



# Encontrando vulnerabilidades de código na Globo.com antes do deploy

Rafael dos Santos  @rafasantos5



# \$ whoami

Rafael dos Santos  @rafasantos5  
[github.com/rafaveira3](https://github.com/rafaveira3)

 Volante Clássico (Camisa 5)

 OSCP + OSCE

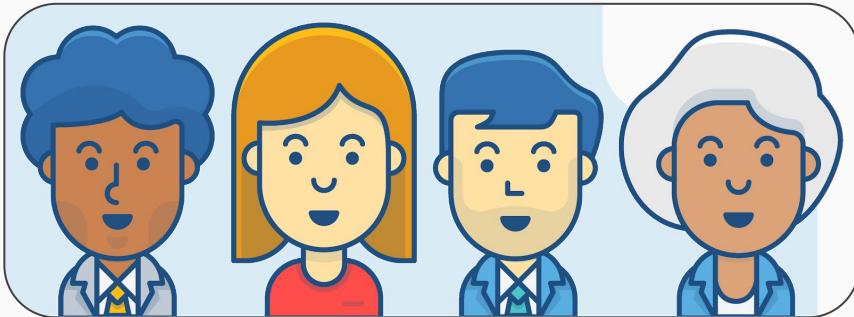
 Analista de Segurança @ globo.com

 Sec Tools + Desenvolvimento de Exploit

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



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



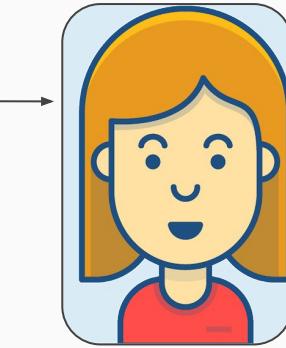
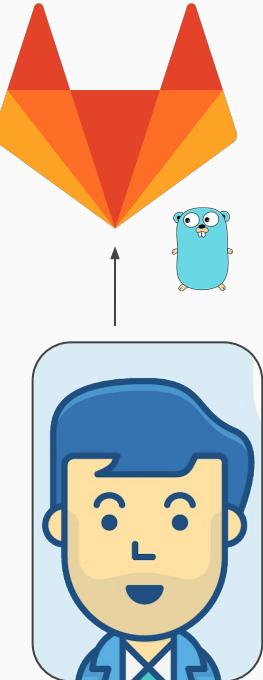
**tsuru**



Motorista nu bate em carro parado e capota veículo no Ceará	CR7 chama Messi para jogar na Itália: 'Como eu, aceite o desafio'	Ex-paquitas se reúnem para amigo secreto na casa de Xuxa
Executiva da Huawei presa pede liberação por motivos de saúde	Após anunciar Carille, Timão tenta acelerar montagem de elenco	Sasha posa dectada e capricha no 'carão' para encantar fãs
Ghosn é acusado formalmente no Japão por violação financeira	Cobrado por clubes do Brasil, Sassá seguirá no Cruzeiro, diz diretoria	Gavassi mostra Bruna 'desesperada' em show de Sandy; vídeo
Operação mira suposto esquema de médicos e empresários para furar fila do SUS	Santos não tem avanços após 'não' de Abel e inicia semana decisiva por novo técnico	Alok passa mal durante show no Festival de Verão e relata suspeita de zika



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



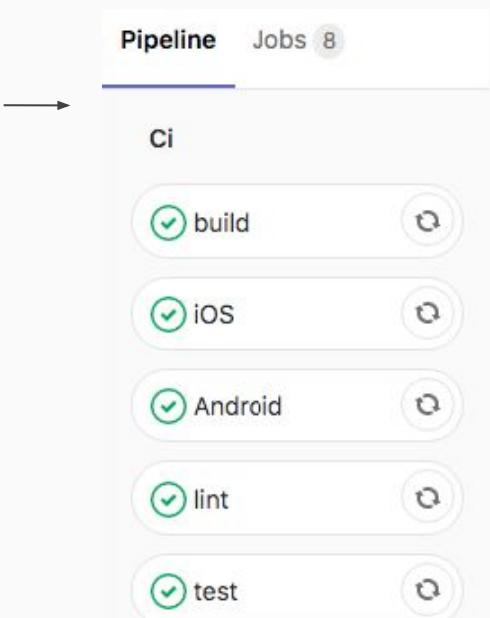
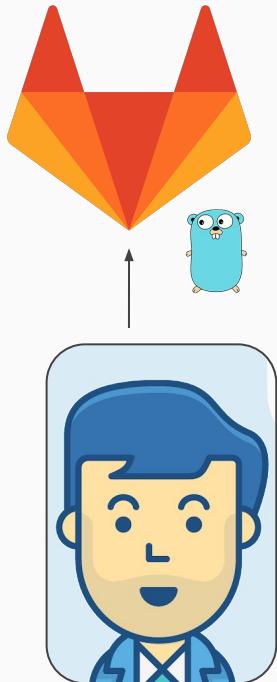
"Parece bom!"



**tsuru** ✓



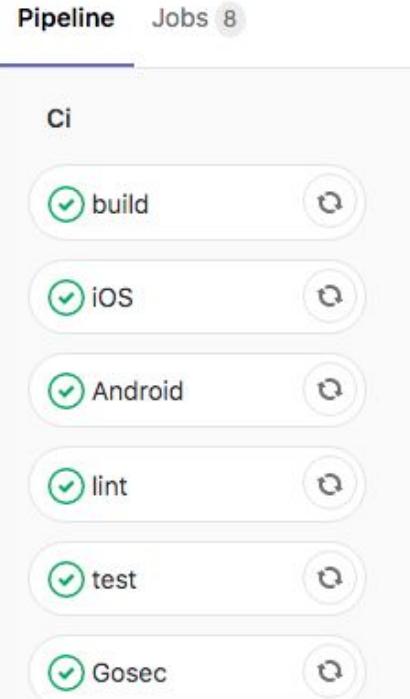
# Um dia na vida de um time de desenvolvimento...



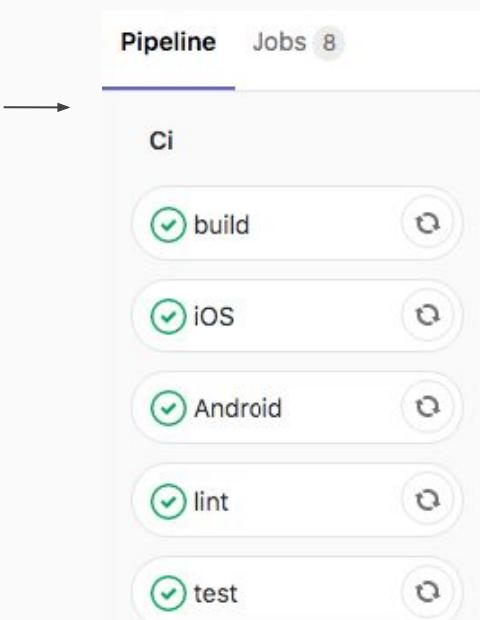
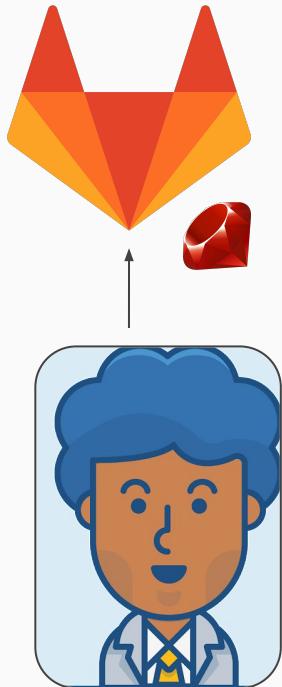
Time de Segurança



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



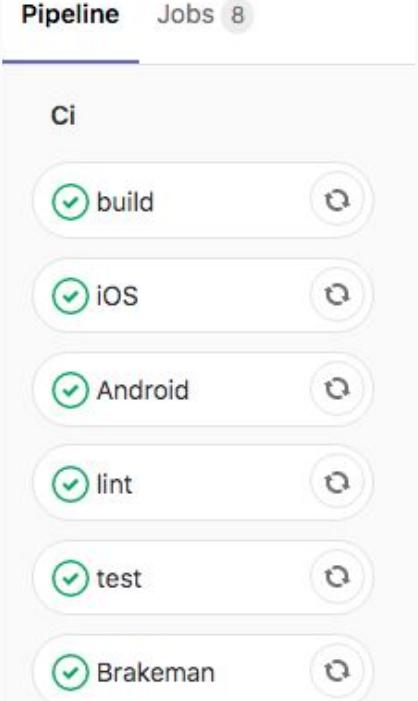
# Um dia na vida de um time de desenvolvimento...



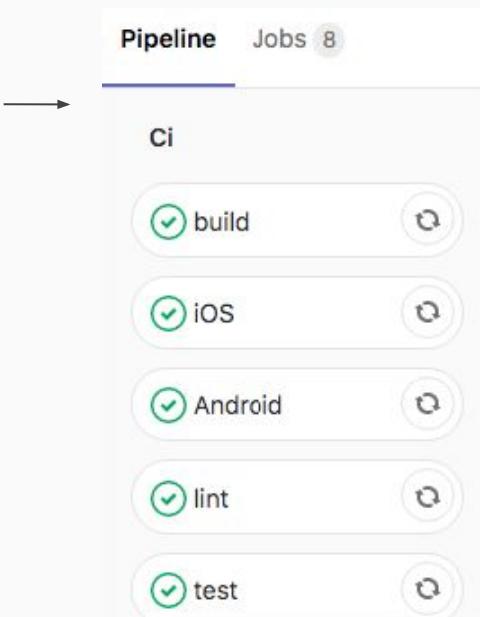
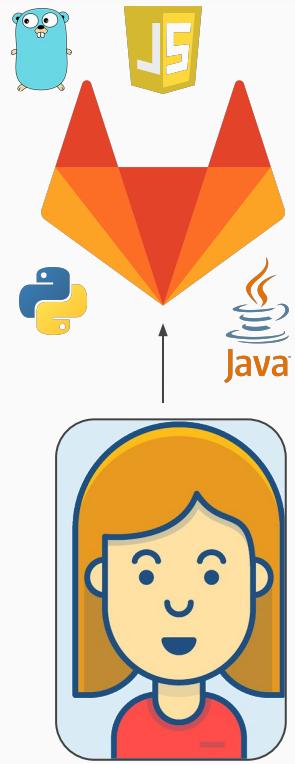
Time de Segurança



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



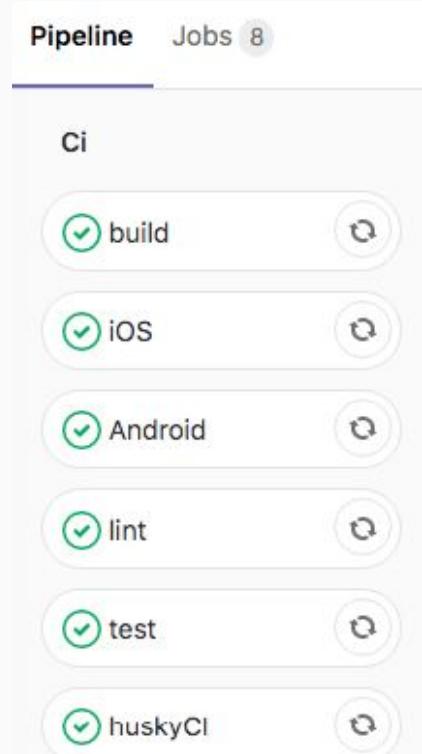
# Um dia na vida de um time de desenvolvimento...



Time de Segurança



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

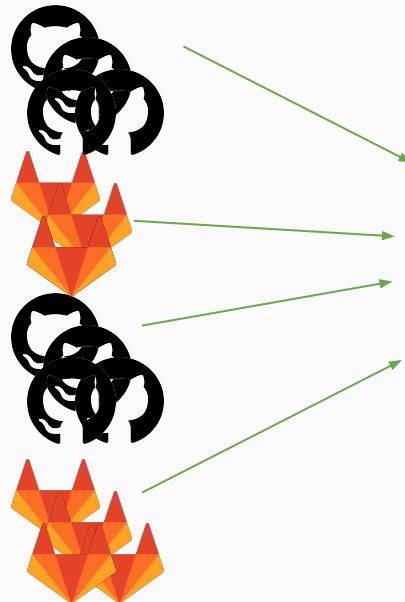
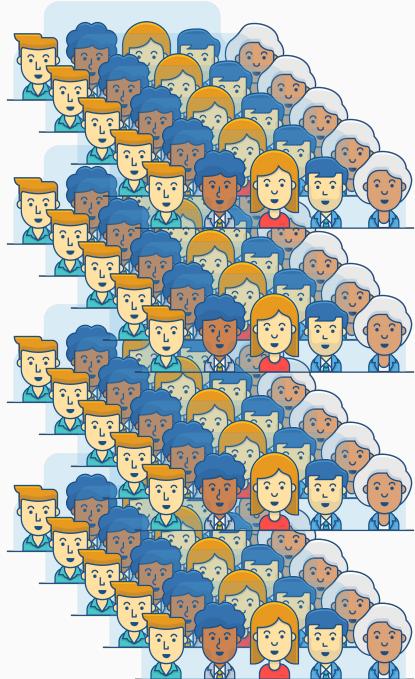




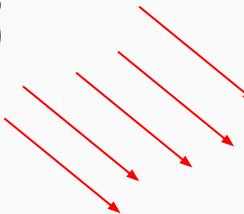
Um dia na vida de uma grande  
organização...

# Um dia na vida de uma grande organização...

## Times de Desenvolvimento



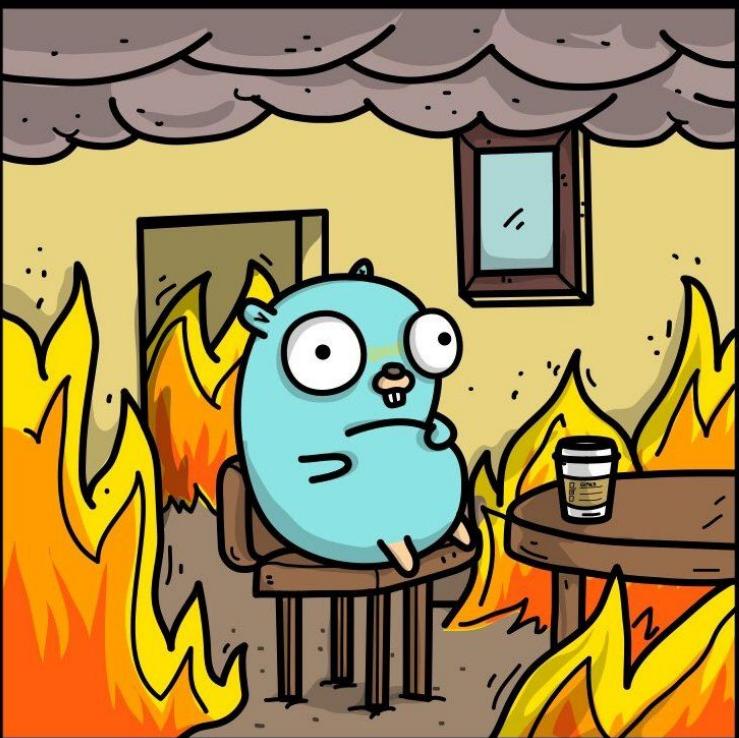
## Time de Segurança



**tsuru** →



tos não tem avanços após 'não' de Abel e a semana decisiva por novo técnico



Let's hack! 🐾

# Let's hack!



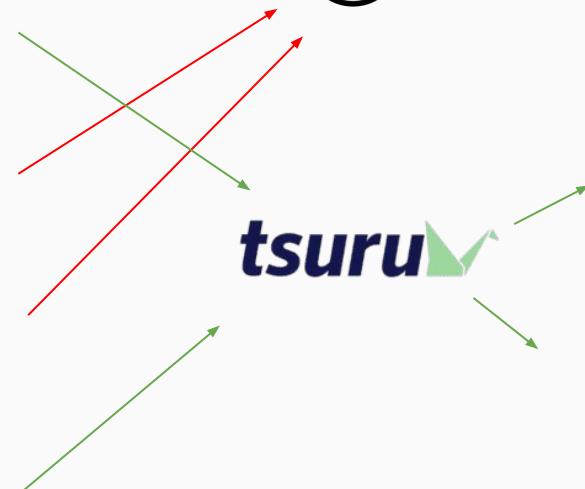
# Let's hack!



## Times de Desenvolvimento



## Time de Segurança



Homem é morto dentro de carro  
em Ceará

CR7 chama Messi para jogar na Itália: 'Como eu, aceite o desafio'

Ex-paquitas se reúnem para amigo secreto na casa de Xuxa

Portuguese actress Sasha posa de biquíni e pede liberdade  
motivos de saúde

Após anunciar Carille, Timão tenta acelerar montagem de elenco

Sasha posa de biquíni e pede liberdade  
motivos de saúde

Brasileiro é acusado  
violentemente no Japão  
de violação financeira

Cobrada por clubes do Brasil, Sassá seguirá no Cruzeiro,  
diz diretoria

Gavassi mostra Bruna  
'desesperada' em show de Sandy: 'video'

queima de médicos  
na Ilha do SUS

Santos não tem avanços após 'não' de Abel  
inicia semana decisiva por novo técnico

Alok passa mal durante show no Festival de  
Verão e relata suspeita de zika

# Let's hack!



## Times de Desenvolvimento



## Time de Segurança



**tsuru** ✓



# Let's hack!



## Times de Desenvolvimento



## Time de Segurança



**tsuru** ✓



Homem morre em acidente de carro no Ceará



CR7 chama Messi para jogar na Itália: 'Como eu, aceite o desafio'



Ex-paquitas se reúnem para amigo secreto na casa de Xuxa



Chefe da Huawei a pede libertação de executivo detido no Japão



Após anunciar Carille, Timão tenta acelerar montagem de elenco



Sasha posa decotada e capricha no 'carão' para encantar fãs



Homem é acusado de violência sexual no Japão



Cobiçado por clubes do Brasil, Sassá seguirá no Cruzeiro, diz diretoria



Gavassi mostra Bruna 'desesperada' em show de Sandy: 'video'



Brasília: queima de médicos é realizada no Rio de Janeiro



Santos não tem avanços após 'não' de Abel



Alckmin passa mal durante show no Festival de Verão e relata suspeita de zika

# Let's hack!



## Times de Desenvolvimento



## Time de Segurança



**tsuru** ✓



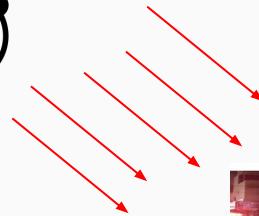
# Let's hack!



## Times de Desenvolvimento



## Time de Segurança



Homem morre em carro  
acidente no Ceará

CR7 chama Messi para jogar na  
Itália: 'Como eu, aceite o desafio'

Ex-paquitas se reúnem para  
amigo secreto na casa de Xuxa

Portuguese  
activist  
Huawei  
pede  
libertação  
motivos  
saúde

Após anunciar Carille,  
Timão tenta acelerar  
montagem de elenco

Sasha posa decotada e  
capricha no 'carão'  
para encantar fãs

Brasileiro é acusado  
salientemente no Japão  
de violação financeira

Cobiçado por clubes  
do Brasil, Sassá  
seguirá no Cruzeiro,  
diz diretoria

Gavassi mostra Bruna  
'desesperada' em  
show de Sandy; vídeo

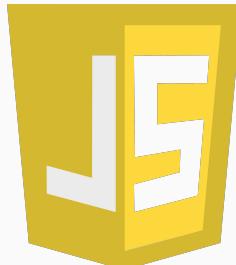
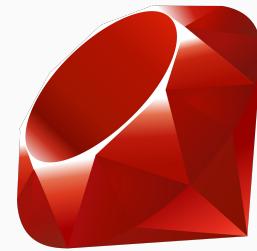
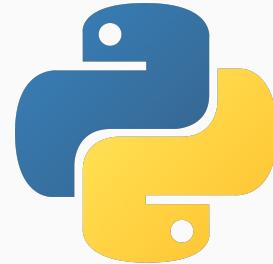
queima de médicos  
militares do SUS

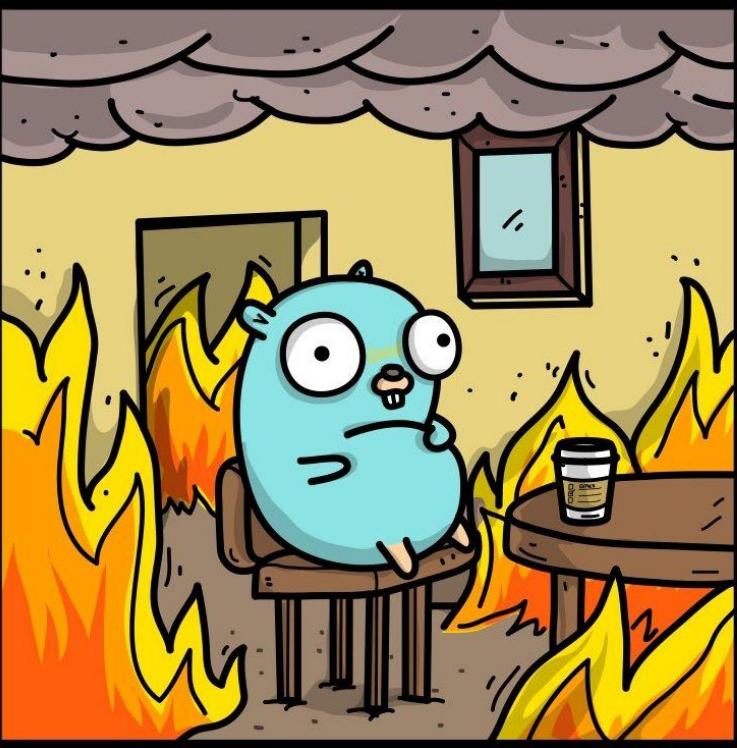
Santos não tem avanços após 'não' de Abel  
inicia semana decisiva por novo técnico

Alok passa mal durante show no Festival de  
Verão e relata suspeita de zika

Beleza, mas quais linguagens  
usamos? ☕

# Beleza, mas quais linguagens usamos?

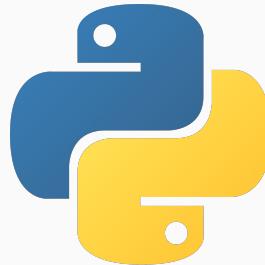




# Beleza, mas quais linguagens usamos?



gosec



Bandit



Brakeman

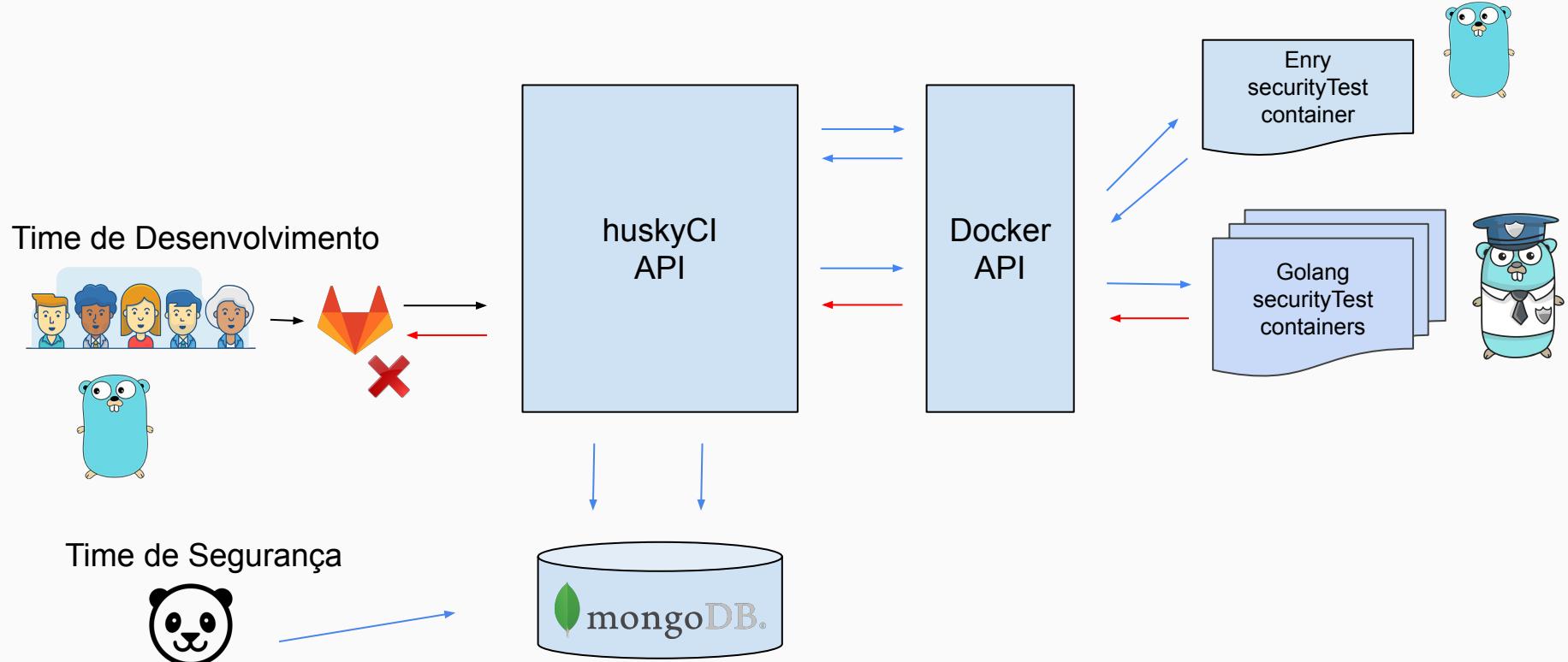
Como queremos construir esta  
ferramenta? 🔧

# Como queremos construir esta ferramenta?

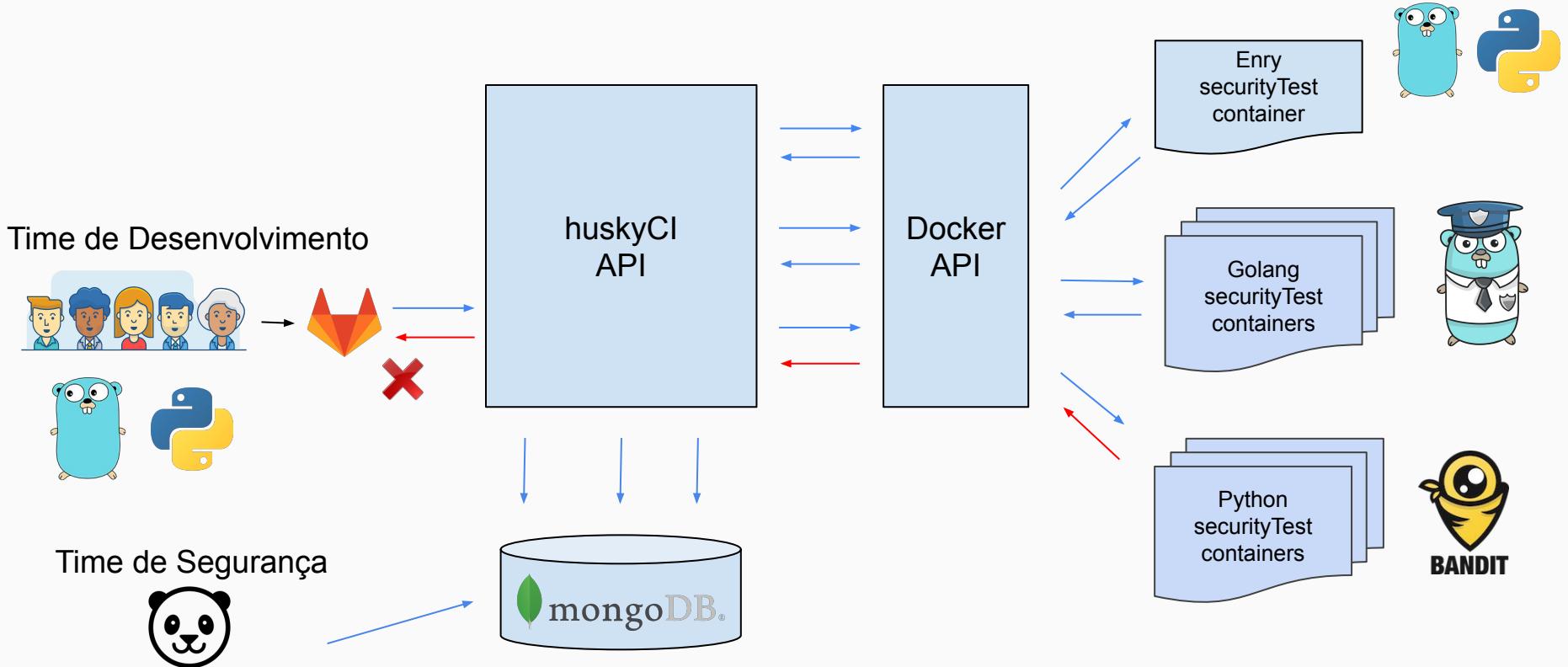
Time de Desenvolvimento



# Como queremos construir esta ferramenta?



# Como queremos construir esta ferramenta?



E o que gostaríamos de ver? 🐾

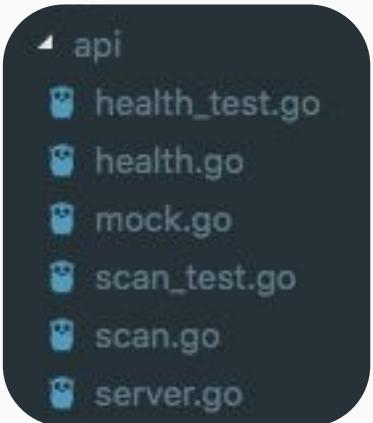
# E o que gostaríamos de ver?



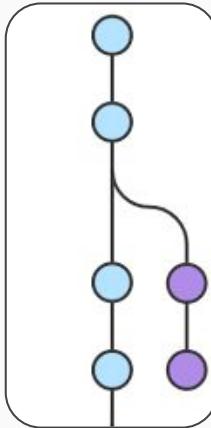
Autores de  
commit



Linguagem do  
repositório



Arquivos  
encontrados

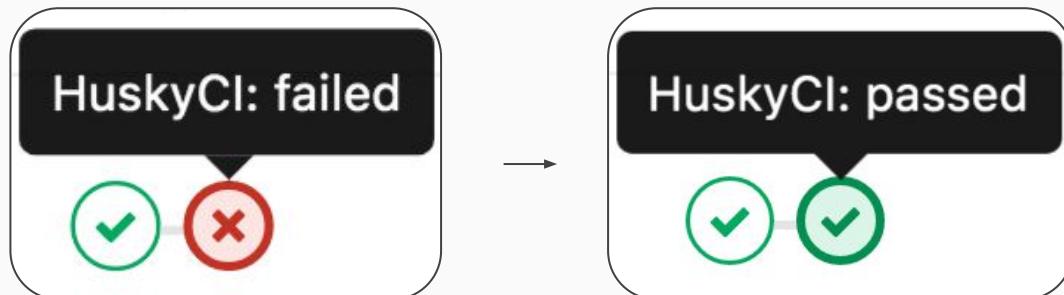


Nome da Branch

# 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?

▼ (1) ObjectId("5d4bb517d57854d4070b7816... { 12 fields }		Object
└ _id	ObjectId("5d4bb517d57854d4070b7816")	ObjectId
└ RID	IRMQTpLla1djyWviq03ifmzvK59pTCP0	String
└ repositoryURL	https://github.com/tsuru/cst.git	String
└ repositoryBranch	master	String
▶ securityTests	[ 2 elements ]	Array
└ status	finished	String
└ result	passed	String
▶ containers	[ 2 elements ]	Array
└ startedAt	2019-08-08 05:37:27.425Z	Date
└ finishedAt	2019-08-08 05:40:38.004Z	Date
▶ codes	[ 3 elements ]	Array
▼ huskyciresults	{ 1 field }	Object
└ goresults	{ 1 field }	Object
└ gosecoutput	{ 1 field }	Object
└ lowvulns	[ 13 elements ]	Array
└ [0]	{ 8 fields }	Object
└ [1]	{ 8 fields }	Object
└ language	Go	String
└ securitytool	GoSec	String
└ severity	LOW	String
└ confidence	HIGH	String
└ file	/go/src/code/cmd/server/server.go	String
└ line	63	String
└ code	viper.BindPFlag("server.cert-file", serverCmd.Fla...	String
└ details	Errors unhandled.	String
└ [2]	{ 8 fields }	Object
└ [3]	{ 8 fields }	Object

repository

Containers (Entry + Gosec)

Resultados



DEV, foque no desenvolvimento ❤



# Foque no desenvolvimento

```
! .gitlabci.yml ✘

1 stages:
2   - HuskyCI
3
4 test-huskyci:
5   stage: HuskyCI
6   script:
7     - wget urlto.huskyci.com/huskyci-client
8     - chmod +x huskyci-client
9     - ./huskyci-client
10
```

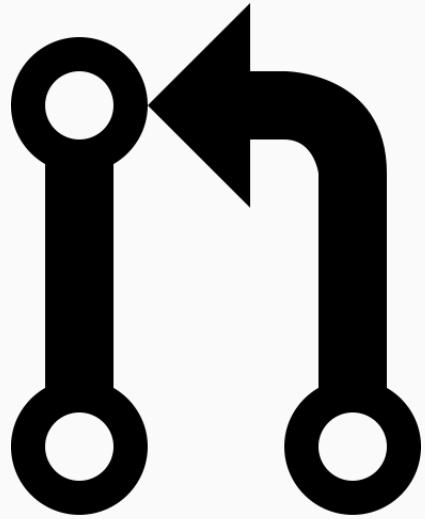


Demo 🔥



Resultados Globo.com (até agora) 🚀

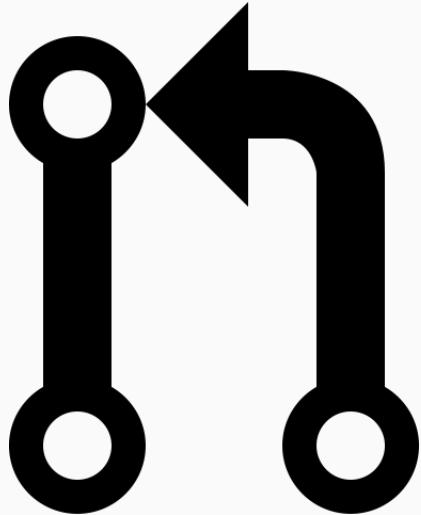
# Resultados Globo.com (até agora)



projetos globo.com  
com huskyCI



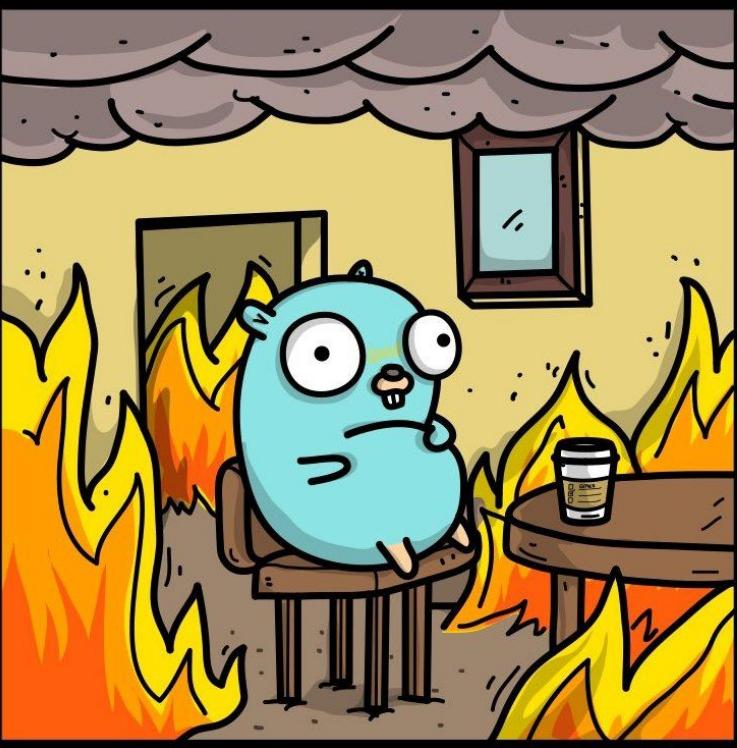
# Resultados Globo.com (até agora)



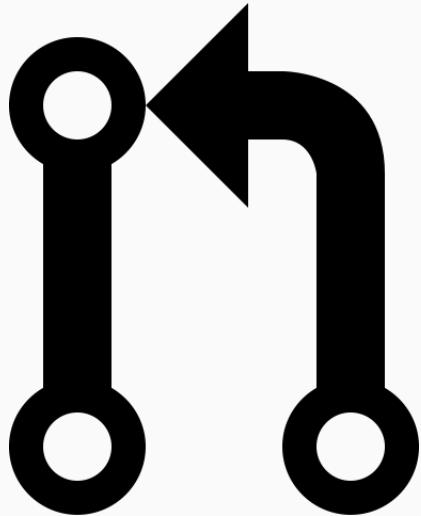
projetos globo.com  
com huskyCI

Developers **39** Analyses **2345** Repositories **92**

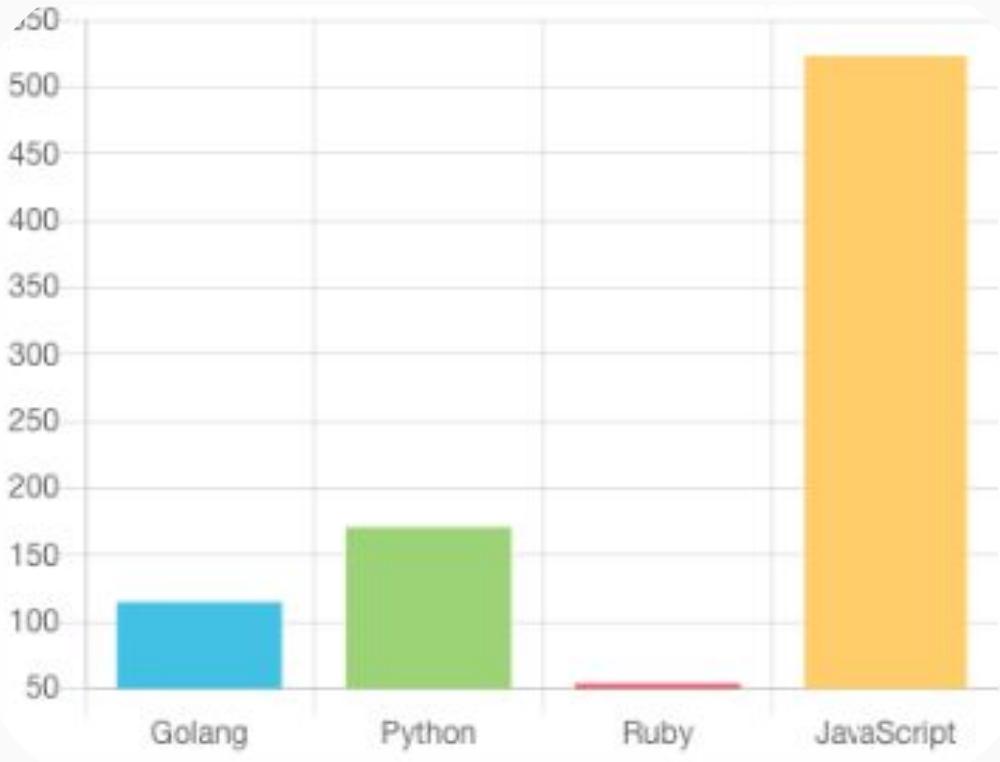




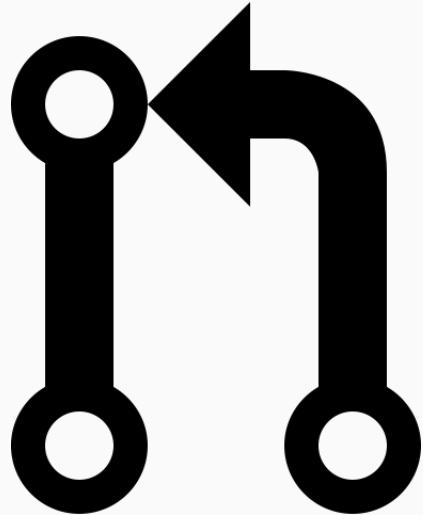
# Resultados Globo.com (até agora)



projetos globo.com  
com huskyCI



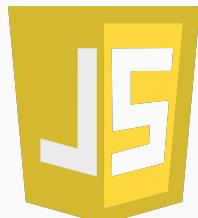
# Resultados Globo.com (até agora)



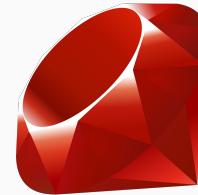
projetos globo.com  
com huskyCI



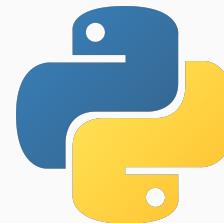
error unhandled



dependências vulneráveis



dependências vulneráveis

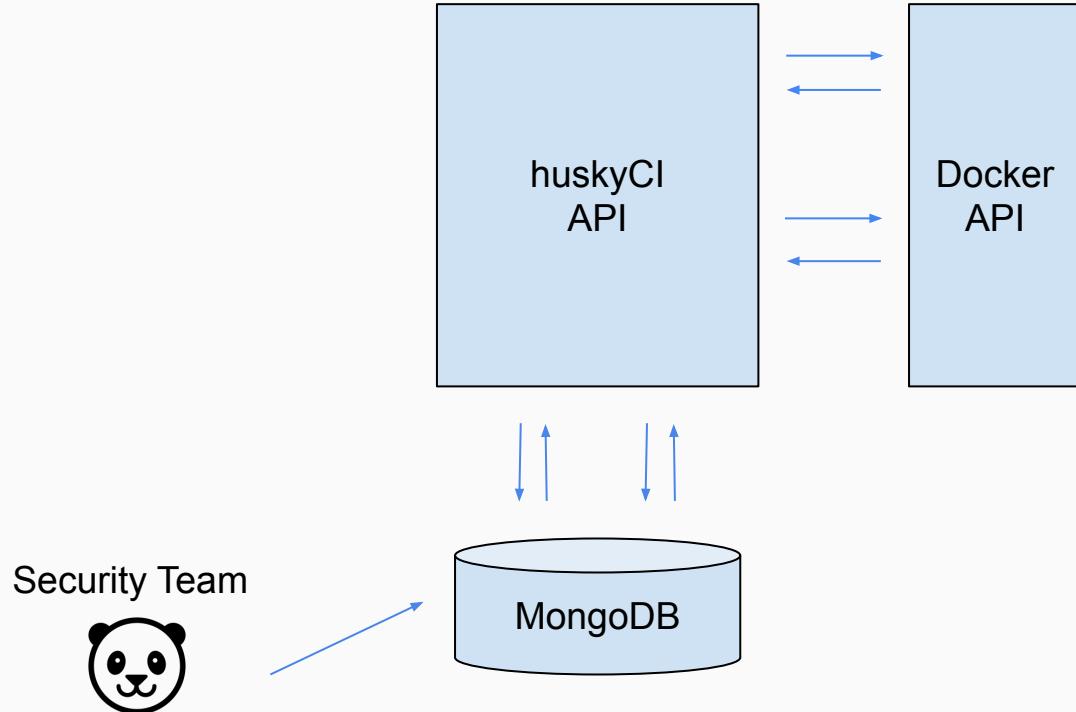


dependências vulneráveis

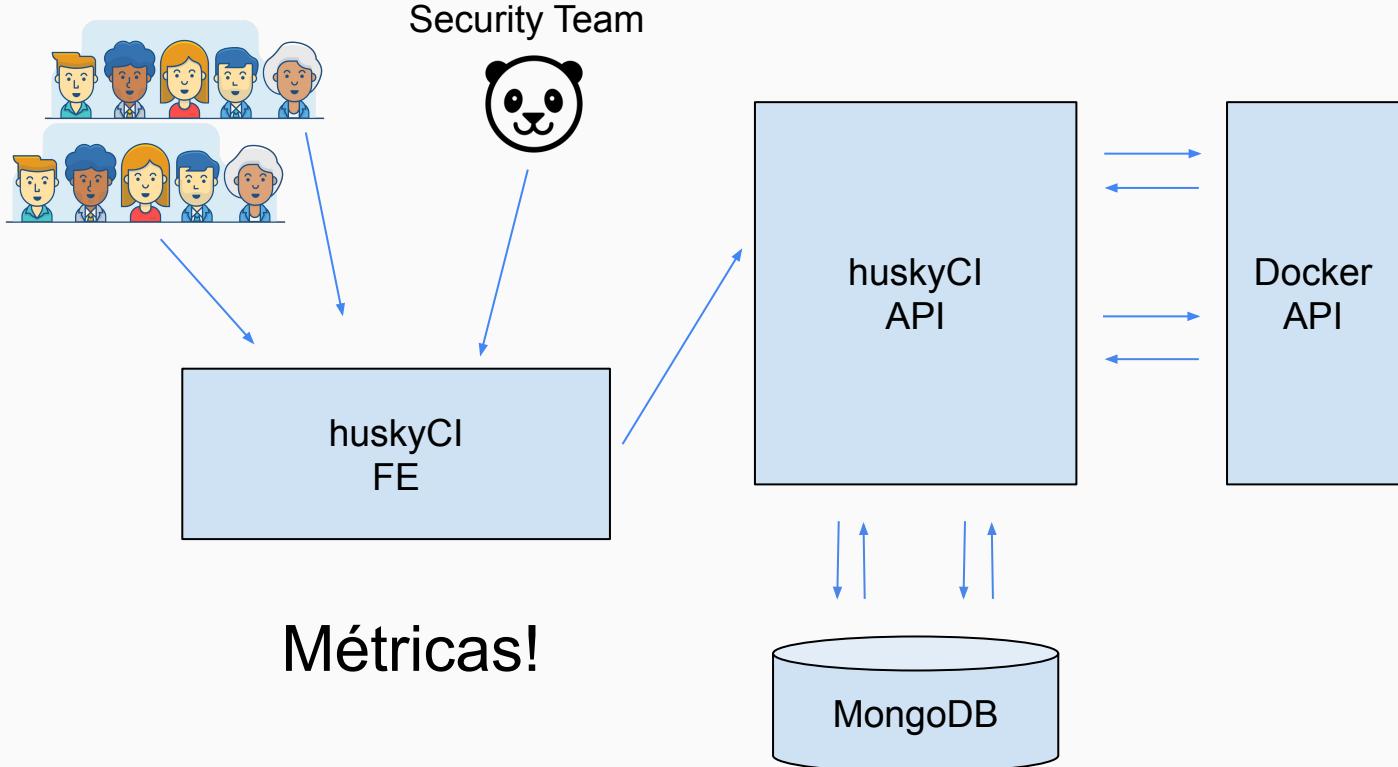


Próximas etapas ★

# Próximas etapas: Front-end



# Próximas etapas: Front-end



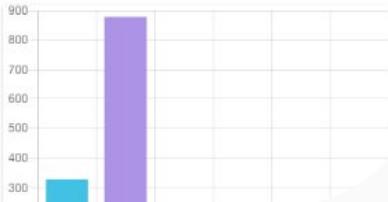
# Próximas etapas: Front-end



[release v.0.0.2](#) [chat on gitter](#) [build passing](#) [DEFCON 27 AppSec Village](#) [Black Hat Arsenal](#) [Europe 2019](#)

## How does it work?

The main goal of this project is to provide a front-end for every huskyCI user to check the stats of the analyses done. If you don't know yet what huskyCI is, check it out [here](#).



# Próximas etapas: Suportar mais linguagens



# Próximas etapas: Integração com o SonarQube?



**sonarQube**

# Próximas etapas: Contribuir com as ferramentas



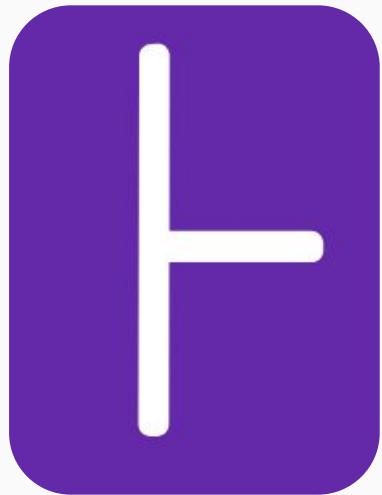
 **Safety**

**Retire.js**

# Próximas etapas: Adicionais mais Security Tests



## Security Code Scan



CHECKMARX

SpotBugs



Awesome Static Analysis!

Awesome DevSecOps

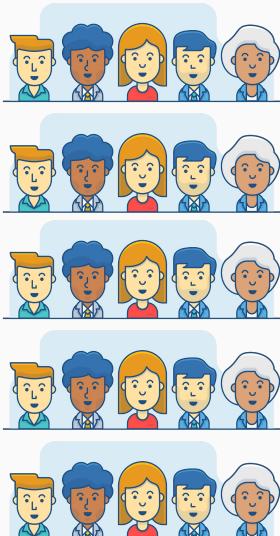


# Próximas etapas: E muito mais!

	Author	Labels	Projects	Milestones	Assignee	Sort
<input type="checkbox"/> ⓘ 21 Open ✓ 95 Closed						
<input type="checkbox"/> ⓘ Use Qualitative Severity Rating Scale (CVSS 3.0) in HuskyCI Vulnerabilities		feature-request				
	#316 opened 4 days ago by rafaveira3					
<input type="checkbox"/> ⓘ Refactor huskyCI-Client to consume new Analysis Output		refact				
	#314 opened 5 days ago by rafaveira3					
<input type="checkbox"/> ⓘ Add yarn support for other dependencies libraries		refact				
	#292 opened 18 days ago by Krlier					
<input type="checkbox"/> ⓘ Add commit author into Analysis struct		feature-request				
	#286 opened 19 days ago by rafaveira3					
<input type="checkbox"/> ⓘ Add container version into Container struct		feature-request				1
	#259 opened on Jun 14 by rafaveira3					
<input type="checkbox"/> ⓘ Create an env var to enable or not containers to be "cleaned" after some time		feature-request				
	#252 opened on Jun 7 by rafaveira3					
<input type="checkbox"/> ⓘ Start building a huskyCI Front-End to consume database metrics		help wanted				1
	#251 opened on Jun 7 by gildasio					

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

# Próximas etapas: E muito mais!



**huskyCI - Performing security tests inside your CI**



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?**

Open Source

<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](https://gitlab.com/rafaveira3/appsec-defcon27-huskyci/merge_requests)

Set, 2019



# Perguntas?



[github.com/globocom/huskyCI](https://github.com/globocom/huskyCI)

Rafael dos Santos @rafasantos5

Set, 2019



Obrigado!



[github.com/globocom/huskyCI](https://github.com/globocom/huskyCI)

Rafael dos Santos  @rafasantos5