55. OWASP Frankfurt Stammtisch July 2022

25.07.2022

Program Highlights

Introduction Round & OWASP Overview
Daniel Gora & Jonas Becker

Learn (In)Secure Secrets Management OWASP WrongSecrets
Daniel Gora

The Forensic Hunt for Malware Campaigns of Cyber Criminals
Nicole Rother

Threat Modeling - A pragmatic approach
Jonas Becker

Outro & After-Party Socializing!

Housekeeping Rules

Introduction Round - Tell us about yourself!

Who are you?

What are you interested in?

Why are you here?

What is OWASP

What is OWASP

Open **W**eb **A**pplication **S**ecurity **P**roject

Non profit organization driven by **volunteers**

Focused on **improving software security**

Supported through **sponsorship and membership**

Projects, Local Chapters (250+) and **Events**

OWASP Frankfurt Stammtisch

Established in 2011, organised through Meetup and OWASP site

Open Community for **Information Security** and **Professional Networking**

Takes place on the **last wednesday of every 2-3 months**

owasp.org/www-chapter-germany/stammtische/frankfurt/

Call for Speakers and Event Venues!

OWASP Updates

Latest News

Upcoming OWASP Events

OWASP German Day (GOD) to be announced…

Stay Tuned - god.owasp.de

OWASP WrongSecrets

Learn (In)Secure Secrets Management OWASP WrongSecrets

/bin/whoami

Daniel Gora
OWASP Frankfurt Co-Lead

Lead Cloud Security Architect @ Cloudreach (ATOS)

DevSecOps, , 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

Can you keep a secret?

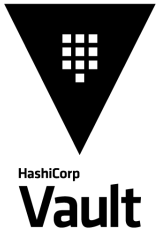
Imagine if you had to rotate all your secrets…

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

What is a Secret?

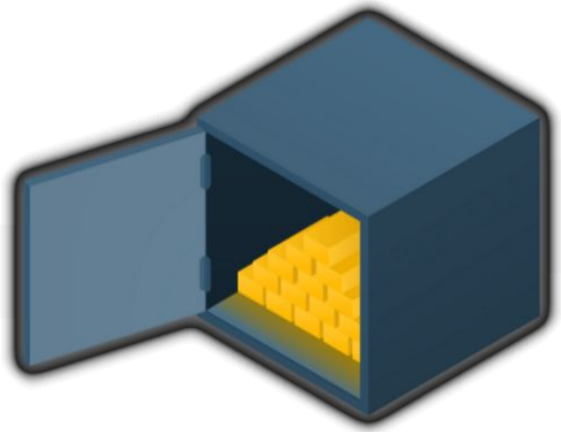
- Passwords, e.g. user or database
- API Keys
- SSH Keys
- Certificates
- MFA Tokens
- Cloud Access Keys
- Session Tokens
- Connection Strings

Cloud Secret Management Systems

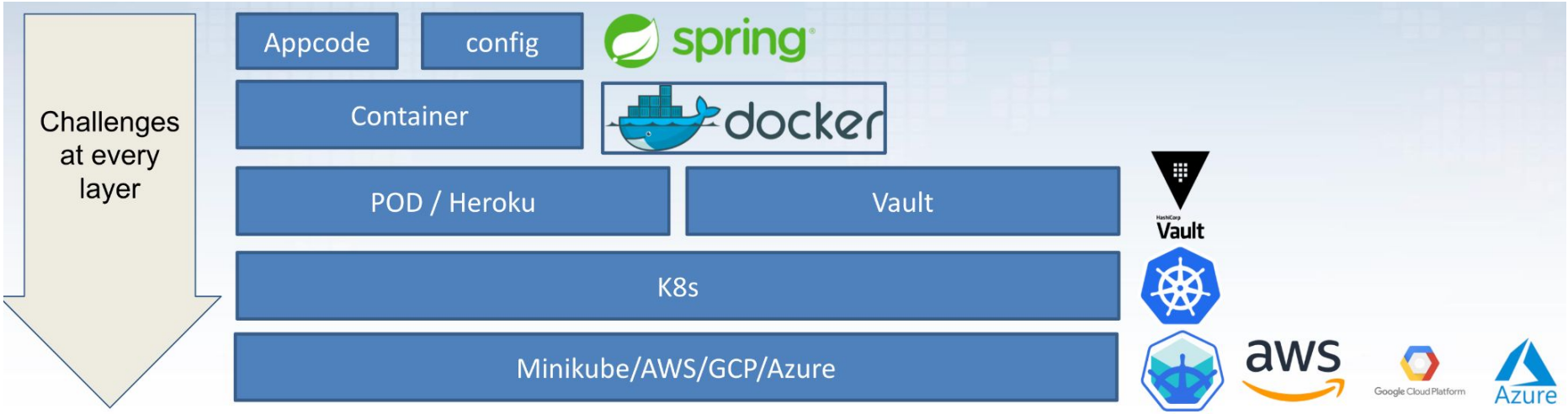


OWASP WrongSecrets Overview

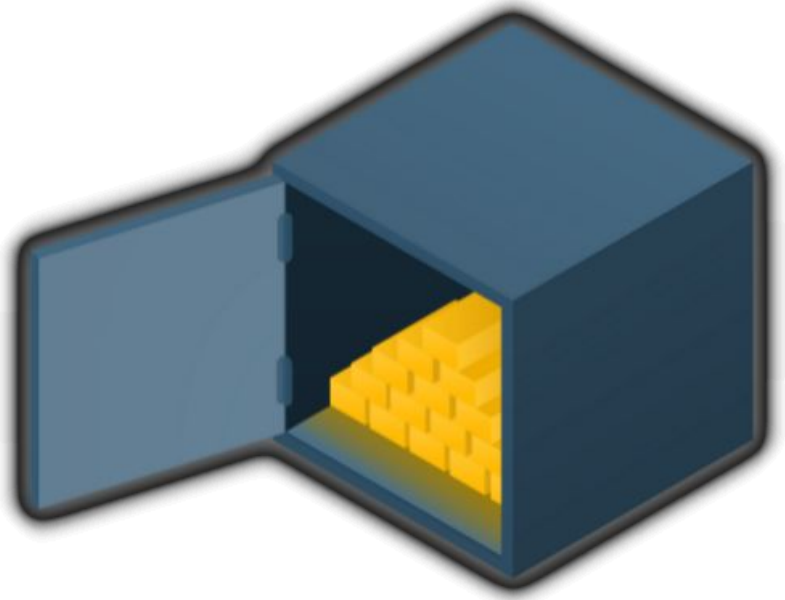
- Secrets app to learn common pitfalls
- Guinea pig for your secrets scanning tools
- OWASP Project since October 2021
- Java, Terraform, Docker, Kubernetes, Vault, Public Cloud
- Project Leaders
  - Jeroen willemsen @commjoen
  - Ben de Haan @bendehaan
- Lab Project



WrongSecrets Architecture



OWASP WrongSecrets Demo



owasp.org/www-project-wrongsecrets/

Lab Project

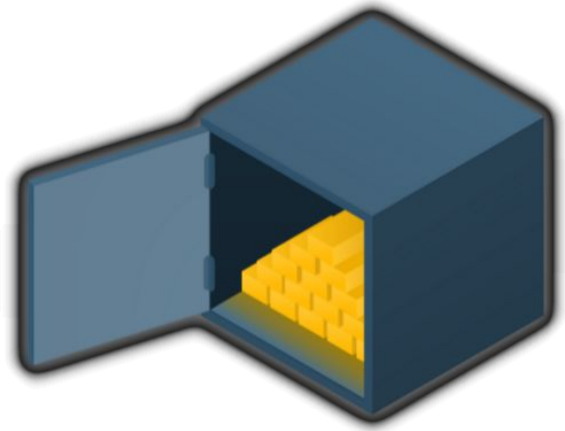
Mitigation Techniques

- 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



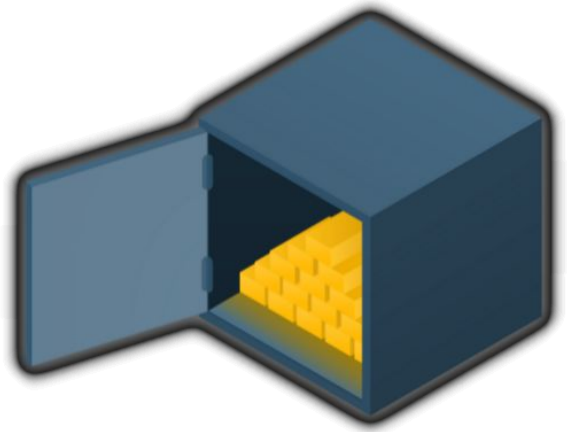
Try it out!

Project Page: **owasp.org/www-project-wrongsecrets**

Online Demo: **wrongsecrets.herokuapp.com**

OWASP CheatSheet on Secrets Management

Try out relevant challenges yourself!




Questions?

The Hunt for Cyber Criminals and Malware Campaigns

an International IT-Forensic Investigation Story


Break

Threat Modeling - A pragmatic approach

A battle-hardened approach to threat modeling


Outro

Next OWASP Meetups

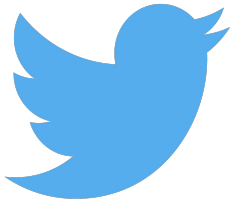
Online Meeting via Zoom!

August 24, 2022 - 18:00

Location - Zoom

IT-Security Collective Kassel with OWASP Frankfurt!

Keep in Touch



Twitter

@owasp_frankfurt
@owasp_de

Meetup

meetup.com/IT-Security-Stammtisch-Frankfurt-OWASP-u-w

Slack

slack.owasp.org
Channel: #chapter-germany

Website

https://www.owasp.org/www-chapter-germany/stammtische/frankfurt

After Party!


OWASP®
Appendix

OWASP Project Overview

OWASP Project Overview

256+ Projects

Flagship Projects

Lab Projects

Incubator Projects

www.owasp.org/projects

Flagship Projects 

- OWASP Amass
- OWASP Application Security Verification Standard
- OWASP Cheat Sheet Series
- OWASP CSRFGuard
- OWASP CycloneDX
- OWASP Defectdojo
- OWASP Dependency-Check
- OWASP Dependency-Track
- OWASP Juice Shop
- OWASP Mobile Security Testing Guide
- OWASP ModSecurity Core Rule Set
- OWASP OWTF
- OWASP SAMM
- OWASP Security Knowledge Framework
- OWASP Security Shepherd
- OWASP Top Ten
- OWASP Web Security Testing Guide
- OWASP ZAP

OWASP Projects

- Wide-range of Open Source tools for various purposes
- No pre-investment needed
- Build and supported by the community
- Freely available tools and material
- Every project has documentation, maling list and Slack Channel

www.owasp.org/projects