

# Vulnerability & Misconfiguration Scanner - Trivy



aqua  
trivy

@guzhongren 2021-10

# 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

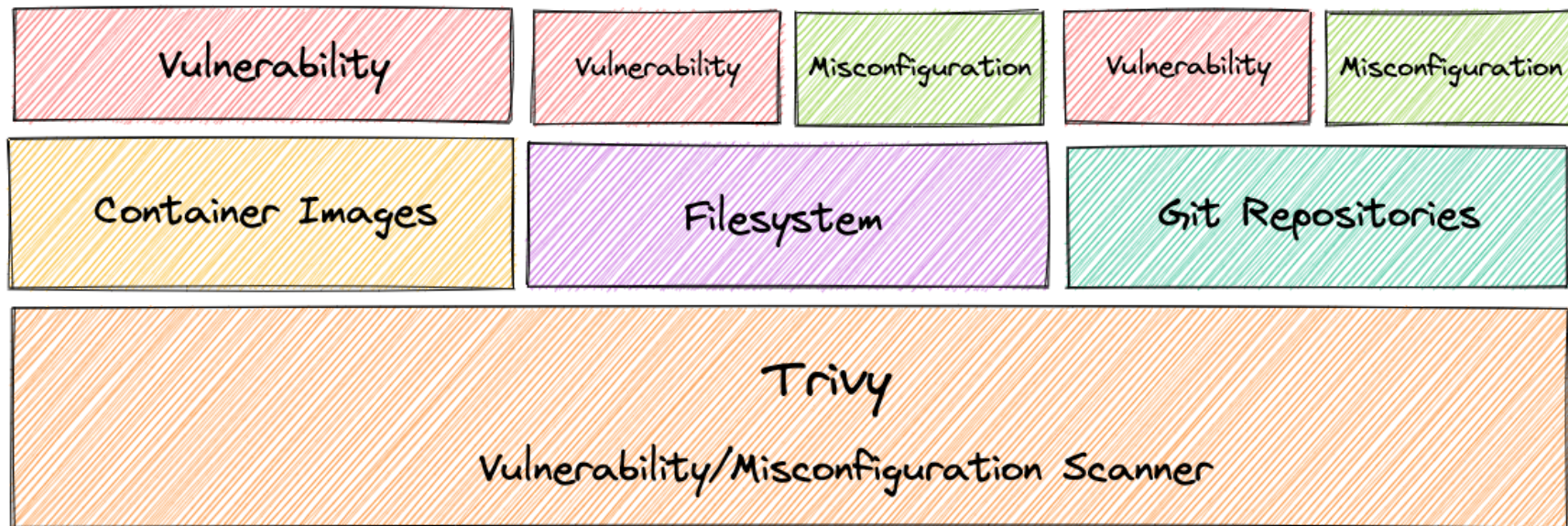
**What kind of concern are?**

# 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

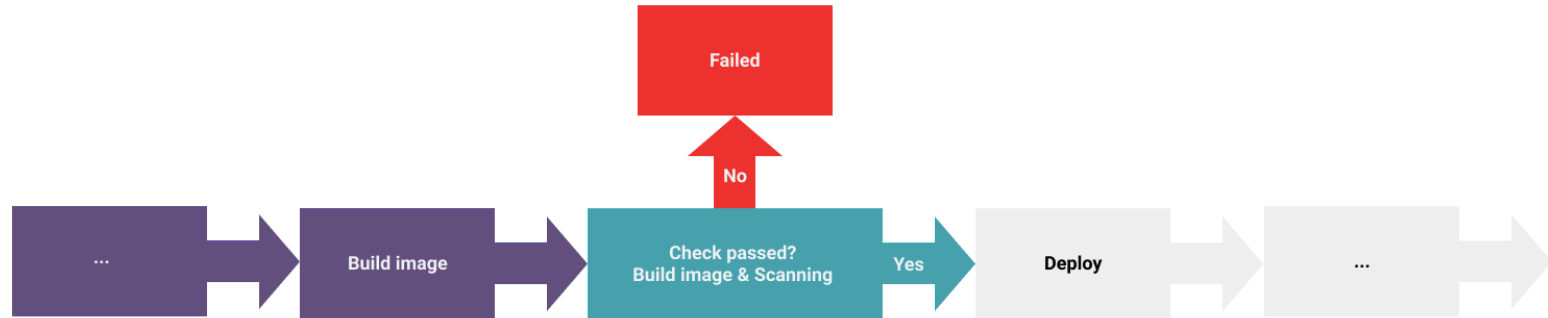


2

# 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.ref }}
```

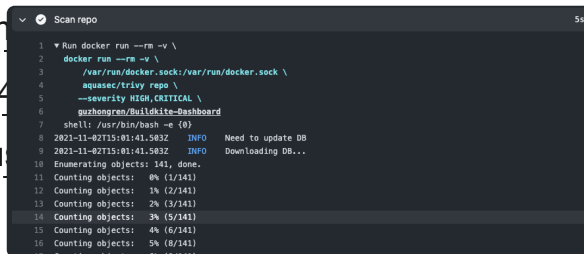
- <https://github.com/aquasecurity/trivy>
- Dashboard/runs/4
- check\_suite\_focus

```
Trivy scanner
1 Run docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \
2 docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \
3 aquasec/trivy image --severity HIGH,CRITICAL --exit-code 1
4 dashboard:dc266d8268f8589813d5d83797cebdfe72b7842
5 shell: /usr/bin/bash -e (0)
6 Unable to find image 'aquasec/trivy:latest' locally
7 latest: Pulling from aquasec/trivy
8 a0d8a0d46f8b: Already exists
9 bff55a771f2: Pulling fs layer
10 818276ee1efb: Pulling fs layer
11 c83f618988b2: Pulling fs layer
12 c83f618988b2: Verifying Checksum
13 c83f618988b2: Download complete
14 818276ee1efb: Verifying Checksum
15 818276ee1efb: Download complete
16 bff55a771f2: Verifying Checksum
17 bff55a771f2: Download complete
18 bff55a771f2: Pull complete
19 818276ee1efb: Pull complete
20 c83f618988b2: Pull complete
21 Digest: sha256:14f0bec72d1f84bc5e2b08081865ce5831c14d41d4af571cd8a78fe3981e83
22 Status: Downloaded newer image for aquasec/trivy:latest
23 2021-11-03T00:21:02.723Z INFO Need to update DB
24 2021-11-03T00:21:02.723Z INFO Downloading DB...
25 2021-11-03T00:21:07.346Z INFO Detected OS: debian
26 2021-11-03T00:21:07.346Z INFO Detecting Debian vulnerabilities...
27 2021-11-03T00:21:07.367Z INFO Number of language-specific files: 0
28
29 dashboard:dc266d8268f8589813d5d83797cebdfe72b7842 (debian 10.11)
30 =====
31 Total: 30 (HIGH: 26, CRITICAL: 4)
32
33 +-----+
34 | LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |
35 +-----+
36 | curl | CVE-2021-22946 | HIGH | 7.64.0-4+deb10u2 | |
37 | | | | | |
38 | | | | | |
39 | | | | | |
40 | | | | | |
41 | | | | | |
42 | | | | | |
43 | | | | | |
44 | | | | | |
45 | | | | | |
46 | | | | | |
47 | | | | | |
48 | | | | | |
49 | | | | | |
50 | | | | | |
51 | | | | | |
52 | | | | | |
53 | | | | | |
54 | | | | | |
55 | | | | | |
56 | | | | | |
57 | | | | | |
58 | | | | | |
59 | | | | | |
60 | | | | | |
61 | | | | | |
62 | | | | | |
63 | | | | | |
64 | | | | | |
65 | | | | | |
66 | | | | | |
67 | | | | | |
68 | | | | | |
69 | | | | | |
70 | | | | | |
71 | | | | | |
72 | | | | | |
73 | | | | | |
74 | | | | | |
75 | | | | | |
76 | | | | | |
77 | | | | | |
78 | | | | | |
79 | | | | | |
80 | | | | | |
81 | | | | | |
82 | | | | | |
83 | | | | | |
84 | | | | | |
85 | | | | | |
86 | | | | | |
87 | | | | | |
88 | | | | | |
89 | | | | | |
90 | | | | | |
91 | | | | | |
92 | | | | | |
93 | | | | | |
94 | | | | | |
95 | | | | | |
96 | | | | | |
97 | | | | | |
98 | | | | | |
99 | | | | | |
100 | | | | | |
```

# 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/4141414141>  
check\_suite\_focus



```
Scan repo 5s  
1 Run docker run --rm -v \  
2 docker run --rm -v \  
3 /var/run/docker.sock:/var/run/docker.sock \  
4 aquasec/trivy repo \  
5 --severity HIGH,CRITICAL \  
6 guzhongren/Buildkite-Dashboard  
7 shell: /usr/bin/dash -e (0)  
8 2021-11-02T15:01:41.583Z INFO Need to update DB  
9 2021-11-02T15:01:41.583Z INFO Downloading DB...  
10 Enumerating objects: 141, done.  
11 Counting objects: 0% (1/141)  
12 Counting objects: 1% (2/141)  
13 Counting objects: 2% (3/141)  
14 Counting objects: 3% (5/141)  
15 Counting objects: 4% (6/141)  
16 Counting objects: 5% (8/141)  
17 Counting objects: 6% (9/141)
```

# 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](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/aquasecurity/trivy>  
Dashboard/runs/4  
check\_suite\_focus

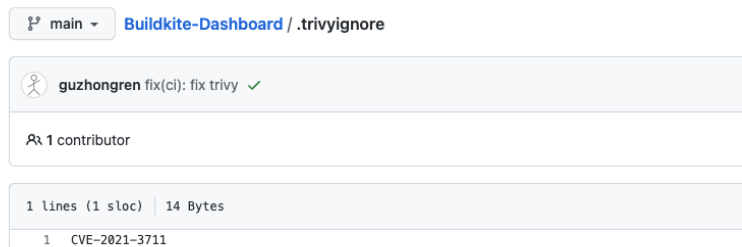


```
Scan config
1 Run docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \
2 docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \
3 aquasec/trivy fa \
4 --security-checks vuln,config \
5 --severity HIGH,CRITICAL \
6 ./
7 shell: /usr/bin/bash -e (x)
8 2021-11-05T00:10:40.200Z INFO Need to update DB
9 2021-11-05T00:10:40.200Z INFO Downloading DB...
10 2021-11-05T00:10:40.200Z INFO Need to update the built-in policies
11 2021-11-05T00:10:40.200Z INFO Downloading the built-in policies...
12 2021-11-05T00:10:40.200Z INFO Detected CVE: alpine
13 2021-11-05T00:10:40.200Z INFO Detecting Alpine vulnerabilities...
14 2021-11-05T00:10:40.200Z INFO Number of language-specific files: 0
15 2021-11-05T00:10:40.200Z INFO Detected config files: 0
16
17 f8de079505 (alpine 3.14.2)
18
19 Total: 0 (HIGH: 0, CRITICAL: 0)
20
21 2.52 MiB / 24.58 MiB [-----] 10.27% 7 p/s 75.47 MiB / 24.58 MiB [-----] 36.27%
22 7 p/s 73.40 MiB / 24.58 MiB [-----] 22.20% 7 p/s 78.52 MiB / 24.58 MiB [-----] 36.27%
23 7 p/s 73.40 MiB / 24.58 MiB [-----] 10.27% 17.68 MiB p/s ETA 0:01.79 MiB / 24.58 MiB [-----] 36.27%
24 71.99% 17.68 MiB p/s ETA 0:02.28 MiB / 24.58 MiB [-----] 98.29% 17.68 MiB p/s ETA 0:02.58 MiB
25 / 24.58 MiB [-----] 200.00% 22.14 MiB p/s 24
```

# .trivyignore

CVE-2021-3711

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





# 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!**