|  |  |
| --- | --- |
| *A close up of a logo  Description automatically generated* | *DEPARTMENT OF INFORMATION TECHNOLOGY* |

|  |  |
| --- | --- |
| Semester | T.E. Semester V – Information Technology |
| Subject | Advance DevOps Lab |
| Subject Professor In-charge | Prof. Indu Anoop |
| Laboratory | (Leave blank for now) |

|  |  |  |
| --- | --- | --- |
| Student Name |  | |
| Roll Number |  | |
| Grade and Subject Teacher’s Signature |  |  |

|  |  |  |
| --- | --- | --- |
| Experiment | 7 | |
| Problem Statement | To understand static analysis SAST process and learn to integrate Jenkins SAST to SonarQube/GitLab | |
| Resources / Apparatus Required | Hardware: Computer System | Software: Web Browser |
| Details | 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. SAST scans an application before the code is compiled. It's also known as white box testing.  What is SonarQube?  SonarQube is an open-source platform to check the quality of the code. We can generate reports of code with duplicate codes, dead codes, logical error, null-pointers, coding guidelines, testing, bugs, security vulnerabilities, code coverage, etc. We can set up Quality Gates, which allows setting policies like coverage by the new code, bugs count, security rating, reliability rating, etc. This ensures that no build is deployed to production or other environments without passing the quality standard. SonarQube support quality check for most of the well-known languages like Java, C/C++, Groovy, Python, Javascript, PHP, Swift, etc.  What is Jenkins?  Jenkins is an open-source automation tool written in Java with plugins built for Continuous Integration purposes. It helps automate the parts of software development related to building, testing, and deploying, facilitating continuous integration and continuous delivery.  Both SonarQube and Jenkins require java version 11. | |
| Code | **Prerequisites [Installation steps attached-AWS instances used]**   1. A SonarQube Server [Refer SonarQube Installation document] 2. A Jenkins server [Refer Jenkins Installation document] 3. GitLab account   **Overview of Integration Steps**  **PART A: Integrating SonarScanner to Jenkins**  *A.1 Generate a SonarQube token to authenticate from Jenkins*  Graphical user interface, text, application  Description automatically generated  *A.2 Install and Configure SonarScanner Plugin*  Graphical user interface, text, application, email  Description automatically generated  Graphical user interface, text, application, email  Description automatically generated  **PART B: Integration of GitLab to Jenkins**  *B.1 Generate a GitLab Token to authenticate from Jenkins*    Graphical user interface, text, application  Description automatically generated    Figure: Integration of GitLab Token with Jenkins  Graphical user interface, application  Description automatically generated | |
| Conclusion | Understood static analysis SAST process and learnt to integrate Jenkins SAST to SonarQube/GitLab | |