Learn how to (not) use secrets with OWASP Wrong Secrets

Jeroen Willemsen

Project leader OWASP WrongSecrets & PSA

OWASP

Carnegie Mellon University
Software Engineering Institute

About me

Jeroen Willemsen

https://allmylinks.com/commjoenie

OWASP
Open Web Application Security Project

Can you keep a secret?

Examples of secrets

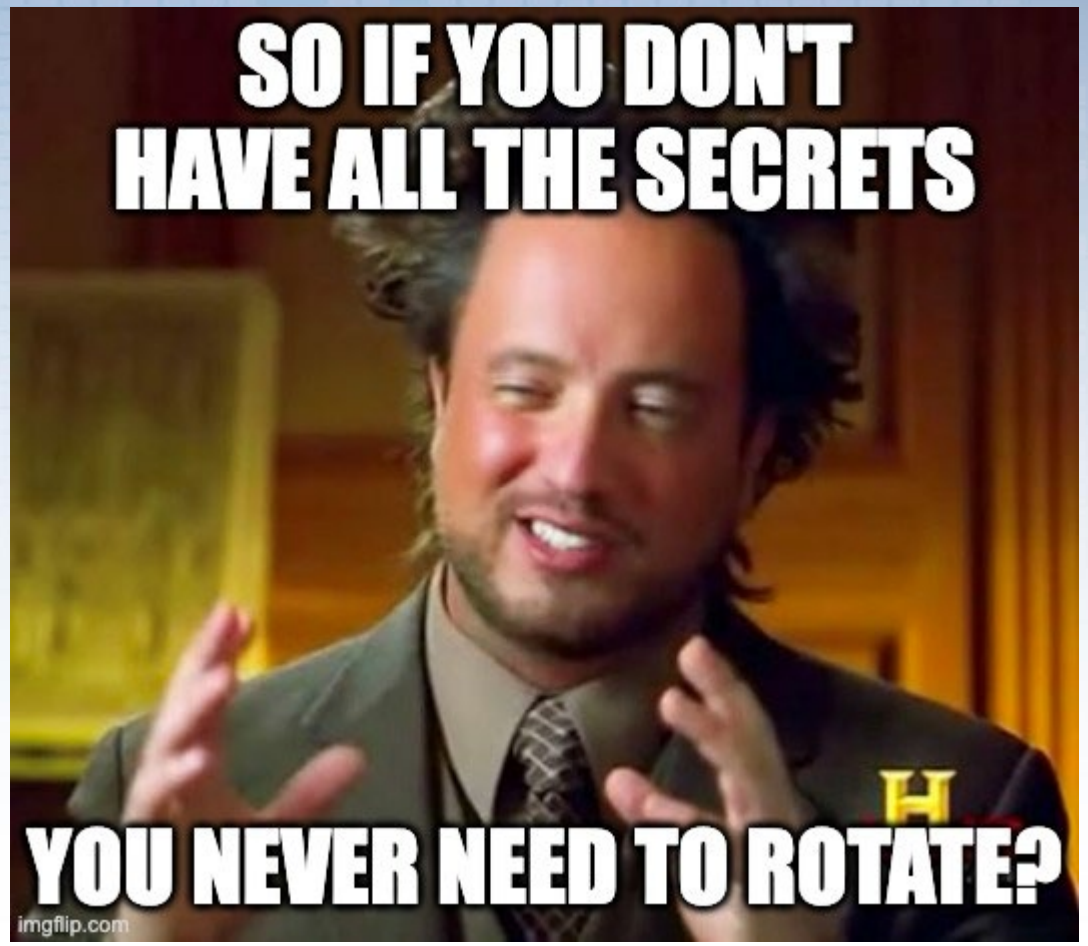
OWASP
Open Web Application Security Project

Where would you store a secret when on K8S?

- In code?
- In your container?
- In your K8s…?
- In your secrets manager?
- In your platform providing solution?
- In your… ?

If you had to rotate all your organization's secrets…

- Do you know where they are?
- Do you know their purpose?
- Can you rotate timely?
- Do you….

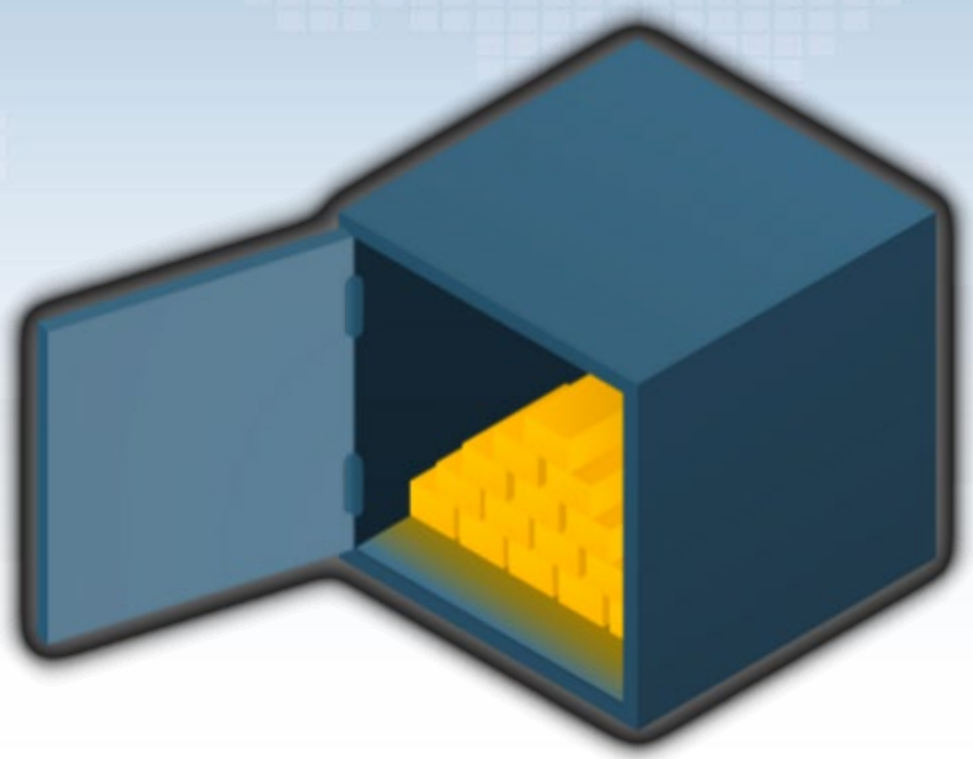


Can you tell us

- When your secret was last “borrowed” by your ex-colleague?
- When your secret was not working anymore?


SO APPARENTLY
SECRETS MANAGEMENT IS "SPECIAL"
imgflip.com

Introducing Project WrongSecrets



OWASP
Open Web Application Security Project

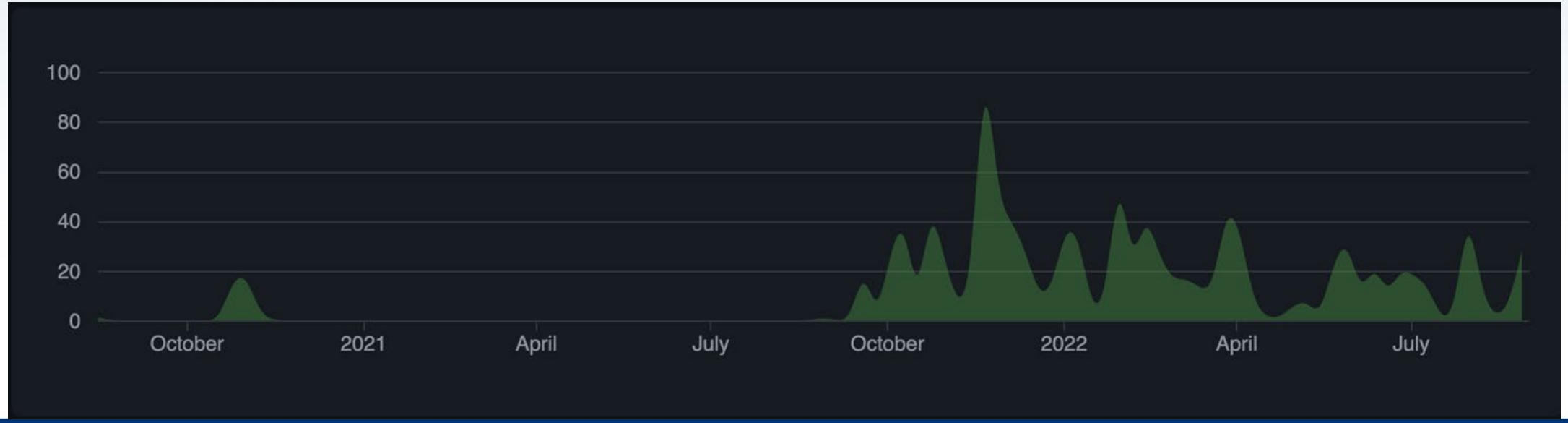
Today

- Project WrongSecrets
- Docker Demo on Heroku
- AWS Demo
- A few take-aways
- Where do we go from Here?

What is it?

- Vulnerable app & secret detector testbed
- Goals:
  - Educate on secret management and its pitfalls
  - Help people reflect on their secrets management strategy
  - Promote secrets management as important facet of security

Lab Project



Special Thanks

Leaders:

- Ben de Haan @bendehaan
- Jeroen willemsen @commjoen

Top contributors:

- Nanne Baars @nbaars
- Marcin Nowak @MarcinNowak-codes
- Joss Sparkes @remakingeden
- Tibor Hercz @tiborhercz
- Filip Chyla @fchyla
- Dmitry Litosh @Dlitosh
- Josh Grossman @tghosth
- Spyros @northdpole
- Mike Woudenberg @mikewoudenberg
- Ruben Kruiver @RubenAtBinx
- Finn @f3rn0s
- Alex Bender @alex-bender
- Rick M @kingthorin

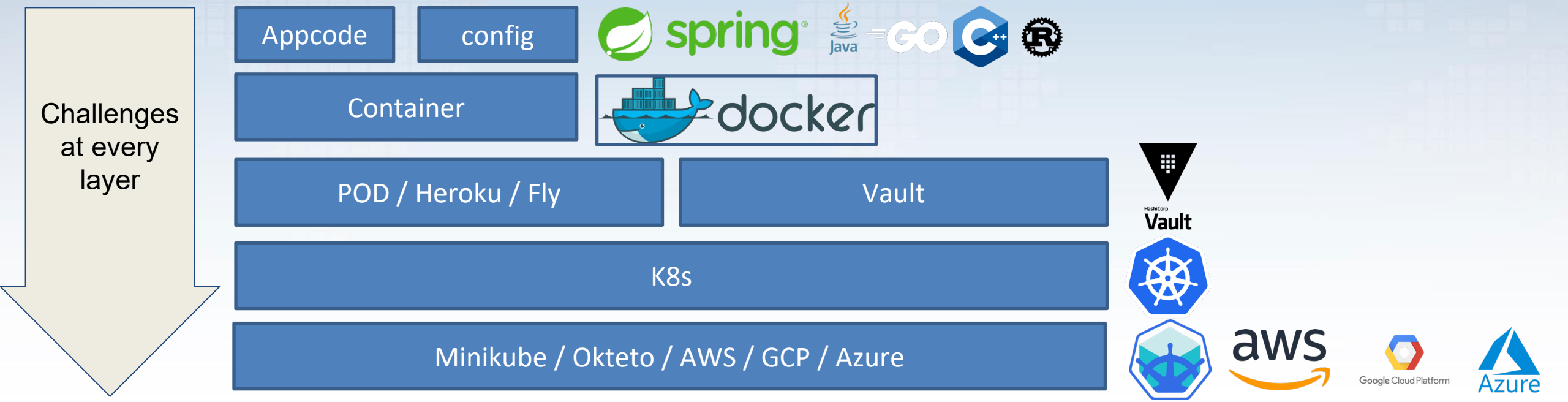
Testers:

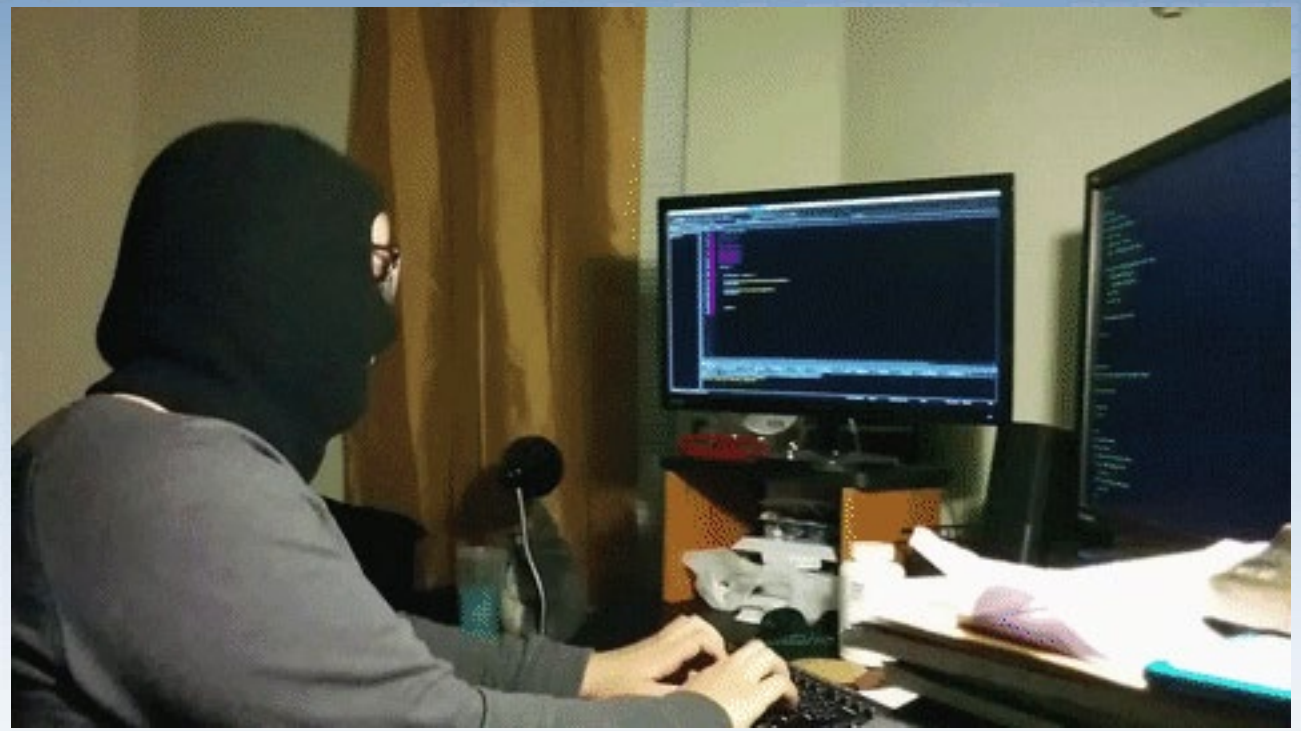
- Dave van Stein @davevs
- Marcin Nowak @MarcinNowak-codes
- Marc Chang Sing Pang @mchangsp

Special mentions for helping out:

- Madhu Akula @madhuakula
- Björn Kimminich @bkimminich

Overall architecture

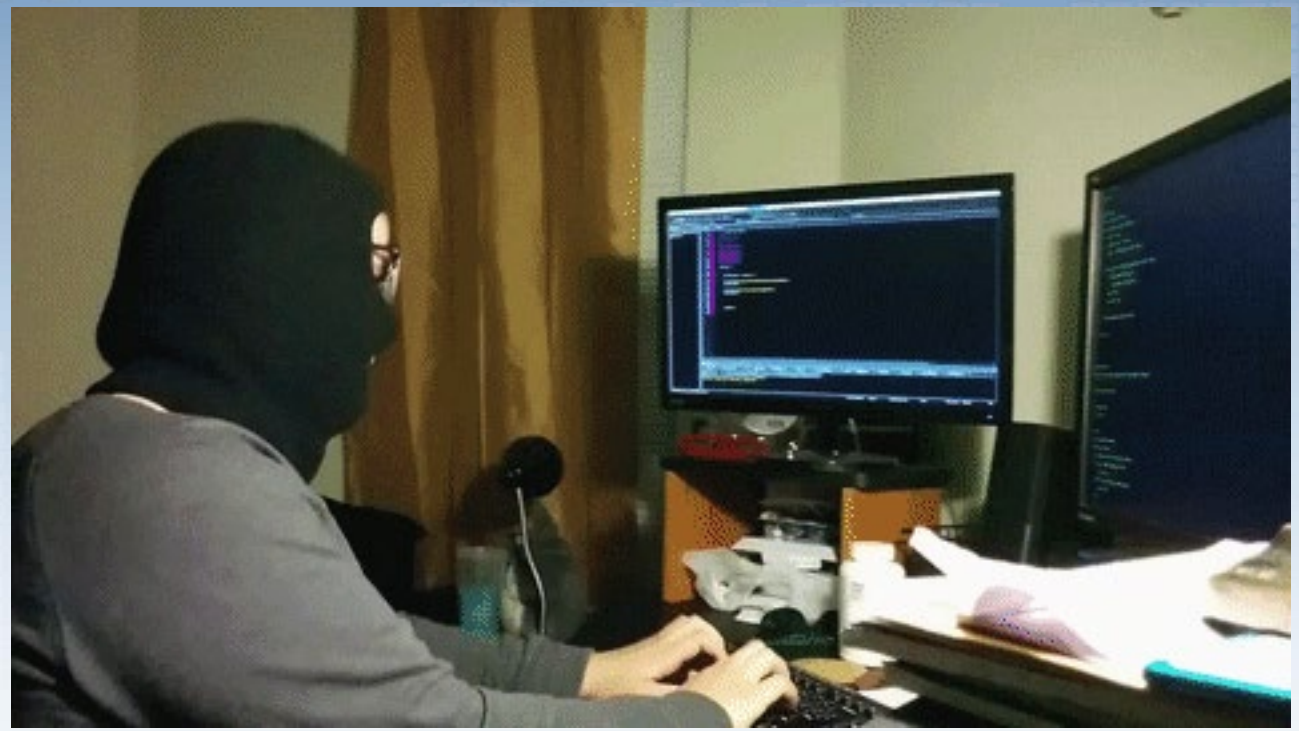




Docker Demo at Heroku

Why hardcoding secrets in application code & docker containers are a bad idea

OWASP
Open Web Application Security Project



AWS Demo

Terraform State should always be protected & Kubernetes defaults might not be helpful either.

Soo how should we do it?

So how should we do it?

Resources/further reading on secrets management:

- Blog: 10 Pointers on Secrets Management
- OWASP SAMM on Secret Management
- The secret detection topic at Github
- OWASP Secretsmanagement Cheatsheet
- Open CRE on Secrets Management

Use OWASP WrongSecrets as a secret detection benchmark

A few takeaways

- Never hardcode anywhere
- Don’t just trust defaults
- Rotate secrets/use ephemeral secrets
- Reduce blast radius
- Reduce exposure
- Have logging & alerting in place!

Where do we go from here?

- LCM activities (Dependencies, K8s version, Terraform version)
- Improve development experience with better live-reloading
- Secret hiding in binaries (Swift?)
- Other type of challenges and mistakes spotted in the wild

OWASP
Open Web Application Security Project

Where do we go from here?

- UI Improvements
- Secret detection testbed extension.
- Expanded CTF mode!

See: https://github.com/commjoen/wrongsecrets/issues

We can really use your help!

☆ Promote https://github.com/commjoen/wrongsecrets

GitHub Stars & social media

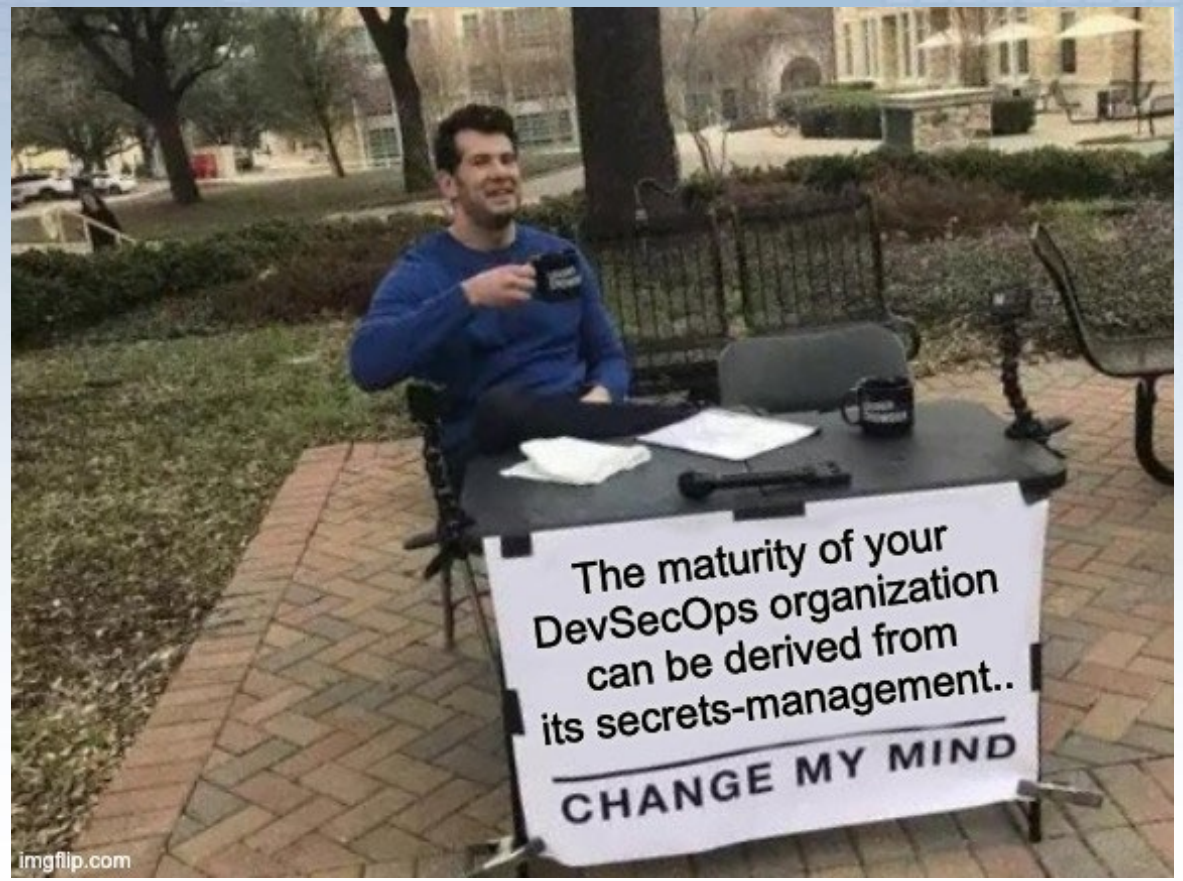
💻 Take the project for a spin

💬 Give feedback

File an issue or contact us on OWASP Slack in channel #project-wrongsecrets

🔧 Improve the project: File PRs!

Questions?



Twitter: @BJFdeHaan
Email: ben.dehaan@owasp.org

Twitter: @commjoenie
Email: jeroen.willemsen@owasp.org

OWASP
Open Web Application Security Project