How to Scan WordPress for Vulnerabilities and Secure It with WP Toolkit

WordPress explanations · https://www.hyyat.com/en/knowledgebase/wordpress-vulnerability-scan-wp-toolkit/

> **In short:** The most common WordPress attacks are brute force, DDoS through XML-RPC, vulnerable plugins and themes, and code injection. WordPress Toolkit in cPanel (Applications section) scans your site and applies security measures such as blocking PHP execution in uploads, turning off pingbacks and protecting wp-config, and it updates WordPress and plugins from one place.

WordPress is the most used content management system on the web, and that popularity has a price: it is also the most attacked. Not because it is insecure, but because one WordPress vulnerability opens the door to millions of sites. As soon as a WordPress site goes online, automated bots start checking it for weaknesses.

Security hardening used to be long and manual, but **WordPress Toolkit for cPanel** makes it one click. See also what WordPress Toolkit is.

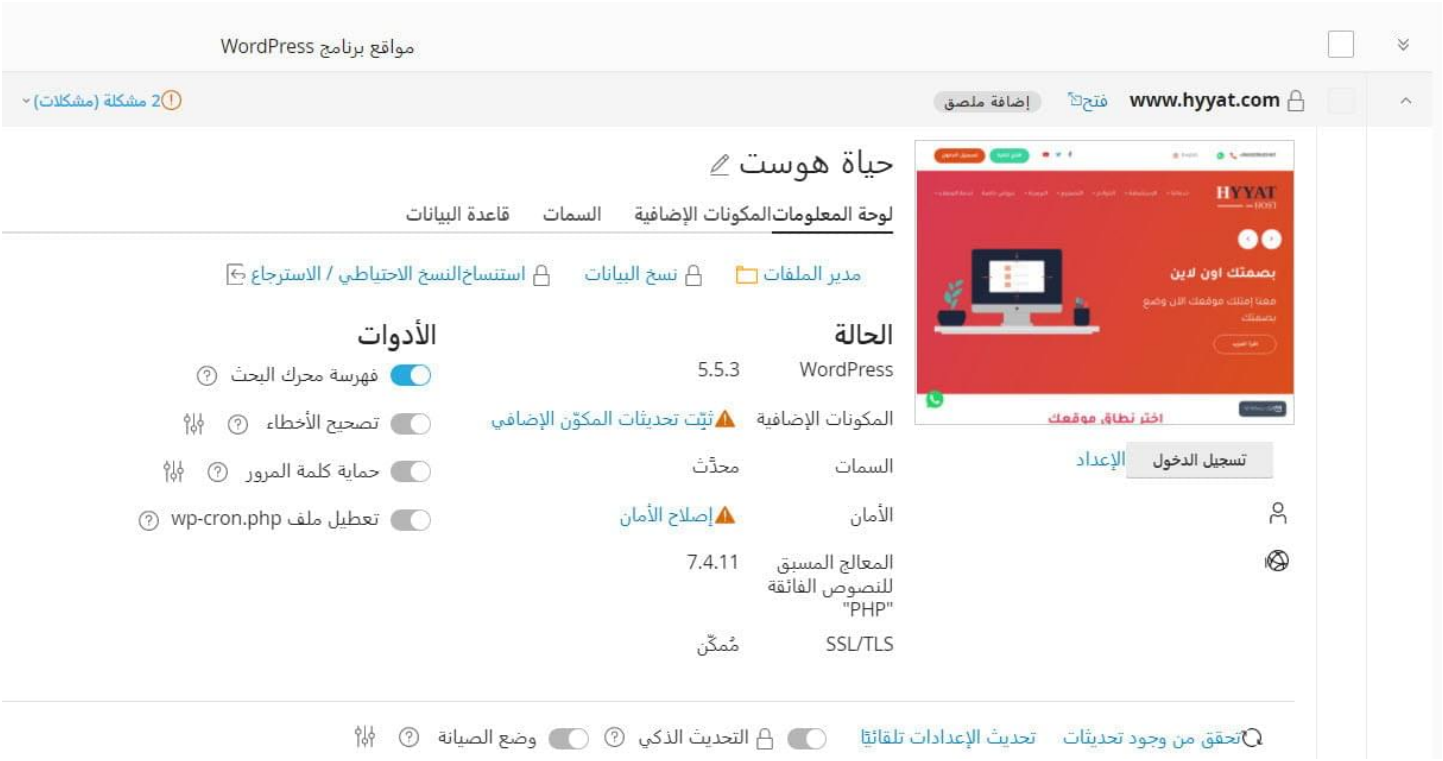
Common WordPress vulnerabilities

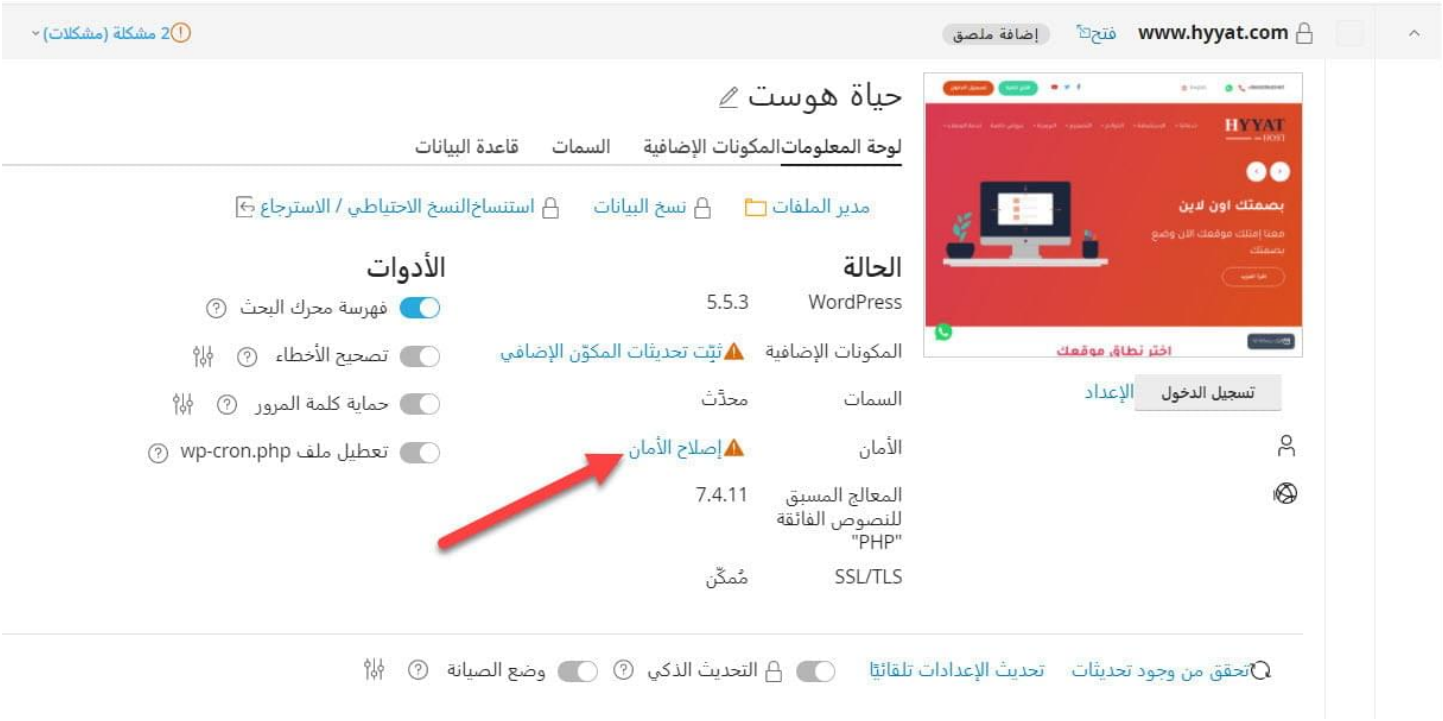
- **Brute force and dictionary attacks:** bots try to guess usernames and passwords, flooding the login with attempts.
- **DoS and DDoS attacks:** attackers flood the site with requests to use up resources and slow it down or take it offline. WordPress's XML-RPC system is often abused for this.
- **Core, plugin and theme vulnerabilities:** bugs in code can be used to bypass logins, upload malicious code or gain extra privileges.
- **Code injection:** attackers look for weaknesses that let them inject PHP, JavaScript or SQL code.

Security check with WordPress Toolkit

WordPress Toolkit is a complete WordPress management tool in cPanel: one dashboard for all your WordPress sites that automates installation, updates and backups. It checks for critical weaknesses during installation, and scans existing sites for weak security settings that you can fix with one click. Some measures can affect how certain plugins work, so apply them carefully or ask our support.

You will find WordPress Toolkit under **Applications** on the cPanel home page. Your sites appear with their status and settings. If a site shows an orange warning next to **Security**, some recommended measures are not applied yet.





Key security measures

- **Block PHP execution** in wp-includes and wp-content/uploads, a common target for uploaded malicious files.
- **Block directory browsing** and set secure permissions for wp-config.php and other files.
- **Bot protection** to block bad bots that scan your site and waste resources.
- **Change the default "admin" username**, which bots target in brute force attacks.
- **Turn off pingbacks**, which rely on XML-RPC and can be abused in DoS attacks.
- **Hotlink protection** to stop other sites from using your images and bandwidth.

WordPress Toolkit also makes it easy to update WordPress core, plugins and themes from one screen and to enable automatic updates. Regular updates are the most important way to close known vulnerabilities.

> **Related service:** Hyyat Host WordPress hosting is optimized and secured for WordPress, from $2.86/month with free SSL.

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

WordPress HostingWordPress design