

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Trancar o editor de ficheiros do WordPress e algumas definições do wp-config que valem a pena

WordPress e CMS

CÓDIGO

RLX-MZ-KB-1936

VERSÃO

v2026.10.15

PAÍS · IDIOMA

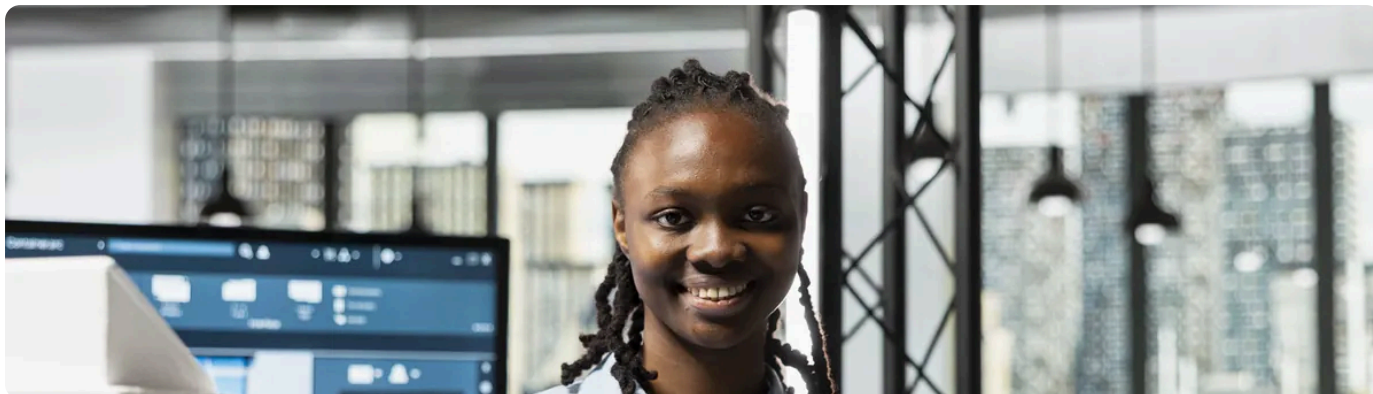
Moçambique · Português

Interweb Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

<https://www.meu.interweb.co.mz/knowledgebase/1936>



A resposta curta: o WordPress tem, no painel, um **editor de ficheiros** que deixa mudar o código do tema e dos plugins. Uma gralha ali tira o site do ar, e quem entrar no painel sem licença pode meter código malicioso. Uma linha no **wp-config.php** desliga-o. Há mais duas ou três definições do mesmo ficheiro que reforçam o site.

As definições

Linha	O que faz
<pre>define('DISALLOW_FILE_EDIT', true);</pre>	Esconde os editores de temas e de plugins do painel. Não mexe em mais nada. A mais útil.
<pre>define('FORCE_SSL_ADMIN', true);</pre>	Obriga o painel e o início de sessão a usar https. Só se o site já tem certificado.
<pre>define('WP_POST_REVISIONS', 10);</pre>	Guarda só as últimas versões de cada artigo, em vez de todas: ajuda a manter a base de dados magra.
<pre>define('DISALLOW_FILE_MODS', true);</pre>	Cuidado: bloqueia também instalar e atualizar plugins, temas e o próprio WordPress. Só para sites geridos por outra via.
Chaves de segurança (salts)	Mudá-las desliga toda a gente do painel. Útil depois de uma suspeita de intrusão.

Passo a passo

1

Faça uma cópia do wp-config.php. Um erro de escrita neste ficheiro tira o site do ar.

2

Abra o wp-config.php (Gestor de Ficheiros do cPanel) e ponha a linha escolhida **antes** da frase «That's all, stop editing».

3

Grave e abra o painel: em Aspeto e em Plugins já não deve haver os editores de ficheiros.

4

Confira as permissões do wp-config.php: ele guarda a senha da base de dados e não deve ser legível por todos: **Permissões de ficheiros**.

5

Faça as alterações de código de outra forma (num tema filho, ou por SFTP), e não pelo painel: **Tema filho**.

Isto reforça, não protege sozinho. O editor desligado não impede quem já tem uma senha de administrador de instalar um plugin malicioso. A defesa verdadeira é o login bem protegido e os plugins em dia: **Proteger o login do WordPress**.

Se o ficheiro foi estragado, veja **Refazer a ligação do wp-config.php**. Outra porta a considerar: **XML-RPC**.

Quer ajuda a rever a segurança do seu WordPress? Abra um pedido com o endereço.

[Abrir pedido de suporte](#)

VEJA TAMBÉM

Proteger a entrada do WordPress: três passos por ordem de efeito

Permissões de ficheiros explicadas: o que significam 755, 644 e 777

Tema filho ou edição directa: porque as actualizações apagam as suas alterações

Um plugin abandonado ou um PHP antigo: como descobrir os riscos do seu site

Recriar a ligação do wp-config.php



Versão online deste documento

A Interweb é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020

FUNDADA

37 mil+

CLIENTES

130+

INSCRIÇÕES POR DIA

Interweb Moçambique

RLX Holdings, S.A. • Grupo RLX Holdings

NUIT 401 191 607

NUEL 105 045 974

CAE 62022

SEDE Bairro 7 de Setembro
Vilankulo 1304 • CEP 0411-02, Inhambane, Moçambique

CONTACTOS info@interweb.co.mz • +258 84 635 1111 • +258 86 635 1111 • www.interweb.co.mz

HORÁRIO 2ª. à 6ª. Feira - 08 à 16 Horas
Sábado & Domingo - Fechado