

POKP - Ponas Obuolys kodo patikra: detali analizė

ponasObuolys/demo-projektas

Skenuota: 2026 m. liepos 8 d.

74/100

Kategorijų įvertinimai

Saugumas (40 % svorio)	68/100
Kodo kokybė (20 % svorio)	78/100
Struktūra (15 % svorio)	82/100
Dokumentacija (10 % svorio)	76/100
AI parengtis (15 % svorio)	72/100

Santrauka

Detali analizė pagilina pirminius radinius pagal realų kodą, prideda priklausomybių pažeidžiamumų sąrašą ir repo saugumo praktikų įvertinimą. Žemiau - prioritetinis planas ir konkretūs žingsniai.

Veiksmų planas (rekomenduojama tvarka)

- Atnaujink pažeidžiamas priklausomybes iki saugių versijų.
- Pridėk klaidų valdymą į išorinius API kvietimus.
- Papildyk README skiltimi apie aplinkos kintamuosius.

Ką pataisysi greitai (kelios minutės darbo)

- Paleisk paketų atnaujinimą pažeidžiamiems paketams.
- Pridėk .env.example failą su reikalingų kintamųjų sąrašu.

Detalūs radiniai (2)

Saugumas

1. [AUKŠTA] Pasenusi HTTP kliento priklausomybė su žinoma spraga

Failas: package-lock.json · Pastangos: mažos pastangos

Naudojama axios versija turi žinomą pažeidžiamumą, kuris tam tikromis sąlygomis leidžia apeiti apsaugą. Atnaujinimas pašalina riziką.

Įrodymai kode:

"axios": "1.6.0" (package-lock.json)

Taisymo žingsniai:

1. Atnaujink axios iki 1.7.4 ar naujesnės versijos.
2. Perleisk testus ir patikrink, ar niekas nesulūžo.

Kaip turėtų atrodyti:

npm install axios@^1.7.4

Užduotis AI įrankiui (įklijuok į Claude Code / Cursor):

Atnaujink axios priklausomybę iki saugios 1.7.4+ versijos, perleisk testus ir patikrink API kvietimus.

Kodo kokybė

1. [VIDUTINĖ] Trūksta klaidų valdymo išoriniams kvietimams

Failas: src/services/api.ts · Pastangos: vidutinės pastangos

Funkcija, kviečianti išorinį API, neturi try/catch, todėl tinklo klaida nutildoma be jokio pranešimo naudotojui ar žurnalo įrašo.

Įrodymai kode:

```
const data = await fetch(url).then(r => r.json()) // be klaidų valdymo
```

Taisymo žingsniai:

1. Apgaubk kvietimą try/catch bloku.
2. Klaidos atveju užlogink ją ir grąžink aiškų rezultatą.

Užduotis AI įrankiui (įklijuok į Claude Code / Cursor):

Pridėk try/catch į išorinį API kvietimą src/services/api.ts, užlogink klaidą ir grąžink aišką fallback rezultatą.

Priklausomybių pažeidžiamumai

Šaltinis: OSV.dev (Google atviro kodo pažeidžiamumų bazė).

Patikrinta priklausomybių: 214. Pažeidžiamų paketų: 2.

axios@1.6.0 (npm)

- GHSA-8hc4-vh64-cxmj [aukšta]: Serverio pusės užklausų klastojimo (SSRF) rizika tam tikrose konfigūracijose. (pataisyta versijoje 1.7.4)

tar-fs@2.1.1 (npm)

- GHSA-pq67-2wwv-3xjx [vidutinė]: Kelio apėjimo (path traversal) rizika išskleidžiant archyvus. (pataisyta versijoje 2.1.2)

Kaip atnaujinti saugiai:

1. Atnaujink pažeidžiamus paketus iki saugių versijų:
 - npm install axios@1.7.4
 - npm install tar-fs@2.1.2
2. Po atnaujinimo paleisk testus ir įsitikink, kad projektas veikia kaip anksčiau.
3. Jei iškart atnaujinti negali, suplanuok atnaujinimą ir kol kas apribok pažeidžiamo funkcionalumo naudojimą.

Užduotis AI įrankiui (įklijuok į Claude Code / Cursor):

Atnaujink šias pažeidžiamas priklausomybes iki saugių versijų: axios iki 1.7.4 (npm), tar-fs iki 2.1.2 (npm). Po atnaujinimo paleisk testus ir build, įsitikink, kad niekas nenustojo veikti.

Repo saugumo praktikos (OpenSSF Scorecard)

OpenSSF Scorecard įvertinimas: 6,4/10 (informacinis rodiklis, į POKP balą neįskaičiuojamas).

- Branch-Protection: 8/10
- Vulnerabilities: 4/10 - patarimas: sutvarkyk žinomus pažeidžiamumus (žr. priklausomybių skyrių)

- Maintained: 10/10
- Code-Review: 5/10

Kas jau gerai

- Nuoseklus kodo formatavimas
- Aiškūs funkcijų pavadinimai

Jau pataisei, ką radau? Paleisk naują patikrą – pakartotinė šios repozitorijos analizė kainuoja 50 % pigiau.

Kad šios klaidos nesikartotų

Dauguma šioje analizėje rastų problemų atsiranda, kai AI įrankiai dirba be taisyklių ir patikrų. „Ponas Obuolys Workflow“ – Claude Code ir Codex darbo sistema su apsaugos agentais, automatinėmis patikromis ir gyvu projekto žinių sluoksniu, kuri neleidžia AI apsimesti, kad darbas atliktas.

ponasobuolys.lt/irankiai/ponas-obuolys-workflow

Viešas rezultato puslapis: ponasobuolys.lt/irankiai/kodo-patikra/r/pavyzdys