

PRODUCTION-READINESS CHECKLIST FOR AI-BUILT APPS

35 checks across the eight areas that decide whether a vibe-coded app (Lovable, Bolt, Cursor, v0, Replit) survives real users, a security review, or a fundraiser. Tick what is genuinely true today. Anything you can't tick is a gap between you and a safe launch.

DAPPASOL.COM · TAKE A PROTOTYPE TO PRODUCTION · SENIOR ENGINEERS, FIXED PRICE

SCORE YOURSELF: MOST APPS STRAIGHT OUT OF A VIBE-CODING TOOL TICK 10-18 OF 35.

01 AUTHENTICATION & ACCESS

5 CHECKS

- ☐ Every protected route checks auth on the server, not just by hiding UI
- ☐ Sessions and tokens expire and refresh correctly
- ☐ Password reset and account recovery works and is rate-limited
- ☐ Roles and permissions are enforced server-side, not client-side
- ☐ No admin route or action is reachable without auth

02 SECRETS & KEYS

4 CHECKS

- ☐ No secret is prefixed NEXT_PUBLIC_ or VITE_ or shipped to the browser
- ☐ API keys and tokens live in server-side env, never committed to git
- ☐ Any key that was ever exposed has been rotated
- ☐ Third-party webhooks verify a signature

03 DATA ACCESS (RLS)

5 CHECKS

- ☐ Row-Level Security is enabled on every table holding user data
- ☐ A user cannot read another user's records by changing an ID
- ☐ The service_role / admin database key is never used in client code
- ☐ Personal data is encrypted in transit and at rest
- ☐ Backups exist and have actually been test-restored

04 INPUT VALIDATION

4 CHECKS

- ☐ Every user input is validated on the server
- ☐ Inputs are sanitized against SQL injection and XSS
- ☐ File uploads are type- and size-checked and stored safely
- ☐ Rate limiting protects expensive and auth endpoints

05 ERROR HANDLING & LOGGING

4 CHECKS

- ☐ Stack traces and database errors are never shown to users
- ☐ Secrets never appear in logs
- ☐ Errors are captured to a monitoring tool (Sentry or similar)
- ☐ The app fails gracefully, no blank white screens

06 PAYMENTS

4 CHECKS

- ☐ Payment amounts are verified server-side, never trusted from the client
- ☐ Payment webhooks are signature-verified and idempotent
- ☐ No raw card data touches your servers (hosted fields / Stripe Elements)
- ☐ Refund and dispute flows are handled

07 INFRASTRUCTURE & LAUNCH

4 CHECKS

- ☐ HTTPS everywhere, no mixed content
- ☐ Automated tests and CI run before every deploy
- ☐ You can roll back a bad deploy quickly
- ☐ Uptime and error monitoring with alerts is live

08 LEGAL & LIABILITY

5 CHECKS

- ☐ A privacy policy is published and reflects what you actually collect
- ☐ Terms of service are in place
- ☐ Lawful basis + consent for EU users (GDPR) and a CCPA/CPRA notice for California
- ☐ You know exactly where user data lives and who can access it
- ☐ A data deletion and export path exists for user requests

Can't tick them all? That's the norm, and it's exactly what we fix. Book a free 15-minute build audit and we'll tell you the specific blockers and a fixed price to close them. We find every blocker or the audit is free. Free live version: dappasol.com/production-readiness-check/

BOOK A FREE AUDIT →
CALENDLY.COM/ISHANRANAWORK