Nikolas Gannon | Free resource

Website security check

A ten-minute check that your PHP website is up to date, and what to do if it is not

Nikolas Gannon
Workflow automation for small service businesses

Prepared by
Nikolas Gannon
Workflow and systems consultant

Edition
October 2026
Free to copy and use

Why check this now

In October 2026, two critical vulnerabilities were disclosed in PHP itself, CVE-2026-109618 and CVE-2026-109619, known together as PHP2Shell. Patches were released on 21 October, and exploitation has been reported since. If your site runs PHP, this checklist helps you confirm it is up to date and shows what to do if it is not.

What it is	A five-step check of versions, updates, users and files.
Who it's for	Anyone with a site built on PHP: WordPress, Drupal, Joomla, Magento, Laravel, Symfony or custom PHP.
How long	About ten minutes. Longer if you find a problem.
What you need	Access to the site's admin and to the server or hosting panel.

01 Check your PHP version

This is the foundation check. Everything else runs on top of PHP.

Patched versions are PHP 8.2.35, 8.3.36, 8.4.27 and 8.5.12, released 21 October 2026. If your version is older, it needs updating. Many hosts can do this for you.

How to check

- Ask your host, or look in the hosting panel for the PHP version
- In WordPress, the Site Health screen shows the PHP version
- For a custom site, check the version report or ask your developer

If you are behind

Update to a patched version as soon as you can, restart PHP, your web server and any containers, then re-run this check.

02 Update everything

With PHP updated, the next layer is your CMS, plugins and themes.

- [ ] WordPress core (or your CMS) is the latest version
- [ ] Every plugin is updated to the latest version
- [ ] Every theme is updated to the latest version
- [ ] Old, unused plugins and themes are deleted, not just deactivated
- [ ] Updates run on a schedule, not when something breaks

03 Check for signs of a problem

Most sites will pass this step. It is still worth a careful look.

- [ ] No unknown admin or user accounts exist
- [ ] No plugins or themes you do not recognise are installed
- [ ] No PHP files in the web root have changed recently without your knowledge
- [ ] No unexpected files appear in uploads or in the site root
- [ ] The site is not showing unusual CPU use or sending unexpected traffic

04 If you find something

Deleting the file you found is usually not enough, because there may be another way back in.

01 **Restore** from a clean backup taken before the problem started

02 **Rotate** every password, API key and admin credential

03 **Remove** unknown accounts and anything you did not install

04 **Update** PHP, your CMS and plugins so the same gap cannot be used again

05 **Ask for help** from your host or a developer if you are unsure

05 Keeping on top of it

For most PHP sites, regular updates are the answer. If you would rather have less to maintain, a static site is one option.

Static site	A folder of files served from a CDN. No PHP, database or plugins to update.
What you keep	Forms, booking, search and payments, connecting to services in the background.
Hosting	Free tiers on major CDNs cover typical business traffic.
Still needed	Strong passwords and two-factor login on your domain, hosting and form services.

WordPress, Drupal, Joomla, Magento, Laravel, Symfony and phpMyAdmin were all shown to be exploitable by PHP2Shell. If your site runs PHP, updating is the first step. Whether to move off PHP later is a separate decision, and there is no rush to make it.

About Nikolas Gannon

Nikolas Gannon	I find where small businesses lose hours and money to repeated admin, and I build the simpler system. Workflows, websites and systems, built in the tools you already use.

BOOK A FREE SYSTEMS AUDIT

Choose a time

EMAIL

hello@nikolasgannon.com.au

BASED IN

Sydney, working across Australia