Mozout

Generated on 21/10/2026 15:58

KNOWLEDGE BASE · PUBLIC DOCUMENT

Keeping passwords out of your PHP code: .env files and the right permissions

PHP & Development

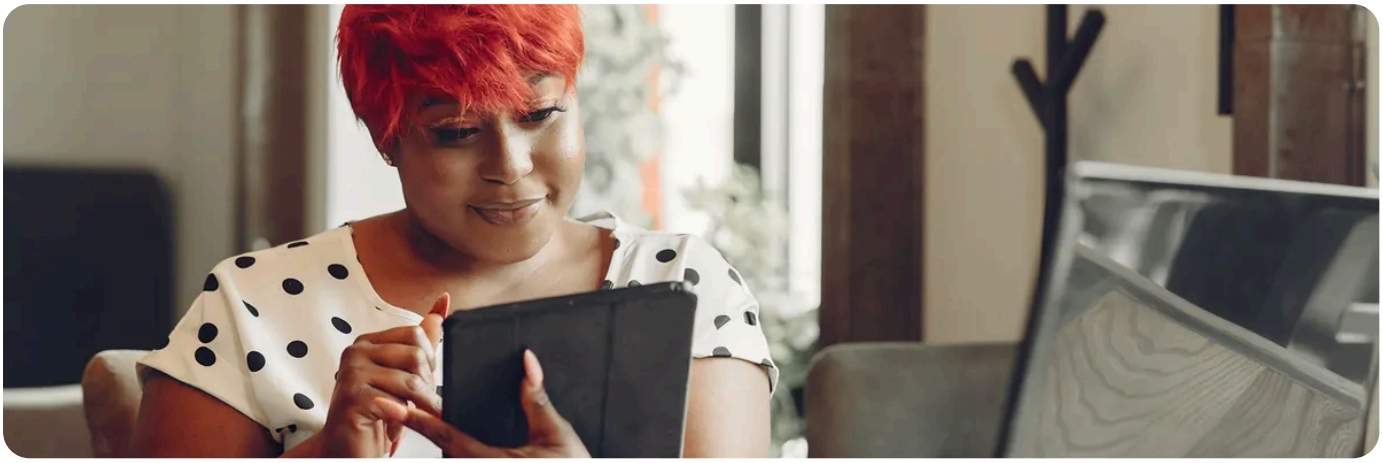
CODE	VERSION	COUNTRY · LANGUAGE
RLX-INT-KB-2520	v2026.10.10	International · English

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/2520

Keeping passwords out of your PHP code: .env files and the right permissions

PHP & Development Created on **October 10, 2026** 3 min read



Put passwords and keys in a **configuration file outside the public folder**, readable only by your account, and let the code read that file. That way a password never sits in a file the browser can open, never goes into a repository, and is changed in one place.

Setting it up, step by step

1. In the File Manager, create a folder **next to public_html** (not inside it), for example `/home/YOURACCOUNT/config`.
2. In it, create a file, for example `app.env`, with one line per secret, in the form `NAME=value`.
3. Give the file permission **600** (Change Permissions, in the File Manager): only the owner reads and writes. Your account's PHP runs as the account itself, so it can read it.
4. In the code, read the file instead of writing the password into it.
5. Check that the file is **not reachable**: try opening it in the browser from your own site's address. It must give a 403 or a 404.

The file:

```
DB_HOST=localhost
DB_NAME=account_database
DB_USER=account_user
DB_PASS=the-password
```

And the reading, with nothing to install:

```
<?php
$cfg = parse_ini_file('/home/YOURACCOUNT/config/app.env', false, INI_SCANNER_RAW);
$pass = $cfg['DB_PASS'];
```

If the project uses Composer, the *vlucas/phpdotenv* library reads `.env` files and is what frameworks usually bring. See **Composer on shared hosting**.

If the .env has to stay inside the site

Some applications expect the `.env` in the project root. Then what protects you is the structure: the public folder should be only the application's `public`, as described in **getting a Laravel application running**. And add the block that denies files starting with a dot, described in **.htaccess for PHP projects**.

Two good habits to add. Use **different values** for the test site and the real one, so a slip in one does not touch the other. And give **each service its own password**: if one leaks, you change only one.

A .env in public_html is public.
Anyone who types the address downloads your passwords, and bots look for exactly those file names. If that happened, **change the passwords now** (the database one, in cPanel, and the keys for any outside service), rather than just deleting the file.

Do not push the .env to a repository.
Put it in `.gitignore`. A secret that went through Git stays in the history even after it is deleted. See **Git in cPanel**.

This encrypts nothing.
Whoever has access to the account's files reads the file, and our daily copies contain it, as do the ones you download. Keep your own copies carefully. Give the database a user with only the privileges the application needs: **creating a database user and giving it the right privileges**.

NEED A HAND?

Not sure whether a file with secrets can be reached from a browser? Tell us the domain and we will check it with you.

Open a support ticket →

SEE ALSO

- Creating a database user and giving it the right privileges
- Where each application keeps its database connection details
- .htaccess for PHP projects
- Environment variables and secrets for your application

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

Online version of this document

RLX-INT-KB-2520 · v2026.10.10 · Generated on 21/10/2026 15:58