



LAUNCH
GATE

KI-APP AN KUNDEN?

7 Checks, bevor dein Vibe-Code echten Schaden macht

Wenn die App nur bei dir läuft, ist sie noch kein Produkt. Erst prüfen, dann ausliefern.

01

Secrets raus aus dem Code

API-Keys, Tokens und Passwörter gehören nicht in GitHub, Frontend oder Screenshots. Nutze

Tools: [GitHub Secret Scanning](#), [Doppler](#), [1Password](#), [Infisical](#).

Prüfsatz: Prüfe mein Projekt auf hartcodierte Secrets und zeige mir Datei, Risiko und sicheren Ersatz.

02

Rechte pro Nutzer prüfen

Jeder Kunde darf nur seine eigenen Daten sehen. Versteckte Buttons sind keine Sicherheit;

Tools: [Supabase RLS](#), [Auth0](#), [Clerk](#), [Firebase Rules](#).

Prüfsatz: Prüfe alle Datenbankzugriffe: Kann Nutzer A Daten von Nutzer B lesen oder ändern?

03

Lasttest vor Kunden-Launch

Wenn 50 Leute gleichzeitig klicken, darf deine App nicht hängen. Teste

Tools: [k6](#), [Grafana Cloud](#), [Loader.io](#).

Prüfsatz: Erstelle mir einen einfachen Lasttest für Login, Dashboard und wichtigste Kundenaktion.

04

API-Limits und Kostenbremse

Ohne Limits kann ein Bug oder Bot deine OpenAI-, Stripe- oder Datenbankkosten sprengen.

Tools: [Upstash Rate Limit](#), [Cloudflare](#), [API Gateway](#).

Prüfsatz: Finde alle teuren API-Aufrufe und schlage Rate Limits, Quotas und Fehlermeldungen vor.

05

Eingaben hart validieren

Formulare, Uploads und Freitext nicht blind weitergeben. Prüfe Länge, Dateityp,

Tools: [Zod](#), [Valibot](#), [Yup](#), [file-type](#).

Prüfsatz: Prüfe alle Eingaben und Uploads auf fehlende Validierung und baue sichere Regeln ein.

06

Logs und Fehleralarme einschalten

Wenn der Kunde sagt „es geht nicht“, brauchst du Fehler, Latenz, Login-Versuche und Kosten

Tools: [Sentry](#), [PostHog](#), [Logtail](#), [Datadog](#).

Prüfsatz: Wo fehlen Logs, Error Tracking und Alerts? Gib mir eine minimale Monitoring-Liste.

07

Backup und Rollback vorbereiten

Vor dem Launch muss klar sein: Wie sicherst du Daten? Wie gehst du auf die letzte

Tools: [Supabase Backups](#), [Neon Branching](#), [Vercel Rollback](#), [Git Tags](#).

Prüfsatz: Schreibe mir einen Backup- und Rollback-Plan für diese App vor Kunden-Launch.

Mini-Regel: Vibe Coding ist nicht das Problem. Blindes Ausliefern ist das Problem.

Basis: OWASP API Security / Proactive Controls + GitHub Code Scanning / Actions Security Hardening.