Set, 2019

huskyCI

Encontrando vulnerabilidades de código na Globo.com antes do deploy

Rafael dos Santos 🇧🇷 @rafasantos5

$ whoami

Rafael dos Santos 🇧🇷 @rafasantos5

github.com/rafaveira3

⚽ Volante Clássico (Camisa 5)

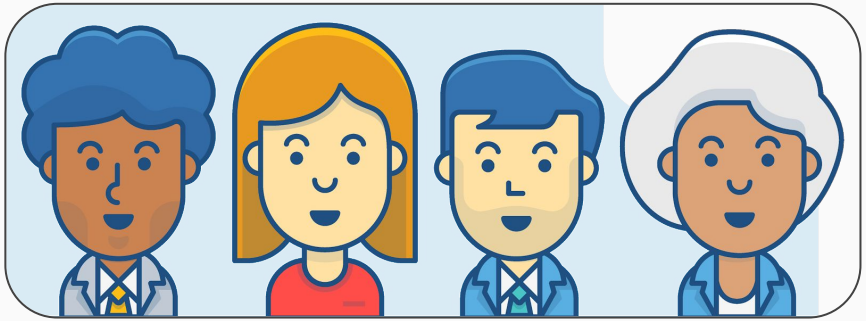
☕ OSCP + OSCE

🐼 Analista de Segurança @ globo.com

🚀 Sec Tools + Desenvolvimento de Exploit

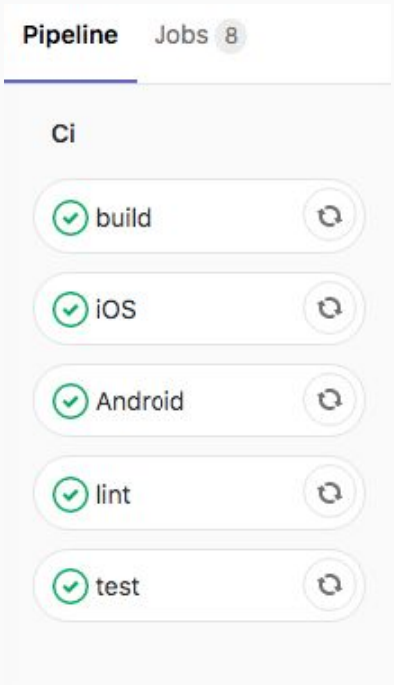
Um dia na vida de um time de desenvolvimento...

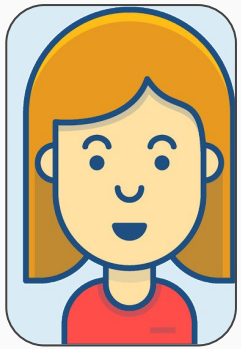
Um dia na vida de um time de desenvolvimento...



Um dia na vida de um time de desenvolvimento...

Nova feature!

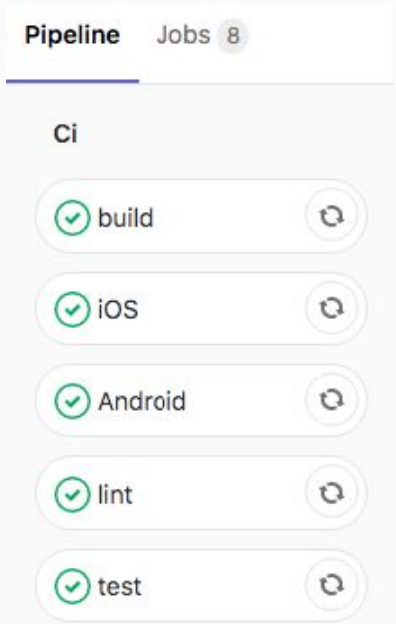




"Parece bom!"

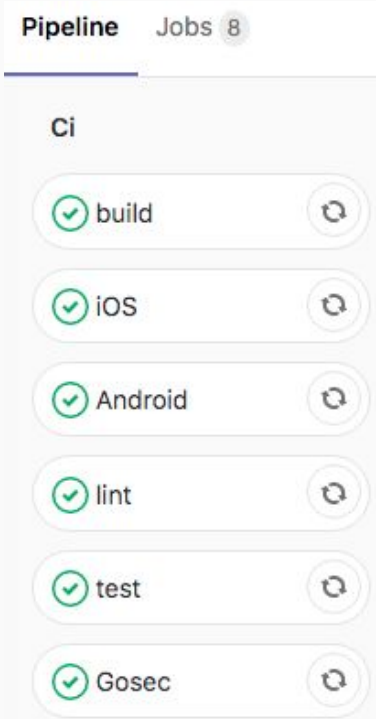
Um dia na vida de um time de desenvolvimento...

Nova feature!

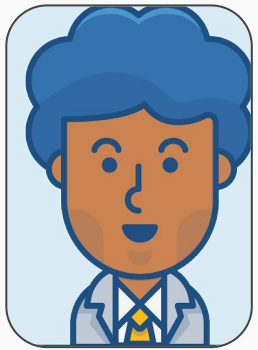


Time de Segurança

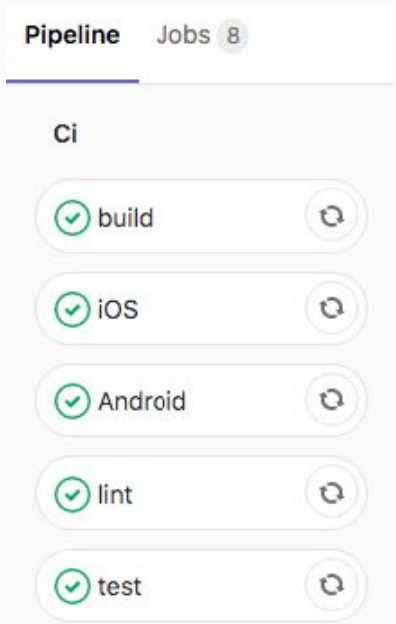
"Opa, o que acham de usar o **Gosec**?"



Um dia na vida de um time de desenvolvimento...

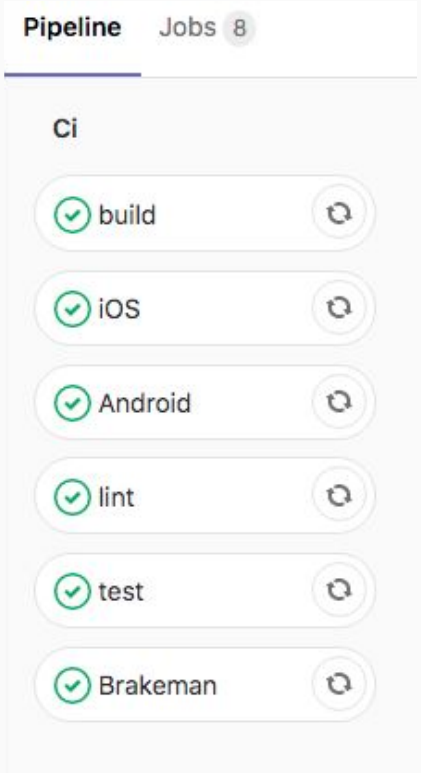


Nova feature!

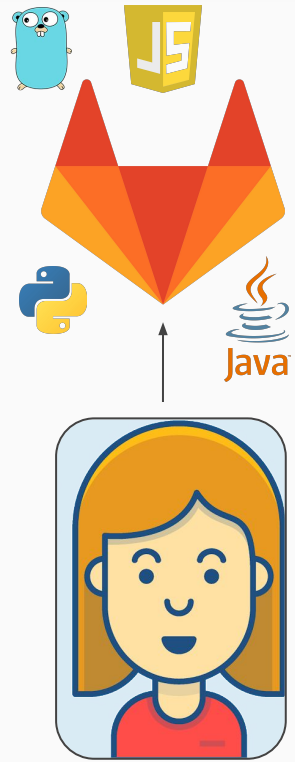


Time de Segurança

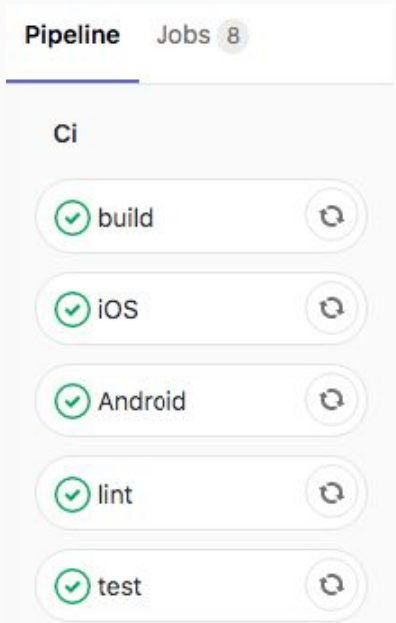
"Opa, o que acham de usar o **Brakeman**?"



Um dia na vida de um time de desenvolvimento...

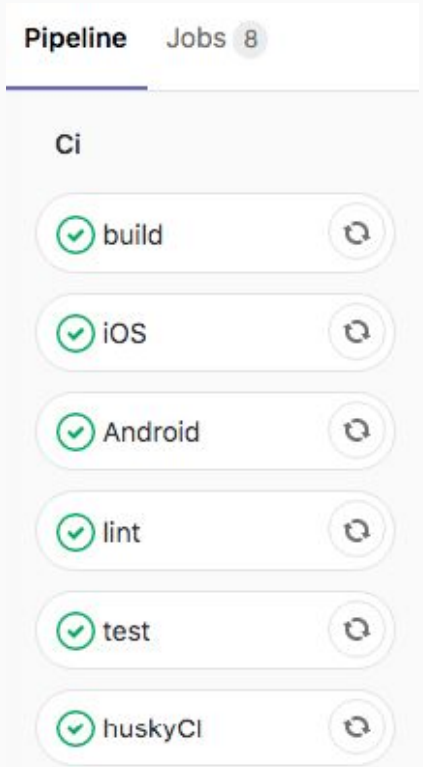


Nova feature!



Time de Segurança

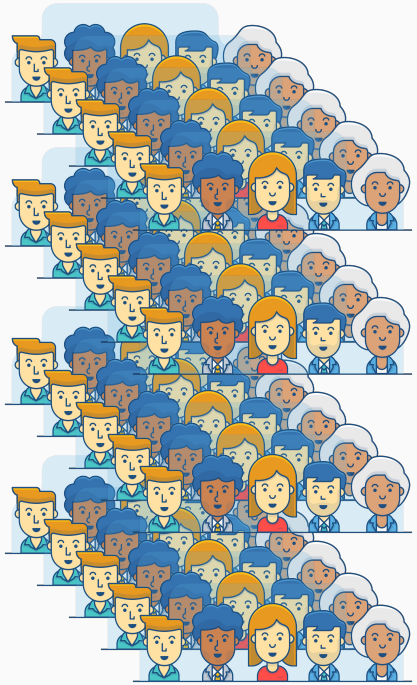
"Opa, o que acham de usar o ... ?"

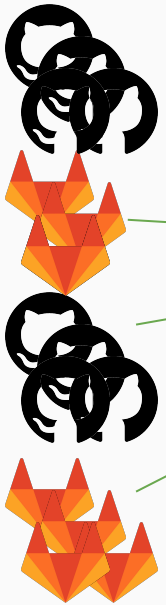


Um dia na vida de uma grande organização...

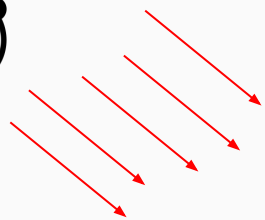
Um dia na vida de uma grande organização...

Times de Desenvolvimento





Time de Segurança



tsuru


THIS IS FINE
GOPHER

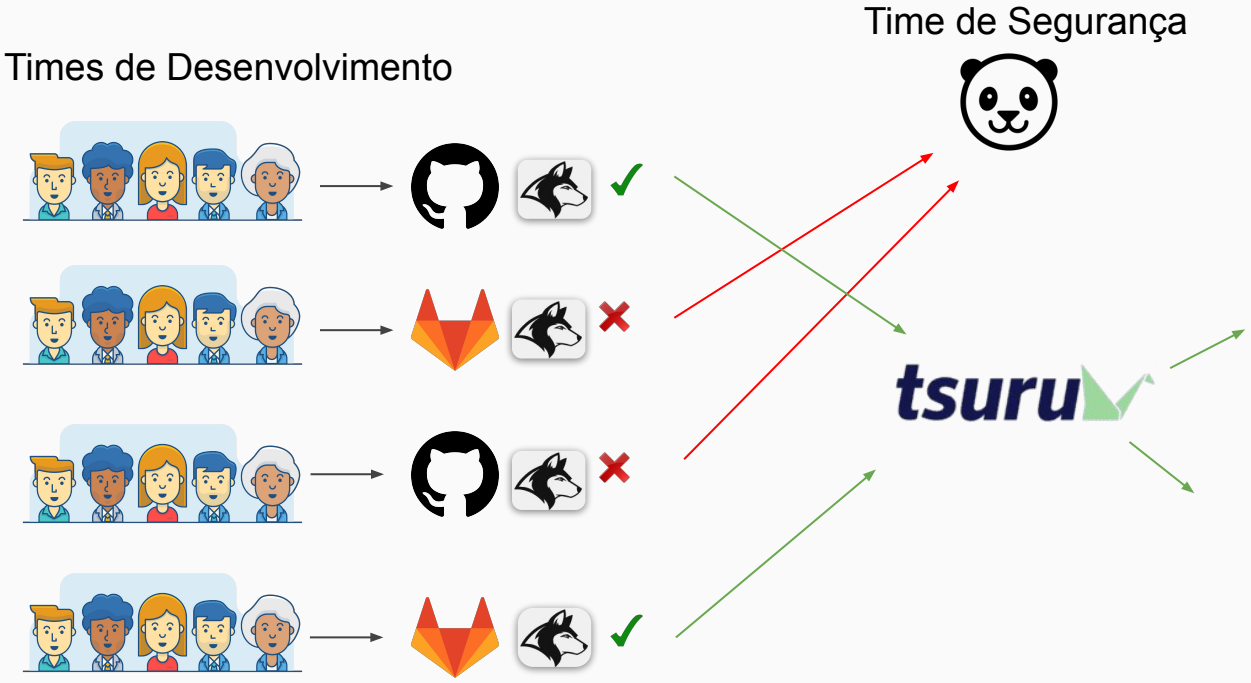
Let's hack! 🐼

Let's hack!

Let's hack!

Times de Desenvolvimento

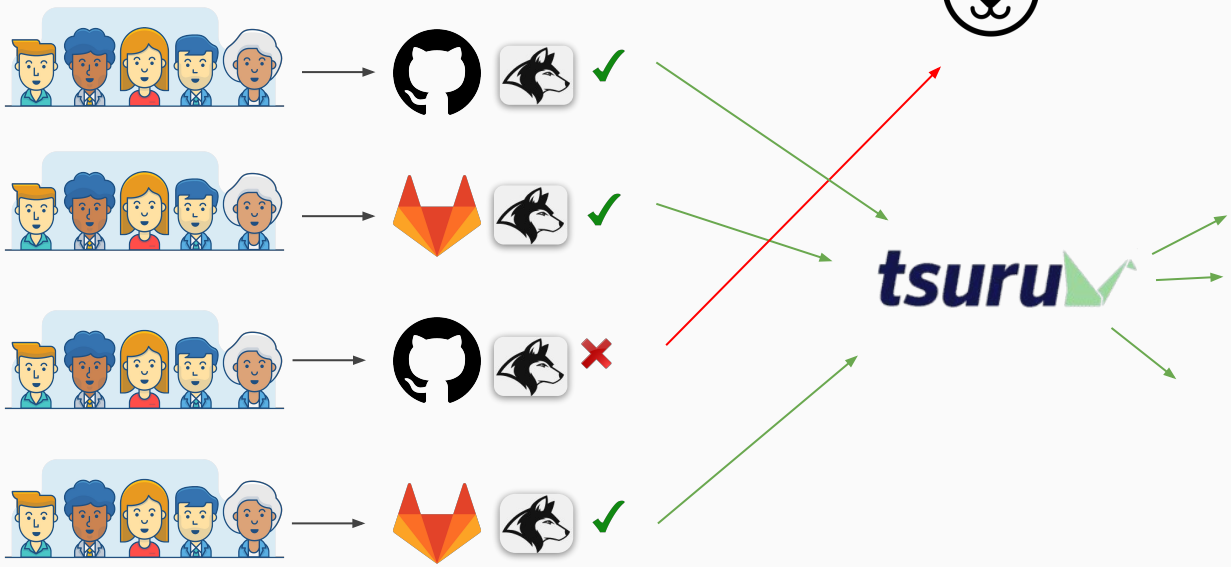
Time de Segurança



Let's hack!

Times de Desenvolvimento

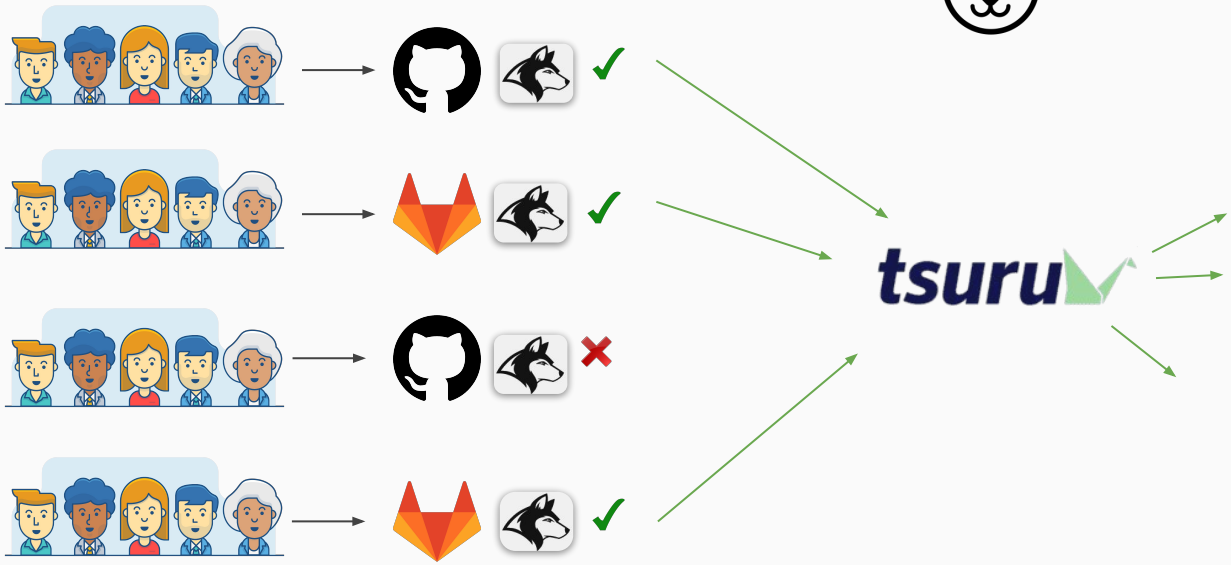
Time de Segurança



Let's hack!

Times de Desenvolvimento

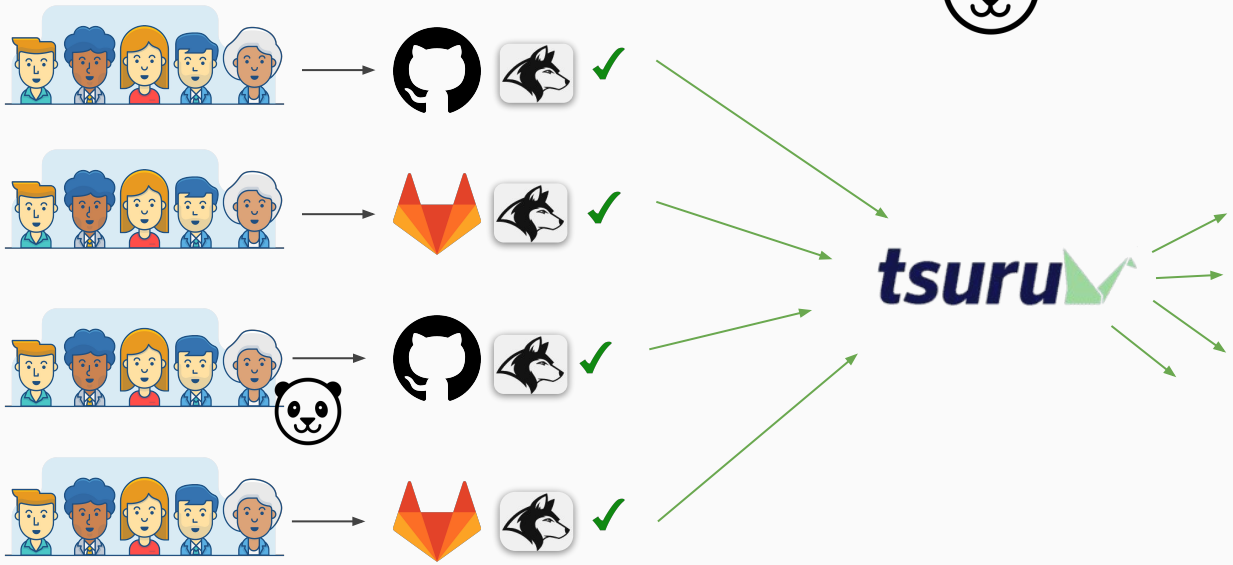
Time de Segurança



Let's hack!

Times de Desenvolvimento

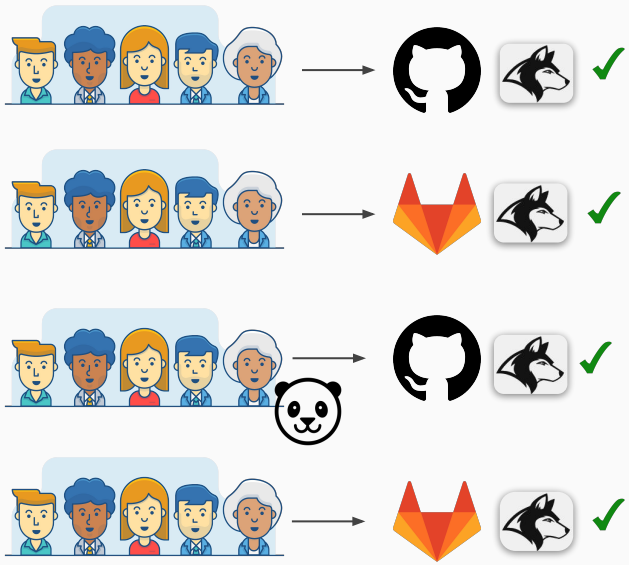
Time de Segurança



Let's hack!

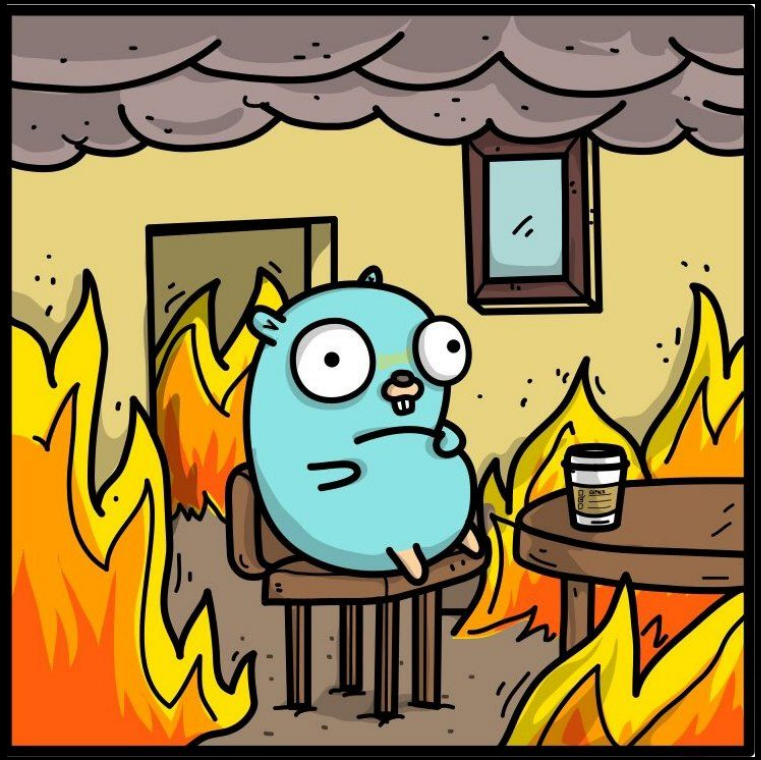
Times de Desenvolvimento

Time de Segurança



Beleza, mas quais linguagens usamos? ☕

Beleza, mas quais linguagens usamos?



Beleza, mas quais linguagens usamos?

gosec

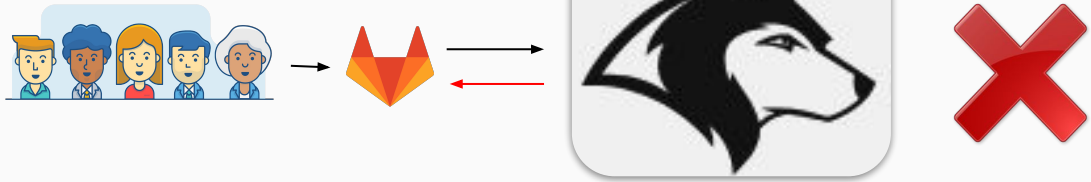
Bandit

Brakeman

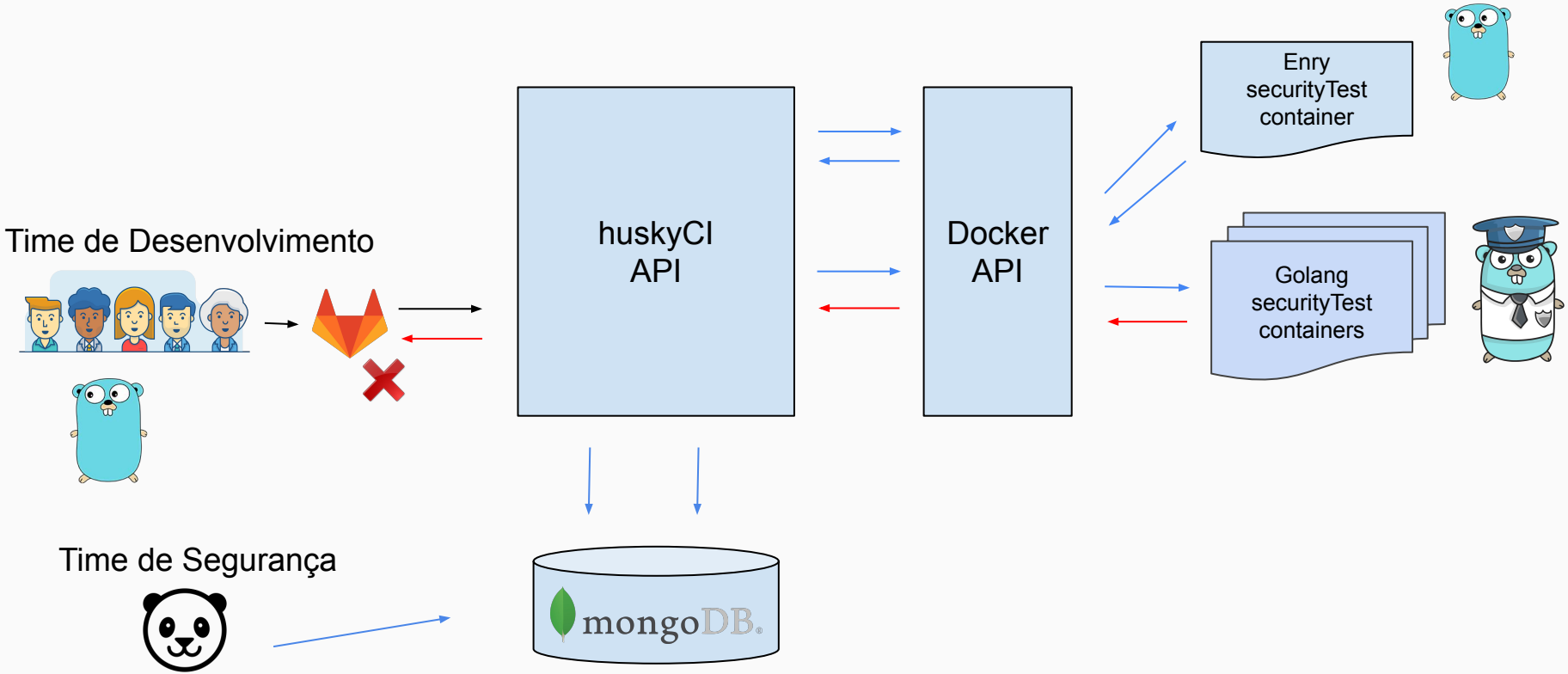
Como queremos construir esta ferramenta? 🛠️

Como queremos construir esta ferramenta?

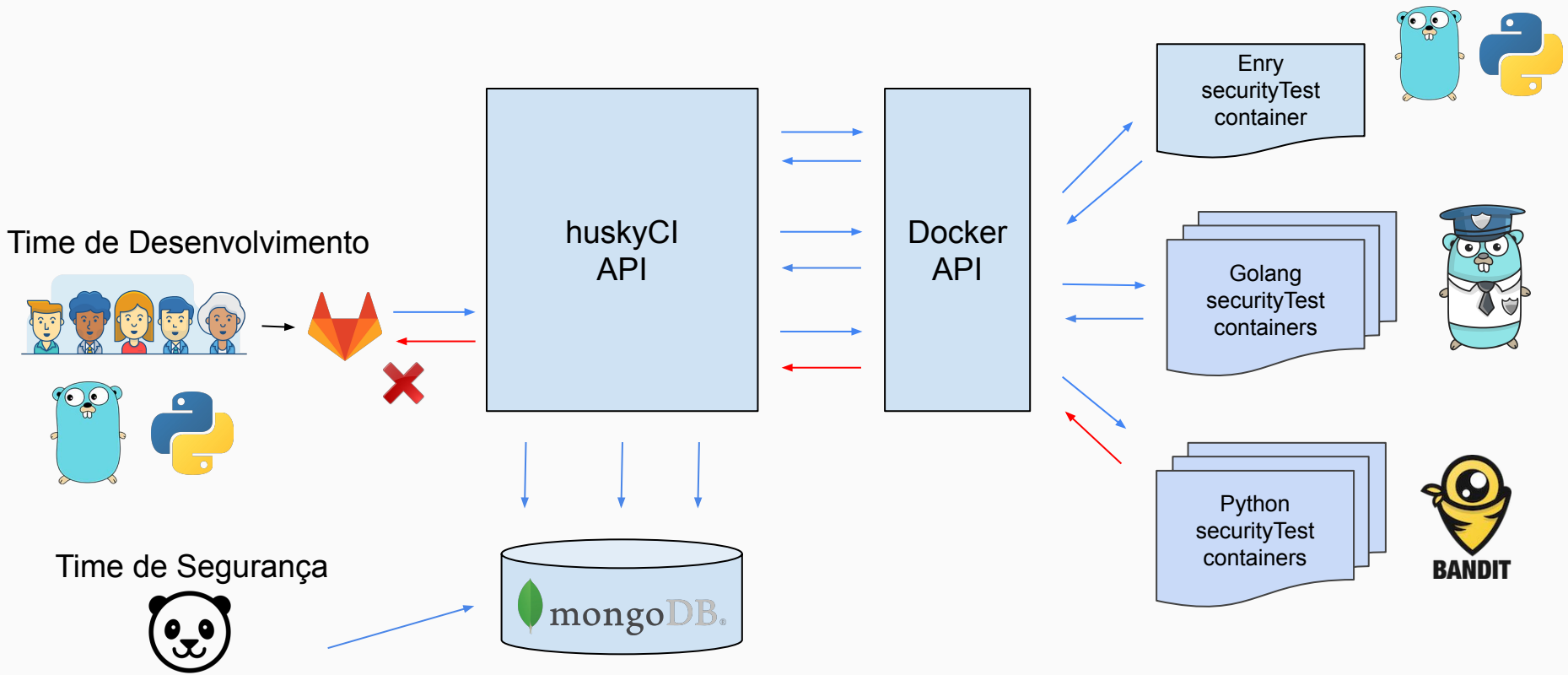
Time de Desenvolvimento



Como queremos construir esta ferramenta?



Como queremos construir esta ferramenta?

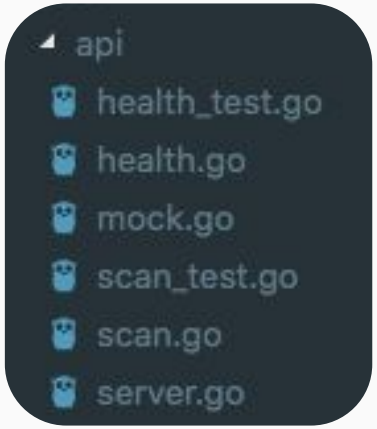


E o que gostaríamos de ver? 👀

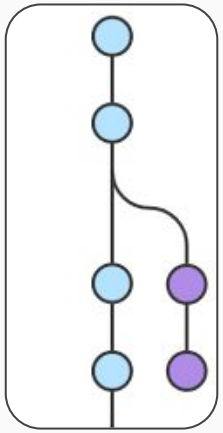
E o que gostaríamos de ver?

Autores de commit

Linguagem do repositório



Arquivos encontrados

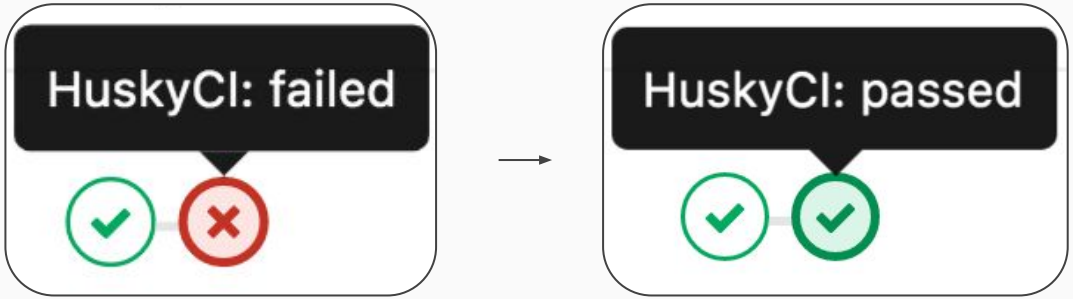


Nome da Branch

E o que gostaríamos de ver?

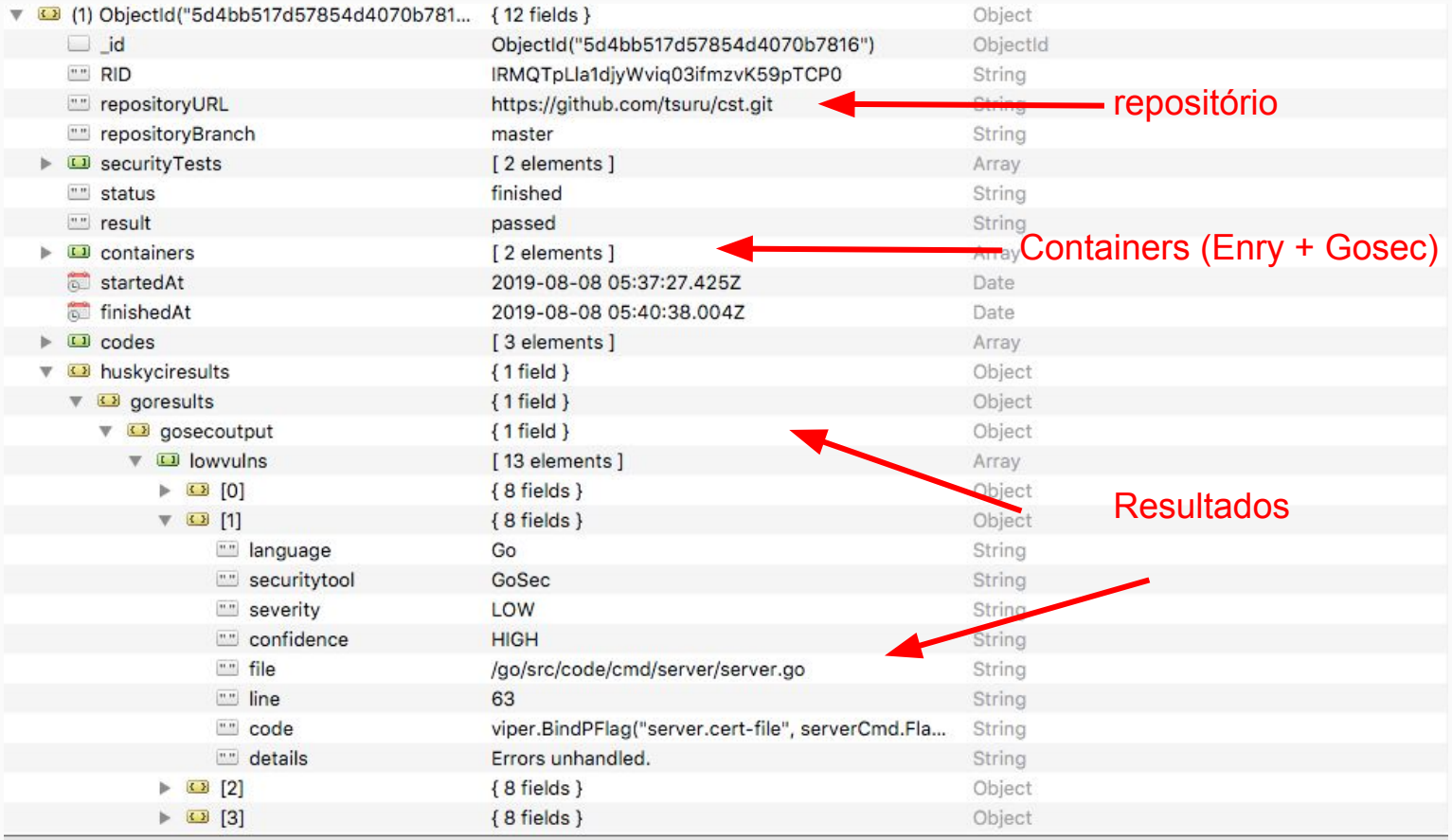
```
[HUSKYCI][!] Severity: MEDIUM
[HUSKYCI][!] Confidence: HIGH
[HUSKYCI][!] Details: Blacklisted import crypto/sha1: weak cryptographic primitive
[HUSKYCI][!] File: /go/src/code/api/token.go
[HUSKYCI][!] Line: %!d(string=6)
[HUSKYCI][!] Code: "crypto/sha1"
```

Vulnerabilidades
Encontradas



Mitigação feita

E o que gostaríamos de ver?



DEV, foque no desenvolvimento ❤️

Foque no desenvolvimento

.gitlabci.yml

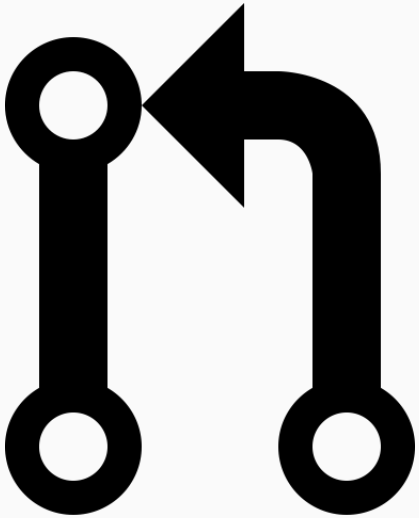
```
stages:
  - HuskyCI

test-huskyci:
  stage: HuskyCI
  script:
    - wget urlto.huskyci.com/huskyci-client
    - chmod +x huskyci-client
    - ./huskyci-client
```

Demo 🔥

Resultados Globo.com (até agora) 🚀

Resultados Globo.com (até agora)



projetos globo.com
com huskyCI

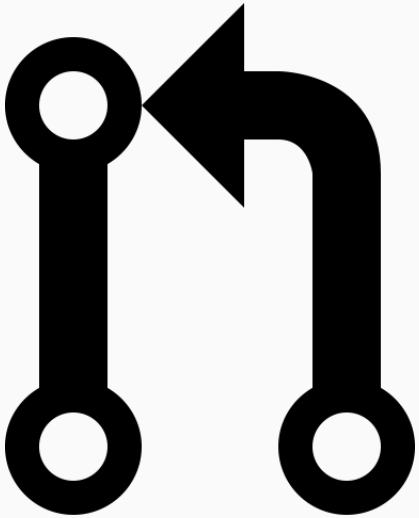
Big Brother Brasil

GLOBOPLAY

CartolaFC

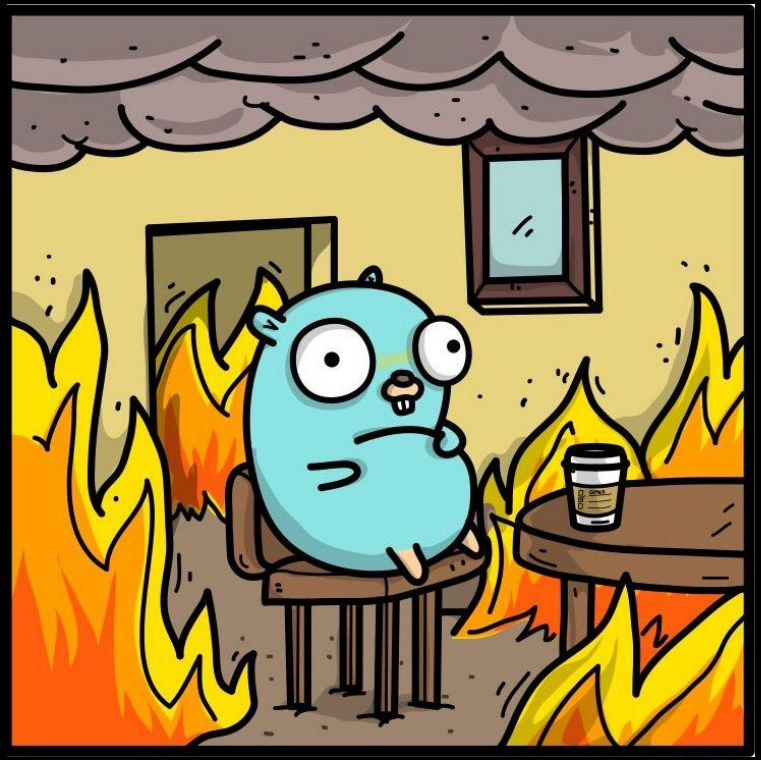
The Voice Brasil

Resultados Globo.com (até agora)

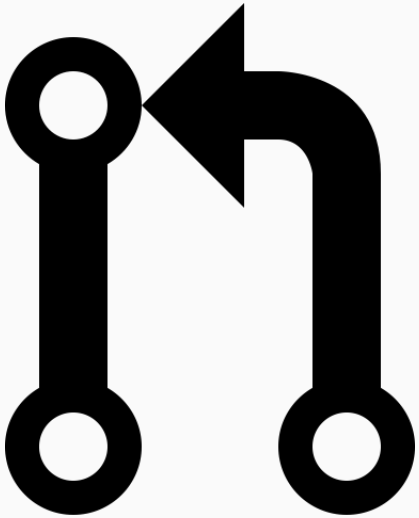


projetos globo.com
com huskyCI

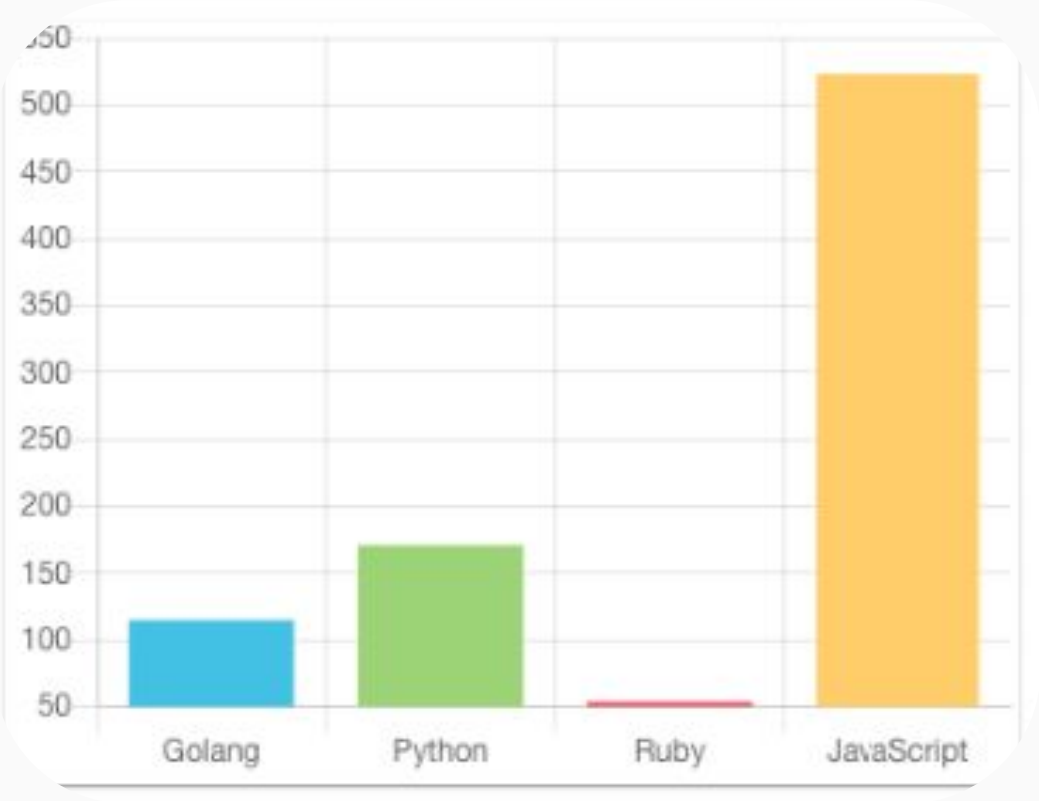
Developers	Analyses	Repositories
39	2345	92



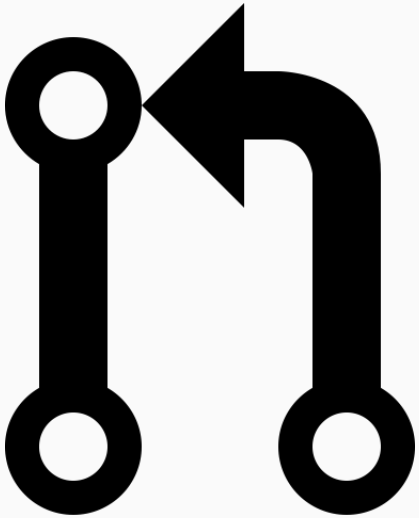
Resultados Globo.com (até agora)



projetos globo.com
com huskyCI



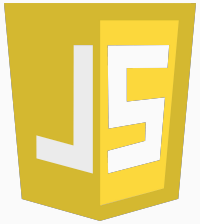
Resultados Globo.com (até agora)



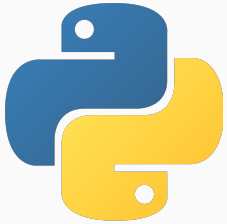
projetos globo.com com huskyCI

error unhandled

dependências vulneráveis



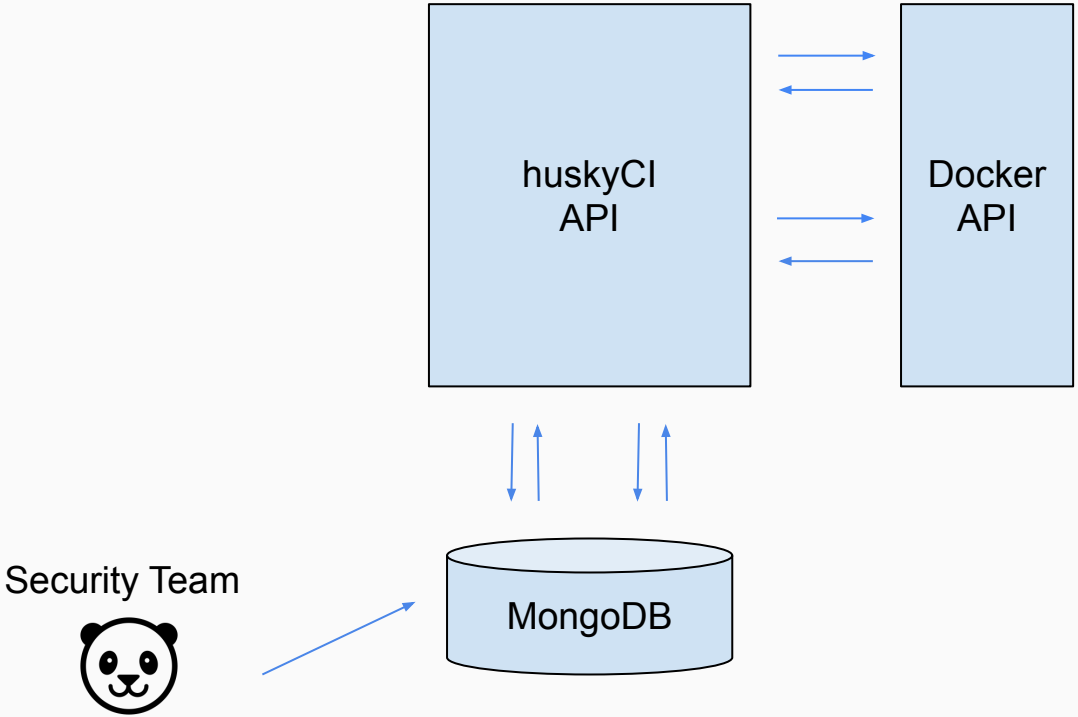
dependências vulneráveis



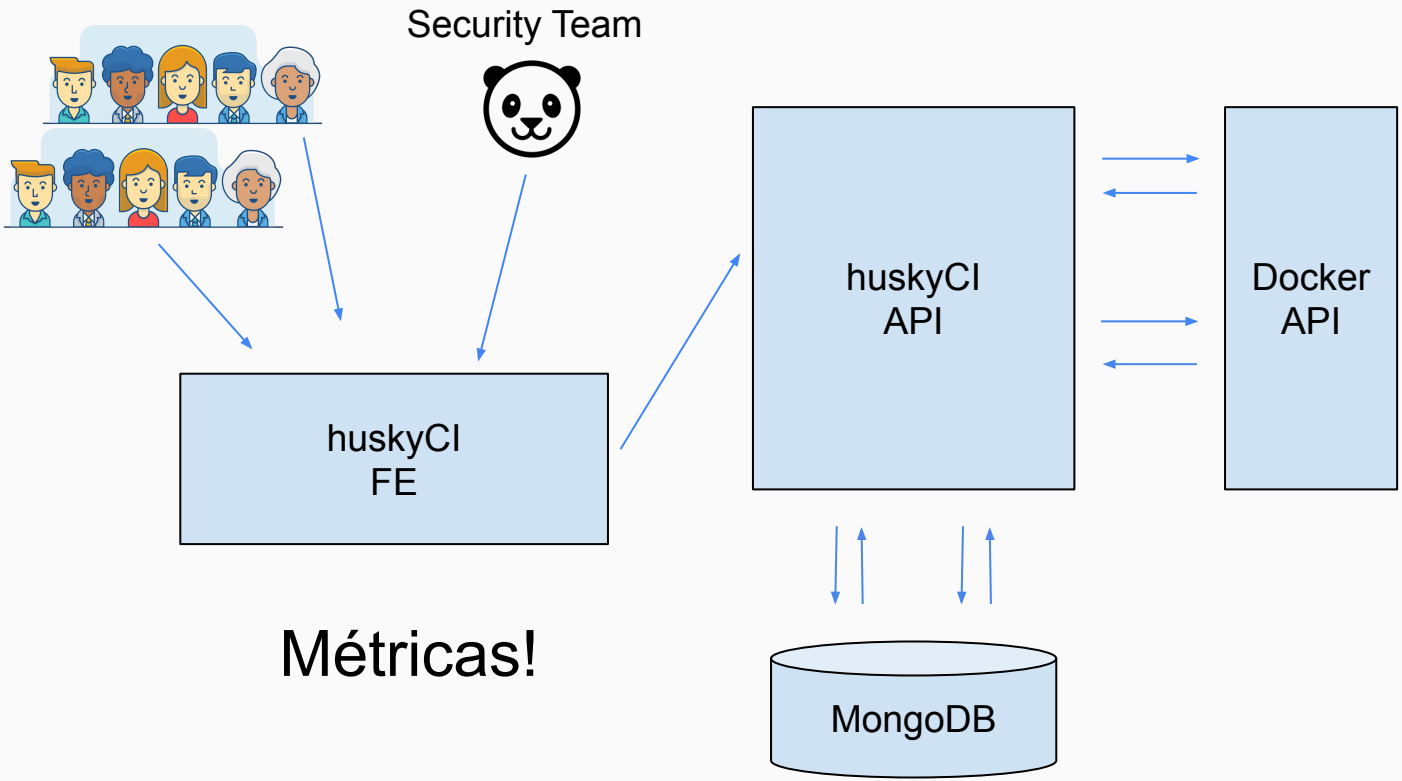
dependências vulneráveis

Próximas etapas ⭐

Próximas etapas: Front-end

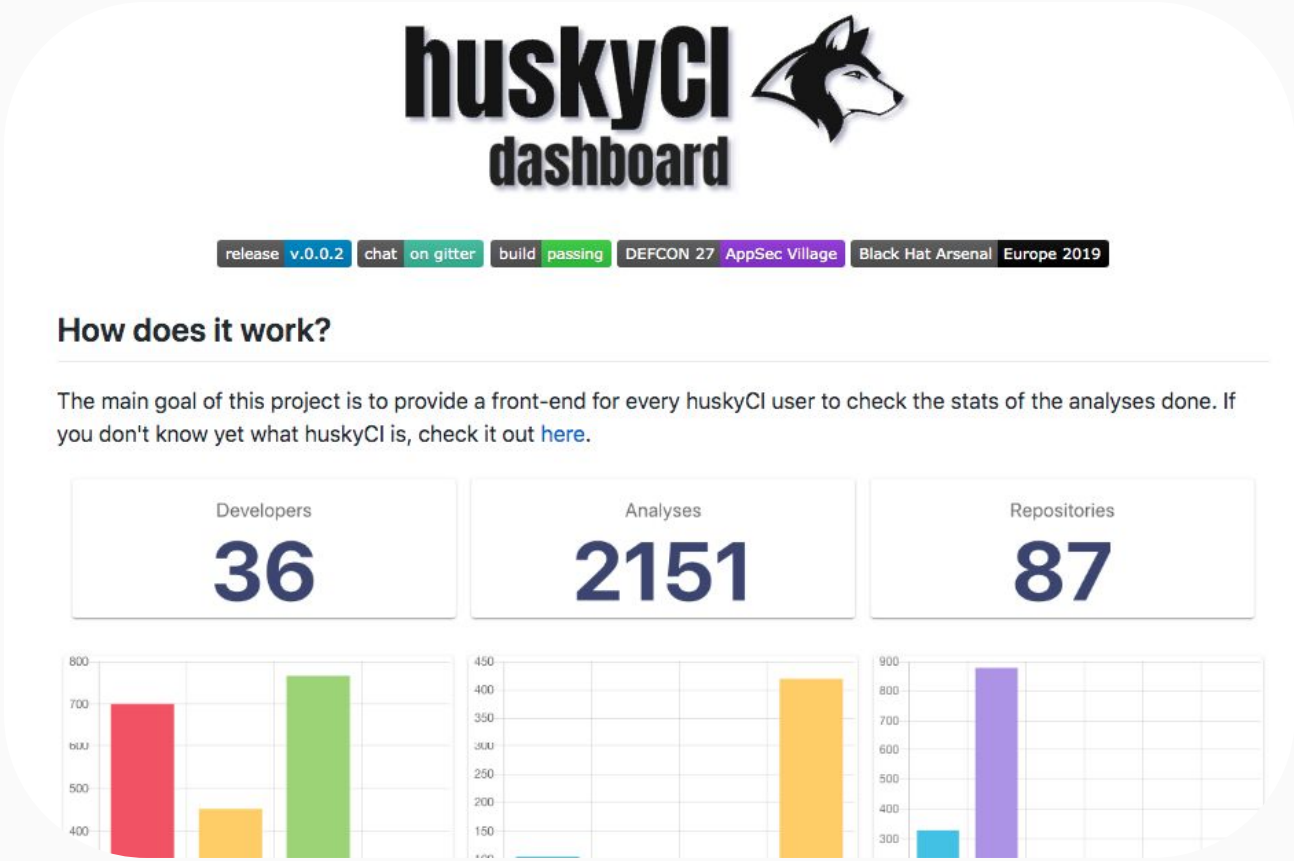


Próximas etapas: Front-end



Métricas!

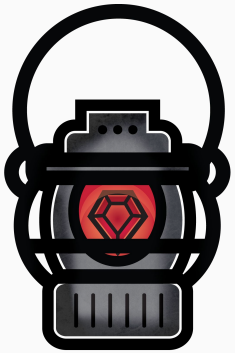
Próximas etapas: Front-end



Próximas etapas: Suportar mais linguagens

Próximas etapas: Integração com o SonarQube?

Próximas etapas: Contribuir com as ferramentas

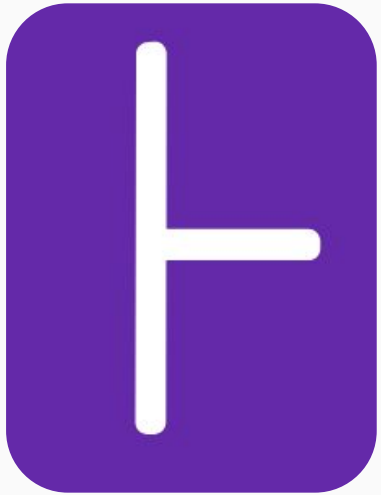


npm

Safety

Retire.js

Próximas etapas: Adicionais mais Security Tests



Security Code Scan

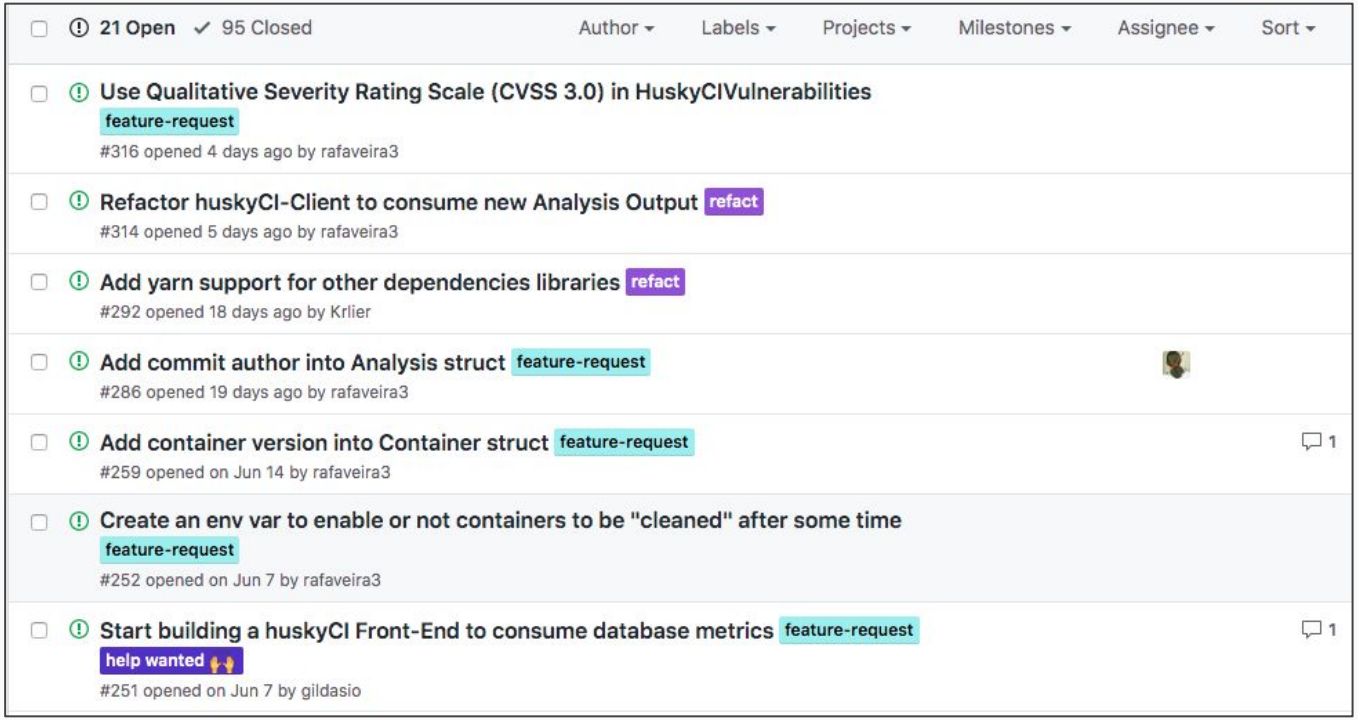
CHECKMARX

SpotBugs

Awesome Static Analysis!

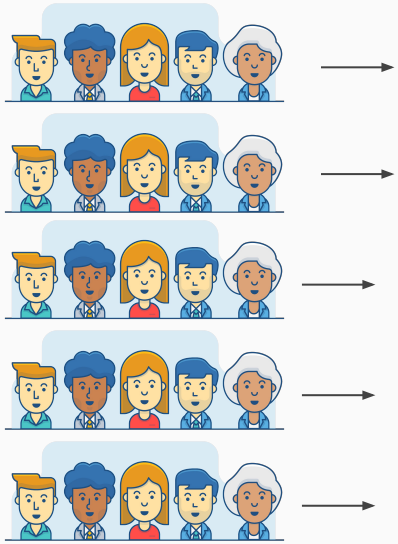
Awesome DevSecOps awesome

Próximas etapas: E muito mais!



https://github.com/globocom/huskyCI/issues

Próximas etapas: E muito mais!



Open Source

huskyCI - Performing security tests inside your CI

huskyCI

release v.0.7.0 | coverage 45% | build passing | chat on gitter | docs wiki | DEFCON 27 AppSec Village | Black Hat Arsenal Europe 2019

huskyCI is an open-source tool that performs security tests inside CI pipelines of multiple projects and centralizes all results into a database for further analysis and metrics.

How does it work?

https://github.com/globocom/huskyCI

Referências 📖

- [huskyCI] https://github.com/globocom/huskyCI
- [huslyCI-dashboard] https://github.com/globocom/huskyCI-dashboard
- [enry] https://github.com/src-d/enry
- [Safety] https://github.com/pyupio/safety
- [Bandit] https://github.com/PyCQA/bandit
- [gosec] https://github.com/securego/gosec
- [Brakeman] https://github.com/presidentbeef/brakeman
- [npm audit] https://docs.npmjs.com/cli/audit
- [gcom Hackday] https://www.instagram.com/talentosgcom/
- [Docker API] https://docs.docker.com/engine/api/v1.24/
- [SonarQube] https://www.sonarqube.org
- [Infer] http://fbinfer.com
- [SpotBugs] https://github.com/spotbugs/spotbugs
- [Security Code Scan] https://security-code-scan.github.io/
- [Checkmarx] https://www.checkmarx.com/
- [Awesome-Static-Analysis] https://github.com/mre/awesome-static-analysis
- [Awesome DevSecOps] https://github.com/devsecops/awesome-devsecops
- [huskyCI POC] https://gitlab.com/rafaveira3/appsec-defcon27-huskyci/merge_requests

Set, 2019

huskyCI

Perguntas?

🤔

github.com/globocom/huskyCI

Rafael dos Santos 🇧🇷 @rafasantos5

Set, 2019

huskyCI

Obrigado!

🙃

github.com/globocom/huskyCI

Rafael dos Santos 🇧🇷 @rafasantos5