?

A plugin helps, but it works only after the request reaches WordPress. Server protection stops the attack earlier and saves resources too. Use both.

Does changing the login URL stop the attack?

It reduces automated attempts, but it does not replace a strong password and two-factor authentication.

Related guides

- How to Keep Your Website Secure: Practical Tips to Prevent Hacking
- Hacking Tools: C99 Shell
- What is a Slowloris DDoS attack?
- How to Protect Your Customers' Data on Your Website: A Practical Guide

All website security guides →

Need this service from Hyyat Host?Our team handles it for you, with support replying to tickets within 24 hours at most.

Web HostingSaudi Hosting