interweb

Generated on 15/11/2026 00:18

KNOWLEDGE BASE · PUBLIC DOCUMENT

# Locking down the WordPress file editor and a few wp-config settings worth changing

Users, Logins & Security

| CODE | VERSION | COUNTRY · LANGUAGE |
| --- | --- | --- |
| RLX-AO-KB-1918 | v2026.10.15 | 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/1918

# Locking down the WordPress file editor and a few wp-config settings worth changing

Users, Logins & Security Created on **October 15, 2026** 2 min read



**The short answer:** WordPress has, in the dashboard, a **file editor** that lets you change the code of the theme and plugins. One typo there takes the site down, and whoever gets into the dashboard without permission can plant malicious code. One line in **wp-config.php** switches it off. There are two or three more settings in the same file that harden the site.

## The settings

| Line | What it does |
|---|---|
| `define( 'DISALLOW_FILE_EDIT', true );` | **Hides the theme and plugin editors** in the dashboard. Touches nothing else. The most useful. |
| `define( 'FORCE_SSL_ADMIN', true );` | Forces the dashboard and login onto https. Only if the site already has a certificate. |
| `define( 'WP_POST_REVISIONS', 10 );` | Keeps only the latest versions of each post, instead of all: it helps keep the database lean. |
| `define( 'DISALLOW_FILE_MODS', true );` | **Careful:** it also blocks installing and updating plugins, themes and WordPress itself. Only for sites managed another way. |
| **Security keys (salts)** | Changing them logs everybody out of the dashboard. Useful after a suspected break-in. |

## Step by step

1. **Take a copy of wp-config.php.** A typing mistake in this file takes the site down.

2 **Open wp-config.php** (cPanel File Manager) and put the chosen line **before** the phrase “That’s all, stop editing”.

3 **Save and open the dashboard:** under Appearance and Plugins the file editors should be gone.

4 **Check the permissions** of wp-config.php: it holds the database password and should not be readable by everyone: **File permissions**.

5 **Make code changes** another way (in a child theme, or over SFTP), not from the dashboard: **Child theme**.

**This reinforces; it does not protect on its own.**
A switched-off editor does not stop someone who already has an administrator password from installing a malicious plugin. The real defence is a well-protected login and up-to-date plugins: **Protecting the WordPress login**.

If the file was damaged, see **Rebuilding the wp-config.php connection**. Another door to consider: **XML-RPC**.

NEED A HAND?

Want help reviewing your WordPress security? Open a ticket with the address.

Open a support ticket →

SEE ALSO

- **Protecting the WordPress login: three steps in order of effect** →
- **File permissions explained: what 755, 644 and 777 mean** →
- **A child theme or editing the theme directly: why updates wipe your changes** →
- **An abandoned plugin or an old PHP version: how to spot the risks on your site** →
- **Rebuilding the wp-config.php connection** →

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<br>Belas, Luanda, Angola |
| CONTACT | info@interweb.ao · +244 942 011 191 · www.interweb.ao |
| OPENING HOURS | Monday to Friday - 08 AM to 04 PM<br>Saturday & Sunday - Closed |


Online version of this document

RLX-AO-KB-1918 · v2026.10.15 · Generated on 15/11/2026 00:18