interweb

Generated on 21/10/2026 17:19

KNOWLEDGE BASE · PUBLIC DOCUMENT

How to clean up a compromised site

Security

CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-76	v2026.10.18	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/76

How to clean up a compromised site

Security Created on **August 14, 2026** Updated on **October 18, 2026** 2 min read



Cleaning up is only half the job - if the door that let the infection in stays open, it comes back. Work through this in order.

1. Check what was found

1. In cPanel, open **Imunify Security** and review what's listed under detected or quarantined items - this tells you which files are affected before you change anything.

2. Change every password, immediately

1. Most infections start with a stolen or guessed password, not a mysterious exploit. Change your cPanel password, your CMS admin password (WordPress, Joomla...), and its database password.
2. If several people have access (see **managing sub-accounts**, if applicable), have everyone change theirs too - not just the account owner.

3. Update everything

1. Update your CMS core, every plugin and every theme to their latest versions. An outdated plugin is the single most common way sites get compromised.
2. Remove any plugin or theme you no longer use entirely, rather than leaving it deactivated - unused code is still a target.

4. Restore from a clean backup, if you have one

1. If you have a backup from before the infection, restoring it can be faster than manual cleanup - just make sure you also complete steps 2 and 3 afterwards, or the same hole lets the infection straight back in.

Don't just delete the warning banner or the flagged file.
If a plugin was exploited to place it there, removing only that one file leaves the vulnerability open and the infection typically returns within days.

Still showing warnings after this, or not sure where to start? **Open a support ticket** and describe what Imunify Security flagged - we can advise on next steps.

NEED A HAND?

Want a second pair of eyes on this before you touch anything? Ask us first.

Open a support ticket →

In our plans

- All hosting plans have an automatic daily backup, and restoring it costs nothing.
- To see which restore points your account has, open JetBackup (or Backups) in cPanel. Choose one dated before the oldest file Imunify Security flagged.
- If there is none before the infection, or you would rather we do it, open a ticket with your domain, the date you want restored and the Imunify Security report (file paths, threat names and dates, or a screenshot).
- Restoring does not close the hole: change the passwords and update everything straight after, as described above.

SEE ALSO

Not sure yet that it was hacked?
How to tell if your site has been compromised →

WEB HOSTING

Looking for hosting that stays out of your way?

cPanel, a free SSL certificate, backups every night before dawn kept for a year, and support that answers in your language.

See hosting plans →

Free migration of your current site · no lock-in

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-76 · v2026.10.18 · Generated on 21/10/2026 17:19