8 kroků bezpečného vibe codingu

Tento checklist použijte jako základní návod při práci s vibe codingem. Projdete s ním krok za krokem od startu projektu až po finální release.

1. Pravidla a hranice použití

- Schválit nástroje a určit, kde je vibe coding povolen
- Vypsat zakázané zóny vyžadující dohled seniora (identity, kryptografie, platby, ...)
- Dohledatelnost: kdo zadal / kdo schválil + neobcházet automatické kontroly

2. Secure starter + šablony

- Vytvořit secure starter (přihlášení/role, session, logování, chyby, základní ochrany)
- Připravit promptové šablony pro typické situace (API, databáze, integrace)
- Vždy vyžadovat: validaci vstupů, oprávnění, chování při chybách, logování

3. Secrets a citlivá data

- Zakázat klíče/hesla/tokeny v promtech i repozitáři
- Citlivá data držet mimo kód (v nastavení systému/prostředí, bezpečného úložiště)
- Do AI neposílat citlivé kontexty (konfigurace, logy, výpisy, zákaznická data)
- Postup při kompromitaci: rotace/ zneplatnění + ověření dopadů

4. Malé dávky změn

- Dělejte malé změny: upravujte jednu část aplikace v jednom balíku
- Ke každé změně mějte jasný cíl a ověření

5. Vstupy a oprávnění

- Validace vstupů na serveru
- Autorizace pro konkrétní objekt (nejen „přihlášený“)
- Chyby nic neprozrazují

6. Knihovny a balíčky

- Schvalování nových závislostí (z pohledu údržby, správce, reputace)
- Zamykání verzí
- Kontrola zranitelností závislostí

7. Povinné automatické kontroly

- Minimálně: testy, statická analýza kódu, kontrola závislostí, kontrola vložených klíčů/hesel
- Co neprojde, nepustit dál (bez výjimek)

8. Merge a release pod kontrolou

- Merge až po review + automatických kontrolách
- Release přes staging + jasné go/no-go
- Rollback / rychlé vypnutí připravené
- Kontrola po releasu: nárůst chyb, podezřelé požadavky, neobvyklé přístupy