interweb

Generated on 15/11/2026 00:16

KNOWLEDGE BASE · PUBLIC DOCUMENT

An abandoned plugin or an old PHP version: how to spot the risks on your site

Hacked Sites & Malware

CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-1486	v2026.10.10	Angola · English

Interweb Angola
RLX Angola, Lda. · Group RLX Holdings
Tax ID (NIF) 500 260 5724 · Commercial registration no. 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/1486

An abandoned plugin or an old PHP version: how to spot the risks on your site

Hacked Sites & Malware Created on **October 10, 2026** 3 min read



The short answer: most hacked sites were not caught by a clever attack, but by **an old part with a known flaw**: a plugin its author stopped updating, a forgotten theme, a PHP version that no longer gets fixes. The risk is not in having installed a lot, it is in having installed things **that nobody maintains**.

The three places where neglect hides

Part	Sign it is abandoned	What to do
WordPress plugin	On the plugin's official page, the last update date is old, a notice says it has not been tested with the latest WordPress versions, or it has been "closed" in the repository.	Find a maintained alternative, migrate, and delete the old one.
Theme	The same. A theme whose author stopped updating it, or one bought from unofficial sites, gets no fixes.	Move to a maintained theme: see **switching WordPress themes without losing the site**.
PHP version	PHP has versions that stop receiving security fixes. An unsupported version is not patched even if the site runs perfectly.	Move up to a version that is still maintained. See **which PHP version your site should use**.
Forgotten installs	Folders like `old`, `test` or `new-site` holding a WordPress nobody has updated for years.	Delete what you do not use. A copy stays in the backup if you ever need it.

How to take stock in ten minutes

1. **See what is out of date.** In the WordPress "Updates" list, and in the "WordPress Management" tool in cPanel, which shows on one screen what needs updating across every site on the account (the one mentioned in **protecting the WordPress login**).

2 **Open the page of each important plugin** and read the last update date and what recent reviews say. A plugin that has worked well for years may have been abandoned long ago.

3 **Search the plugin's name with the word "vulnerability"**, or check a public database of WordPress plugin flaws. If you find a flaw with no fix, that is a reason to take it off the site.

4 **Confirm the PHP version** of the site in "Select PHP Version" in cPanel and compare it with the list of versions still maintained at php.net/supported-versions.php.

5 **Delete, do not deactivate.** A deactivated plugin does not run, but the file is still there, flaw included, waiting to be called directly.

! **Take a backup before you update or delete.**
Raising the PHP version or swapping a plugin can break a feature. Do it first on a test site, as explained in **updating themes and plugins without breaking anything**, or at least with a fresh backup and the time you did it written down.

Cut down the number of parts that depend on someone else. Every plugin is an author your site depends on. Ask yourself how many you really need, and prefer those with recent updates, many users and an author who answers.

NEED A HAND?

Want us to look with you at the PHP version and tools your site is using? Give us the domain.

Open a support ticket →

SEE ALSO

- Updating themes and plugins without breaking anything →
- Which PHP version should your site use →
- Updating WordPress itself →
- WordPress hosting →

interweb

Interweb Angola

RLX Angola, Lda. · Group RLX Holdings

TAX ID (NIF)	500 260 5724
COMMERCIAL REGISTRATION NO.	26464-25/250724
REGISTERED OFFICE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACT	info@interweb.ao · +244 942 011 191 · www.interweb.ao
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-AO-KB-1486 · v2026.10.10 · Generated on 15/11/2026 00:16