Mozout

Generated on 15/11/2026 00:41

KNOWLEDGE BASE · PUBLIC DOCUMENT

Security headers explained: what they do and how to add them in .htaccess

Website Protection & Privacy

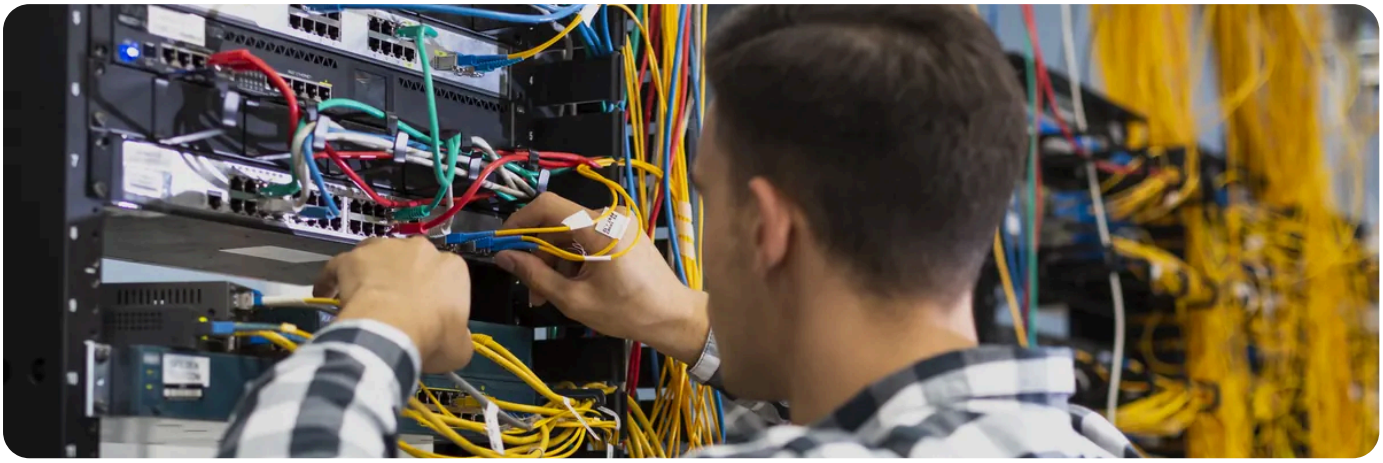
CODE	VERSION	COUNTRY · LANGUAGE
RLX-INT-KB-4626	v2026.10.10	International · English

MozOut International
RLX Holdings (Pty) Ltd. · Group RLX Holdings
Tax no. (SARS) 943 907 6234 · Registration no. (CIPC) 2025/667953/07

https://www.my.mozout.com/knowledgebase/4626

Security headers explained: what they do and how to add them in .htaccess

Website Protection & Privacy Created on **October 10, 2026** 3 min read



The short answer: security headers are small instructions your site sends the browser with every page (“do not let anyone put me inside another site”, “do not guess the type of this file”). They cost three lines in `.htaccess`, do not change how the site looks, and close known kinds of attack. Three can be switched on by almost any site without risk, and others need care.

The headers, one by one

Header	What it does	Risk in switching it on
X-Content-Type-Options: nosniff	Stops the browser “guessing” a file’s type and running as a program one that presented itself as an image.	Hardly any.
X-Frame-Options: SAMEORIGIN	Stops other sites showing yours inside a frame (a click-tricking technique).	Breaks embeds of your own site on another domain of yours, if you have any.
Referrer-Policy	Controls how much of the originating address is sent to the sites the visitor goes on to.	Low. Some statistics tools may see less.
Permissions-Policy	Says which browser features (camera, microphone, location) the page may use.	Low, if you do not use them.
Strict-Transport-Security (HSTS)	Forces the browser to always use https.	**High if switched on early.** It has its own article: **HSTS explained**.
Content-Security-Policy	A list of where the page may load scripts, images and styles from. The strongest defence against injected scripts.	**High.** A rule that is too tight breaks the site: forms, maps, statistics, videos.

How to add the three safe ones

1. **Open the** `.htaccess` in the site root, in cPanel File Manager (with hidden files showing). Make a copy of the file before you change it.

2. **Add these lines at the end of the file:**

```
<IfModule mod_headers.c>
Header always set X-Content-Type-Options "nosniff"
Header always set X-Frame-Options "SAMEORIGIN"
Header always set Referrer-Policy "strict-origin-when-cross-origin"
</IfModule>
```

3. **Save and check.** Open the site and press F12, the Network tab, click the page request and read the response headers: the new ones should appear. Public services also read the headers of an address and give it a grade.

4. **Browse the site** and confirm that forms, videos and maps still work. If something broke, remove the latest line and test again.

Content-Security-Policy: start in report-only mode.
Instead of enforcing it, use the `Content-Security-Policy-Report-Only` header. It blocks nothing; it just records, in the browser console, what it would block. Move to the enforcing version only when the list is clean. A WordPress with many plugins has so many script sources that a fair rule takes work.

If the site goes through Cloudflare, some of these headers can also be set there. Pick one place only, so you do not have two rules disagreeing. And if your WordPress already has a security plugin that adds them, check before duplicating.

NEED A HAND?

Added a line and the site stopped opening? Tell us the domain and the line: we will help you undo it.

Open a support ticket →

SEE ALSO

- HSTS explained →
- How to redirect HTTP to HTTPS with .htaccess →

.htaccess for PHP projects: friendly URLs and redirects →

The Cloudflare options worth having, and the ones that cause trouble →

Mozout

MozOut International

RLX Holdings (Pty) Ltd. · Group RLX Holdings

TAX NO. (SARS)	943 907 6234
REGISTRATION NO. (CIPC)	2025/667953/07
REGISTERED OFFICE	1111 Olive Street Saint Louis 63101, Missouri, United States
CONTACT	info@mozout.com · +27 78 823 3325 · www.mozout.com
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

RLX-INT-KB-4626 · v2026.10.10 · Generated on 15/11/2026 00:41

Online version of this document