Sonarqube-Day-1

28 November 2023 17:36

Sonarqube-1

- ► In this you will get understand
    - ○ What is sonarqube?
    - ○ Why do we need Sonarqube?
    - ○ How to setup sonarqube on Linux server?
- ► Sonarqube is **Static code analysis tool.**
- ► **Why do we need Static code analysis tool?**

  Before we understand what is Sonarqube let's jump into the development phase of the project

    - ○ During project development the developer will write a code, once the code development of completed this code has to be review ed by the another peer developer like Team lead/Architect of the project.
    - ○ So now what Team Lead/Architect will check the code & try to identify,
        - ▪ Is it containing any bugs?
        - ▪ Is it secure issues?
            - □ It means that any passwords or personal email ids are mentioned in the source code?
        - ▪ Is there any duplication code?
            - □ There might be situation developers has to write **same piece of code in many locations of the files related to project**.
            - □ Using same lines of code at many files can be called as duplication of code.
            - □ **Architect** will check possibility of **creating function for same piece of code at one location & will call that code rest of the places**.
        - ▪ Is that code tested properly or not?
            - □ As we know **developer job is not only writing code for the functionality of the application but also they have to write test code to check the functionality**. This test code called as **UNIT TEST** Code.
            - □ So Architect will check will the code sufficient UNIT TEST code or not?
        - ▪ Is there any complex code written?
            - □ As an architect/team-lead if there is any complex code, you have to find-out is there any better way of rewriting the coding easiest way of understanding without affecting functionality.
        - ▪ Easy to integrate with another developers code?
            - □ Architect will review the code and check if that code is easy to integrate or not with the another developers code when he is working in a group of team.
        - ▪ All this actions are doing manually by the people like Architect/Team Lead, so every time whenever developer pushed/check-in latest code this review process will come into picture & it will kill the time of developers.
        - ▪ We can automate all these actions with static code analysis tool came into picture.
- ► We have so many **static code analysis tools in the market**
    - ○ Sonarqube
    - ○ Coverity
    - ○ Codescene
    - ○ Veracode
- ► Apart from these static analysis tools why most of the companies are choosing sonarqube?
    - ○ Sonarqube is not only **static code analysis but it is also a code quality management tool**.
    - ○ Just assume you are a java developer & you have a requirement to **develop a calculator** application for mobile phones.
        - ▪ So developer what you will do you write a code for functionality development like,
            - □ addition
            - □ subtraction
            - □ multiplication and
            - □ division, correct or not? - Correct

          As a developer you are not only taking care of the functionality development but you also have to write a code to test your functionalities, this code called as unit testing.

        - **Sonarqube** as a code quality management tool it will **provide the unit test code reports** of your project.

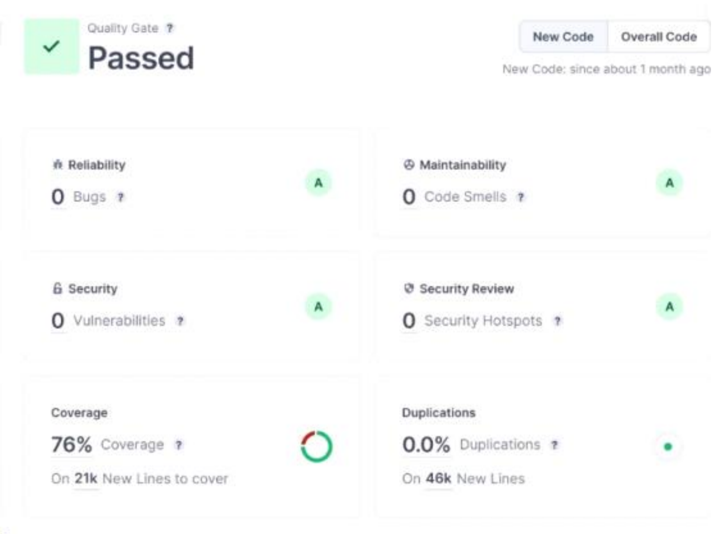
    - Even Sonarqube will provide the details about **code coverage**.

      What is an code coverage?

        - Suppose as a developer you wrote a hundred functions to complete your application development so out of those hundred functions how many functions are successfully tested based on that this code coverage will be calculated the projects.

        - The projects which are having the more coverage those projects will be considered as stable projects.

- So all these information whatever we have discussed so far like



Quality Gate ?
Passed

New Code | Overall Code
New Code: since about 1 month ago

Reliability
0 Bugs ? A

Maintainability
0 Code Smells ? A

Security
0 Vulnerabilities ? A

Security Review
0 Security Hotspots ? A

Coverage
76% Coverage ?
On 21k New Lines to cover

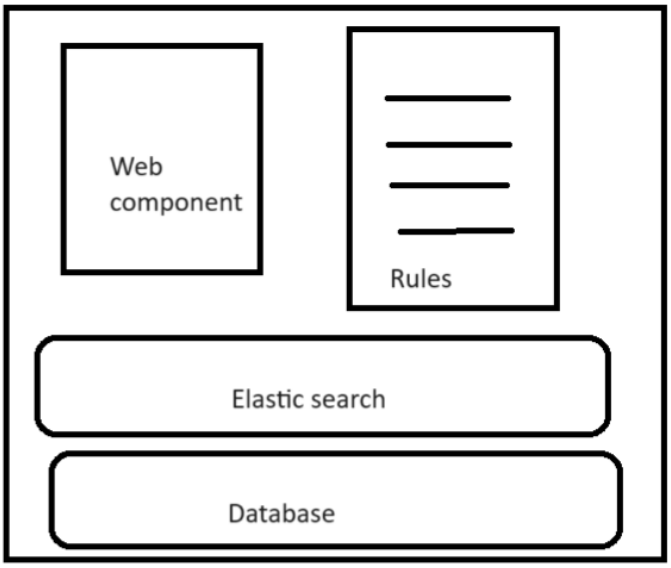
Duplications
0.0% Duplications ?
On 46k New Lines

    - Number of bugs your project.
    - Number of vulnerabilities
    - Code coverage
    - Duplications code
    - Code smells

      like this information we can easily see in the sonarqube dashboards.

- Now let's understand the **sonarqube components**
    - In sonarqube we have mainly two sections
        - Sonarqube server
        - Sonar-scanner

    - In sonarqube-server we have mainly 4 components,



EC2-SERVER With SonarQube server

        - **Rules**
            - □ Rules are nothing but the guidelines/best practices that developers has to follow during the code development.

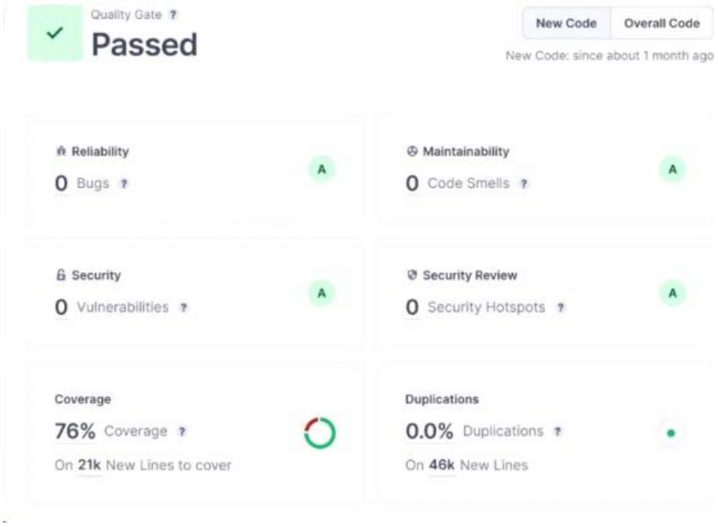
    - Whenever we install sonarqube server by default we get rules for each programming language that developer has to follow while writing code.

    - If there is **any deviation in the code for the rules defined** it will be considered as a **bug/vulnerability/code smell** & displayed in the sonarqube dashboard.

  - **Database**
    - Once the rules are executed successfully & it will generate the analysis reports.

    - The analysis report which is created based on the sonarqube rules triggered on source code of the developer.

  - **Web component**
    - It will display the analysis report that is stored in the database in nice graphical interface.



Quality Gate ?
✓ Passed

New Code | Overall Code

New Code: since about 1 month ago

Reliability
0 Bugs ? A

Maintainability
0 Code Smells ? A

Security
0 Vulnerabilities ? A

Security Review
0 Security Hotspots ? A

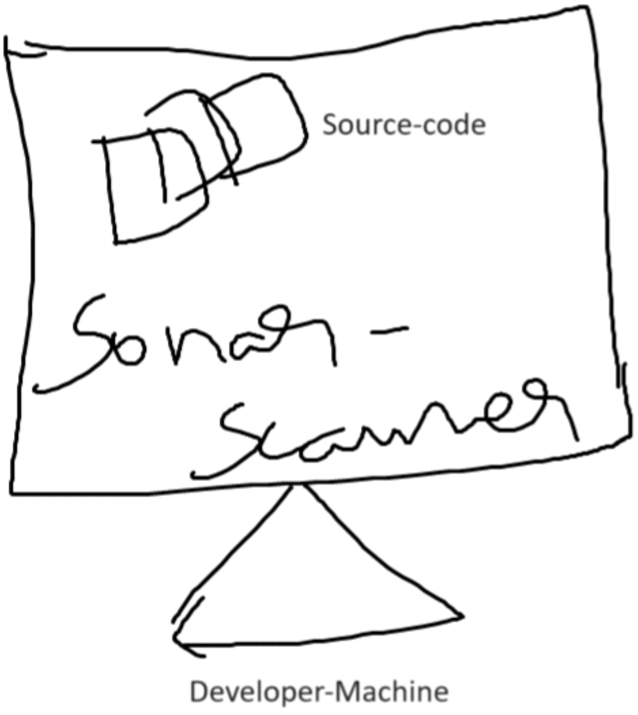
Coverage
76% Coverage ?
On 21k New Lines to cover

Duplications
0.0% Duplications ?
On 46k New Lines

  - **Elastic search**
    This component will help the web component to fetch the information from database in quickest way.

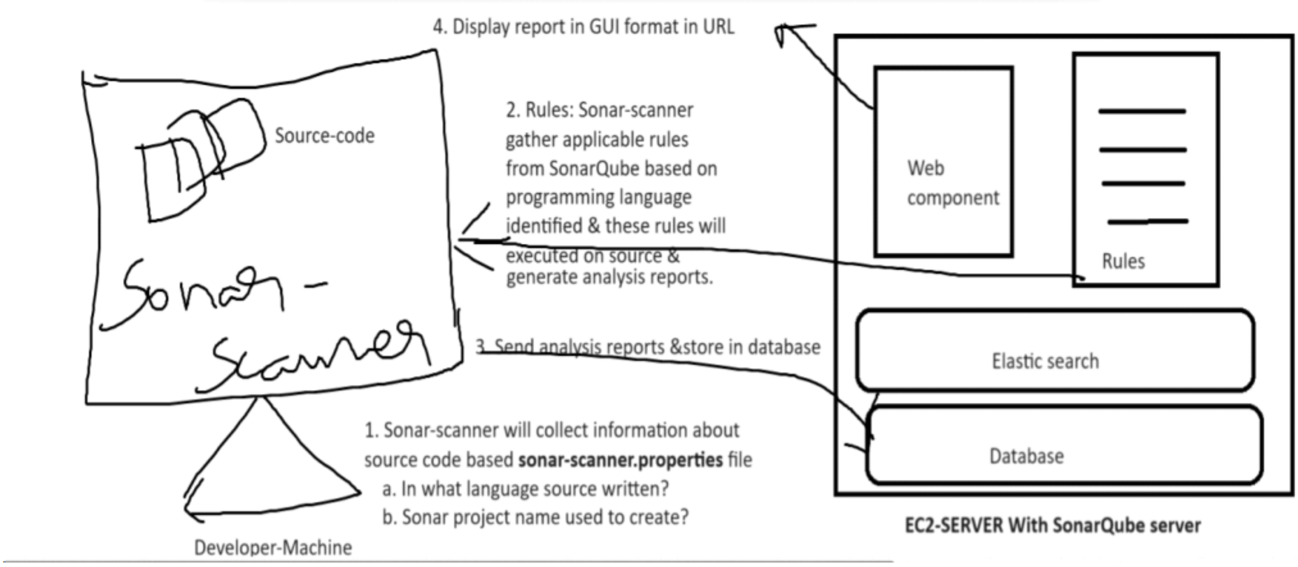
- **Sonar-scanner**
  - Sonar-scanner agent which is normally installed on the machine very were the source code is existed.

  - Sonar-scanner will run on the source code and generates the analysis report later that this analysis report is push to the Sonarqube server.



- Sonarqube supports almost **27 plus programming languages** and generates analysis reports.

- **How communication established between sonar-scanner & sonarqube-server,**


4. Display report in GUI format in URL

2. Rules: Sonar-scanner gather applicable rules from SonarQube based on programming language identified & these rules will executed on source & generate analysis reports.

3. Send analysis reports &store in database

1. Sonar-scanner will collect information about source code based **sonar-scanner.properties** file
   a. In what language source written?
   b. Sonar project name used to create?

- **How to install sonarqube server with inbuilt database**
  - Let's discuss the pre-requisites to install Sonarqube server
    Perquisites:
    - **JAVA**
    - **Why we need Java as it request it to install sonarqube?**
      Because Sonarqube is developed based on Java programming language.
    - To install Java on Linux machine we have to run a command like
      yum install java-17* -y (sonarqube LTS 9.9.3)
  - Sonarqube provides LTS(Long Term stable) sonarqube-server products & latest release sonarqube-server products.
    - LTS means its stable version of product & if its containing any bugs/vulnerabilities in feature you can get fixes for those without being impacted with other functionalities.
    - Latest products continuous improvements for the product & can't guarantee on few of features.
  - Now to download the sonarqube installer from LTS model & go to the official site of sonarqube.
    There we can find the different level of products will be available like
    - Community
    - Enterprise level
    - Cloud level

    Like this different products available.
  - **Installation steps:**
    - So in this session we are going to install the community edition.
      https://binaries.sonarsource.com/Distribution/sonarqube/sonarqube-9.9.3.79811.zip
    - **Extract the zip file**
      - □ unzip sonarqube-9.9.3.79811.zip
      - □ mv sonarqube-9.9.3.79811 /opt/sonarqube
    - Create sonar user
      useradd sonar
    - Change ownership of /opt/sonarqube to sonar

chown -R sonar:sonar /opt/sonarqube

- Start sonarqube as non-root user
  cd /opt/sonarqube/bin/
  ./sonar.sh start

- Now access the sonarqube in browser http://<ip-address>:9000
  Username: admin
  Password: admin

- **How to install sonar-scanner**
  - Download sonar-scanner
    https://binaries.sonarsource.com/Distribution/sonar-scanner-cli/sonar-scanner-cli-5.0.1.3006-linux.zip

  - Extract it
    unzip sonar-scanner-cli-5.0.1.3006-linux.zip
    mv sonar-scanner-cli-5.0.1.3006-linux /opt/sonar-scanner

  - Check sonar-scanner version
    Sonar-scanner --version