WordPress Toolkit Security Brief

WordPress® is one of the most popular website building platforms in use today; estimates gauge the CMS as currently being utilized by over 40% of all websites. Unfortunately, the popularity of WordPress has also resulted in it becoming arguably the biggest target for hackers on the web.

Though the vast majority of WordPress vulnerabilities and compromises are related to outdated plugins, themes, and installations, other potential vulnerabilities do exist as well. WordPress Toolkit includes many powerful solutions to mitigate risk and keep WordPress websites secure, while also saving you time. These solutions include:

- **Smart Updates**
- **Security Hardening**
- **Plugin Blocklist**
- **Core Checksum Verification**
- **Vulnerability Detection**
- **Virtual Patching**

Smart Updates

Before any core file, theme, or plugin updates are made, WordPress Toolkit creates a temporary clone of the website in a safe environment to ensure compatibility and security. If updates are determined to be safe, they are applied to the live website. Otherwise, you are provided with a side-by-side comparison and report of the detected issues along with the choice to apply or discard the updates.

Security Hardening

Upon any new installation, WordPress Toolkit automatically applies all critical security measures, as recommended by WordPress experts. Additional security measure can also be specified and implemented, from forbidding the execution of PHP scripts in certain directories to turning off pingbacks, blocking .htaccess and .htpasswd files, bot protection, and much more.

Plugin Blocklist

Poorly-developed, or unsupported, plugins can serve as an entry point for attackers. For this reason, WordPress Toolkit has an integrated blocklist for server administrators to prevent specified plugins from being installed. Any plugin added to this list will no longer be installable through WordPress Toolkit; if one is installed via other means, WordPress Toolkit will automatically remove it.

Core Checksum Verification

Certain types of malware are designed to infect the core .php files of WordPress. Using md5 checksums, WordPress Toolkit can verify the integrity of these files and notify you of any anomaly. These files can then be replaced with the original files without reinstalling WordPress. Certain installation-specific files are excluded from this feature, including index.php and wp-config.php.

Vulnerability Detection (available in WordPress Toolkit v5.8)

Although keeping themes and plugins updated is not difficult in theory, the underlying problem is knowing that a relevant vulnerability exists in a timely manner. Using a constantly updated vulnerability database provided by Patchstack service, WordPress Toolkit monitors all sites (in 30-minute increments) and notifies you in-app and via email, with an option to also auto-update or disable the vulnerable asset.

Virtual Patching (available in early 2022)

Resolving any plugin or theme vulnerability includes inherent risks – updating to an untested version can break your site, and disabling a compromised asset isn't always a viable option. WordPress Toolkit can, on an opt-in basis, apply a virtual patch on a theme or plugin. This temporary solution allows you time to resolve the issue, with the patch then automatically unapplying once the fix is installed.

1.0. DECEMBER.06.21 | cPanel WordPress Toolkit & Online Security

WordPress Toolkit was created to both save you time and keep your customers secure. Enable WordPress Toolkit on your cPanel server today.