

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

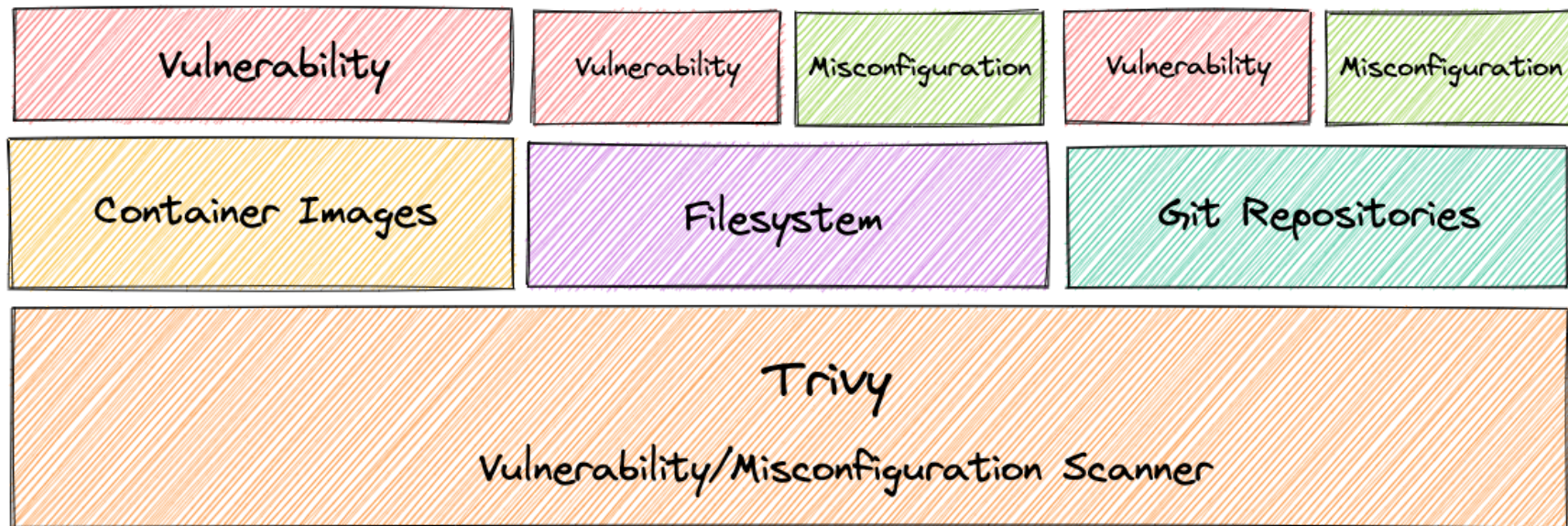
What kind of concern are?

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

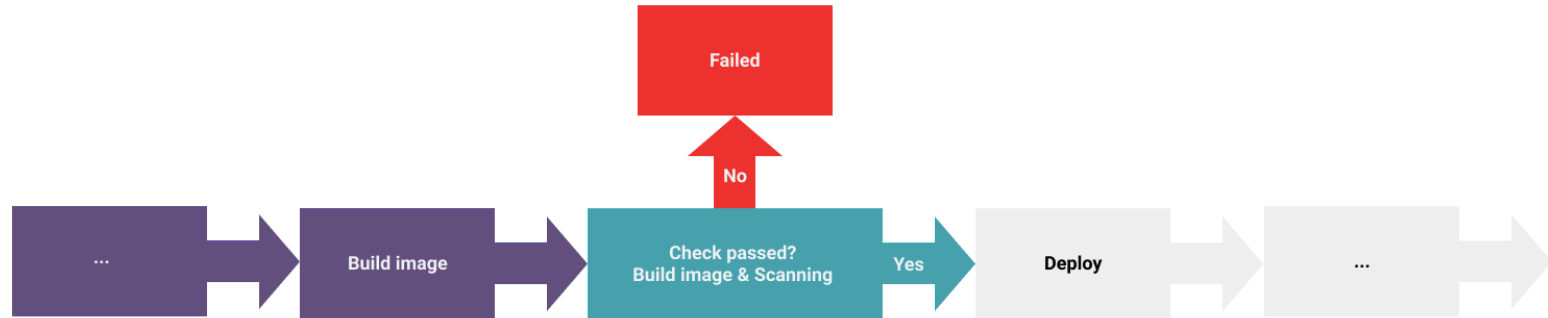


2

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: sha256:14f0bec72d1f14bc5e2b08081865ce5831c14d41d4af571cd8a78fe3981e83
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 2021-11-03T00:21:07.307Z 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 | TITLE |
36 +-----+
37 | curl | CVE-2021-22946 | HIGH | 7.64.0-4+deb10u2 | |
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 | |
372 | |
373 | |
374 | |
375 | |
376 | |
377 | |
378 | |
379 | |
380 | |
381 | |
382 | |
383 | |
384 | |
385 | |
386 | |
387 | |
388 | |
389 | |
390 | |
391 | |
392 | |
393 | |
394 | |
395 | |
396 | |
397 | |
398 | |
399 | |
400 | |
401 | |
402 | |
403 | |
404 | |
405 | |
406 | |
407 | |
408 | |
409 | |
410 | |
411 | |
412 | |
413 | |
414 | |
415 | |
416 | |
417 | |
418 | |
419 | |
420 | |
421 | |
422 | |
423 | |
424 | |
425 | |
426 | |
427 | |
428 | |
429 | |
430 | |
431 | |
432 | |
433 | |
434 | |
435 | |
436 | |
437 | |
438 | |
439 | |
440 | |
441 | |
442 | |
443 | |
444 | |
445 | |
446 | |
447 | |
448 | |
449 | |
450 | |
451 | |
452 | |
453 | |
454 | |
455 | |
456 | |
457 | |
458 | |
459 | |
460 | |
461 | |
462 | |
463 | |
464 | |
465 | |
466 | |
467 | |
468 | |
469 | |
470 | |
471 | |
472 | |
473 | |
474 | |
475 | |
476 | |
477 | |
478 | |
479 | |
480 | |
481 | |
482 | |
483 | |
484 | |
485 | |
486 | |
487 | |
488 | |
489 | |
490 | |
491 | |
492 | |
493 | |
494 | |
495 | |
496 | |
497 | |
498 | |
499 | |
500 | |
501 | |
502 | |
503 | |
504 | |
505 | |
506 | |
507 | |
508 | |
509 | |
510 | |
511 | |
512 | |
513 | |
514 | |
515 | |
516 | |
517 | |
518 | |
519 | |
520 | |
521 | |
522 | |
523 | |
524 | |
525 | |
526 | |
527 | |
528 | |
529 | |
530 | |
531 | |
532 | |
533 | |
534 | |
535 | |
536 | |
537 | |
538 | |
539 | |
540 | |
541 | |
542 | |
543 | |
544 | |
545 | |
546 | |
547 | |
548 | |
549 | |
550 | |
551 | |
552 | |
553 | |
554 | |
555 | |
556 | |
557 | |
558 | |
559 | |
560 | |
561 | |
562 | |
563 | |
564 | |
565 | |
566 | |
567 | |
568 | |
569 | |
570 | |
571 | |
572 | |
573 | |
574 | |
575 | |
576 | |
577 | |
578 | |
579 | |
580 | |
581 | |
582 | |
583 | |
584 | |
585 | |
586 | |
587 | |
588 | |
589 | |
590 | |
591 | |
592 | |
593 | |
594 | |
595 | |
596 | |
597 | |
598 | |
599 | |
600 | |
601 | |
602 | |
603 | |
604 | |
605 | |
606 | |
607 | |
608 | |
609 | |
610 | |
611 | |
612 | |
613 | |
614 | |
615 | |
616 | |
617 | |
618 | |
619 | |
620 | |
621 | |
622 | |
623 | |
624 | |
625 | |
626 | |
627 | |
628 | |
629 | |
630 | |
631 | |
632 | |
633 | |
634 | |
635 | |
636 | |
637 | |
638 | |
639 | |
640 | |
641 | |
642 | |
643 | |
644 | |
645 | |
646 | |
647 | |
648 | |
649 | |
650 | |
651 | |
652 | |
653 | |
654 | |
655 | |
656 | |
657 | |
658 | |
659 | |
660 | |
661 | |
662 | |
663 | |
664 | |
665 | |
666 | |
667 | |
668 | |
669 | |
670 | |
671 | |
672 | |
673 | |
674 | |
675 | |
676 | |
677 | |
678 | |
679 | |
680 | |
681 | |
682 | |
683 | |
684 | |
685 | |
686 | |
687 | |
688 | |
689 | |
690 | |
691 | |
692 | |
693 | |
694 | |
695 | |
696 | |
697 | |
698 | |
699 | |
700 | |
701 | |
702 | |
703 | |
704 | |
705 | |
706 | |
707 | |
708 | |
709 | |
710 | |
711 | |
712 | |
713 | |
714 | |
715 | |
716 | |
717 | |
718 | |
719 | |
720 | |
721 | |
722 | |
723 | |
724 | |
725 | |
726 | |
727 | |
728 | |
729 | |
730 | |
731 | |
732 | |
733 | |
734 | |
735 | |
736 | |
737 | |
738 | |
739 | |
740 | |
741 | |
742 | |
743 | |
744 | |
745 | |
746 | |
747 | |
748 | |
749 | |
750 | |
751 | |
752 | |
753 | |
754 | |
755 | |
756 | |
757 | |
758 | |
759 | |
760 | |
761 | |
762 | |
763 | |
764 | |
765 | |
766 | |
767 | |
768 | |
769 | |
770 | |
771 | |
772 | |
773 | |
774 | |
775 | |
776 | |
777 | |
778 | |
779 | |
780 | |
781 | |
782 | |
783 | |
784 | |
785 | |
786 | |
787 | |
788 | |
789 | |
790 | |
791 | |
792 | |
793 | |
794 | |
795 | |
796 | |
797 | |
798 | |
799 | |
800 | |
801 | |
802 | |
803 | |
804 | |
805 | |
806 | |
807 | |
808 | |
809 | |
810 | |
811 | |
812 | |
813 | |
814 | |
815 | |
816 | |
817 | |
818 | |
819 | |
820 | |
821 | |
822 | |
823 | |
824 | |
825 | |
826 | |
827 | |
828 | |
829 | |
830 | |
831 | |
832 | |
833 | |
834 | |
835 | |
836 | |
837 | |
838 | |
839 | |
840 | |
841 | |
842 | |
843 | |
844 | |
845 | |
846 | |
847 | |
848 | |
849 | |
850 | |
851 | |
852 | |
853 | |
854 | |
855 | |
856 | |
857 | |
858 | |
859 | |
860 | |
861 | |
862 | |
863 | |
864 | |
865 | |
866 | |
867 | |
868 | |
869 | |
870 | |
871 | |
872 | |
873 | |
874 | |
875 | |
876 | |
877 | |
878 | |
879 | |
880 | |
881 | |
882 | |
883 | |
884 | |
885 | |
886 | |
887 | |
888 | |
889 | |
890 | |
891 | |
892 | |
893 | |
894 | |
895 | |
896 | |
897 | |
898 | |
899 | |
900 | |
901 | |
902 | |
903 | |
904 | |
905 | |
906 | |
907 | |
908 | |
909 | |
910 | |
911 | |
912 | |
913 | |
914 | |
915 | |
916 | |
917 | |
918 | |
919 | |
920 | |
921 | |
922 | |
923 | |
924 | |
925 | |
926 | |
927 | |
928 | |
929 | |
930 | |
931 | |
932 | |
933 | |
934 | |
935 | |
936 | |
937 | |
938 | |
939 | |
940 | |
941 | |
942 | |
943 | |
944 | |
945 | |
946 | |
947 | |
948 | |
949 | |
950 | |
951 | |
952 | |
953 | |
954 | |
955 | |
956 | |
957 | |
958 | |
959 | |
960 | |
961 | |
962 | |
963 | |
964 | |
965 | |
966 | |
967 | |
968 | |
969 | |
970 | |
971 | |
972 | |
973 | |
974 | |
975 | |
976 | |
977 | |
978 | |
979 | |
980 | |
981 | |
982 | |
983 | |
984 | |
985 | |
986 | |
987 | |
988 | |
989 | |
990 | |
991 | |
992 | |
993 | |
994 | |
995 | |
996 | |
997 | |
998 | |
999 | |
1000 | |
```

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/g
```

- <https://github.com/aquasecurity/trivy>
Dashboard/runs/4
check_suite_focus

Scan repo

219 package-lock.json (npm)
220 =====
221 Total: 1 (HIGH: 1, CRITICAL: 0)
222
223
224

LIBRARY	VULNERABILITY ID	SEVERITY	INSTALLED VERSION	FIXED VERSION	TITLE
lodash	CVE-2021-23337	HIGH	4.17.19	4.17.21	nodejs-lodash: command injection via template

225
226
227
228
229
230

231 yarn.lock (yarn)
232 =====
233 Total: 2 (HIGH: 2, CRITICAL: 0)
234
235
236

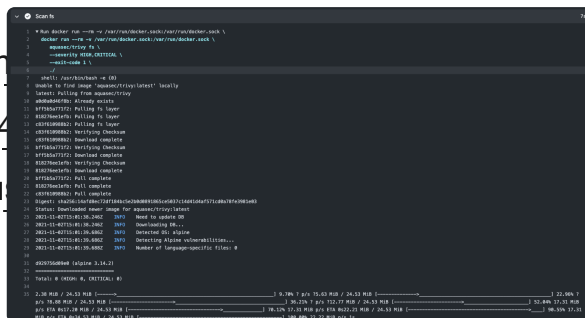
LIBRARY	VULNERABILITY ID	SEVERITY	INSTALLED VERSION	FIXED VERSION	TITLE
ansi-regex	CVE-2021-3887	HIGH	3.0.0	5.0.1, 6.0.1	nodejs-ansi-regex: Regular expression denial of service (ReDoS) matching ANSI escape codes

237
238
239
240
241
242
243
244

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/GoogleCloudPlatform/terraform-google-cloud-antenna/blob/master/.github/workflows/check_suite_focus.yml



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

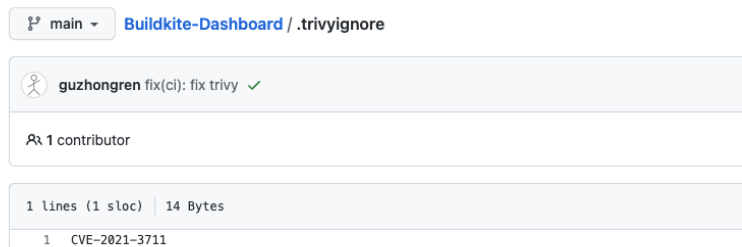


```
Scan config
1 Run docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \
2 docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \
3 aquasec/trivy fa \
4 --security-checks vuln,config \
5 --severity HIGH,CRITICAL \
6 ./
7 shell: /usr/bin/bash -e
8 2021-11-05T00:18:49.280Z INFO Need to update DB
9 2021-11-05T00:18:49.380Z INFO Downloading DB...
10 2021-11-05T00:18:50.479Z INFO Need to update the built-in policies
11 2021-11-05T00:18:50.479Z INFO Downloading the built-in policies...
12 2021-11-05T00:18:51.280Z INFO Detected CVE: alpine
13 2021-11-05T00:18:51.280Z INFO Detecting alpine vulnerabilities...
14 2021-11-05T00:18:51.280Z INFO Number of language-specific files: 0
15 2021-11-05T00:18:51.280Z INFO Detected config files: 0
16
17 f8dee0795105 (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 73.48 MiB / 24.58 MiB [-----] 30.12% 17.68 MiB p/s ETA 0:17.79 MiB / 24.58 MiB [-----] 71.99% 17.68 MiB p/s ETA 0:22.28 MiB / 24.58 MiB [-----] 98.29% 17.68 MiB p/s ETA 0:24.58 MiB
23 / 24.58 MiB [-----] 200.00% 22.14 MiB p/s 1s
```

.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!