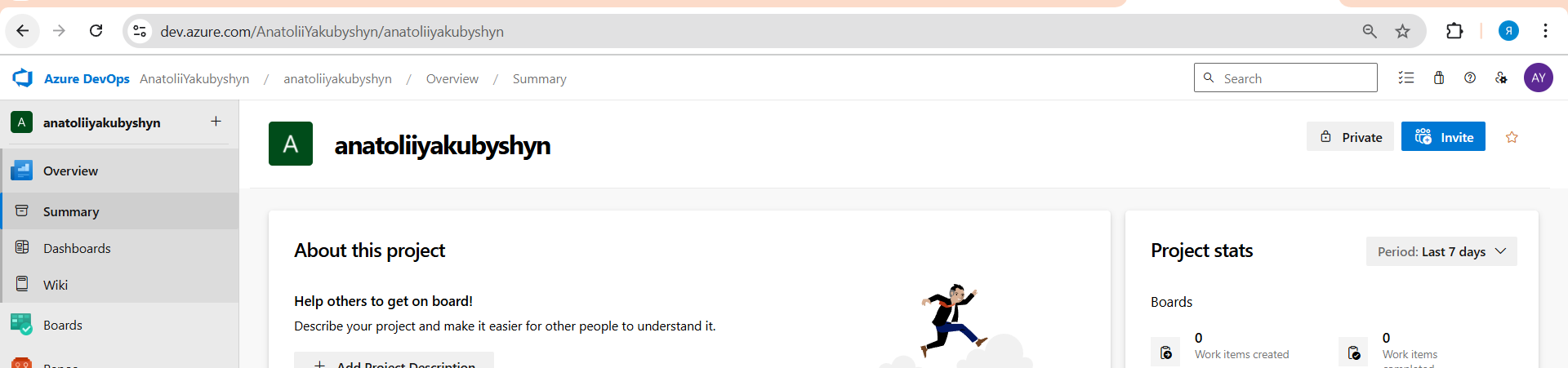
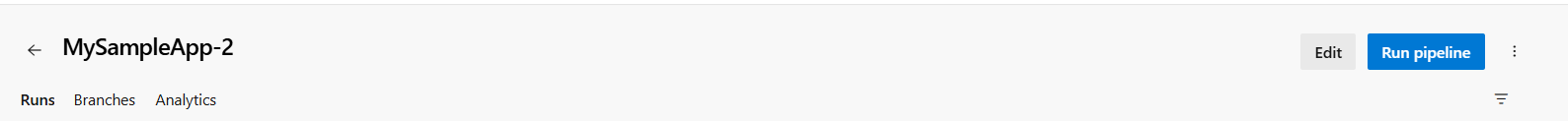
**Task 1: Implementing Basic Security Scans in Azure Pipelines**

**Objective:** Set up a basic security scanning tool in an Azure DevOps pipeline to analyze code for vulnerabilities during the CI/CD process, using tools that offer free tiers or are open-source.

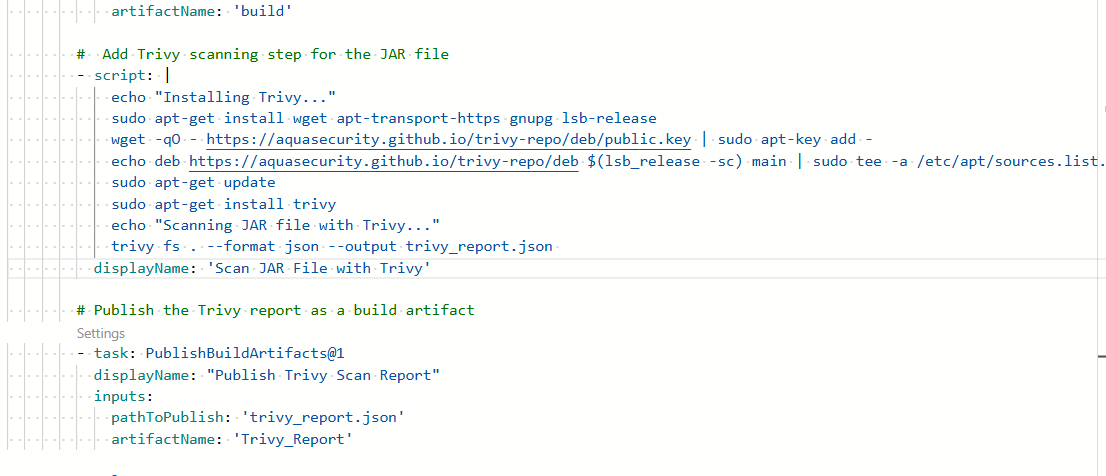
**Steps:**

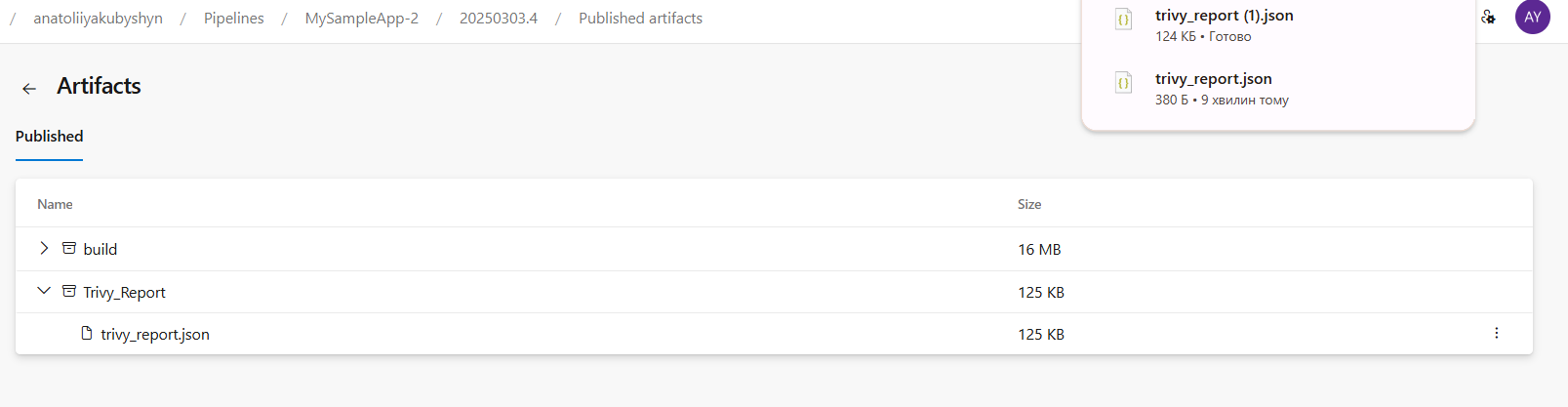
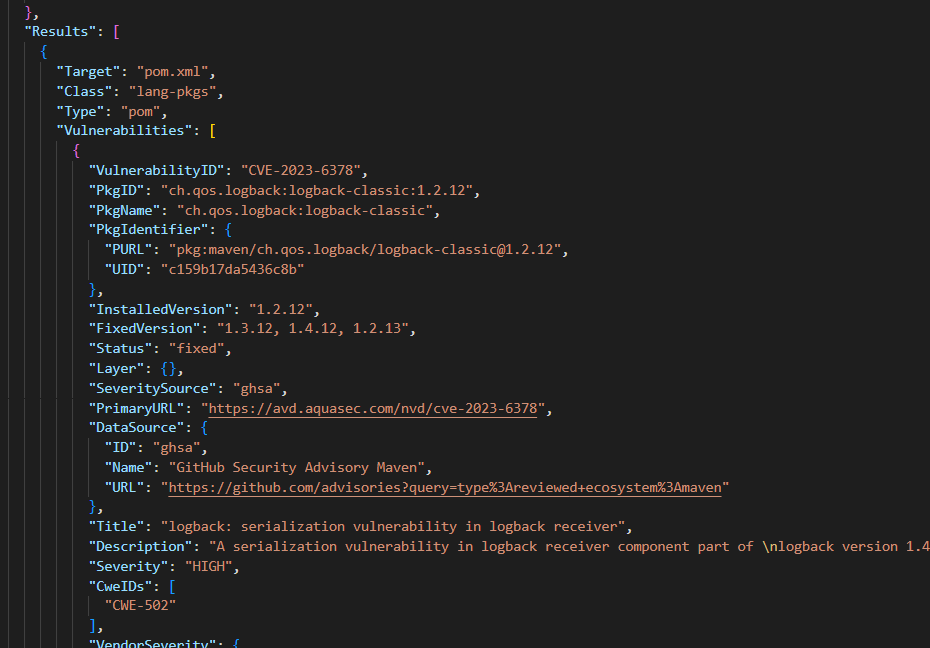
**Log in to your Azure DevOps account and navigate to your project.**

**Create a new pipeline or edit an existing one**

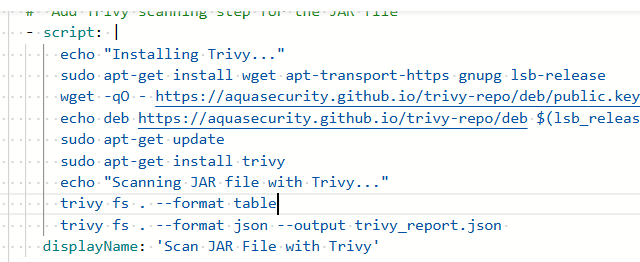
**Choose one of the following tools to integrate into your pipeline:**

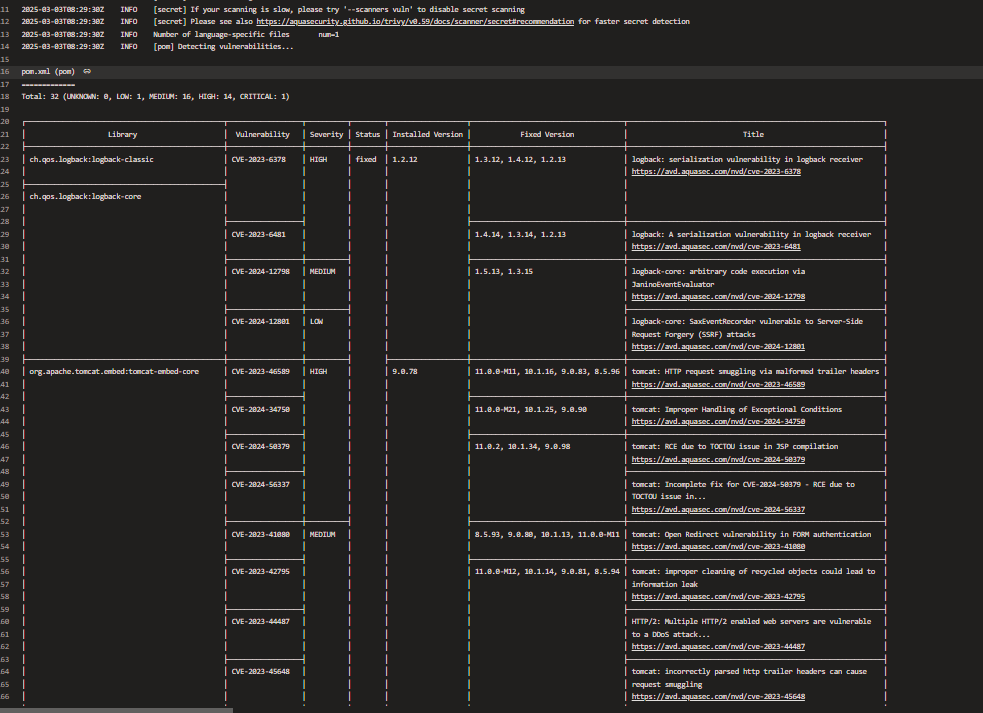
**Trivy**

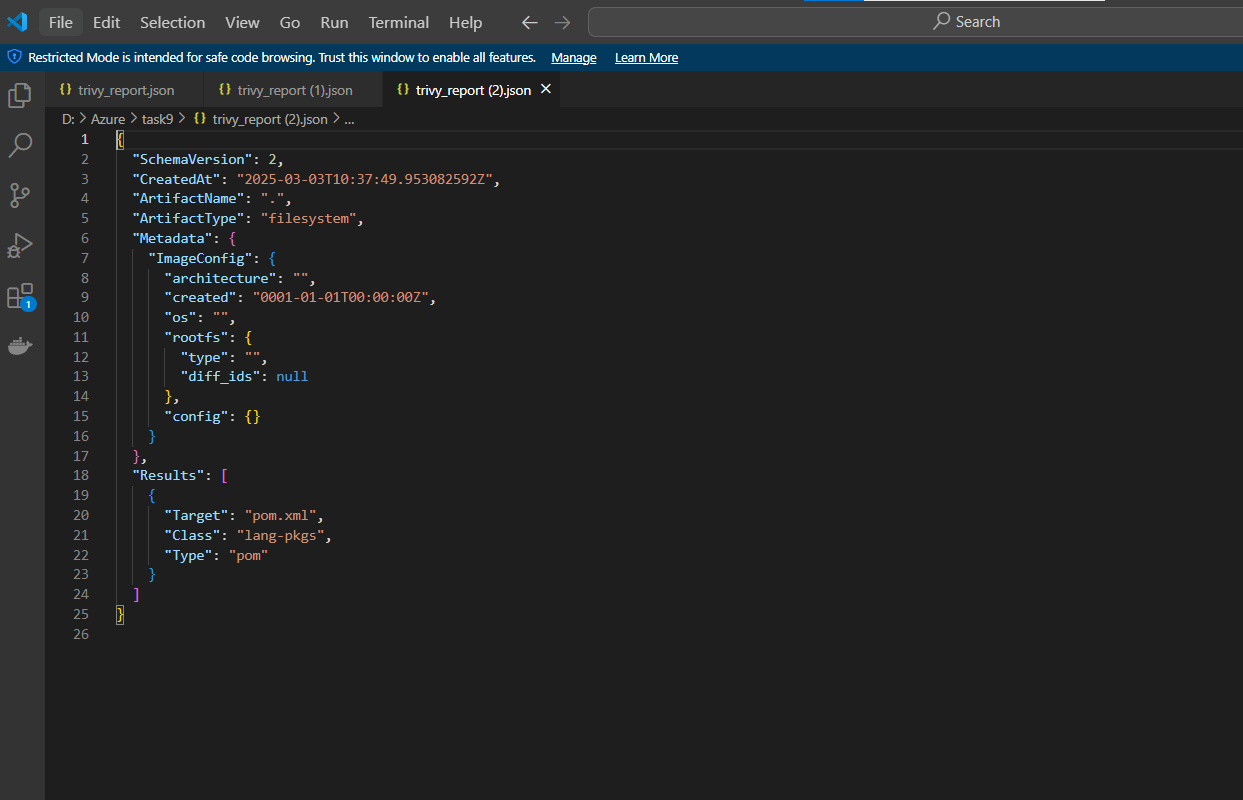
**Configure the selected tool to run during the build stage and analyze the code or artifacts for vulnerabilities.**

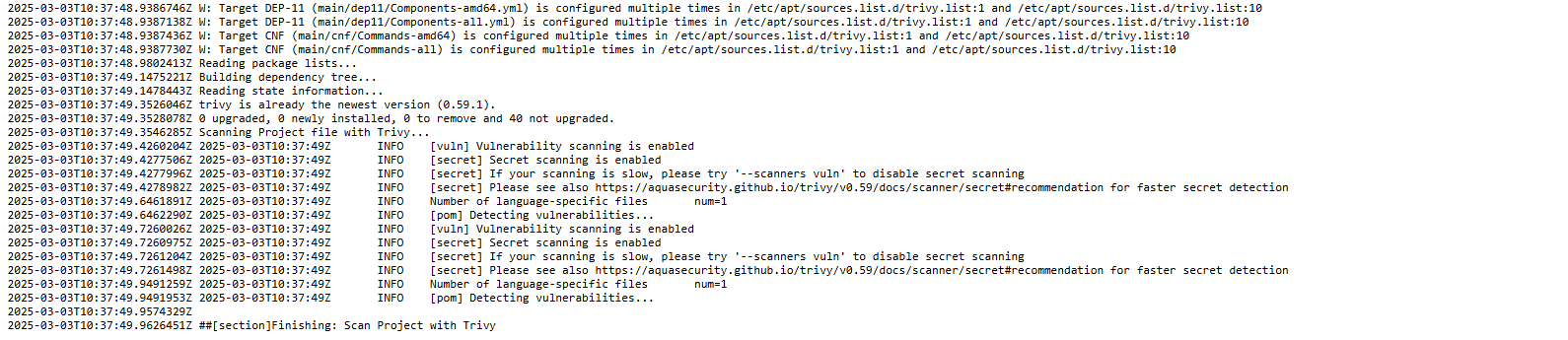
****• Run the pipeline and review the scan results to identify any vulnerabilities.

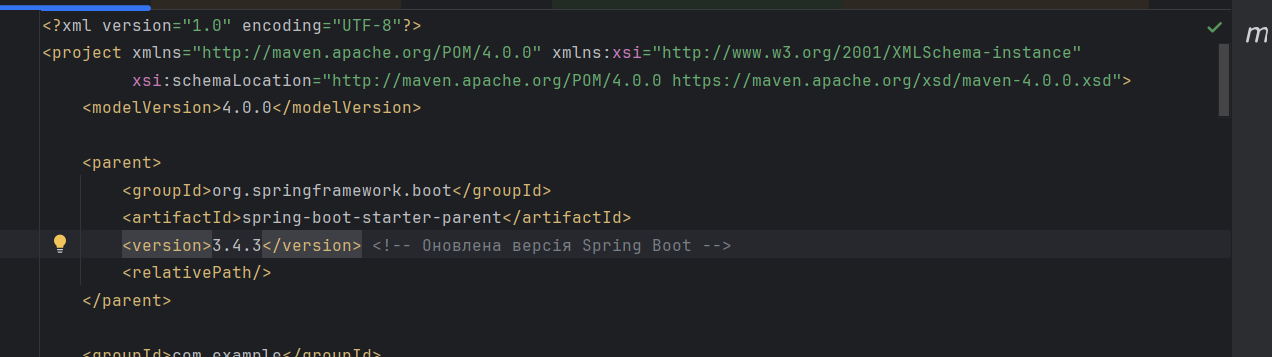
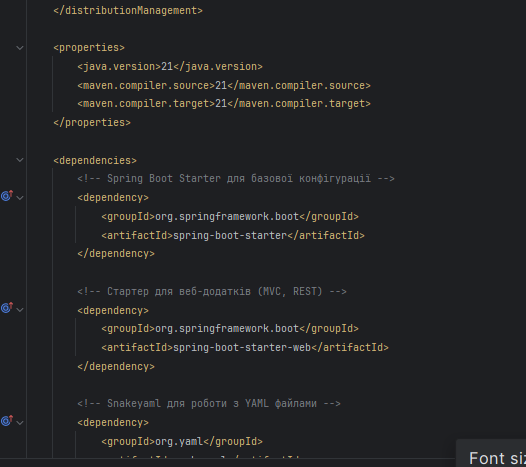
• Address any identified issues and re-run the pipeline to ensure they are resolved.

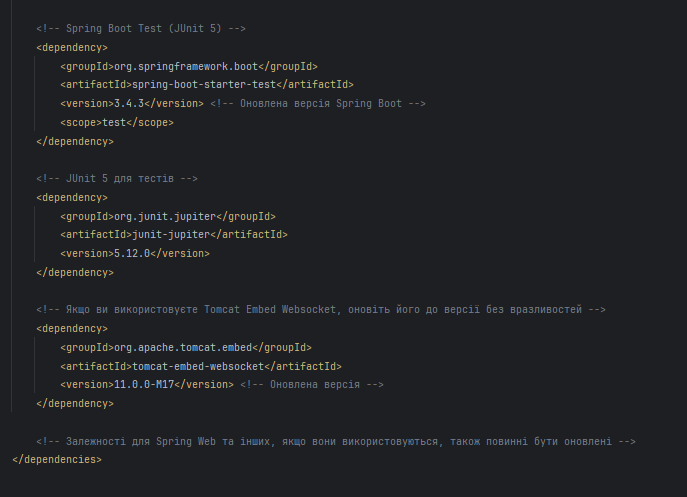
****Refactor to use table

**• Address any identified issues and re-run the pipeline to ensure they are resolved**

**Fixed java version to 21 and upgraded packages**

**No issues in packages founded after that**

****

****

**Task 2: Integrating Azure Security Center with DevOps Workflows**

**Objective**: Configure Azure Security Center to monitor resources and integrate its alerts into Azure DevOps workflows for automated security incident response.

**Steps:**

Enable Azure Security Center in your Azure subscription