

## FREE RESOURCE

# The Vibe-Coder's Security Checklist

15 security checks for apps built with AI tools, each with a test you can run yourself. Start with the High severity items.

**Fix these first: High severity**

**Secret API keys in front-end code.** Open your browser's developer tools (Sources and Network tabs) and search for "key", "token" and "secret". Publishable keys, such as a Supabase publishable (anon) key or a Stripe publishable key, are designed to be public. Secret keys, service-role keys and third-party API keys (an OpenAI key, for example) are not. If you find one, move that call to the server and rotate the key.

**Login that is only enforced in the browser.** Copy the URL of a logged-in page and open it in a private window, or call the API it uses without a session. If the data still comes back, the login check lives in the interface and the server is not enforcing it.

**No row-level security or per-user access rules.** Signed in as user A, change an ID in a request (or the URL) to one belonging to user B. If B's data comes back, access is not being enforced where the data lives.

**Database tables reachable from the browser without access rules.** If the browser queries your database directly (common with Supabase), that is only safe when row-level security is enabled on every exposed table, with policies that match your rules. Check each table in your database dashboard. A table without row-level security can be read or changed by anyone holding the public key.

**No server-side input validation.** Send unexpected input straight to the API rather than through the form: very long text, script tags, wrong data types, negative quantities. If the server accepts it, add validation on the server; checks in the form alone can be bypassed.

**Secrets committed to the code repository.** Search the repository and its history for keys, passwords and .env values. Anything found should be rotated (deleting it from the latest version is not enough) and moved into environment variables or your host's secrets store.

**Unprotected admin or internal endpoints.** List every admin page, internal API route and scheduled job. Each should require a signed-in user with the right role. A hard-to-guess URL is not protection.

**Passwords handled insecurely.** Passwords should be hashed by a proven auth service or library, never stored in plain text and never written to logs. If the AI tool

wrote its own login system, replace it with a managed auth provider.

**No backups or recovery plan.** Confirm the database is backed up automatically, check how far back you can restore, and do a test restore. A backup nobody has restored is an assumption, not a plan.

**Then these: Medium severity**

**No rate limiting.** On your own app, call a login, sign-up or AI-powered endpoint many times in quick succession. If nothing slows you down, you are open to password guessing, spam sign-ups and unexpected usage bills.

**Overly permissive CORS.** Check which websites your API accepts browser requests from. A wildcard (\*) is acceptable for genuinely public data; for anything behind a login, allow only your own domains.

**Pages or requests not on HTTPS.** Confirm every page loads over HTTPS and the browser console shows no "mixed content" warnings for scripts, images or API calls.

**Error messages that expose internals.** Trigger an error, for example by submitting a broken form or visiting a missing record. If users see stack traces, database queries or file paths, log the detail privately and show a plain message instead.

**Unreviewed dependencies.** Run your package manager's audit (npm audit, for example) for known vulnerabilities, update what it flags and remove packages the app no longer uses.

**Unrestricted file uploads.** If users can upload files, check that type and size are limited on the server, uploaded files cannot run as code, and private files are not reachable at a public or guessable URL.

#### ABOUT MAXENIUS

**A senior engineering, design and marketing team.** We take AI-built apps to production, build AI agents, and deliver white-label work for agencies. If you would like a second opinion on anything in this document, email [contact@maxenius.com](mailto:contact@maxenius.com) or visit [maxenius.com](https://maxenius.com).