**CONTAINER SCANNING**

Same tool for both CI/CD pipelines: **Trivy** -> <https://trivy.dev/latest/>

The tool has been chosen due to its easy implementation and easy troubleshooting.

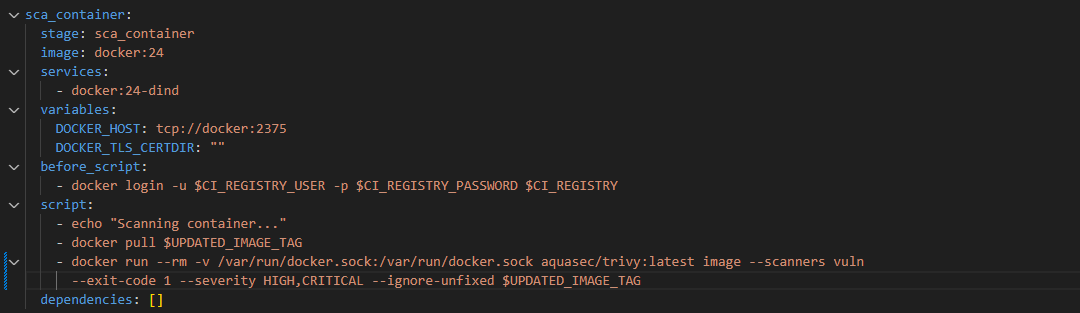
We have to scan the containers created from the base custom Image, therefore we need to pull said container inside of an outer container that has Trivy to scan it. For that purpose we have to use:

* Dind (docker in docker) service, to run a container inside a container
* aquasec/trivy, an official docker image that already posseses trivy

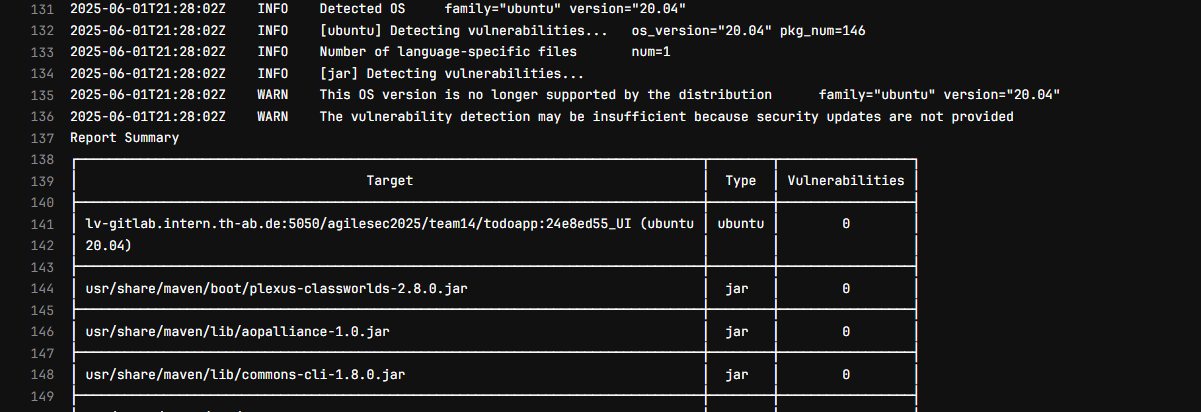
**Implementation**

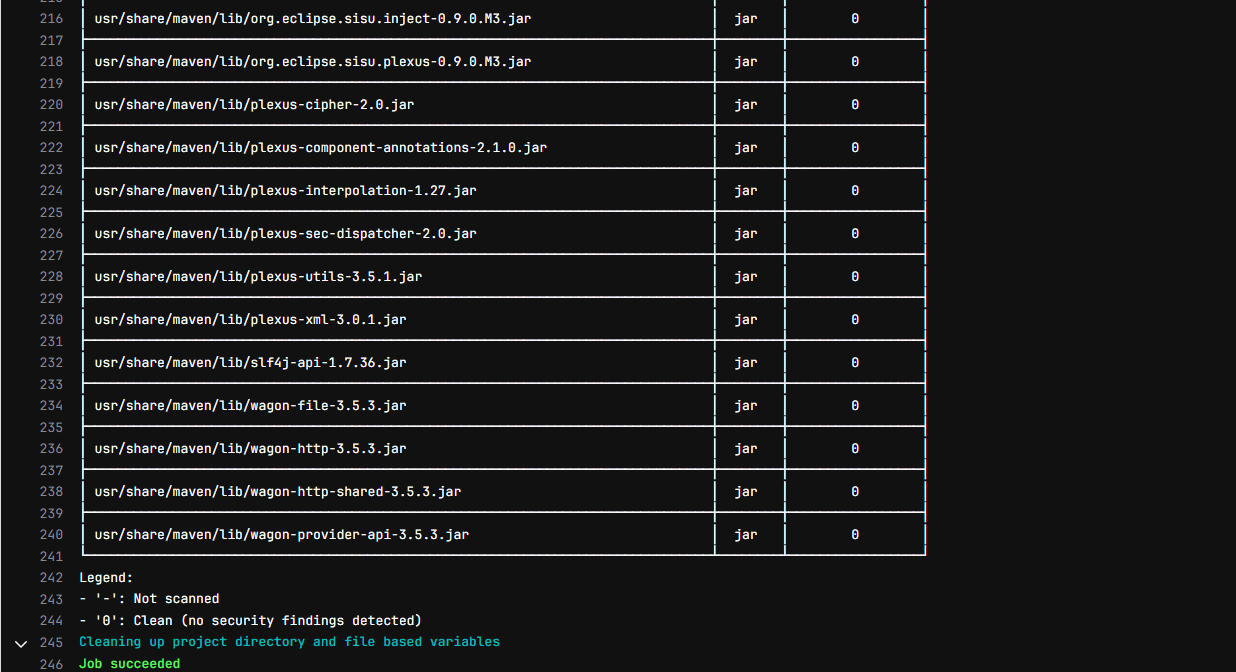
* Login to docker with gitlab
* Use a basic docker image to create a basic container in which we can work
* Ensure that the dind service is running and matches the same versión as the image we are using
* Pull our base image from the container registry
* Scanning using docker with the aquasec/trivy image our base image

Making the implementation looking like this:



And obtaining the next result:





A table that shows if the files provided in the image have certain vulnerabilities.