

REFACTOR

The 50-point production-readiness checklist

If your AI-built app fails more than 10 of these, it isn't ready for paying customers. Go through it before your next demo, audit, or funding round.

Security (10)

- Row-level security enabled on every user-data table
- No `service_role` or admin keys in client bundle
- All secrets in env vars, never committed
- Rate limiting on `/auth` and password reset
- Email confirmation required before account is active
- Input validated server-side with a schema (Zod, valibot, ...)
- Webhooks verify signatures before processing
- File uploads bucketed, size-capped, type-checked
- Auth-protected routes can't be loaded via SSR/prerender
- Roles stored in a roles table, NEVER on profiles

Data integrity (8)

- Foreign keys + cascade rules declared
- Unique constraints on emails, slugs, external IDs
- Migrations checked in and runnable from zero
- No `SELECT *` — explicit columns
- Pagination on every list endpoint
- Soft delete (`deleted_at`) where users can undo
- Money stored as integer cents, never float
- Timestamps are `timestampz`, never `timestamp`

Reliability (8)

- Error boundaries around every async surface
- Server functions return typed errors, not 500s
- Retries + idempotency keys on writes
- Background jobs survive restarts
- Health check endpoint
- Structured logs with request IDs
- Sentry / error reporting wired in

- Uptime monitor pinging prod every minute

Performance (8)

- Initial JS bundle < 500 KB gzipped
- Images served as AVIF/WebP at the size rendered
- Route-level code splitting
- List queries indexed (EXPLAIN ANALYZE'd)
- No n+1 queries on hot paths
- Suspense or skeletons, not spinners-on-spinners
- Caching headers on static assets
- LCP < 2.5s on a mid-tier phone over 4G

Maintainability (8)

- No file over 400 lines
- No 'any' or '@ts-ignore' without a comment explaining why
- Lint + format run on every PR
- Type errors block merge
- README explains how to run locally in < 5 minutes
- Runbook for the 3 things that break most
- ADRs for non-obvious decisions
- Onboarding doc for a new engineer's first PR

Testing (8)

- Vitest/Jest covers business-critical logic
- Playwright smoke test for signup → checkout → logout
- Coverage report visible (target > 60%)
- Tests run in CI on every PR
- Seed script for local + staging data
- Mocks for external APIs (no live calls in CI)
- Visual regression on hero/checkout pages
- Load test on the most expensive endpoint

Failing more than 10? Send the repo. We'll mark every miss for free. refactorai.se