Docker FIle

###################

FROM ubuntu

MAINTAINER sai@gmail.com

RUN apt-get update

RUN apt-get install –y nginx

COPY /artifacts/nginx/conf.d /etc/nginx/conf.d

RUN apt-get install -y unzip

ADD unzip code.zip

COPY ../artifacts/code.zip /etc/nginx/sites-available

EXPOSE 80

CMD [“service nginx restart”]

1a) Run the below commands to build the image

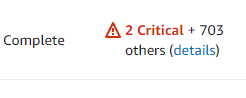
-> docker build -t sai-application:latest

-> Docker images

-> docker run sai-application:latest

-> docker ps

1b) When I test it with sonarqube analysis and cve I have found 2 vulnarablities.



Part2

Jenkins Pipeline

#################

pipeline {

agent {

docker {

image 'maven:3-alpine'

args '-v $HOME/.m2:/root/.m2'

}

}

stages {

stage('Build') {

steps {

sh 'docker run <image name>'

}

}

stage('unit-tests'){

steps {

sh 'mvn test' ##Here we have added the junit plugin in the maven

}

}

}

}

2b) We must add any other server from docker file or else we need to ssh into the container and make necessary changes. If we go through the docker file we can say `add <file name>`. If we install it using the ssh [docker exec -it <Container name> --bash] it will be temporary. Once the container is killed, we will lose all the data.