BUILDER TOOLKIT

AI build safety review

A 15-minute security and privacy review for anything built with AI.

Use it: Before launch and after any big AI-made change to sign-in, data or payments.

Secrets

☐ Searched the code for key, secret, token and password

☐ .env listed in .gitignore

☐ Paid APIs (AI, payments, email) only called from server code

☐ Any leaked key rotated, not just deleted

Data

☐ Every table has row level security, deny by default

☐ Signed in as user A, could not read user B's data

☐ Only collect what the app needs

☐ Backups on, or an export taken before big changes

AI-written code

☐ Read every change touching sign-in, payments, permissions or deletes

☐ Packages checked on the official registry

☐ Asked two AI tools to review for security issues; fixed the top finding

Fill it in with AI

Review this project for security and privacy issues: exposed secrets, missing access checks, unsafe database rules, and risky packages. List findings by severity with the file and line, explain each in plain words, and suggest the smallest fix. Don't change anything yet.

https://digitalbuilders757.com/university/study/toolkit/safety-review