

KNOWLEDGE BASE · PUBLIC DOCUMENT

Files that must never be public: .git folders, .env, backups and database dumps

Security

CODE

RLX-MZ-KB-1980

VERSION

v2026.10.15

COUNTRY · LANGUAGE

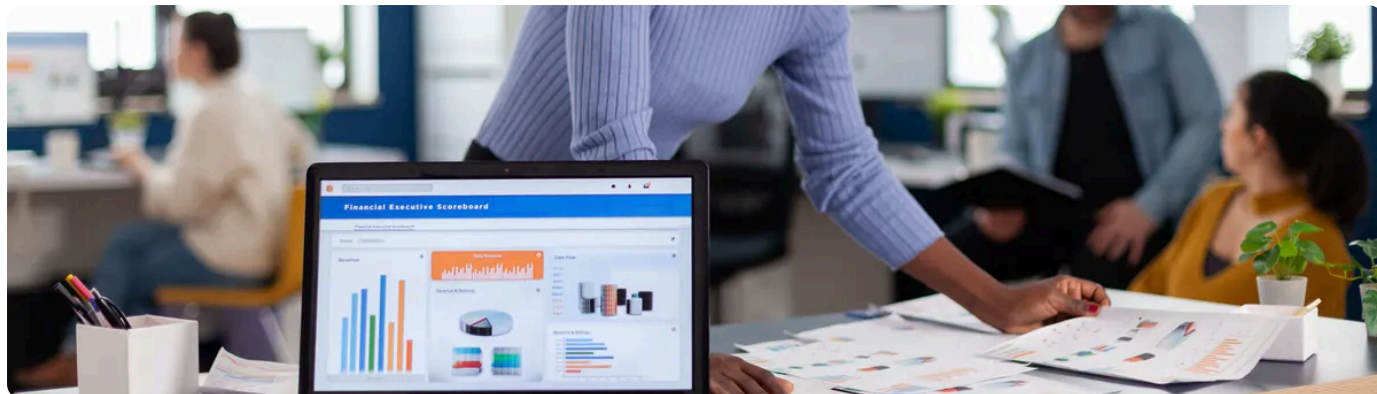
Mozambique · English

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/1980>



The short answer: everything in the site folder **can be requested by anyone** who guesses the file name. Git folders, files with passwords (**.env**), copies like **wp-config.php.bak** and database dumps (**.sql**) get forgotten there. Bots look for those names every day. Check, delete and block.

What the site needs

What	What to do
The .git folder	It holds all the code and the history, including old passwords someone wrote and then deleted. <code>your-domain.com/.git/config</code> must not open.
The .env file	The application's passwords and keys: Keeping passwords out of your PHP code.
File copies	wp-config.php.bak, config.old, a .zip of the site, "backup" folders: the server hands them over as text or as a download.
Database dumps	An .sql file in the site folder is the whole database, one address away.
Logs and test tools	debug.log, error_log, phpinfo.php, installers: Debug mode.

Getting started

1

Look in the File Manager (with "show hidden files") for anything that is not the site: .git, .env, .sql, .zip, .bak, .old, .log.

2

Test in the browser a few addresses a bot would try (.env, .git/config, an .sql with the site's name). You should see "404" or "403", never the contents.

3

Move or delete what is not needed. Backups are kept **outside** the public folder: **Your own backup**.

4

Block what has to stay, by adding to .htaccess: `<FilesMatch "\.(env|sql|bak|old|log)$">`
`Require all denied`
`</FilesMatch>` and, for Git folders, a rule that refuses them.

5

If any secret was exposed, change it: the database password, API keys, whatever was in .env. Deleting the file does not undo what has already been read.

Deleting the file is not enough if someone already read it. If it was public, assume it was copied and change the passwords. Then check for strange access: **After a hack**.

To publish with Git without exposing the .git folder, see **Git in cPanel**. Security headers help, but do not replace this: **Security headers**.

Found something exposed and do not know how to close it? Open a ticket with the address, without copying the file's contents.

[Open a support ticket](#)

SEE ALSO

[Keeping passwords out of your PHP code: .env files and the right permissions](#)

[Git in cPanel: publishing your site from a repository](#)

[Making and keeping your own backup, and testing that it works](#)

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

[After a hack, which backup do you restore? Choosing a clean copy](#)



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