DevSecOps with Jenkins

Setting up the DevSecOps tools

DockerHub:

```
Go to "manage jenkins"
click on "credentials"
click on "global"
click on "add credentials"
now enter username and password of dockerhub
enter the identifier of the password; DockerHubCreds
```

SonarQube:

```
setting up sonarqube server

- docker run -itd --name sonarqube-server -p 9000:9000 sonarqube:lts-community
- add port 9000 in the SG inbound rule
- access sonarqube server on port number 9000 on the public ip of the server
- initially login: admin, password: admin
- then set up the new password

# generate token for the existing user/new user on the sonarqube server

- administration > security > users > three dots > enter token name > generate > copy and
keep the token safe somewhere
```

DevSecOps with Jenkins

# integrate sonarqube server with jenkins

- install the plugin of the "sonarqube scanner" on jenkins
- click on restart jenkins when installation is complete
- add the credentials of the sonarqube in the jenkins
- select "secret text" as kind of the credentials
- enter the token of the sonarqube and give this credential an ID (Sonar)

# link sonarqube server with jenkins

- (in jenkins)system > find sonarqube > add SonarQube > enter name (Sonar) and sonarqube server url
- server authentication token > select the credential ID you have set in the previous step > save

# configuring sonar scanner tool

- (in jenkins)tools > sonarQube scanner installations > add sonarQube scanner
- enter name (Sonar) > check the box "install automatically" > save

# setting up sonarQube webhook for jenkins in the sonarQube server

- go to SonarQube > administration > configuration > webhook
- create > enter the_name_of_the_webhook > enter the_url_of_the_jenkins/sonarqube-webhook/ > create

DevSecOps with Jenkins

Trivy:

installing Trivy

official url: https://aquasecurity.github.io/trivy/v0.52/getting-started/installation/

```
sudo apt-get install wget apt-transport-https gnupg
wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | gpg --dearmor | sudo
tee /usr/share/keyrings/trivy.gpg > /dev/null
echo "deb [signed-by=/usr/share/keyrings/trivy.gpg] https://aquasecurity.github.io/trivy-
repo/deb generic main" | sudo tee -a /etc/apt/sources.list.d/trivy.list
sudo apt-get update
sudo apt-get install trivy
```

OWASP:

- install "OWASP dependency-check" plugin
- go to tools > dependency-check installations > add dependency-check > add name (OWASP)
- install automatically > from gitHub > save

DevSecOps with Jenkins

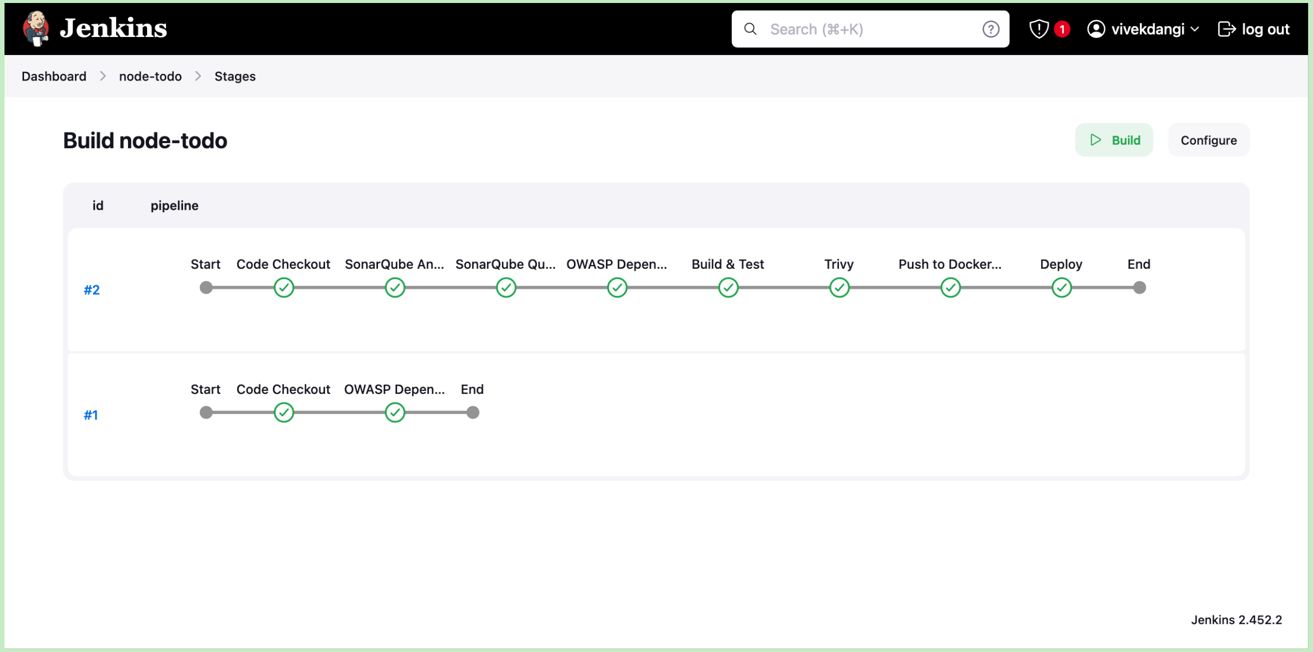
Pipeline Script:

```
pipeline {
    agent any
    environment{
        SONAR_HOME = tool "Sonar"
    }
    stages {
        stage("Code Checkout") {
            steps {
                git url: "https://github.com/LondheShubham153/node-todo-cicd.git", branch: 
"master"
                echo "code cloned successfully"
            }
        }
        stage("SonarQube Analysis") {
            steps {
                withSonarQubeEnv("Sonar"){
                    sh "${SONAR_HOME}/bin/sonar-scanner -Dsonar.projectName=nodetodo 
-Dsonar.projectKey=nodetodoapp -X"
                }
            }
        }
        stage("SonarQube Quality Gates") {
            steps {
                timeout(time: 1, unit: "MINUTES"){
                    waitForQualityGate abortPipeline: false
                }
            }
        }
        stage("OWASP Dependency Check") {
            steps {
                dependencyCheck additionalArguments: '--scan ./', odcInstallation: 'OWASP'
                dependencyCheckPublisher pattern: '**/dependency-check-report.xml'
            }
        }
        stage("Build & Test"){
            steps{
                sh 'docker build -t node-app-batch-6:latest .'
                echo "Code Built Successfully"
            }
        }
        stage("Trivy") {
            steps {
                sh "trivy image node-app-batch-6"
            }
        }
        stage("Push to Docker Hub Repository") {
            steps {

withCredentials([usernamePassword(credentialsId:"DockerHubCreds",passwordVariable:"dockerpass
",usernameVariable:"dockeruser")]){
                sh "docker login -u ${env.dockeruser} -p ${env.dockerpass}"
                sh "docker tag node-app-batch-6:latest ${env.dockeruser}/node-app-
batch-6:latest"
```

DevSecOps with Jenkins

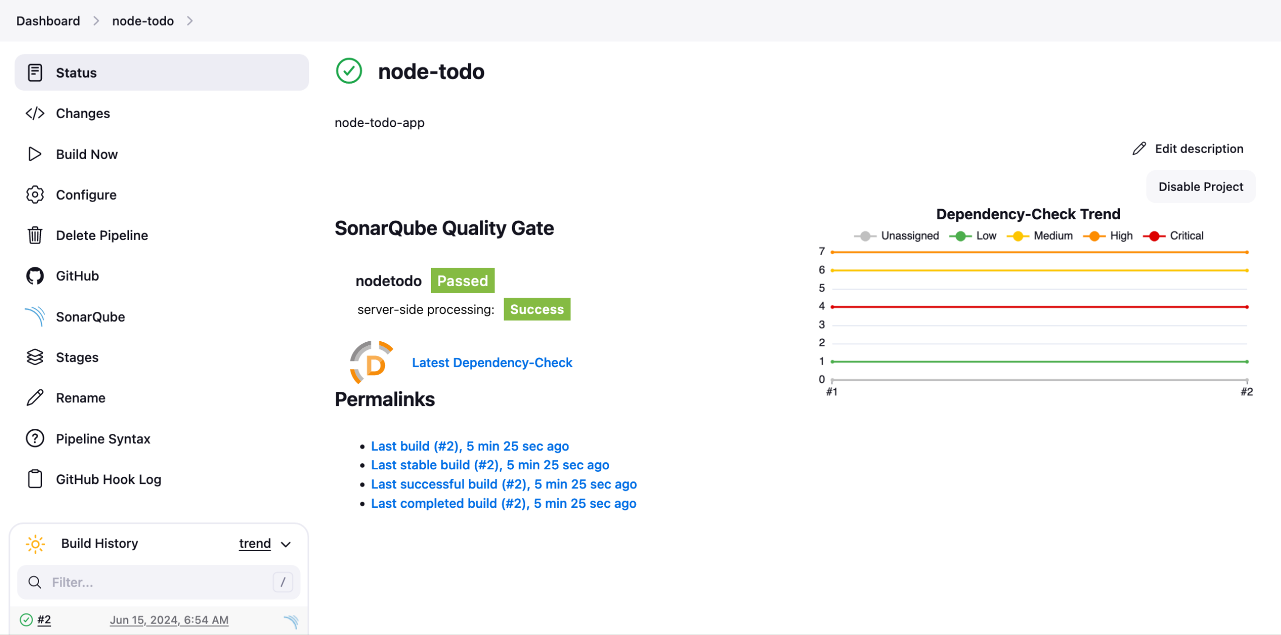
```
                sh "docker push ${env.dockeruser}/node-app-batch-6:latest"
                }
            }
        }
        stage("Deploy"){
            steps{
                sh "docker-compose up -d"
                echo "App Deployed Successfully"
            }
        }
    }
}
```



Build node-todo

id	pipeline
#2	Start, Code Checkout ✓, SonarQube An... ✓, SonarQube Qu... ✓, OWASP Depen... ✓, Build & Test ✓, Trivy ✓, Push to Docker... ✓, Deploy ✓, End
#1	Start, Code Checkout ✓, OWASP Depen... ✓, End

DevSecOps with Jenkins



Dashboard > node-todo >

Build History trend

Filter... /

#2 Jun 15, 2024, 6:54 AM

node-todo

node-todo-app

SonarQube Quality Gate

nodetodo Passed

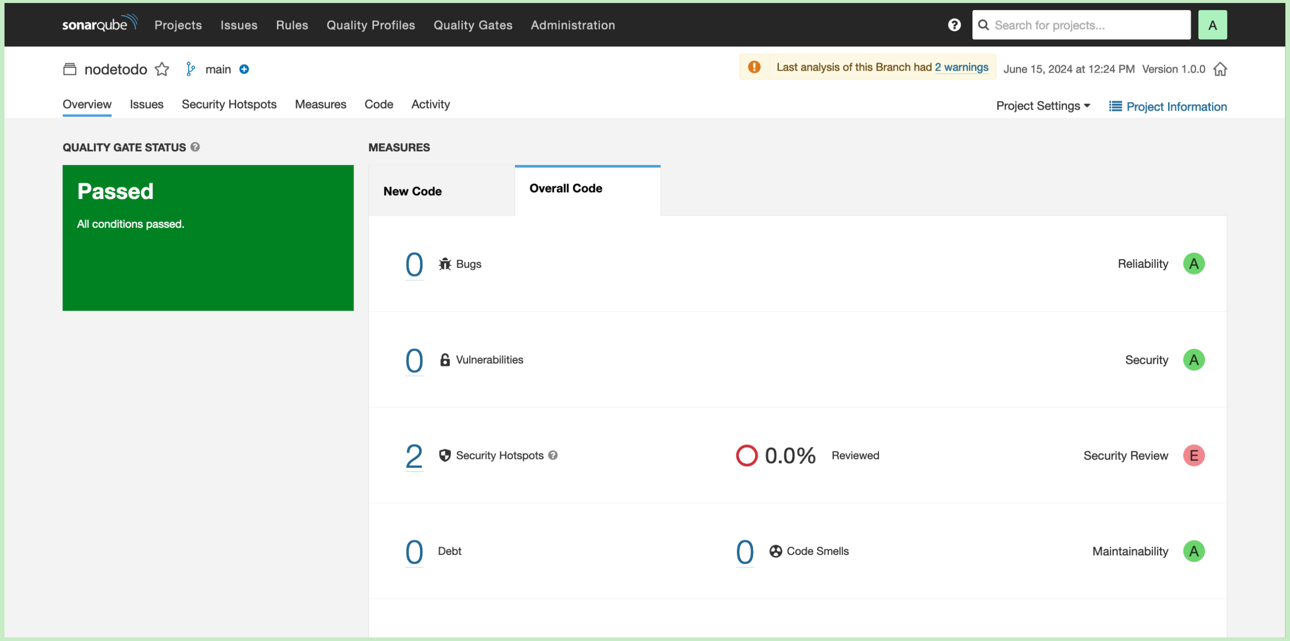
server-side processing: Success

Latest Dependency-Check

Permalinks

- Last build (#2), 5 min 25 sec ago
- Last stable build (#2), 5 min 25 sec ago
- Last successful build (#2), 5 min 25 sec ago
- Last completed build (#2), 5 min 25 sec ago

Dependency-Check Trend



nodetodo main

Last analysis of this Branch had 2 warnings June 15, 2024 at 12:24 PM Version 1.0.0

QUALITY GATE STATUS

Passed

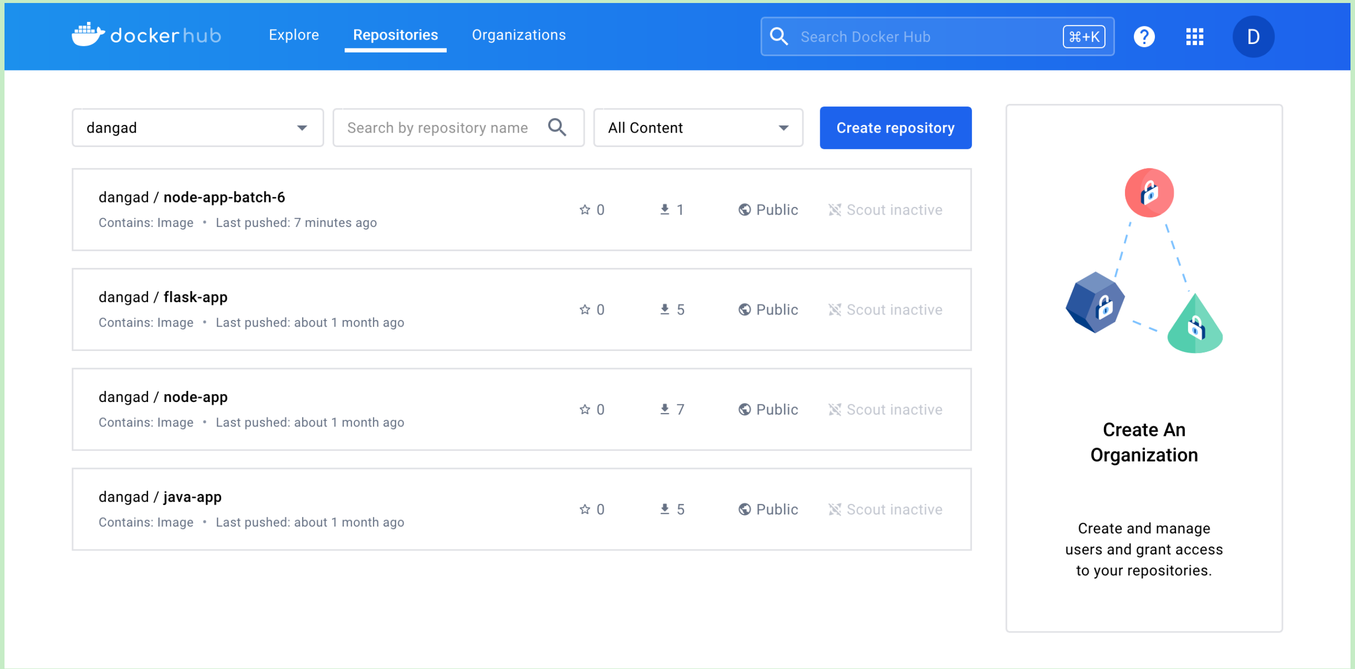
All conditions passed.

MEASURES

New Code | Overall Code

0 Bugs			Reliability A
0 Vulnerabilities			Security A
2 Security Hotspots	0.0% Reviewed		Security Review E
0 Debt	0 Code Smells		Maintainability A

DevSecOps with Jenkins



dangad

Search by repository name

All Content

dangad / node-app-batch-6
Contains: Image • Last pushed: 7 minutes ago
☆ 0 ⬇ 1 Public Scout inactive

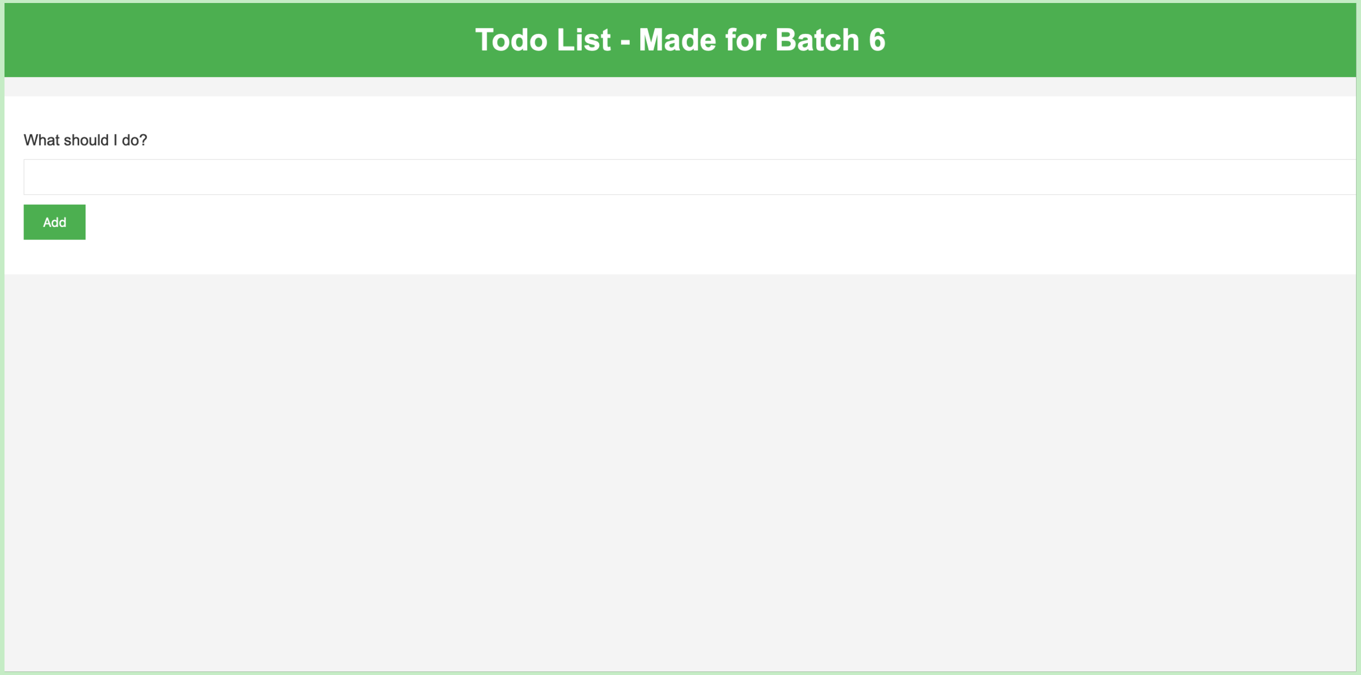
dangad / flask-app
Contains: Image • Last pushed: about 1 month ago
☆ 0 ⬇ 5 Public Scout inactive

dangad / node-app
Contains: Image • Last pushed: about 1 month ago
☆ 0 ⬇ 7 Public Scout inactive

dangad / java-app
Contains: Image • Last pushed: about 1 month ago
☆ 0 ⬇ 5 Public Scout inactive

Create An Organization

Create and manage users and grant access to your repositories.



Todo List - Made for Batch 6

What should I do?