



Security Guide für Vibe Coder

10 Regeln für alle, die Apps mit KI-Tools bauen, in einfacher Sprache.

Version 1.0 · Oktober 2026 · switech-solution.com

Mit Tools wie Cursor, Lovable, Bolt oder v0 kannst du heute ohne Programmierkenntnisse eine App bauen. Das ist grossartig. Die KI schreibt aber nicht automatisch sicheren Code: Sie macht, was du verlangst, und vergisst dabei oft die Sicherheit.

Dieser Guide erklärt die zehn wichtigsten Regeln ohne Fachjargon. Zu jeder Regel findest du einen Satz, den du direkt deiner KI geben kannst.

01 Geheime Schlüssel gehören nie in den Code

WARUM

API-Schlüssel (z. B. von OpenAI oder Stripe) im Code oder im Frontend kann jeder Besucher auslesen und auf deine Kosten nutzen.

SO GEHST DU VOR

- Schlüssel in eine .env-Datei schreiben und diese Datei in .gitignore eintragen.
- Achtung: Alles mit NEXT_PUBLIC_ oder VITE_ im Namen ist öffentlich sichtbar.
- Ist ein Schlüssel einmal geleakt, sofort beim Anbieter sperren und neu erstellen. Den Commit zu löschen reicht nicht.

SO FRAGST DU DEINE KI

«Prüfe mein Projekt auf API-Schlüssel oder Passwörter im Code und im Frontend. Verschiebe sie in Umgebungsvariablen, die nur auf dem Server verfügbar sind.»

02 Sperr deine Datenbank ab

WARUM

Viele KI-Apps nutzen Supabase oder Firebase. Ohne Regeln kann jeder mit dem öffentlichen Schlüssel alle Daten lesen und ändern.

SO GEHST DU VOR

- Supabase: Row Level Security (RLS) für jede Tabelle aktivieren und Regeln definieren.
- Firebase: Security Rules setzen und niemals «allow read, write: if true» verwenden.
- Testen: Mit einem zweiten Konto prüfen, ob du fremde Daten siehst.

SO FRAGST DU DEINE KI

«Aktiviere Row Level Security für alle Tabellen und schreibe Regeln, damit jeder Nutzer nur seine eigenen Daten lesen und ändern kann.»

03 Rechte immer auf dem Server prüfen

WARUM

Ein ausgeblendeter Button schützt nichts. Wer die Anfrage direkt schickt, umgeht das Frontend.

SO GEHST DU VOR

- Bei jeder Aktion auf dem Server prüfen: Ist der Nutzer angemeldet, und gehört ihm dieses Objekt?
- Admin-Funktionen nur für Admins freigeben, serverseitig geprüft.

SO FRAGST DU DEINE KI

«Prüfe alle API-Routen: Wird serverseitig kontrolliert, ob der Nutzer angemeldet ist und auf das angefragte Objekt zugreifen darf?»

04 Login nicht selbst bauen

WARUM

Eigene Login-Systeme sind eine häufige Quelle für Sicherheitslücken.

SO GEHST DU VOR

- Bewährte Anbieter nutzen, z. B. Supabase Auth, Clerk, Auth0 oder Firebase Auth.
- Zwei-Faktor-Authentifizierung mindestens für dein eigenes Admin-Konto aktivieren.

SO FRAGST DU DEINE KI

«Ersetze die eigene Login-Logik durch [Anbieter] und entferne alle selbst gebauten Passwort-Funktionen.»

05 Trau keiner Eingabe

WARUM

Formulare und Uploads können manipuliert werden. KI-Code prüft Eingaben oft nur im Browser.

SO GEHST DU VOR

- Eingaben zusätzlich auf dem Server prüfen (z. B. mit zod).
- Bei Uploads Dateityp und Grösse begrenzen.

SO FRAGST DU DEINE KI

«Füge für alle Formulare und API-Routen eine serverseitige Validierung hinzu, mit Längen- und Formatprüfung.»

06 Schütz teure APIs vor Missbrauch

WARUM

Ein offener KI-Endpunkt kann über Nacht hohe Kosten verursachen.

SO GEHST DU VOR

- KI-Aufrufe nur über deinen Server laufen lassen, nie direkt aus dem Browser.
- Rate Limiting pro Nutzer einbauen.
- Beim Anbieter ein Ausgabenlimit und Budget-Warnungen einstellen.

SO FRAGST DU DEINE KI

«Baue Rate Limiting für alle Routen ein, die kostenpflichtige APIs aufrufen, z. B. maximal 20 Anfragen pro Nutzer und Stunde.»

07 Vorsicht bei Paketen

WARUM

KI-Tools schlagen manchmal Pakete vor, die es gar nicht gibt. Angreifer registrieren solche Namen mit Schadcode.

SO GEHST DU VOR

- Vor der Installation prüfen: Gibt es das Paket auf npmjs.com, wird es gepflegt und viel genutzt?
- Pakete regelmässig aktualisieren und npm audit laufen lassen.

SO FRAGST DU DEINE KI

«Liste alle installierten Pakete auf. Markiere unbekannte, veraltete oder ungenutzte Pakete.»

08 KI-Funktionen in deiner App absichern

WARUM

Nutzer können versuchen, deine KI mit geschickten Texten zu manipulieren (Prompt Injection).

SO GEHST DU VOR

- Der KI nie mehr Rechte geben als dem Nutzer selbst.
- Keine Geheimnisse in den System-Prompt schreiben.
- Kritische Aktionen der KI (löschen, senden, bezahlen) bestätigen lassen.

SO FRAGST DU DEINE KI

«Prüfe die KI-Funktionen auf Prompt Injection. Welche Aktionen kann die KI auslösen, und sind sie auf die Rechte des Nutzers begrenzt?»

09 Backups und getrennte Umgebungen

WARUM

Ein falscher Befehl der KI kann Daten löschen.

SO GEHST DU VOR

- Automatische Backups der Datenbank aktivieren und die Wiederherstellung einmal testen.
- Änderungen zuerst in einer Testumgebung ausprobieren, nicht direkt in der Live-App.

SO FRAGST DU DEINE KI

«Richte eine getrennte Entwicklungs- und Produktionsdatenbank ein und erkläre mir, wie ich Backups wiederherstelle.»

10 Lass prüfen, bevor echte Kunden kommen

WARUM

Die KI findet viele, aber nicht alle Probleme.

SO GEHST DU VOR

- Die KI regelmässig um ein Security-Review bitten.
- Vor dem Launch mit echten Kundendaten eine erfahrene Person drüberschauen lassen.

SO FRAGST DU DEINE KI

«Mach ein Security-Review meines Projekts nach den OWASP Top 10. Liste die Probleme nach Dringlichkeit und schlage konkrete Korrekturen vor.»

SCHNELLCHECK VOR DEM LAUNCH

- ☐ Keine API-Schlüssel im Code, im Frontend oder im Git-Verlauf
- ☐ Datenbank-Regeln (RLS oder Security Rules) für alle Tabellen aktiv
- ☐ Mit zweitem Konto getestet: keine fremden Daten sichtbar
- ☐ Login über bewährten Anbieter, 2FA für Admin-Konto aktiv
- ☐ Eingaben werden auf dem Server geprüft
- ☐ Rate Limiting und Ausgabenlimit für KI- und Zahlungs-APIs
- ☐ Alle Pakete bekannt und aktuell
- ☐ Backups aktiv und Wiederherstellung getestet
- ☐ Datenschutzerklärung und Impressum vorhanden
- ☐ Security-Review durch KI und durch einen Menschen gemacht

Dieser Guide vermittelt Grundlagen und ersetzt keine professionelle Sicherheitsprüfung, besonders nicht bei Apps mit sensiblen Daten oder Zahlungen.

Fragen oder Unterstützung nötig?

Ich helfe kleinen Unternehmen und Gründern bei sicheren KI-Tools und Automatisierungen. Das Erstgespräch ist kostenlos.

www.switech-solution.com/de/