Building Secure Containers: A Practical Guide to Harbor and Vulnerability Scanning

by Prasanth Baskar (bupd)

About Me

(Just Another Developer)

- Hates Bloated GUIs.
- Creator of git-donkey & TimeOtter
- OSS Software Engineer - 8gears AG
- Core Contributor of Harbor Container Registry (CNCF)

What We’ll See in This Talk

BTW don't run JS/TS on server

- What is Container Security
- Why does it matter?
- Vim: the only editor that matters
- Build Secure Container
- Best Practices

What We’ll See in This Talk

BTW don't run JS/TS on server

- What is Container Security
- Why does it matter?
- Build Secure Container
- Best Practices
- Harbor & SBOMs - DEMO
- Do you actually need it?
- Announcements

What is Container Security

(Nobody cares)

- Containers are the foundation of modern apps. (Hi from GPT)
- Examples attacks

Why Security

(I don't want hackers in my house)

Building Secure Container

(Ah crap, here we go again)

- Let's Look at Principles

Principle 1: Reduce the attack surface

- Choose minimal base images

DEMO

- why you should use scratch as base image

Scratch > Distroless > Alpine > Normal Base Image

Principle 2: Be Specific about what you include

- TLDR; Be Explicit and define every dependencies
- Only include libraries you really need.
- Use Open Source or well maintained libraries/dependencies

Principle 3: Know what you are doing & Why

- Don't follow trends blindly
- Emphasize deliberate, conscious decisions based on your specific project requirements

Now to Harbor & SBOM

- SBOM: Software Bill of Materials (aka cookbook for deps)

Vulnerabilities

Who cares My app is working fine already

- No points (just too lazy to type)

Announcements

- TimeOtter v0.0.1 is Released
- DHAAS - Docker Hub as a Storage (next experiment)

Thanks for Attending!

You Made It Through... Somehow