Exam Synopsis – Securing CI/CD Pipeline with SNYK, CodeQL, and Trivy

PB Software Development

Software Security

Fall 2025

Synopsis by Marco Gabel & Fei Gu

Table of Contents

1. Introduction / Motivation

2. Problem Statement

This project investigates how a CI/CD pipeline can be secured using automated analysis tools such as SNYK (Software Composition Analysis), CodeQL (Static Application Security Testing) and Trivy (Container Scanning). The goal is to identify vulnerabilities during the build process and assess how these security controls support the Cyber Resilience Act requirements for secure software development and supply-chain protection.

3. Implementation

3.1 Pipeline architecture

3.2 Tool integration details

3.3 Security findings

3.4 CRA compliance mapping

4. Analysis & Results

5. Conclusion