

KNOWLEDGE BASE · PUBLIC DOCUMENT

Content Security Policy: a first policy, tried out in report-only mode

Security

CODE

RLX-MZ-KB-1982

VERSION

v2026.10.15

COUNTRY · LANGUAGE

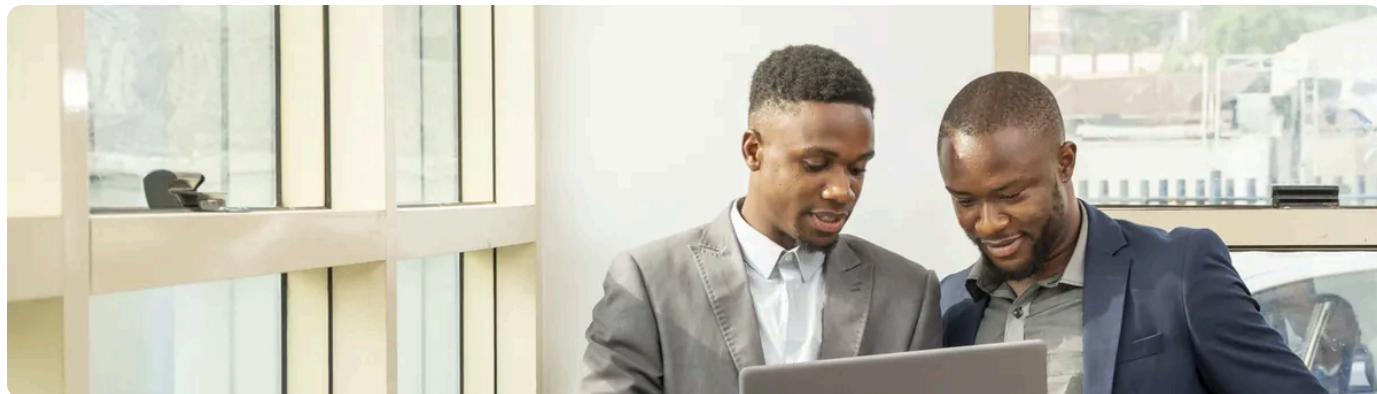
Mozambique · English

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/1982>



The short answer: Content Security Policy (CSP) is a header that tells the browser **where the site may load scripts, styles and images from**. If someone injects an outside script, the browser refuses it. It is strong, but it is also easy to break a site with it; so you start in **report-only mode**, which only warns and blocks nothing.

What the site needs

What	What to do
What it controls	Allowed origins for the site's scripts, styles, images, fonts, videos and connections.
Report-only mode	The Content-Security-Policy-Report-Only header records what it would block, without blocking. It is the mode for rehearsing.
What usually breaks	Scripts and styles written inside the page itself, Google Analytics and Tag Manager, outside fonts, embedded videos: Tag Manager .
A first policy	Accept everything only from the site itself, then add the outside origins the site really uses.
When to start blocking	When the log has been clean for a few days, on all the important pages.

Getting started

1**Take a copy of .htaccess.**

2

Put the policy in report-only mode with a simple line (add the outside origins afterwards): `Header set Content-Security-Policy-Report-Only "default-src 'self'"`

3

Browse the site with the browser console open (F12, Console tab): each thing that would be blocked shows as a warning.

4

Add the outside origins the site uses on purpose (analytics, fonts, video), one at a time.

5

When the warnings stop, switch to the header that blocks (Content-Security-Policy) and test again: **Security headers**.

A policy that is too tight breaks the site. If you go straight to the blocking mode you may lose the menu, the form or the checkout without warning. Always test in report-only mode, and in another browser. If something breaks, go back to the copy of .htaccess.

If your site mixes http and https content, fix that first: **Mixed content**. Another header to turn on with care: **HSTS**.

Want help rehearsing a policy for your site? Open a ticket with the address.

[Open a support ticket](#)

SEE ALSO

[Security headers explained: what they do and how to add them in .htaccess](#)

[HSTS explained: forcing https for good, and the trap of switching it on too early](#)

[Mixed content after moving to HTTPS: the padlock that will not turn on](#)

[Google Tag Manager and tracking pixels: adding them without slowing your site](#)

[ModSecurity and web application firewalls: what they do, and what to do when one blocks you](#)



Online version of this document

Interweb is a leading internet services company, with a mission to help businesses to be born and prosper through technology.

2020

FOUNDED

37,000+

CLIENTS

130+

SIGN-UPS A DAY

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