Mikil Talwani D15B/37

Advance Dev Ops lab

Experiment. 7.

Aim-
To understand static analysis SAST process and learn to integrate Jenkins SAST to SonarQube/GitLab

Theory-

What is SAST?

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

Why is SAST important?

Developers dramatically outnumber security staff. It can be difficult for organizations to find the resources to perform code reviews on even a fraction of its application. A key strength of SAST tools is the ability to analyze 100% of the codebase. 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 code developed.

Conclusion -

Thus, we successfully understood importance of SAST and integrated ~~with~~ Jenkins with SonarQube for SAST.