############################# Major Assignment #################################

**- Problem Statement -**

-------------------------------------------------------------------------------------

Implement Security with DevSecOps to Jenkins Pipeline Stages

**a) Docker Security**

**b) Build Security**

**c) Code Security**

More stages to be added like security in every stage

-------------------------------------------------------------------------------------

**- Solution and approach -**

-------------------------------------------------------------------------------------

**1. Code Security and build security** { Implementation of SAST (Static Application Security Testing)

a. Sonar -> For code quality check and determination of various code standards.

b. owasp dependency check -> Implemented owasp dependency check for Java maven project, it checks all the vulnerabilities in the pom.xml file by checking dependencies against a NVD (National Vulnerability Database) which consists of all the dependencies which contain vulnerabilities.

c. jacoco -> Jacoco is a tool used for measuring the extent by which the test cases of the project covers the code. It gives output in the form of % of code, branches, methods and classes covered.

}

**2. Docker Security** {

a. Trivy -> implemented Trivy tool for scanning of docker images and scans vulnerabilities in the container images with primary purpose to identify security vulnerabilities in the container images.

b. Docker bench security -> Docker bench security implementation was done to exploit the security of docker containers. It tests the docker deployment with various automated tests to identify potential security risks and also provides recommendations for improving the security of the docker environment.

}

**3. OS security** {

a. Implemented Public and Private key login instead of password login in my centos7 machine.

b. Disabled root login and password login configurations.

c. Implemented fail2ban which will make sure that no more than 3 retries are given for login to the machine and then will ban that particular user.

d. Changed the port of my centos7 machine to make it less known.

e. Made sure that the system is up-to-date and regular watch on the logs of machine through LogWatch.

}

**4. Application security** {

- Implemented owasp-Zap security protocol in my web application which will assist with various security testing tasks by scanning the web app during run time which implements DAST (Dynamic Application Security Testing).

}