**Goal of this lecture:**

To pull the supermario docker image from dockerhub and run container scan on docker image. Also to pass/fail the build based on vulnerabilities severity.

**Steps involved:**

1) Add **run-container-scan-supermario-image.yaml** with code as below:

name: "Run Container Scan on Super Mario Docker Image with Quality Gate"

on:

push:

branches:

- main

env:

VERSION: $(( $(cat version.txt) + 1 ))

jobs:

run\_container\_image\_scan\_on\_supermario\_docker\_image:

runs-on: ubuntu-latest

steps:

- name: Checkout Repository

uses: actions/checkout@v3

- name: Login to Docker Hub

run: echo "${{ secrets.DOCKERHUB\_TOKEN }}" | docker login -u "${{ secrets.DOCKERHUB\_USERNAME }}" --password-stdin

- name: Get Docker Image from Docker Hub

run: |

docker pull docker.io/raghuthesecurityexpert/supermariogitopsproject:${{ env.VERSION }}

docker save -o supermariolatestdockerimage.tar docker.io/raghuthesecurityexpert/supermariogitopsproject:${{ env.VERSION }}

- name: Run Trivy vulnerability scanner in tarball mode

uses: aquasecurity/trivy-action@master

with:

input: /github/workspace/supermariolatestdockerimage.tar

exit-code: '1'

severity: 'CRITICAL,HIGH'

2) Push the code to remote Github repo.