Informatikos brandos darbas

Saugumo ir kodo kokybės balansavimas programavimo praktikose ***(VIEŠOJO NAUDOJIMO VERSIJA)***

[full name], [class]
[institution]

Tyrimo tikslas ir problema

Tikslas:

Nustatyti ir įgyvendinti programavimo praktiką, kuri veiksmingai suderina saugumo Ir kodo kokybės aspektus, užtikrinant patvaraus ir patikimo kodo kūrimą.

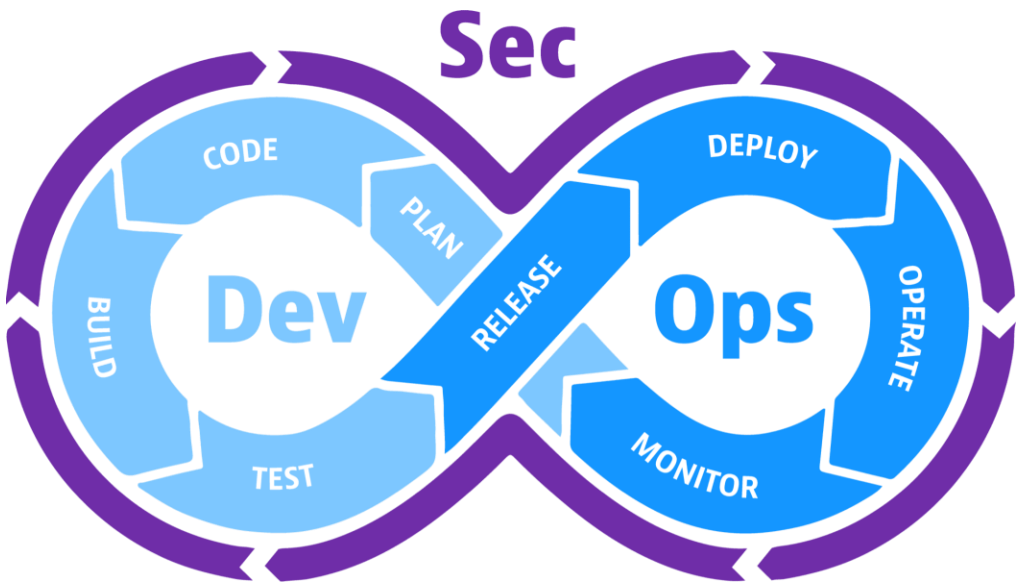
Problema:

Saugumo priemonės neretai apsunkina kodo struktūrą, pablogina įskaitomumą ir priežiūrą. *Kaip pasiekti balansą moderniame kodo kūrimo procese?*

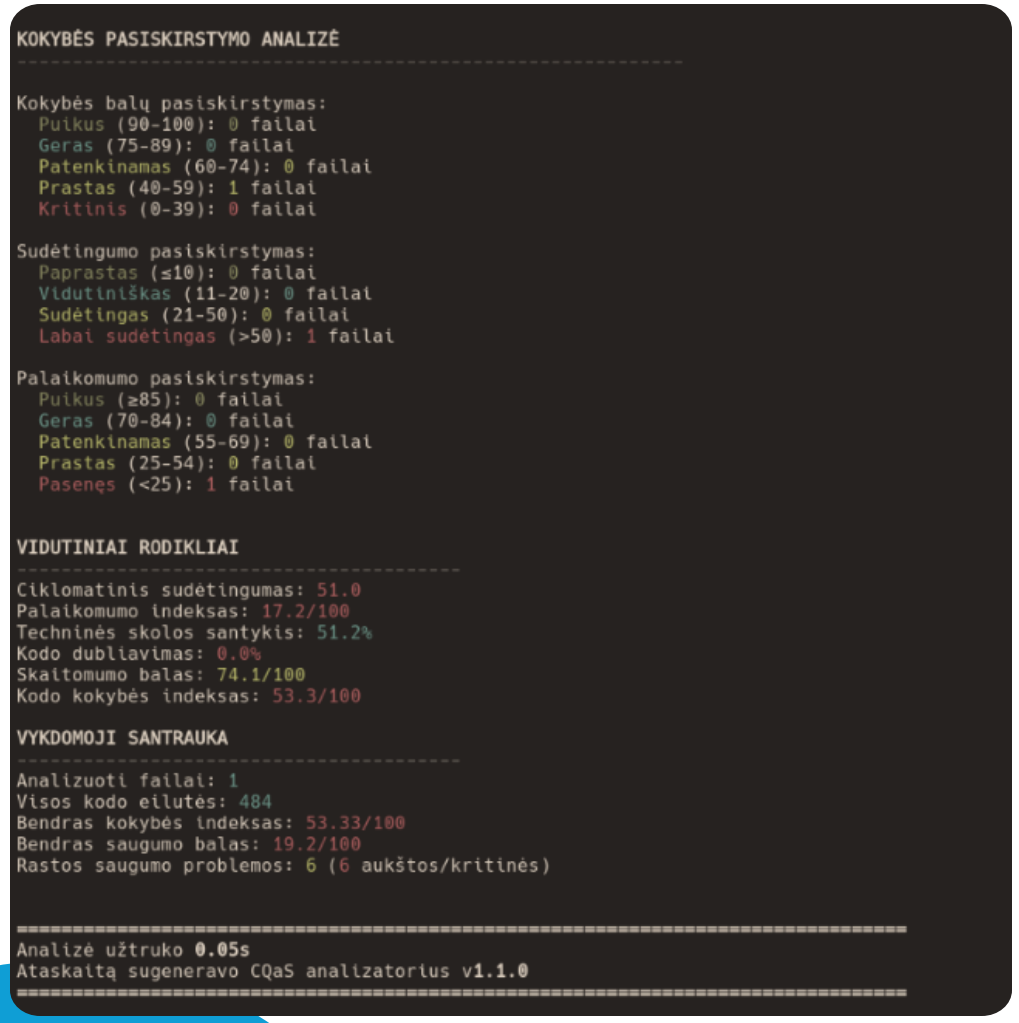
Esminiai principai

1. **Simbiozė:** derinti kalibruotą automatizuotą analizę su koncentruota žmogaus peržiūra
2. **Matavimas:** stebėti kelis rodiklius, o ne vieną
3. **Sisteminimas:** sistemiškai, greitai, patikimai ir tvarkingai atlikti tyrimu
4. **Struktūra:** skatinti kodo išskaidymą į modulius, mažinti nuovargį skaitant ir prižiūrint kodą

Teorija



Buvo išanalizuoti kodo kokybės ir saugumo (*DevSecOps*) principai



Kodo analizės įrankis *CQaS*

- Įrankis sukurtas Python kalba, integruojant teorines žinias
- Naudojamas prižiūrint kodo sudėtingumą, įskaitomumą, oficialaus stiliaus gido atitikimą (*PEP8*), techninę skolą, dubliavimą
- Palaiko lietuvių ir anglų kalbas
- 2.0 versijoje pridėtas peržiūros režimas

Eksperimento tipas:

iteracinė daugiavariatinė analizė

Tipas	Versijos	Vykdytojai	Pagrindiniai akcentai

Eksperimento tipas:

iteracinė daugiavariatinė analizė

Tipas	Versijos	Vykdytojai	Pagrindiniai akcentai
Bazinis kodas	1.0	Žmogus	Pirminė nesaugi, nekokybiška versija

Eksperimento tipas:

iteracinė daugiavariatinė analizė

Tipas	Versijos	Vykdytojai	Pagrindiniai akcentai
Bazinis kodas	1.0	Žmogus	Pirminė nesaugi, nekokybiška versija
Tobulinimas	2.1, 2.2	Žmogus vs DI	Kodo išskaidymas, kodo kokybės atitikimas, savarankiškumas

Eksperimento tipas:

iteracinė daugiavariatinė analizė

Tipas	Versijos	Vykdytojai	Pagrindiniai akcentai
Bazinis kodas	1.0	Žmogus	Pirminė nesaugi, nekokybiška versija
Tobulinimas	2.1, 2.2	Žmogus vs DI	Kodo išskaidymas, kodo kokybės atitikimas, savarankiškumas
Kontroliniai sąrašai	3.1, 3.2, 3.3, 3.4	Žmogus (2) / DI (2)	Saugumo gairių taikymas

Eksperimento tipas:

iteracinė daugiavariatinė analizė

Tipas	Versijos	Vykdytojai	Pagrindiniai akcentai
Bazinis kodas	1.0	Žmogus	Pirminė nesaugi, nekokybiška versija
Tobulinimas	2.1, 2.2	Žmogus vs DI	Kodo išskaidymas, kodo kokybės atitikimas, savarankiškumas
Kontroliniai sąrašai	3.1, 3.2, 3.3, 3.4	Žmogus (2) / DI (2)	Saugumo gairių taikymas
Automatinė kodo analizė	4.1, 4.2	Žmogus (2)	Statinės ir dinaminės kodo analizės pritaikymas

Eksperimento tipas:

iteracinė daugiavariatinė analizė

Tipas	Versijos	Vykdytojai	Pagrindiniai akcentai
Bazinis kodas	1.0	Žmogus	Pirminė nesaugi, nekokybiška versija
Tobulinimas	2.1, 2.2	Žmogus vs DI	Kodo išskaidymas, kodo kokybės atitikimas, savarankiškumas
Kontroliniai sąrašai	3.1, 3.2, 3.3, 3.4	Žmogus (2) / DI (2)	Saugumo gairių taikymas
Automatinė kodo analizė	4.1, 4.2	Žmogus (2)	Statinės ir dinaminės kodo analizės pritaikymas
Kodo peržiūra	5.1, 5.2	Žmogus vs DI	Taikoma kodo peržiūra ir taisymas

Eksperimento tipas:

iteracinė daugiavariatinė analizė

Tipas	Versijos	Vykdytojai	Pagrindiniai akcentai
Bazinis kodas	1.0	Žmogus	Pirminė nesaugi, nekokybiška versija
Tobulinimas	2.1, 2.2	Žmogus vs DI	Kodo išskaidymas, kodo kokybės atitikimas, savarankiškumas
Kontroliniai sąrašai	3.1, 3.2, 3.3, 3.4	Žmogus (2) / DI (2)	Saugumo gairių taikymas
Automatinė kodo analizė	4.1, 4.2	Žmogus (2)	Statinės ir dinaminės kodo analizės pritaikymas
Kodo peržiūra	5.1, 5.2	Žmogus vs DI	Taikoma kodo peržiūra ir taisymas
Sistemos dokumentacija	6.0	DI	Pridedami dokumentacija ir komentarai

DI (*Vibe Coding*) poveikis

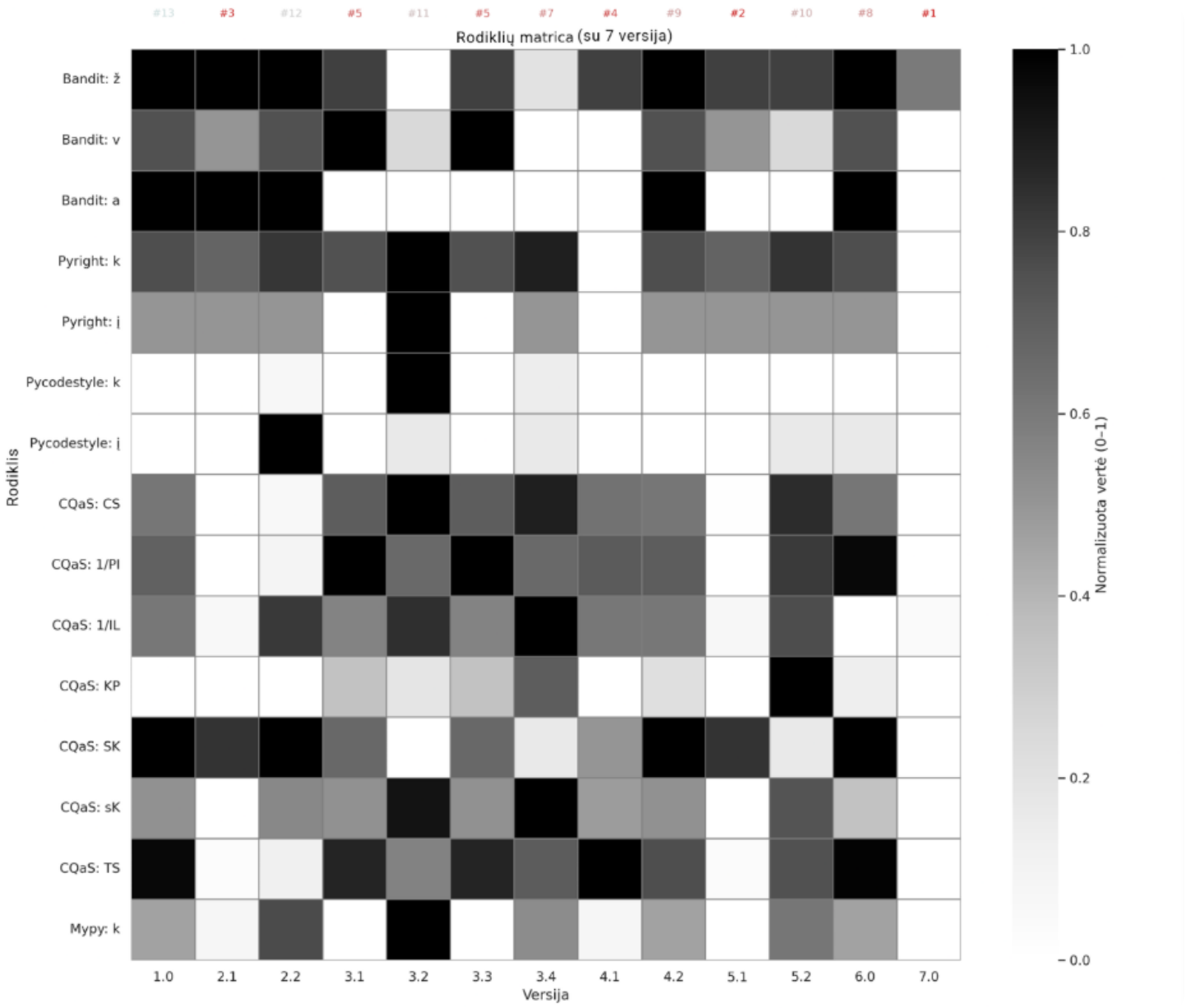
DKM (*ChatGPT-5.2-Thinking*) taikymas dažniausiai pablogino saugumą ir kokybę:

- Nesugeba įvertinti pilno kodo konteksto
- Padaro kodą fragmentuotą ir netvarkingą
- Reikalauja itin kruopščios žmogaus priežiūros

Išvada: DI įrankiai kol kas negali pakeisti sistemingos žmogaus peržiūros

Rezultatų vertinimas (I)

- Duomenys buvo normalizuoti pagal *min-max* metodą
- Pasirinktas triskaitis vidurkis (*angl. Trimean*) dėl stabilumo ir konteksto tolerancijos
- Normalizuoti rezultatai rikiuojami pagal optimalumą rezultatų matricoje (II)



Rezultatų vertinimas (II)

Galutinis rezultatas

1 vieta

Sudarytos praktikos ir *CQaS* įrankio pritaikymas:

- Saugumo klaidos sumažėjo **73%**
- Techninė skola sumažėjo **92%**
- **Visiškas** duomenų tipų užtikrinimas

Patobulėjimas: 79,22%

Rekomendacijos

- **Išskaidymas:** skaidyti kodą į nepriklausomus modulius – tai pamatas kokybei
- **Sąrašai:** naudoti kontrolinius sąrašus kritiniams taškams tikrinti ir skatinti sistemingas kodo peržiūras
- **Peržiūra:** taikyti sistemingas žmogaus vadovaujamas kodo peržiūras
- **DI vengimas:** vengti aklai pasikliauti DI rezultatais
- **SPST:** pasitelkti statinės kodo analizės priemones (*CQaS, Bandit,* ...)

Darbo tikslas pasiektas

- Nustatyta veiksminga praktika, suderinanti saugumą ir kokybę
- Sukurtas įrankis jos automatiniam palaikymui

Dėkoju

- [institution] [profession],
  brandos darbo **vadovui (-ei) [full name].**

- [institution] [profession],
  brandos darbo **konsultantui (-ei) [full name]**.

Jūsų klausimai