

Vulnerability & Misconfiguration Scanner - Trivy



aqua
trivy

Agenda

- What did you do for your artifacts to ensure its security & configuration correct?
- What kind of concern are?
- Trivy - An vulnerability & misconfiguration scanner tool
- Difficult to use?
- Q&A

What did you do for your artifacts to ensure its security & configuration correct?

Docker Image

- Push image to registry directly

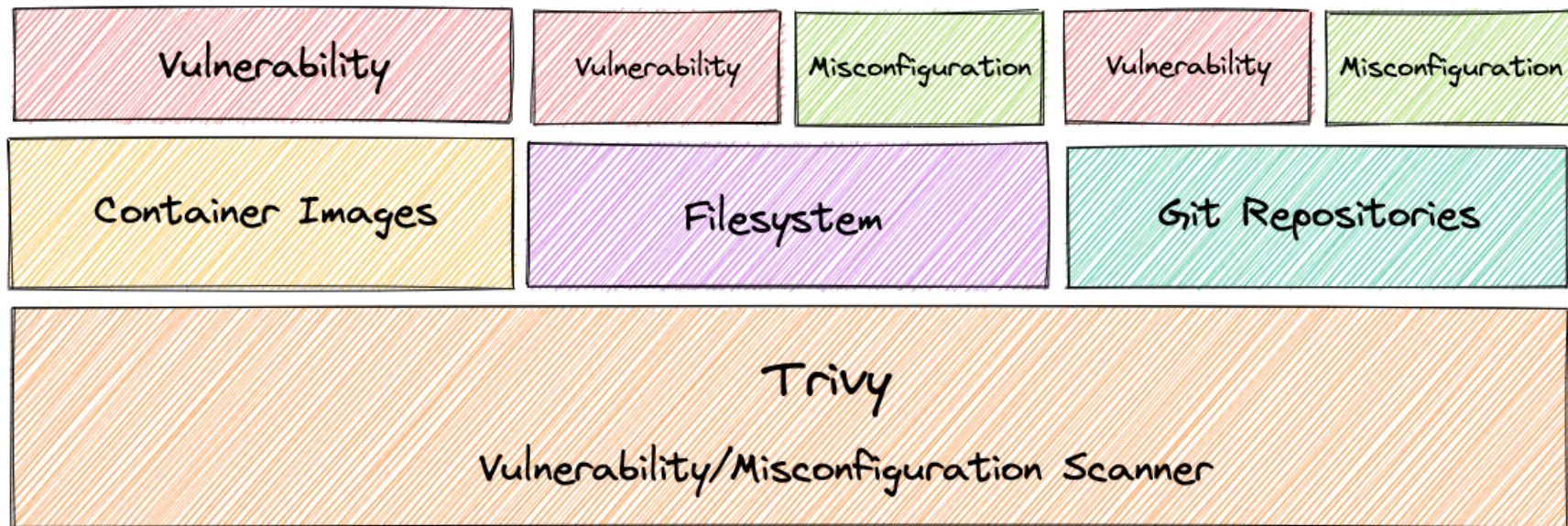
What kind of concern are?

Maybe

- Your base image has know/unfixed vulnerabilities
- Your artifacts contains some wrong config
- Your write some backdoor unconsciously
- ...

Trivy - An vulnerability & misconfiguration scanner tool

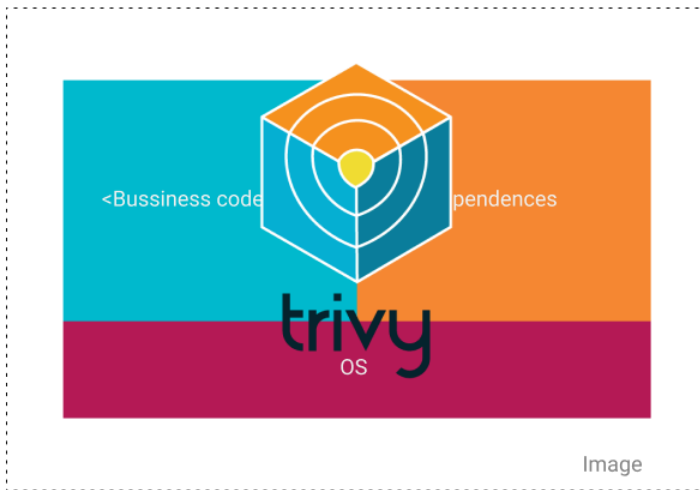
Capability



Working principle



1

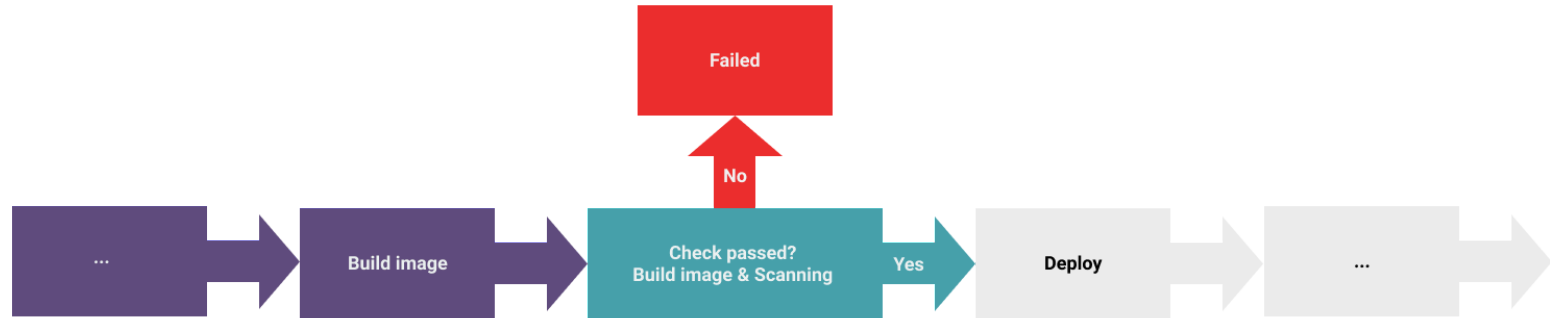


2

Difficult to use?

Talks is cheep, show me code

Pipeline



Image

```
docker run --rm -v \  
  /var/run/docker.sock:/var/run/docker.sock \  
  aquasec/trivy image \  
  --severity HIGH,CRITICAL \  
  --exit-code 1 \  
  dashboard:${{ github.sha }}
```

- [https://github.com/guzhongren/Buildkite-Dashboard/runs/4087037441?
check_suite_focus=true](https://github.com/guzhongren/Buildkite-Dashboard/runs/4087037441?check_suite_focus=true)

Repo

```
docker run --rm -v \  
  /var/run/docker.sock:/var/run/docker.sock \  
  aquasec/trivy repo \  
  --severity HIGH,CRITICAL \  
  --exit-code 1 \  
  https://github.com/guzhongren/Buildkite-Dashboard
```

- https://github.com/guzhongren/Buildkite-Dashboard/runs/4093499534?check_suite_focus=true

FS

```
docker run --rm -v \  
  /var/run/docker.sock:/var/run/docker.sock \  
  aquasec/trivy fs \  
  --severity HIGH,CRITICAL \  
  --exit-code 1 \  
  ./
```

- https://github.com/guzhongren/Buildkite-Dashboard/runs/4093499534?check_suite_focus=true

Config

```
docker run --rm -v \  
  /var/run/docker.sock:/var/run/docker.sock \  
  aquasec/trivy config \  
  --severity HIGH,CRITICAL \  
  --security-checks vuln,config \  
  --exit-code 1 \  
  ./
```

- [https://github.com/guzhongren/Buildkite-Dashboard/runs/4093499534?
check_suite_focus=true](https://github.com/guzhongren/Buildkite-Dashboard/runs/4093499534?check_suite_focus=true)

.trivyignore

CVE-2021-3711

- <https://github.com/guzhongren/Buildkite-Dashboard/blob/main/.trivyignore>

 main ▾

Buildkite-Dashboard / .trivyign



guzhongren fix(ci): fix trivy ✓

 1 contributor

1 lines (1 sloc) | 14 Bytes

1 CVE-2021-3711

Refs

- <https://aquasecurity.github.io/trivy>
- <https://github.com/aquasecurity/trivy>
- <http://guzhongren.github.io/2021/08/container-image-scanner-trivy/>
- ...

Q & A

Thank you!