OWASP WrongSecrets

Learn (In)Secure Secrets Management OWASP WrongSecrets

/bin/whoami

Daniel Gora
OWASP Frankfurt Co-Lead

- Lead Cloud Security Architect @ Cloudreach (ATOS)
- DevSecOps, OWASP, AppSec & Cloud-Native Security
- Somewhere between Edinburgh and Frankfurt, Germany
- Enjoys hillwalking ("munro-bagging") & history

dansecops

danielgora@owasp.org

Why Secrets Management Matters

No. 1 Top Cloud Security Issue

- Insufficient Credential Management
- Access and Key Management & Privileged Accounts

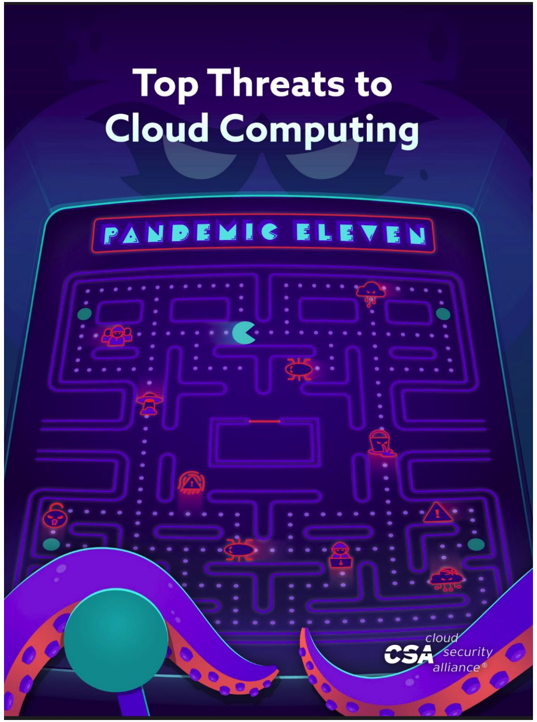
OWASP Top 10 2021

#A01: Broken access control

#A05: Security misconfiguration

CrowdStrike Threat Report 2022

- Cloud credential attacks prevalent exploitation vector



Top Threats to Cloud Computing

PANDEMIC ELEVEN

cloud security alliance®

Imagine if you had to rotate all your secrets…

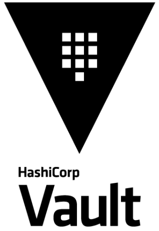
- Would you know where?
- Would you know what secrets?
- Can you rotate them in timely?

What is a Secret?

- Passwords, e.g. user or database
- API Keys
- SSH Keys
- Certificates
- MFA Tokens
- Cloud Access Keys
- Session Tokens
- Connection Strings

Cloud Secret Management Systems

AWS Secrets Manager



OWASP WrongSecrets Overview

Secrets app to learn common pitfalls

Guinea pig for your secrets scanning tools

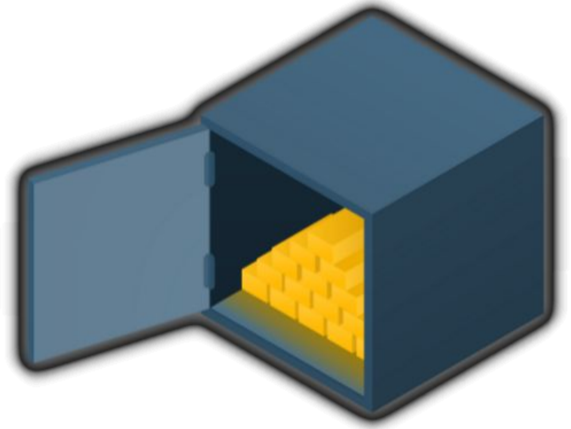
OWASP Project since October 2021

Java, Terraform, Docker, Kubernetes, Vault, Public Cloud

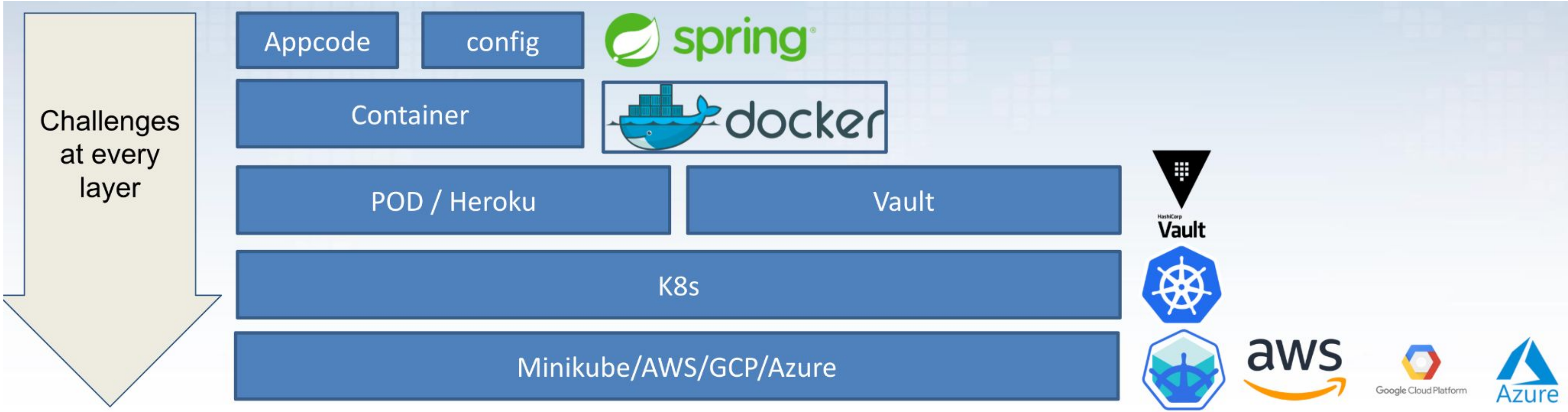
Project Leaders

Jeroen willemsen @commjoen
Ben de Haan @bendehaan

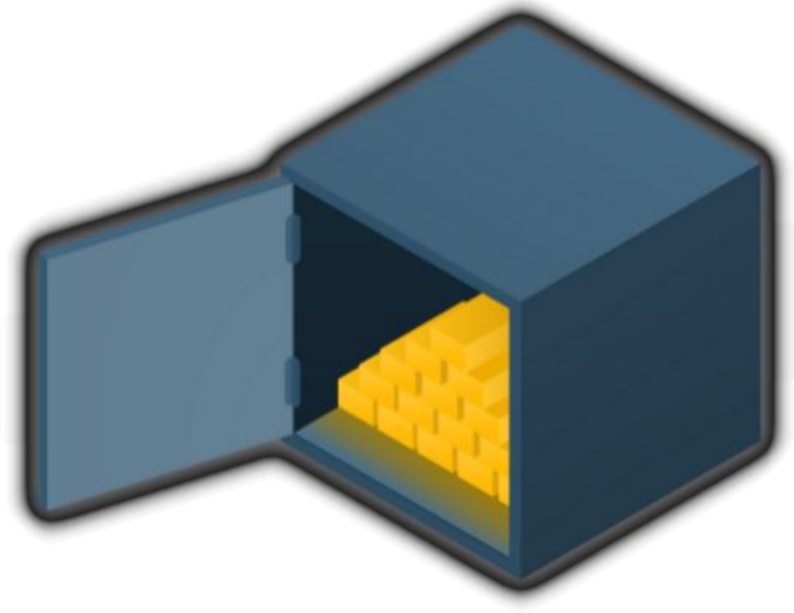
Lab Project



WrongSecrets Architecture



OWASP WrongSecrets Demo



owasp.org/www-project-wrongsecrets/

Lab Project

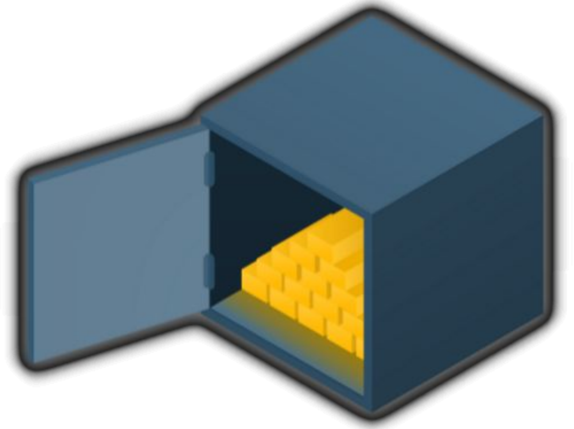
Mitigation Techniques

- Do not hardcode secrets
- Use a secret management system
- Rotate frequently & use dynamic secrets
- Encrypt secrets (storage & rest)
- Restrict access to least privilege
- Audit and monitor secret access

Conclusion

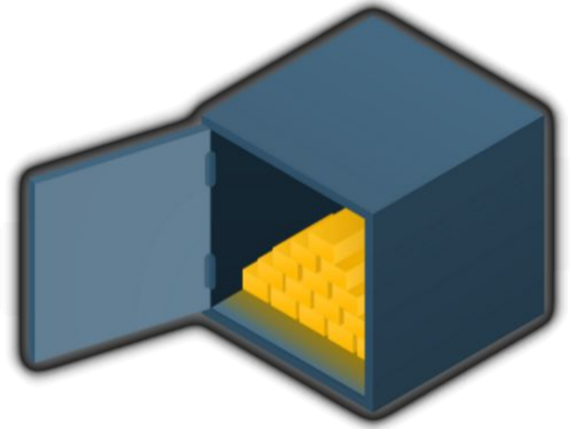
Conclusion

- Why Secrets Management Matters
- What’s a Secrets & Secret Management Systems
- Learn about Wrong Secrets Management with OWASP
- Challenges at every layer
- Hands-On Demo of WrongSecrets
  - Hardcoded password
  - Secret in Docker ENV
  - Secrets in IaC State
  - Misconfigured access
- Mitigation Techniques for Secrets Management



Try it out!

- Project Page: **owasp.org/www-project-wrongsecrets**
- Online Demo: **wrongsecrets.herokuapp.com**
- OWASP CheatSheet on Secrets Management
- **Try out** relevant challenges yourself!



Questions?