**Docker Image Scanning**

* In CI/CD Pipelines we build docker images, so we are expected to scan images for vulnerabilities.
* Docker has its own scan as part of its command line
* To perform extensive Scanning Organizations opt for third party tools
  + Aqua Security
  + ECR Scanning
  + Microsoft Defender for Image Scanning
  + Qualysis
* Refer the below two part articles
  + part 1 <https://www.prplbx.com/resources/blog/docker-part1/>
  + part 2 <https://www.prplbx.com/resources/blog/docker-part2/>
* CIS benchmark for docker
* Scanning for vulnerabilities for docker local images
* Docker images are store in Registries (Docker Hub, Elastic Container Registry, Azure Container Registry) and all of them support image scanning.

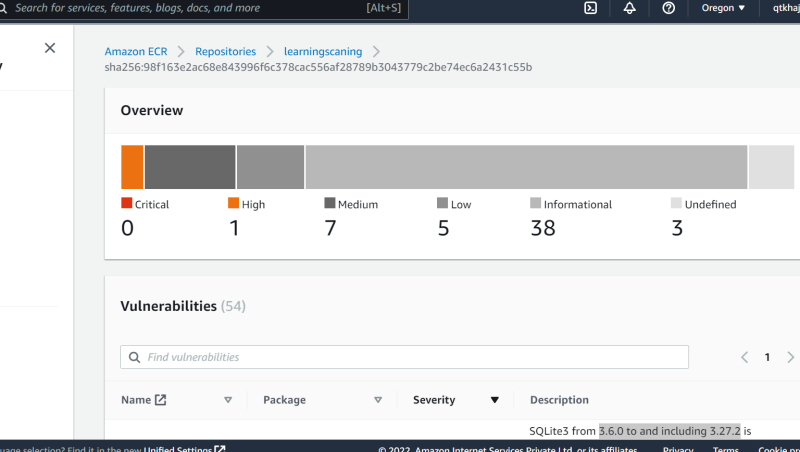
**Sample Scanning of Docker images in Registries**

**AWS ECR**

* Sample Dockerfile

FROM httpd

EXPOSE 80

* After installing docker on the build server
* Create a repository in AWS ECR and select the option to scan on push
* After building the docker image, when we push the report will be ready  
  
* Configuration required on your build server
  + aws cli
  + Create an IAM user and configure
  + Execute aws configure
* In Azure, lets do this activity after some time.

**Linux Vulnerability Scanning**

* Scanning Linux For Vulnerabiliteis <https://geekflare.com/linux-security-scanner/>
* Nessus <https://www.tenable.com/products/nessus>
* Open VAS <https://www.openvas.org/> ss