

Pre-launch checklist for AI-built apps

12 checks you can run yourself in about 20 minutes. Written for Lovable, Bolt, Replit and Cursor apps on Supabase + Stripe; the ideas apply to any stack.

Only check apps you own or are authorized to test.

Who can see what

8 min

- ☐ 01 **Row-Level Security is on for every table.**
Supabase → Advisors → Security Advisor shows no “RLS disabled” errors. Fix tables holding user data first.
- ☐ 02 **No policy says `true` on private data.**
Authentication → Policies: a SELECT or UPDATE policy using `true` lets every signed-in user in. Limit it to the owner or their team.
- ☐ 03 **The two-account test passes.**
Sign up as two users in different teams. As user B, open one of A's pages or swap an ID in the URL. You should see nothing.
- ☐ 04 **Users can't upgrade themselves.**
Columns like `role`, `plan` or `credits` must not be writable by the user. Check your profiles table's UPDATE policy and column grants.

Keys and secrets

4 min

- ☐ 05 **No secret keys in your website.**
Open your live site → DevTools → Sources → Ctrl+Shift+F and search `service_role`, `sk_live`, `sk-` and `secret`. Only your public anon / publishable key belongs there.
- ☐ 06 **Leaked keys are rotated.**
Any key that ever sat in frontend code, a `VITE_` / `NEXT_PUBLIC_` variable or git history: rotate it now. Deleting the line is not enough.

Payments

3 min

- ☐ 07 **Your Stripe webhook verifies signatures.**
The handler calls `constructEvent` with the webhook signing secret and rejects anything unsigned.
- ☐ 08 **Plans change only on the server, after payment.**
Upgrades happen in the webhook once `payment_status` is `paid`, never from a button click in the browser.

Files, backups, sign-up

3 min

- ☐ 09 **User files are private.**
Storage buckets holding uploads are not public; files are served through signed links that expire.
- ☐ 10 **You've tried a restore.**
Backups (or point-in-time recovery) are on, and you've restored a copy at least once, ideally into a staging project.
- ☐ 11 **Sign-up has basic guards.**
Email confirmation on, passwords of 10+ characters, and CAPTCHA or rate limits on sign-up and any AI feature.

Email

2 min

- ☐ 12 **Your emails are authenticated.**
SPF and DKIM for every service that sends as you, plus a DMARC record. Free check: postlaunch.agency/#email-check

Your score

12 / 12	Ahead of most AI-built apps. Re-check after big changes.
1–3 unticked	Fix them this week. Most take under an hour.
4+ unticked, or unsure on 1–3	Get a second pair of eyes before taking more payments.

Not sure about some of these? The Postlaunch Production-Readiness Audit checks all of this and more, with evidence and fixed-price fixes, in 5 business days.