

Vulnerability & Misconfiguration Scanner - Trivy

2021-10@Guzhongren



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

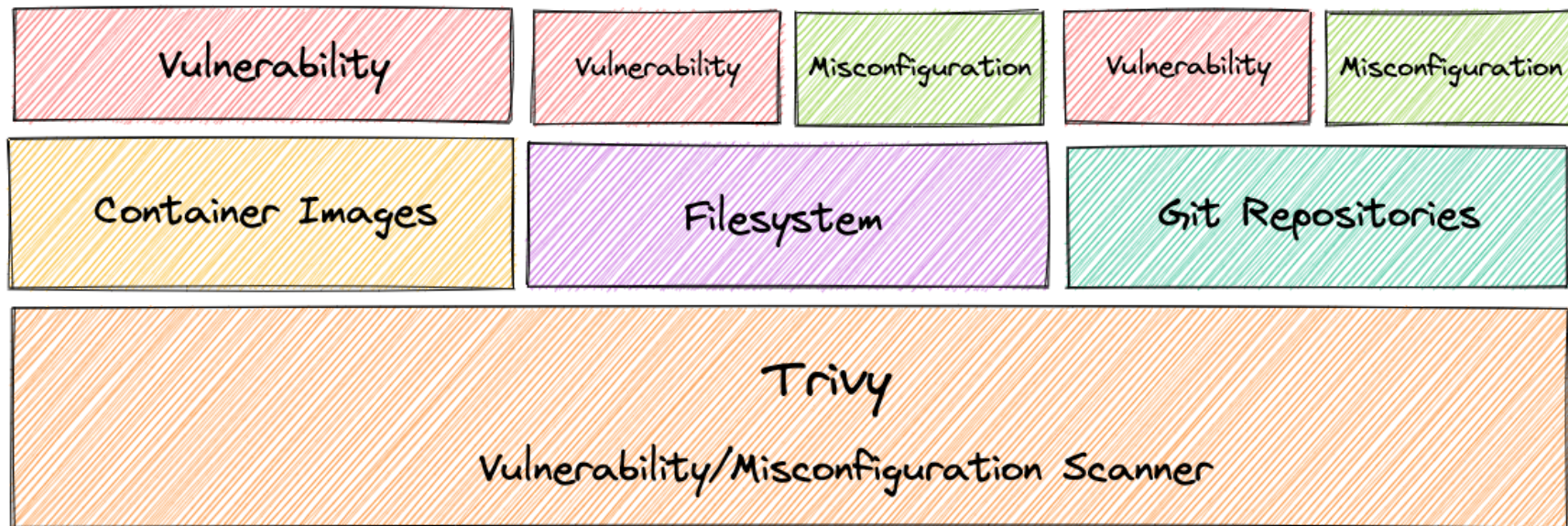
What kind of concern are?

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

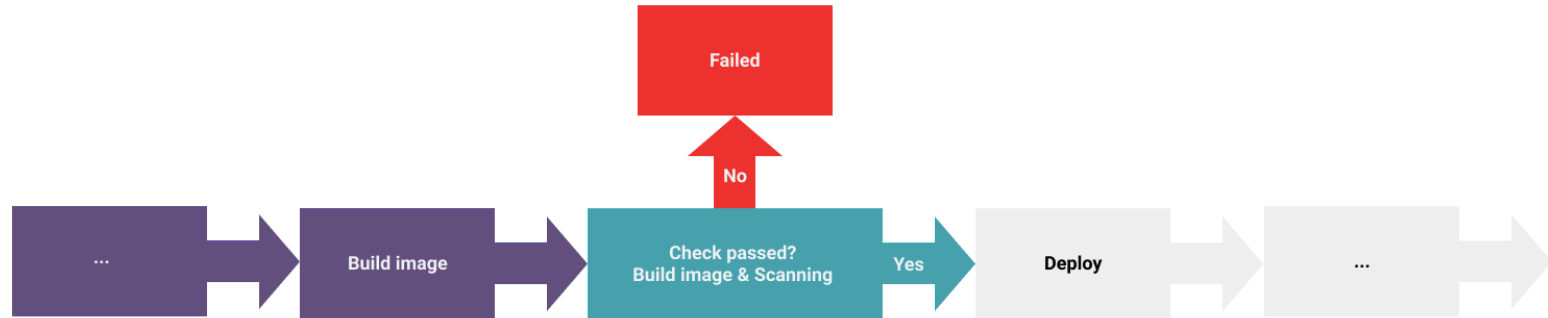


2

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

```

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:dc266d0260f05098138d5b03797cebdfe72b7842
5  shell: /usr/bin/bash -e {0}
6  Unable to find image 'aquasec/trivy:latest' locally
7  latest: Pulling from aquasec/trivy
8  a0d0a0d46f8b: Already exists
9  bff5b5a771f2: Pulling fs layer
10 818276ee1efb: Pulling fs layer
11 c83f610988b2: Pulling fs layer
12 c83f610988b2: Verifying Checksum
13 c83f610988b2: Download complete
14 818276ee1efb: Verifying Checksum
15 818276ee1efb: Download complete
16 bff5b5a771f2: Verifying Checksum
17 bff5b5a771f2: Download complete
18 bff5b5a771f2: Pull complete
19 818276ee1efb: Pull complete
20 c83f610988b2: Pull complete
21 Digest: sha256:14afd8ec72df184bc5e2b0d0891865ce5037c14d41d4af571cd0a78fe3981e03
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:dc266d0260f05098138d5b03797cebdfe72b7842 (debian 10.11)
30 =====
31 Total: 30 (HIGH: 26, CRITICAL: 4)
32
33 +-----+-----+-----+-----+-----+
34 | LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |
35 | TITLE | | | | |
36 +-----+-----+-----+-----+-----+
37 | curl | CVE-2021-22946 | HIGH | 7.64.0-4+deb10u2 | | curl: Requirement to use
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 | | | | | |
101 | | | | | |
102 | | | | | |
103 | | | | | |
104 | | | | | |
105 | | | | | |
106 | | | | | |
107 | | | | | |
108 | | | | | |
109 | | | | | |
110 | | | | | |
111 | | | | | |
112 | | | | | |
113 | | | | | |
114 | | | | | |
115 | | | | | |
116 | | | | | |
117 | | | | | |
118 | | | | | |
119 | | | | | |
120 | | | | | |
121 | | | | | |
122 | | | | | |
123 | | | | | |
124 | | | | | |
125 | | | | | |
126 | | | | | |
127 | | | | | |
128 | | | | | |
129 | | | | | |
130 | | | | | |
131 | | | | | |
132 | | | | | |
133 | | | | | |
134 | | | | | |
135 | | | | | |
136 | | | | | |
137 | | | | | |
138 | | | | | |
139 | | | | | |
140 | | | | | |
141 | | | | | |
142 | | | | | |
143 | | | | | |
144 | | | | | |
145 | | | | | |
146 | | | | | |
147 | | | | | |
148 | | | | | |
149 | | | | | |
150 | | | | | |
151 | | | | | |
152 | | | | | |
153 | | | | | |
154 | | | | | |
155 | | | | | |
156 | | | | | |
157 | | | | | |
158 | | | | | |
159 | | | | | |
160 | | | | | |
161 | | | | | |
162 | | | | | |
163 | | | | | |
164 | | | | | |
165 | | | | | |
166 | | | | | |
167 | | | | | |
168 | | | | | |
169 | | | | | |
170 | | | | | |
171 | | | | | |
172 | | | | | |
173 | | | | | |
174 | | | | | |
175 | | | | | |
176 | | | | | |
177 | | | | | |
178 | | | | | |
179 | | | | | |
180 | | | | | |
181 | | | | | |
182 | | | | | |
183 | | | | | |
184 | | | | | |
185 | | | | | |
186 | | | | | |
187 | | | | | |
188 | | | | | |
189 | | | | | |
190 | | | | | |
191 | | | | | |
192 | | | | | |
193 | | | | | |
194 | | | | | |
195 | | | | | |
196 | | | | | |
197 | | | | | |
198 | | | | | |
199 | | | | | |
200 | | | | | |
201 | | | | | |
202 | | | | | |
203 | | | | | |
204 | | | | | |
205 | | | | | |
206 | | | | | |
207 | | | | | |
208 | | | | | |
209 | | | | | |
210 | | | | | |
211 | | | | | |
212 | | | | | |
213 | | | | | |
214 | | | | | |
215 | | | | | |
216 | | | | | |
217 | | | | | |
218 | | | | | |
219 | | | | | |
220 | | | | | |
221 | | | | | |
222 | | | | | |
223 | | | | | |
224 | | | | | |
225 | | | | | |
226 | | | | | |
227 | | | | | |
228 | | | | | |
229 | | | | | |
230 | | | | | |
231 | | | | | |
232 | | | | | |
233 | | | | | |
234 | | | | | |
235 | | | | | |
236 | | | | | |
237 | | | | | |
238 | | | | | |
239 | | | | | |
240 | | | | | |
241 | | | | | |
242 | | | | | |
243 | | | | | |
244 | | | | | |
245 | | | | | |
246 | | | | | |
247 | | | | | |
248 | | | | | |
249 | | | | | |
250 | | | | | |
251 | | | | | |
252 | | | | | |
253 | | | | | |
254 | | | | | |
255 | | | | | |
256 | | | | | |
257 | | | | | |
258 | | | | | |
259 | | | | | |
260 | | | | | |
261 | | | | | |
262 | | | | | |
263 | | | | | |
264 | | | | | |
265 | | | | | |
266 | | | | | |
267 | | | | | |
268 | | | | | |
269 | | | | | |
270 | | | | | |
271 | | | | | |
272 | | | | | |
273 | | | | | |
274 | | | | | |
275 | | | | | |
276 | | | | | |
277 | | | | | |
278 | | | | | |
279 | | | | | |
280 | | | | | |
281 | | | | | |
282 | | | | | |
283 | | | | | |
284 | | | | | |
285 | | | | | |
286 | | | | | |
287 | | | | | |
288 | | | | | |
289 | | | | | |
290 | | | | | |
291 | | | | | |
292 | | | | | |
293 | | | | | |
294 | | | | | |
295 | | | | | |
296 | | | | | |
297 | | | | | |
298 | | | | | |
299 | | | | | |
300 | | | | | |
301 | | | | | |
302 | | | | | |
303 | | | | | |
304 | | | | | |
305 | | | | | |
306 | | | | | |
307 | | | | | |
308 | | | | | |
309 | | | | | |
310 | | | | | |
311 | | | | | |
312 | | | | | |
313 | | | | | |
314 | | | | | |
315 | | | | | |
316 | | | | | |
317 | | | | | |
318 | | | | | |
319 | | | | | |
320 | | | | | |
321 | | | | | |
322 | | | | | |
323 | | | | | |
324 | | | | | |
325 | | | | | |
326 | | | | | |
327 | | | | | |
328 | | | | | |
329 | | | | | |
330 | | | | | |
331 | | | | | |
332 | | | | | |
333 | | | | | |
334 | | | | | |
335 | | | | | |
336 | | | | | |
337 | | | | | |
338 | | | | | |
339 | | | | | |
340 | | | | | |
341 | | | | | |
342 | | | | | |
343 | | | | | |
344 | | | | | |
345 | | | | | |
346 | | | | | |
347 | | | | | |
348 | | | | | |
349 | | | | | |
350 | | | | | |
351 | | | | | |
352 | | | | | |
353 | | | | | |
354 | | | | | |
355 | | | | | |
356 | | | | | |
357 | | | | | |
358 | | | | | |
359 | | | | | |
360 | | | | | |
361 | | | | | |
362 | | | | | |
363 | | | | | |
364 | | | | | |
365 | | | | | |
366 | | | | | |
367 | | | | | |
368 | | | | | |
369 | | | | | |
370 | | | | | |
371
```

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

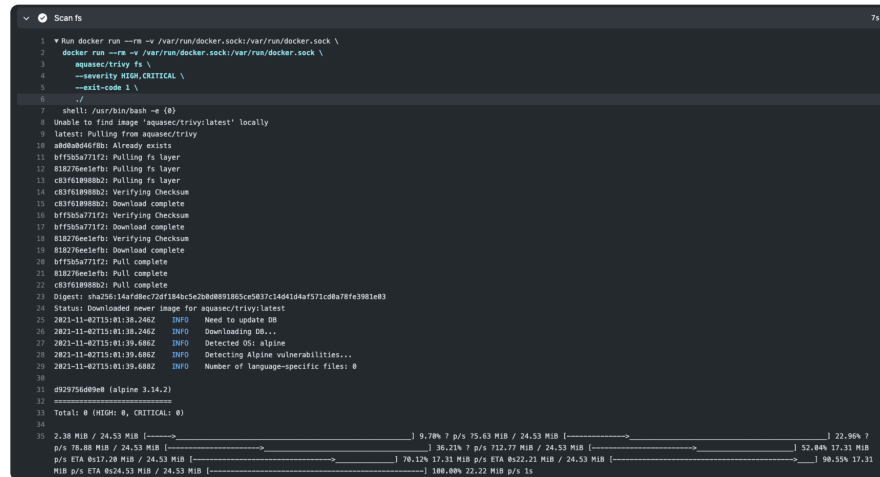
```
Scan repo 5s
1  Run docker run --rm -v \
2  docker run --rm -v \
3    /var/run/docker.sock:/var/run/docker.sock \
4    aquasec/trivy repo \
5    --severity HIGH,CRITICAL \
6    guzhongren/Buildkite-Dashboard
7  shell: /usr/bin/bash -e {0}
8  2021-11-02T15:01:41.503Z INFO Need to update DB
9  2021-11-02T15:01:41.503Z 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 package-lock.json (npm)
220 =====
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-2021-23337 |
230 +-----+
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

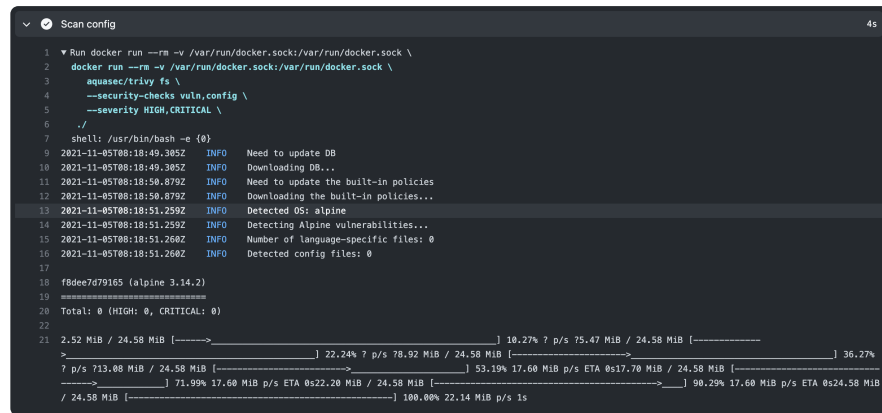


```
1 Run docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \
2   docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \
3   aquasec/trivy fs \
4   --severity HIGH,CRITICAL \
5   --exit-code 1 \
6   ./
7 shell: /usr/bin/bash -e (8)
8 Unable to find image 'aquasec/trivy:latest' locally
9 latest: Pulling from aquasec/trivy
10 sha256:0e0f0b: Already exists
11 bf935a771f2: Pulling fs layer
12 818276ee1efb: Pulling fs layer
13 cb3fe18988b2: Pulling fs layer
14 cb3fe18988b2: Verifying Checksum
15 cb3fe18988b2: Download complete
16 bf935a771f2: Verifying Checksum
17 bf935a771f2: Download complete
18 818276ee1efb: Verifying Checksum
19 818276ee1efb: Download complete
20 bf935a771f2: Pull complete
21 818276ee1efb: Pull complete
22 cb3fe18988b2: Pull complete
23 Digest: sha256:14af8ec72df184bc5e2b0d891865c5837c14041eaf571cd0a78fe3981e03
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 2021-11-02T13:01:39.686Z INFO Detected OS: alpine
28 2021-11-02T13:01:39.686Z INFO Detecting alpine vulnerabilities...
29 2021-11-02T13:01:39.686Z INFO Number of language-specific files: 0
30
31 #020736d09eb (alpine 3.14.2)
32 =====
33 Total: 0 (HIGH: 0, CRITICAL: 0)
34
35 2.38 MiB / 24.53 MiB [-----] 9.70% 7 p/s 75.63 MiB / 24.53 MiB [-----] 22.90% 7
36 p/s 78.68 MiB / 24.53 MiB [-----] 36.21% 7 p/s 712.77 MiB / 24.53 MiB [-----] 52.84% 17.31 MiB
37 p/s ETA 0s17.28 MiB / 24.53 MiB [-----] 70.12% 17.31 MiB p/s ETA 0s22.21 MiB / 24.53 MiB [-----] 90.55% 17.31
38 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?](https://github.com/guzhongren/Buildkite-Dashboard/runs/4093499534?check_suite_focus=true)





```
▼ Scan config 4s
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       --security-checks vuln,config \
5       --severity HIGH,CRITICAL \
6       ./
7   shell: /usr/bin/bash -e {0}
8   2021-11-05T08:18:49.385Z   INFO   Need to update DB
9   2021-11-05T08:18:49.385Z   INFO   Downloading DB...
10  2021-11-05T08:18:50.879Z   INFO   Need to update the built-in policies
11  2021-11-05T08:18:50.879Z   INFO   Downloading the built-in policies...
12  2021-11-05T08:18:51.239Z   INFO   Detected OS: alpine
13  2021-11-05T08:18:51.239Z   INFO   Detecting Alpine vulnerabilities...
14  2021-11-05T08:18:51.260Z   INFO   Number of language-specific files: 0
15  2021-11-05T08:18:51.260Z   INFO   Detected config files: 0
16
17  fbdee7d79165 (alpine 3.14.2)
18  =====
19  Total: 0 (HIGH: 0, CRITICAL: 0)
20
21  2.52 MiB / 24.58 MiB [-----] 10.27% ? p/s 75.47 MiB / 24.58 MiB [-----] 36.27%
22
23  ? p/s 713.00 MiB / 24.58 MiB [-----] 53.19% 17.60 MiB p/s ETA 0s17.70 MiB / 24.58 MiB [-----] 90.29% 17.60 MiB p/s ETA 0s24.58 MiB
24  / 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!