interweb

Generated on 21/10/2026 17:25

KNOWLEDGE BASE · PUBLIC DOCUMENT

The scan says clean but the site still redirects: where an infection hides

Security

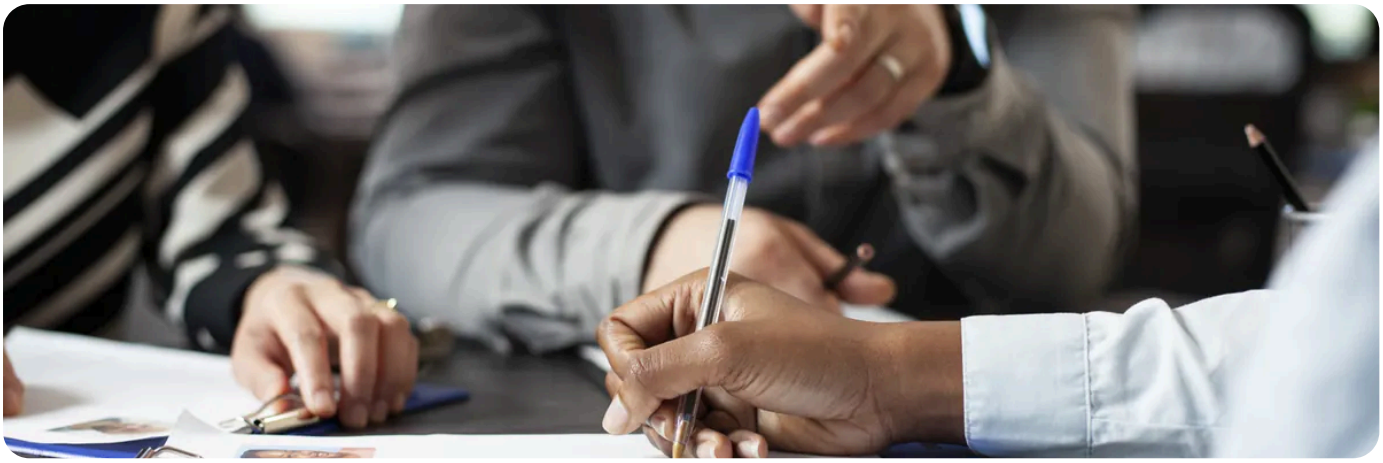
CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-1516	v2026.10.10	Mozambique · English

Interweb Mozambique
RLX Holdings, S.A. · Group RLX Holdings
Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

https://www.meu.interweb.co.mz/knowledgebase/1516

The scan says clean but the site still redirects: where an infection hides

Security Created on **October 10, 2026** 3 min read



The short answer: a scan only sees what it knows how to recognise. A modern infection hides **outside the files you look at first** (in the database, in an `.htaccess`, in a scheduled task, in a forgotten site on the same account) and often **only shows to certain visitors**: people arriving from Google, people on a phone, people who are not signed in. That is why the owner, who always comes in the same way, never sees anything.

The places it usually hides

Where	What to look for
`.htaccess`	Redirect rules you did not write, especially those depending on “where the visitor comes from” or the type of device. Check the one in the root and those in subfolders.
Database	In WordPress, scripts inserted into posts and options (the `wp_options` table), and administrator users you did not create.
“Normal” files	Odd lines at the start or end of `index.php`, `wp-config.php` or the theme’s `footer.php`, with unreadable text and functions such as `eval` or `base64_decode`.
The `uploads` folder	`.php` files in a folder that should hold only images and documents.
Scheduled tasks	Under “Cron Jobs” in cPanel, a task you did not create that downloads the code again after you delete it.
Other sites on the account	An old WordPress in a subfolder or an addon domain, forgotten and out of date, can reinfect everything else.

How to look, step by step

1. **See the site the way a stranger would.** In a private window, sign out of WordPress, open Google, search for your site's name and enter through the result, preferably on a phone. Many infections only act there.

2. **Review what "Imunify Security" in cPanel detected** and the dates: a flagged file nearly always has others nearby. For the starting point, see **how to tell if your site has been compromised**.

3. **Sort the files by modification date** in File Manager and look for what changed without you touching it. It is the simplest method and one of the most effective.

4. **Compare with a clean install.** Download the same version of WordPress, the theme and the plugins from the official source and compare with what is on the site: whatever exists in addition, or differs, is suspect.

5. **Replace instead of patching.** Put back the WordPress core and plugins from clean copies, rather than hunting line by line. Follow the order in **how to clean up a compromised site**, and change every password only *after* you plug the entrance.

If you clean and the problem returns within hours or days, there is a back door.
It is a hidden file that reinstalls the rest, or an administrator account created for that purpose. The cleaning is done only when the door is found and closed, not when the warning goes away.

Before you start, download the current, infected state: it is the evidence of how they got in. If you think it safer to start over, find the most recent clean copy in **after a hack, which backup to restore**.

NEED A HAND?

Cleaned and the infection came back? Give us the domain and what you saw: we read the log to find the way in.

Open a support ticket →

SEE ALSO

- How to tell if your site has been compromised →

- How to clean up a compromised site
- Removing the red Google warning from your site
- After a hack, which backup to restore

interweb

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-MZ-KB-1516 · v2026.10.10 · Generated on 21/10/2026 17:25