

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

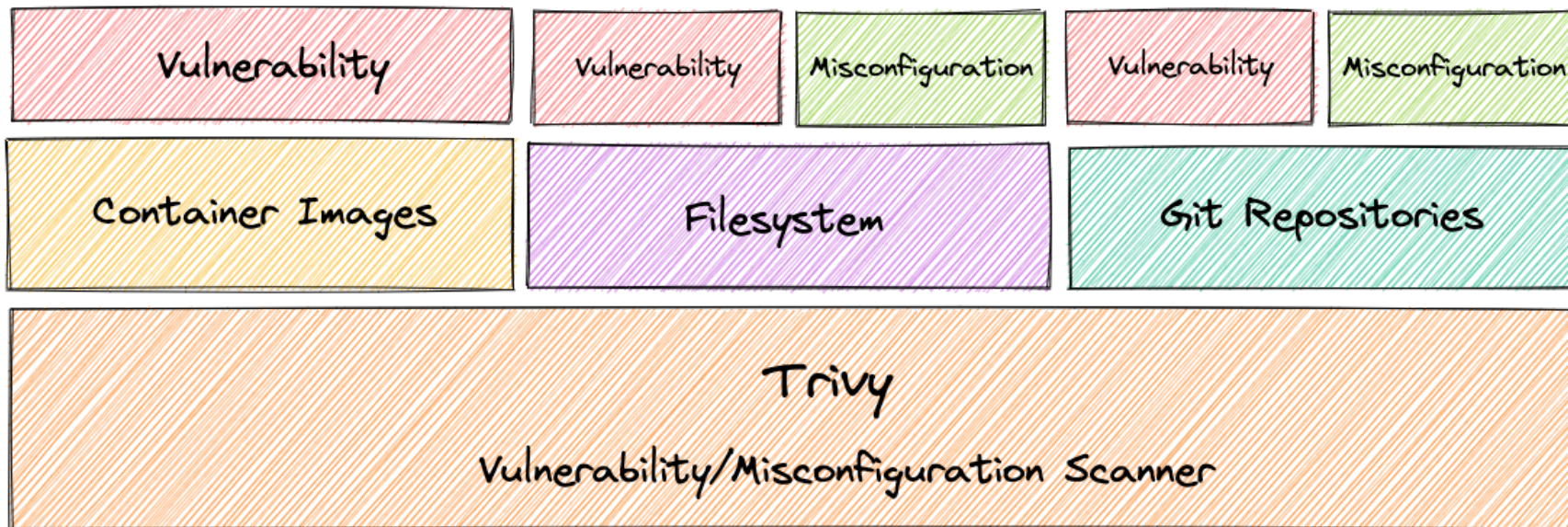
What kind of concern are?

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

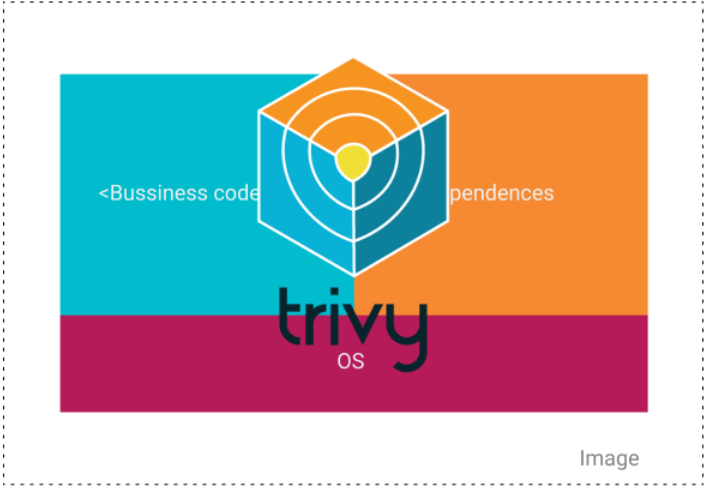
Capability



Working principle



1

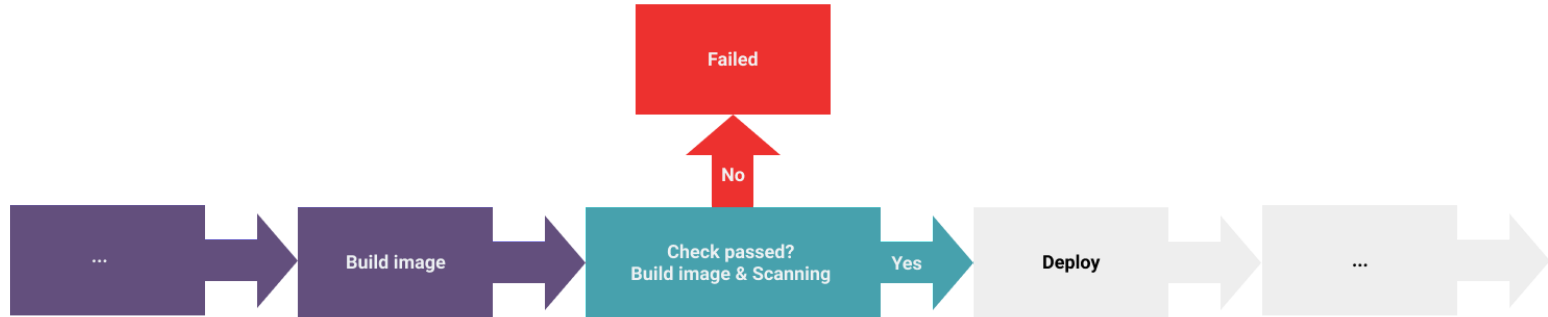


2

Difficult to use?

Talks is cheep, show me code

Pipeline



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

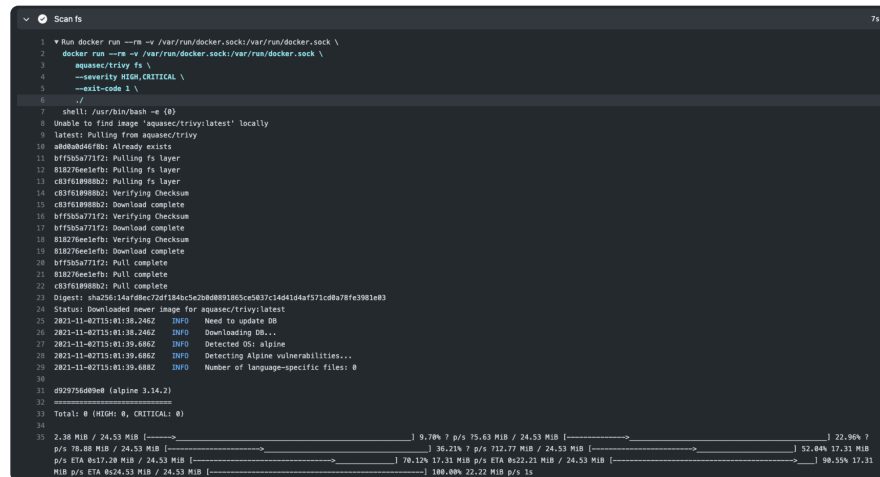
```
Scan repo 5s  
1  ▾ Run docker run --rm -v \  
2  docker run --rm -v \  
3  /var/run/docker.sock:/var/run/docker.sock \  
4  aquasec/trivy repo \  
5  --severity HIGH,CRITICAL \  
6  guzhongren/Buildkite-Dashboard  
7  shell: /usr/bin/bash -e {0}  
8  2021-11-02T15:01:41.503Z INFO Need to update DB  
9  2021-11-02T15:01:41.503Z 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)
```

```
Scan repo 5s  
219  
220 package-lock.json (npm)  
221 =====  
222 Total: 1 (HIGH: 1, CRITICAL: 0)  
223  
224 +-----+  
225 | LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION | TITLE  
226 |-----+  
227 | lodash | CVE-2021-23337 | HIGH | 4.17.19 | 4.17.21 | nodejs-lodash: command  
228 | | | | | | injection via template  
229 | | | | | | -->avd.aquasec.com/nvd/cve-2021-  
230 23337 |  
231 +-----+  
232 yarn.lock (yarn)  
233 =====  
234 Total: 2 (HIGH: 2, CRITICAL: 0)  
235  
236 +-----+  
237 | LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION | TITLE  
238 |-----+  
239 | ansi-regex | CVE-2021-3807 | HIGH | 3.0.0 | 5.0.1, 6.0.1 | nodejs-ansi-regex: Regular  
240 | | | | | | expression denial of service
```

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

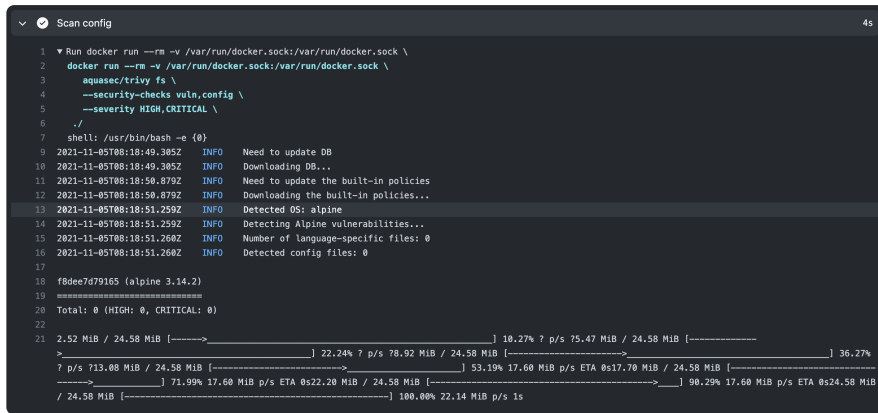


```
Scan fs  
1 Run docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \  
2 docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \  
3 aquasec/trivy fs \  
4 --severity HIGH,CRITICAL \  
5 --exit-code 1 \  
6 ./  
7 shell: /usr/bin/bash -e (0)  
8 Unable to find image 'aquasec/trivy:latest' locally  
9 latest: Pulling from aquasec/trivy  
10 sha256:0e0efb: Already exists  
11 bf950a771f2: Pulling fs layer  
12 818276ee1efb: Pulling fs layer  
13 cb3f618988b2: Pulling fs layer  
14 cb3f618988b2: Verifying Checksum  
15 cb3f618988b2: Download complete  
16 bf950a771f2: Verifying Checksum  
17 bf950a771f2: Download complete  
18 818276ee1efb: Verifying Checksum  
19 818276ee1efb: Download complete  
20 bf950a771f2: Pull complete  
21 818276ee1efb: Pull complete  
22 cb3f618988b2: Pull complete  
23 Digest: sha256:14af8dec72df184bc5e2b08091865c5037c146164af571cd0a78f9381e03  
24 Status: Downloaded newer image for aquasec/trivy:latest  
25 2021-11-02T13:01:38.246Z INFO Need to update DB  
26 2021-11-02T13:01:38.246Z INFO Downloading DB...  
27 2021-11-02T13:01:39.688Z INFO Detected OS: alpine  
28 2021-11-02T13:01:39.688Z INFO Detecting alpine vulnerabilities...  
29 2021-11-02T13:01:39.688Z INFO Number of language-specific files: 0  
30  
31 #92975660ee [alpine 3.14.2]  
32 =====  
33 Total: 0 (HIGH: 0, CRITICAL: 0)  
34  
35 2.38 MiB / 24.53 MiB [-----] 9.70% ? p/s 75.63 MiB / 24.53 MiB [-----] 22.90% ?  
p/s 78.68 MiB / 24.53 MiB [-----] 36.21% ? p/s 712.77 MiB / 24.53 MiB [-----] 52.04% 17.31 MiB  
p/s ETA 0s17.28 MiB / 24.53 MiB [-----] 70.12% 17.31 MiB p/s ETA 0s22.21 MiB / 24.53 MiB [-----] 98.55% 17.31  
MiB p/s ETA 0s24.53 MiB / 24.53 MiB [-----] 100.00% 22.22 MiB p/s 1s
```

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)




```
45  
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 fs \  
4       --severity HIGH,CRITICAL \  
5       --security-checks vuln,config \  
6       --severity HIGH,CRITICAL \  
7     ./ \  
8   shell: /usr/bin/bash -e {0}  
9 2021-11-05T08:18:49.385Z   INFO   Need to update DB  
10 2021-11-05T08:18:49.385Z  INFO   Downloading DB...  
11 2021-11-05T08:18:50.879Z   INFO   Need to update the built-in policies  
12 2021-11-05T08:18:50.879Z  INFO   Downloading the built-in policies...  
13 2021-11-05T08:18:51.259Z  INFO   Detected OS: alpine  
14 2021-11-05T08:18:51.259Z  INFO   Detecting Alpine vulnerabilities...  
15 2021-11-05T08:18:51.260Z  INFO   Number of language-specific files: 0  
16 2021-11-05T08:18:51.260Z  INFO   Detected config files: 0  
17  
18 fbdee7d79165 (alpine 3.14.2)  
19 =====  
20 Total: 0 (HIGH: 0, CRITICAL: 0)  
21  
22  
23  
24 2.52 MiB / 24.58 MiB [-----] 10.27% ? p/s 75.47 MiB / 24.58 MiB [-----]  
25  
26 ? p/s 713.08 MiB / 24.58 MiB [-----] 22.24% ? p/s 78.92 MiB / 24.58 MiB [-----] 36.27%  
27  
28 -----  
29 71.99% 17.60 MiB p/s ETA 0s22.20 MiB / 24.58 MiB [-----] 53.19% 17.60 MiB p/s ETA 0s17.70 MiB / 24.58 MiB [-----]  
30 / 24.58 MiB [-----] 100.00% 22.14 MiB p/s 1s
```

.trivyignore

CVE - 2021 - 3711

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

main ▾ Buildkite-Dashboard / .trivyignore

 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!