

## **Experiment No. 7**

**Aim:** To describe Static Analysis SAST process and learn to integrate Jenkins SAST to SonarQube/GitLab. (LO1, LO4)

### **Theory:**

#### **SAST (Static Analysis Security Testing):**

Static application security testing (SAST), or static analysis, is a testing methodology that analyses source code to find security vulnerabilities that make your organization's applications susceptible to attack. It scans an application before the code is compiled. It's also known as white box testing.

#### **Why SAST is an important Security Activity?**

Developers dramatically outnumber security staff. It can be challenging for an organization to find the resources to perform code reviews on even a fraction of its applications. A key strength of SAST tools is the ability to analyze 100% of the code base. Additionally, they are much faster than manual secure code reviews performed by humans. These tools can scan millions of lines of code in a matter of minutes. SAST tools automatically identify critical vulnerabilities—such as buffer overflows, SQL injection, cross-site scripting, and others—with high confidence. Thus, integrating static analysis into the SDLC can yield dramatic results in the overall quality of the code developed.

#### **SonarQube:**

- SonarQube is an open-source platform developed by SonarSource for continuous inspection of code quality. Sonar does static code analysis, which provides a detailed report of bugs, code smells, vulnerabilities, code duplications.
- It is used to test the quality of the code and execute the automatic reviews with the help of identifying the bugs, code analysis and security exposures on various programming languages such as Java, C#, JavaScript, PHP, Ruby, Cobol, C/C++ and so on of the web applications.
- It supports 25+ major programming languages through built-in rulesets and can also be extended with various plugins.
- SonarQube tool is written on the JAVA programming language.
- It will generate the reports of the code coverage, complexity of code, repeated code, security weakness, and bugs.
- offers complete analysis with multiple tools like Ant, Maven, Gradle, Jenkins, and so on.



### **Benefits of SonarQube:**

1. **Sustainability:** Reduces complexity, possible vulnerabilities, and code duplications, optimizing the life of applications.
2. **Increase productivity:** Reduces the scale, cost of maintenance, and risk of the application; as such, it removes the need to spend more time changing the code.
3. **Quality code:** Code quality control is an inseparable part of the process of software development.
4. **Detect Errors:** Detects errors in the code and alerts developers to fix them automatically before submitting them for output.
5. **Increase consistency:** Determines where the code criteria are breached and enhances the quality.
6. **Business scaling:** No restriction on the number of projects to be evaluated.
7. **Enhance developer skills:** Regular feedback on quality problems helps developers to improve their coding skills.

### **Why to use SonarQube?**

- Developers working with hard deadlines to deliver the required functionality to the customer. It is so important for developers that many times they compromise with the code quality, potential bugs, code duplications, and bad distribution of complexity.
- Additionally, they tend to leave unused variables, methods, etc. In this scenario, the code would work in the desired way.
- To avoid these issues in code, developers should always follow the good coding practice, but sometimes it is not possible to follow the rules and maintain the good quality as there may be many reasons.
- In order to achieve continuous code integration and deployment, developers need a tool that not only works once to check and tell them the problems in the code but also to track and control the code to check continuous code quality. To satisfy all these requirements, here comes SonarQube in the picture.

### **Features of SonarQube:**

- It will integrate with multiple development environments like Visual Studio, Eclipse, and IntelliJ IDEA over the SonarLint plug-ins.
- It also supports some external tools such as GitHub, LDAP, and Active Directory.
- It can record the metric history and deliver the evolution graphs.
- It will help us to identify the complex issues.
- It will provide application security.

Name: Harsh Dalvi  
Roll No: 13

Subject: Advance DevOps , Sem: SEM V  
Class / Batch: TE-IT / Batch B

## Steps to perform the Experiment:

**Step 1:** Download Jenkins, JDK 17, SonarScanner and SonarQube from their respective websites.

The screenshot shows the Jenkins website's 'Thank you for downloading Windows Stable installer' page. The page includes links for 'Download hasn't started?', 'Changing boot configuration', 'Starting/stopping the service', 'Inheriting your existing Jenkins installation', and 'See Also'. The 'See Also' section lists links for running Jenkins behind IIS, nginx, and Apache. A blue banner at the bottom contains links to 'Improve this page' and 'Report a problem'. A taskbar at the very bottom shows icons for sonarqube-9.6.1.59.zip, sonar-scanner-cli-4.zip, jdk-17.0.4.1\_windo...exe, and jenkins.msi.

The screenshot shows the Oracle website's Java SE Development Kit 17.0.4 download page. It features a table with download links for various operating systems and architectures. Below the table, there is a section for the 'Java SE Development Kit 17.0.4' license. A taskbar at the bottom shows icons for sonarqube-9.6.1.59.zip, sonar-scanner-cli-4.zip, jdk-17.0.4.1\_windo...exe, and jenkins.msi.

Product / File Description	File Size	Download
macOS ARM 64 DMG Installer	166.86 MB	<a href="https://download.oracle.com/java/17/archive/jdk-17.0.4.1_macos-aarch64_bin.dmg (sha256 )">https://download.oracle.com/java/17/archive/jdk-17.0.4.1_macos-aarch64_bin.dmg (sha256 )</a>
macOS x64 Compressed Archive	170.01 MB	<a href="https://download.oracle.com/java/17/archive/jdk-17.0.4.1_macos-x64_bin.tar.gz (sha256 )">https://download.oracle.com/java/17/archive/jdk-17.0.4.1_macos-x64_bin.tar.gz (sha256 )</a>
macOS x64 DMG Installer	169.39 MB	<a href="https://download.oracle.com/java/17/archive/jdk-17.0.4.1_macos-x64_bin.dmg (sha256 )">https://download.oracle.com/java/17/archive/jdk-17.0.4.1_macos-x64_bin.dmg (sha256 )</a>
Windows x64 Compressed Archive	171.81 MB	<a href="https://download.oracle.com/java/17/archive/jdk-17.0.4.1_windows-x64_bin.zip (sha256 )">https://download.oracle.com/java/17/archive/jdk-17.0.4.1_windows-x64_bin.zip (sha256 )</a>
Windows x64 Installer	152.78 MB	<a href="https://download.oracle.com/java/17/archive/jdk-17.0.4.1_windows-x64_bin.exe (sha256 )">https://download.oracle.com/java/17/archive/jdk-17.0.4.1_windows-x64_bin.exe (sha256 )</a>
Windows x64 MSI Installer	151.66 MB	<a href="https://download.oracle.com/java/17/archive/jdk-17.0.4.1_windows-x64_bin.msi (sha256 )">https://download.oracle.com/java/17/archive/jdk-17.0.4.1_windows-x64_bin.msi (sha256 )</a>

The screenshot shows the SonarQube website's SonarScanner download page. It includes a search bar, a sidebar with navigation links, and a main content area with details about the scanner. A taskbar at the bottom shows icons for sonarqube-9.6.1.59.zip, sonar-scanner-cli-4.zip, jdk-17.0.4.1\_windo...exe, and jenkins.msi.

**SonarScanner**

By SonarSource | GNU LGPL 3 | Issue Tracker

**4.7**  
2022-02-22  
Ease import of custom certificates with the Docker image, update embedded JRE 11  
[Linux 64-bit](#) [Windows 64-bit](#) [Mac OS X 64-bit](#) [Docker](#)  
[Any \(Requires a pre-installed JVM\)](#) [Release notes](#)

The SonarScanner is the scanner to use when there is no specific scanner for your build system.

**Configuring your project**  
Create a configuration file in your project's root directory called `sonar-project.properties`

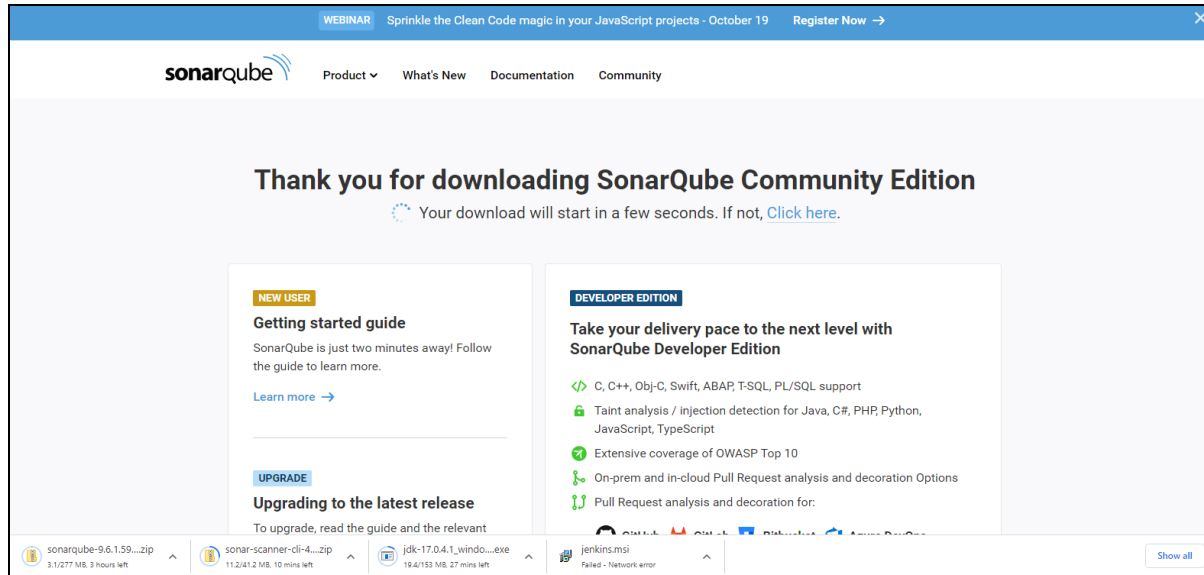
```
# must be unique in a given SonarQube instance
sonar.projectKey=my:project

# --- optional properties ---

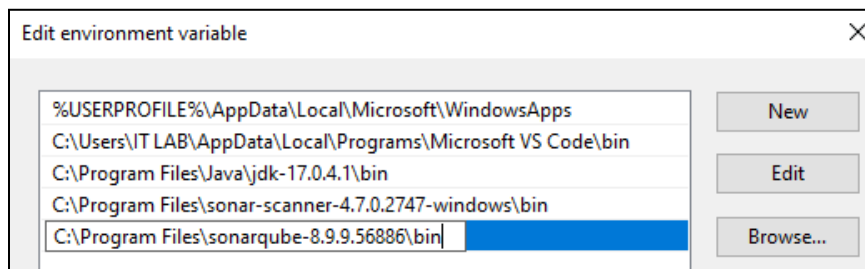
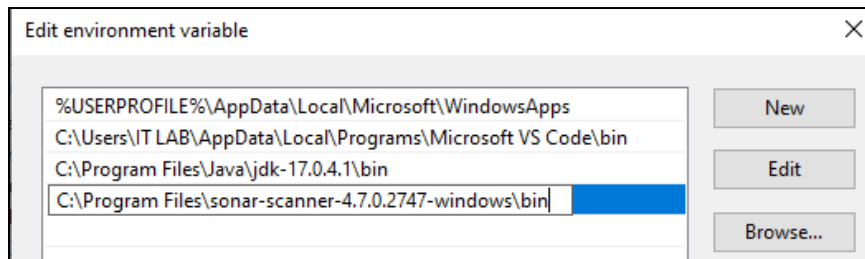
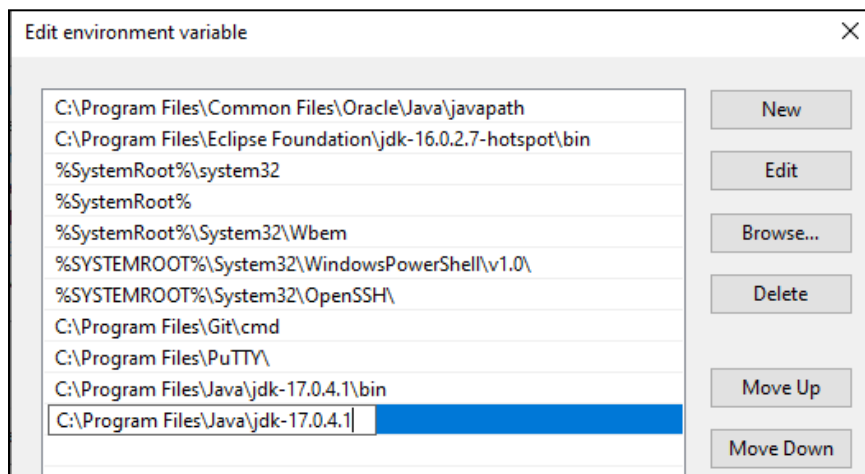
# defaults to project key
#sonar.projectName=my:project
# defaults to 'not provided'
#sonar.projectVersion=1.0
```

Name: Harsh Dalvi  
Roll No: 13

Subject: Advance DevOps , Sem: SEM V  
Class / Batch: TE-IT / Batch B



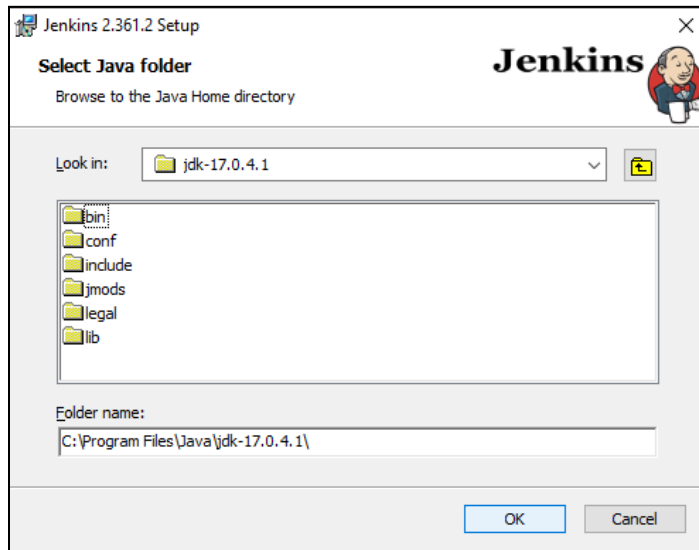
**Step 2:** Now give the path to JDK, SonarScanner and SonarQube in your Environment Variables.



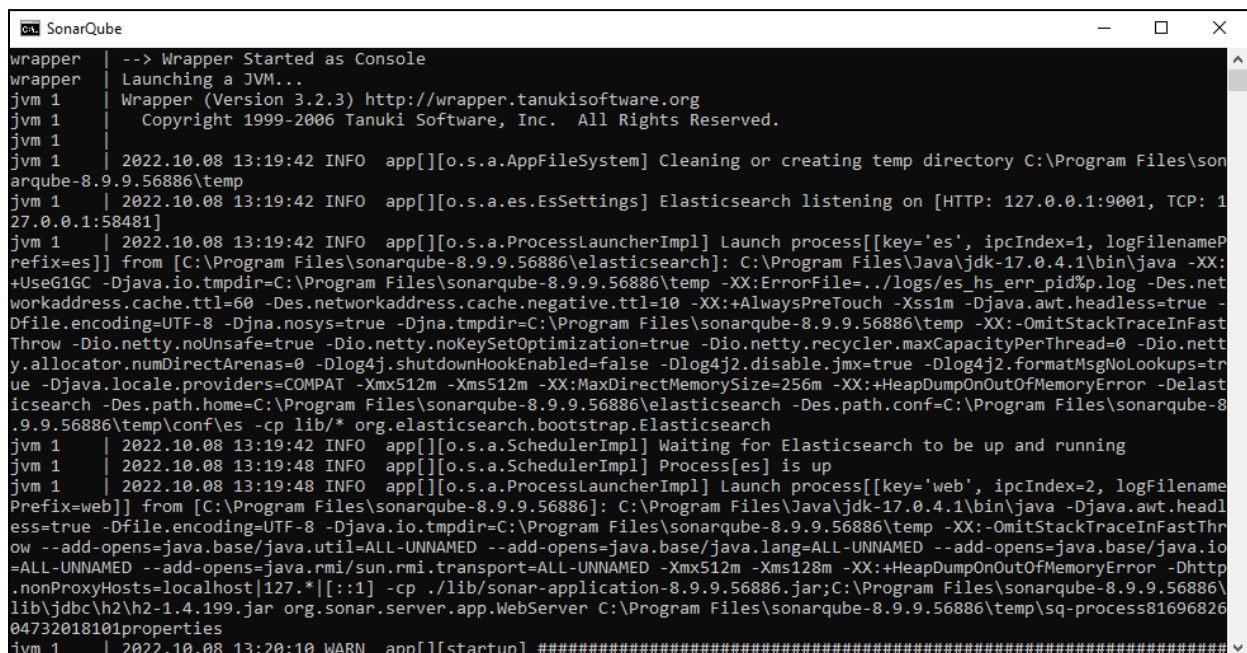
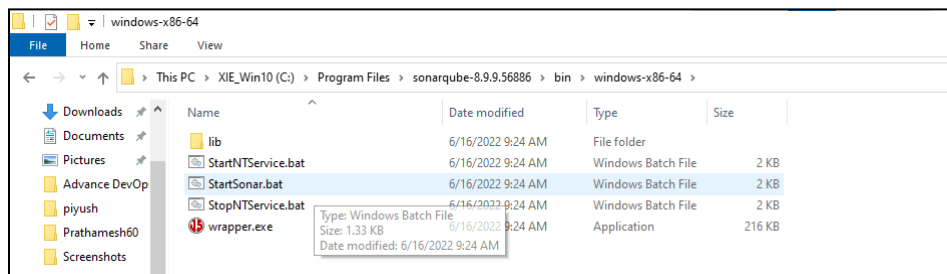
Name: Harsh Dalvi  
Roll No: 13

Subject: Advance DevOps , Sem: SEM V  
Class / Batch: TE-IT / Batch B

**Step 3:** Install Jenkins and select the JDK folder. During the installation download all the recommended plugins.



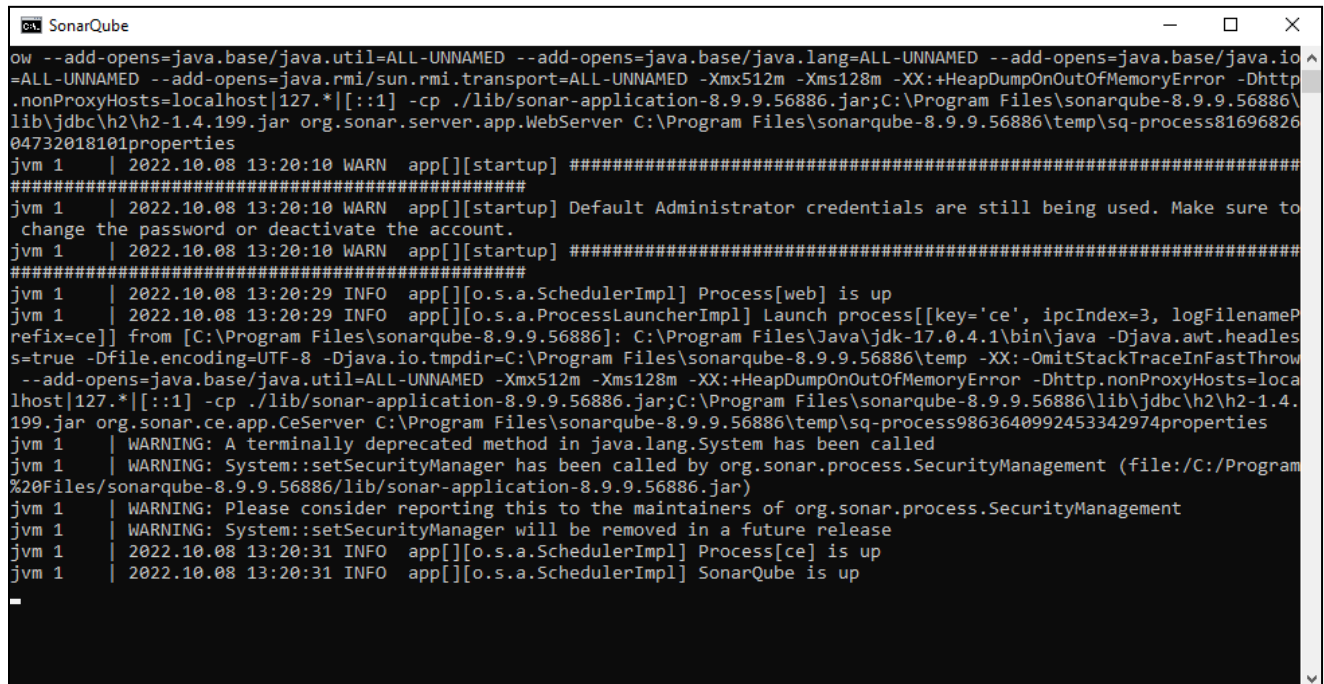
**Step 4:** After the installation of Jenkins, go to the SonarQube folder and open the “StartSonar.bat” file by following the path given below.



Name: Harsh Dalvi  
Roll No: 13

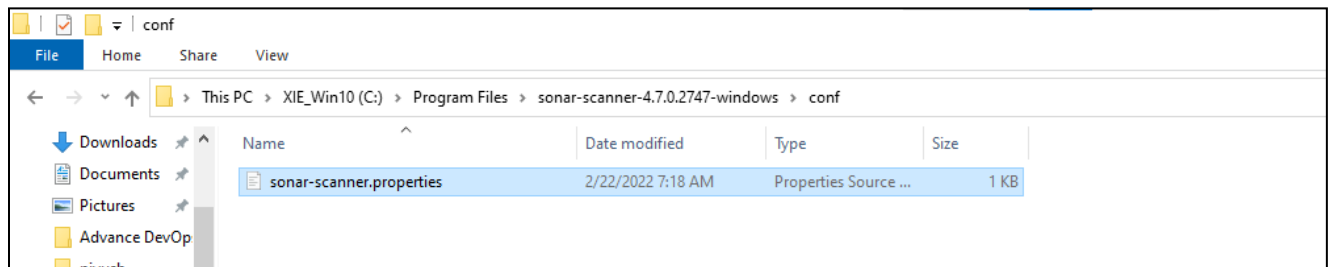
Subject: Advance DevOps , Sem: SEM V  
Class / Batch: TE-IT / Batch B

**Step 5:** The required output is that the terminal should show “Process is up” and “SonarQube is up” to get the desired output as shown below.

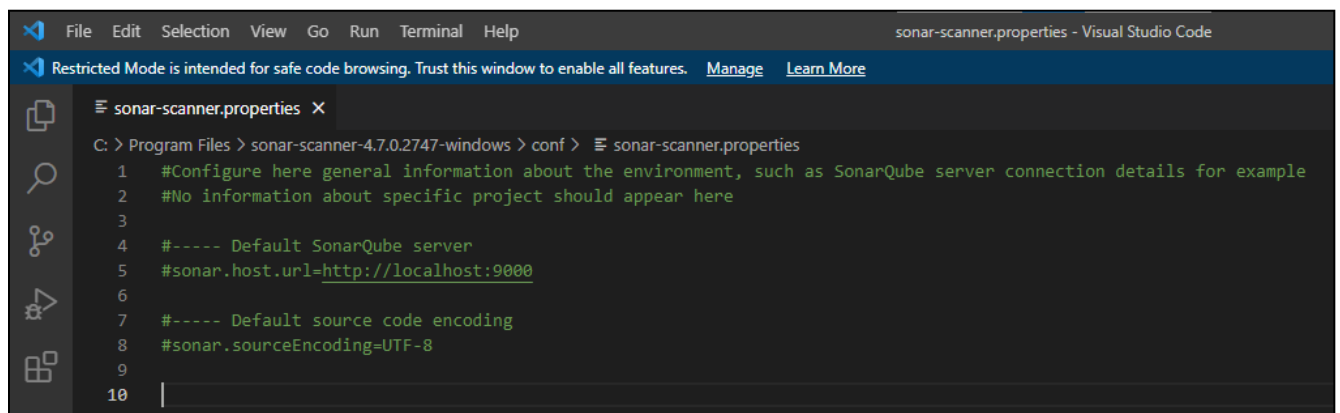


```
ow --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED -Xmx512m -Xms128m -XX:+HeapDumpOnOutOfMemoryError -Dhttp.nonProxyHosts=localhost|127.*|[:1] -cp ./lib/sonar-application-8.9.9.56886.jar;C:\Program Files\sonarqube-8.9.9.56886\lib\jdbc\h2\h2-1.4.199.jar org.sonar.server.app.WebServer C:\Program Files\sonarqube-8.9.9.56886\temp\sq-process8169682604732018101properties
jvm 1 | 2022.10.08 13:20:10 WARN app[][startup] #####
jvm 1 | 2022.10.08 13:20:10 WARN app[][startup] Default Administrator credentials are still being used. Make sure to change the password or deactivate the account.
jvm 1 | 2022.10.08 13:20:10 WARN app[][startup] #####
jvm 1 | 2022.10.08 13:20:29 INFO app[][o.s.a.SchedulerImpl] Process[web] is up
jvm 1 | 2022.10.08 13:20:29 INFO app[][o.s.a.ProcessLauncherImpl] Launch process[[key='ce', ipcIndex=3, logFilenamePrefix=ce]] from [C:\Program Files\sonarqube-8.9.9.56886]: C:\Program Files\Java\jdk-17.0.4.1\bin\java -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djava.io.tmpdir=C:\Program Files\sonarqube-8.9.9.56886\temp -XX:-OmitStackTraceInFastThrow --add-opens=java.base/java.util=ALL-UNNAMED -Xmx512m -Xms128m -XX:+HeapDumpOnOutOfMemoryError -Dhttp.nonProxyHosts=localhost|127.*|[:1] -cp ./lib/sonar-application-8.9.9.56886.jar;C:\Program Files\sonarqube-8.9.9.56886\lib\jdbc\h2\h2-1.4.199.jar org.sonar.ce.app.CeServer C:\Program Files\sonarqube-8.9.9.56886\temp\sq-process9863640992453342974properties
jvm 1 | WARNING: A terminally deprecated method in java.lang.System has been called
jvm 1 | WARNING: System::setSecurityManager has been called by org.sonar.process.SecurityManagement (file:/C:/Program Files/sonarqube-8.9.9.56886/lib/sonar-application-8.9.9.56886.jar)
jvm 1 | WARNING: Please consider reporting this to the maintainers of org.sonar.process.SecurityManagement
jvm 1 | WARNING: System::setSecurityManager will be removed in a future release
jvm 1 | 2022.10.08 13:20:31 INFO app[][o.s.a.SchedulerImpl] Process[ce] is up
jvm 1 | 2022.10.08 13:20:31 INFO app[][o.s.a.SchedulerImpl] SonarQube is up
```

**Step 6:** Now, go to the SonarScanner folder and open the “sonar-scanner.properties” file by following the path given below.



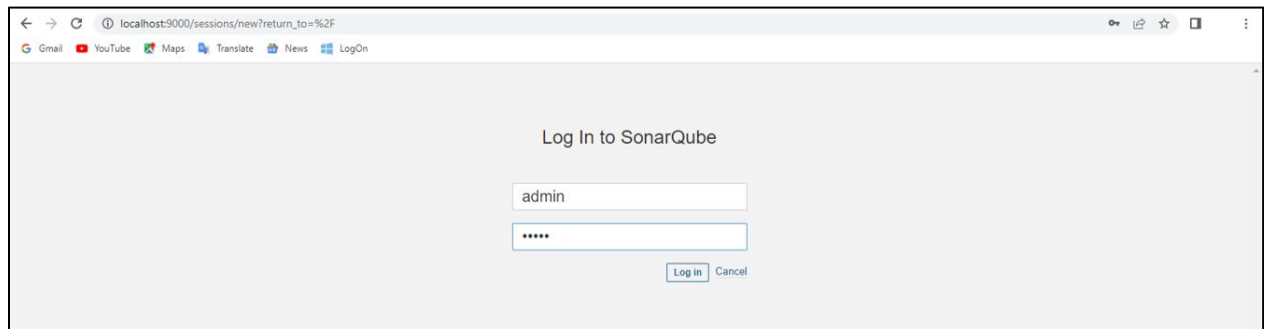
**Step 7:** Copy the URL and paste it on the Browsers Search Bar



Name: Harsh Dalvi  
Roll No: 13

Subject: Advance DevOps , Sem: SEM V  
Class / Batch: TE-IT / Batch B

### Step 8: Sign in as “admin”



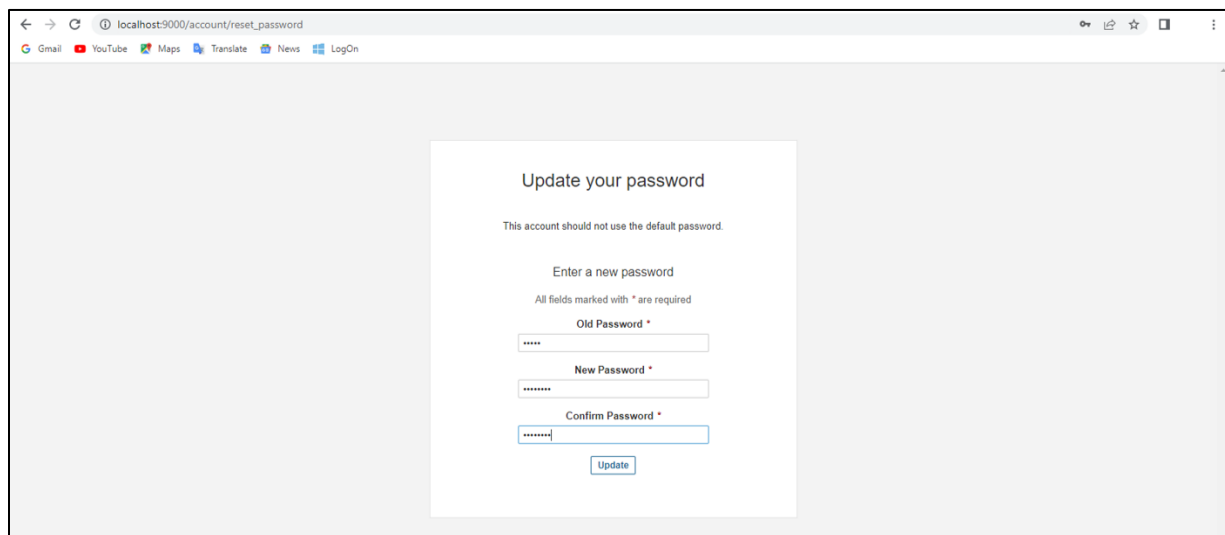
Log In to SonarQube

admin

\*\*\*\*\*

Log In Cancel

### Step 9: Change the Password



Update your password

This account should not use the default password.

Enter a new password

All fields marked with \* are required

Old Password \*

\*\*\*\*\*

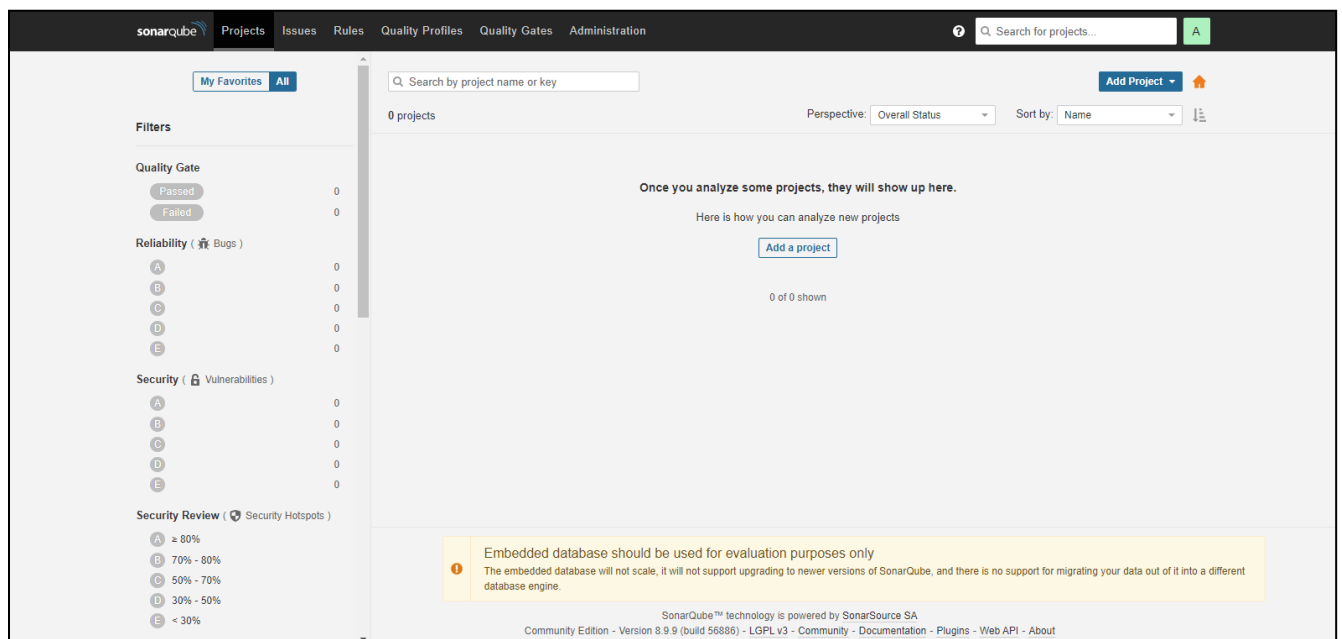
New Password \*

\*\*\*\*\*

Confirm Password \*

\*\*\*\*\*

Update



sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration

Q Search for projects...

My Favorites All

Q Search by project name or key

0 projects

Perspective: Overall Status Sort by: Name

Once you analyze some projects, they will show up here.

Here is how you can analyze new projects

Add a project

0 of 0 shown

Embedded database should be used for evaluation purposes only

The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.

SonarQube™ technology is powered by SonarSource SA

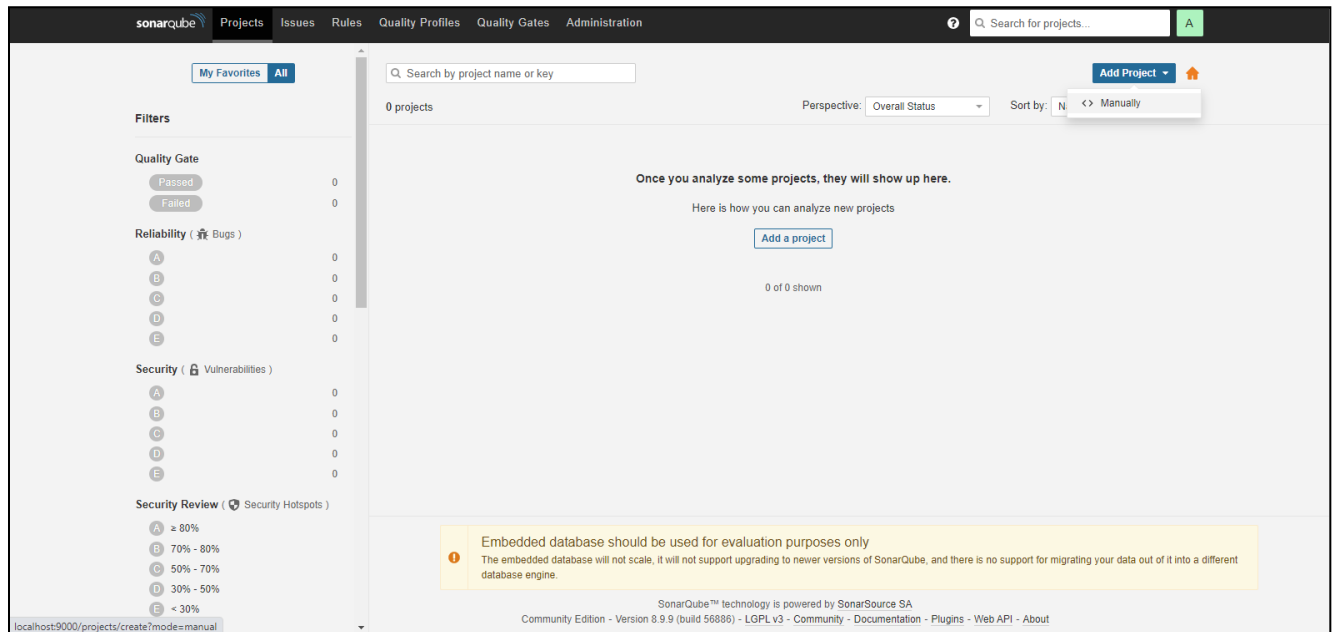
Community Edition - Version 8.9.9 (build 56886) - LGPL v3 - Community - Documentation - Plugins - Web API - About



Name: Harsh Dalvi  
Roll No: 13

Subject: Advance DevOps , Sem: SEM V  
Class / Batch: TE-IT / Batch B

**Step 10:** Click on “Add Project” and select “Manually”.



**Step 11:** Now create a Project by giving a Project Key and Display Name.

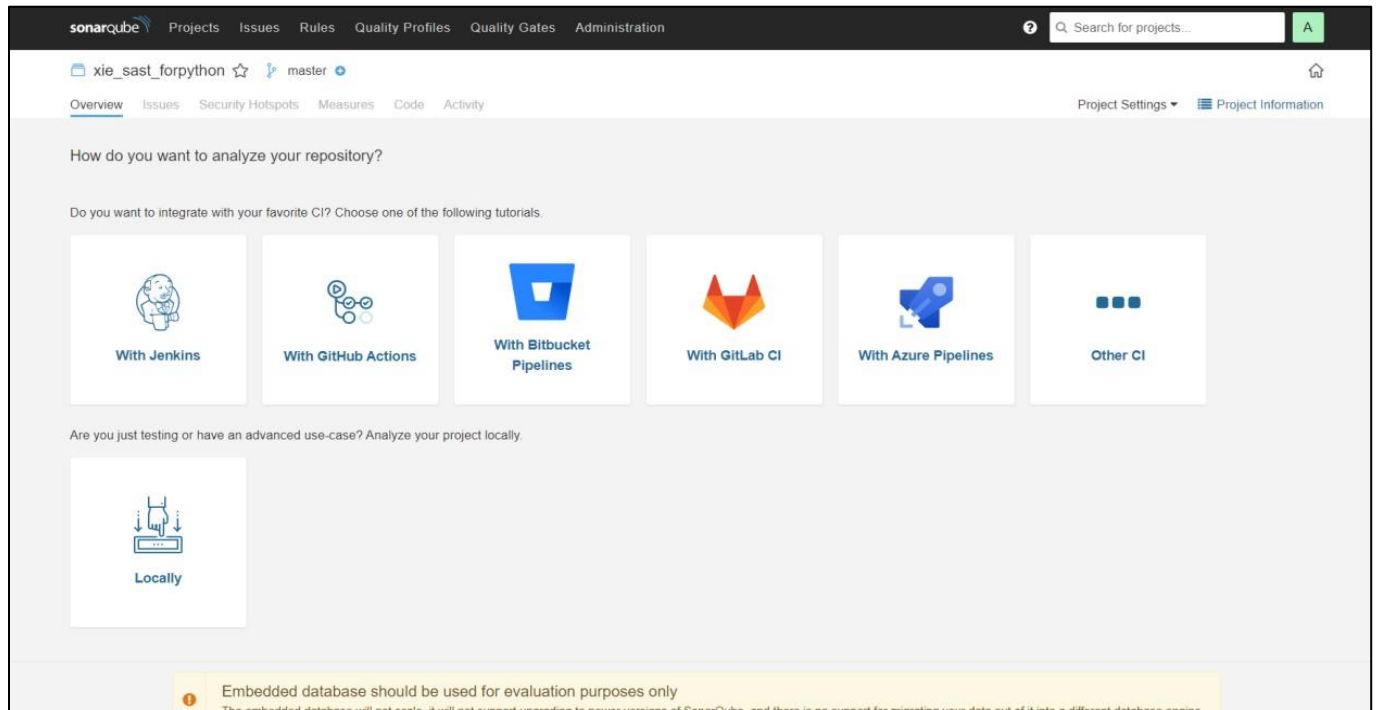
The screenshot shows the 'Create a project' form in SonarQube. The form has two main sections: 'Project display name' and 'Project key'. Both fields are required, indicated by an asterisk (\*). The 'Project display name' field contains the text 'xie\_sast\_forpython' and has a green checkmark icon next to it. The 'Project key' field also contains the text 'xie\_sast\_forpython' and has a green checkmark icon next to it. Below the 'Project key' field, there is a note: 'The project key is a unique identifier for your project. It may contain up to 400 characters. Allowed characters are alphanumeric, '-' (dash), '\_' (underscore), '.' (period) and ':' (colon), with at least one non-digit.' At the bottom of the form, there is a 'Set Up' button.



Name: Harsh Dalvi  
Roll No: 13

Subject: Advance DevOps , Sem: SEM V  
Class / Batch: TE-IT / Batch B

**Step 12:** Therefore, the Project is created.



**Conclusion:** From this experiment it is concluded that, we have learnt the concepts and analyzed the Static Analysis SAST and learned to integrate Jenkins SAST to SonarQube. The ability of SAST tools to catch security problems early in the development process means that even in deadline-driven environments, developers don't need to constantly worry about following best practices. Hence, we have successfully achieved the Lab Outcome One and Four (LO1 and LO4). Also, we have achieved PO1, PO2, PO3, PO4, PO5, PO9, PO10 and PO12 from this experiment.