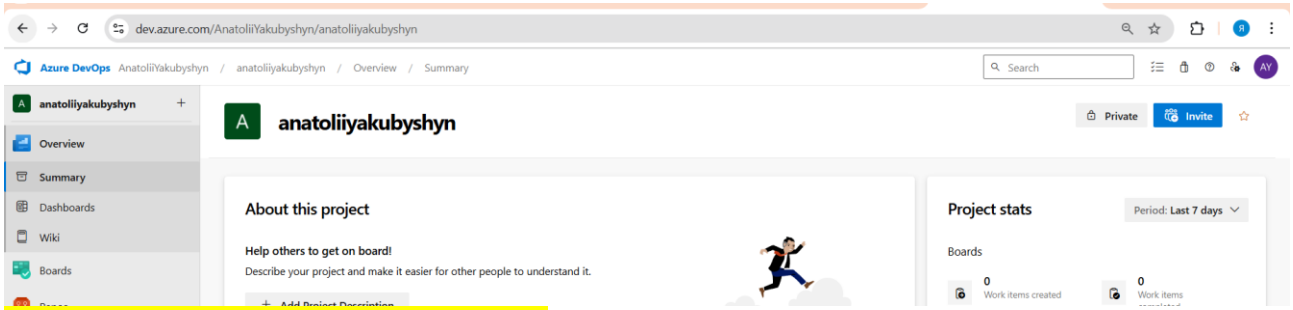
Task 1: Implementing Basic Security Scans in Azure Pipelines

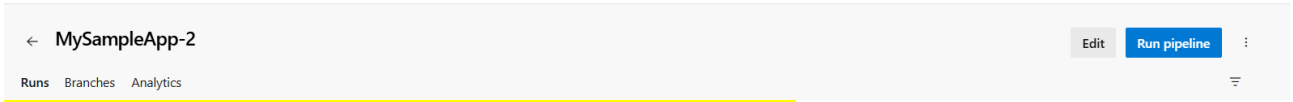
Objective: Set up a basic security scanning tool in an Azure DevOps pipeline to analyze code for vulnerabilities during the CI/CD process, using tools that offer free tiers or are open-source.

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

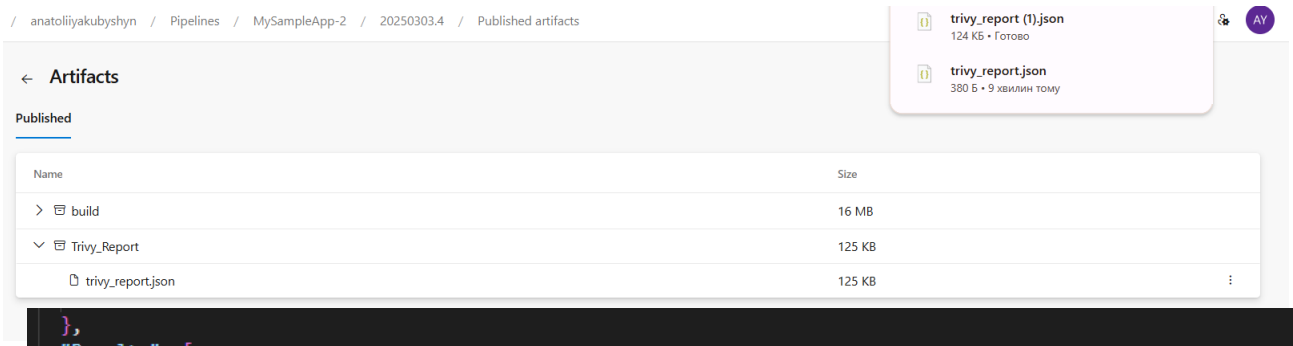
Configure the selected tool to run during the build stage and analyze the code or artifacts for vulnerabilities.

```
    artifactName: 'build'

# Add Trivy scanning step for the JAR file
- script: |
    echo "Installing Trivy..."
    sudo apt-get install wget apt-transport-https gnupg lsb-release
    wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | sudo apt-key add -
    echo deb https://aquasecurity.github.io/trivy-repo/deb $(lsb_release -sc) main | sudo tee -a /etc/apt/sources.list.
    sudo apt-get update
    sudo apt-get install trivy
    echo "Scanning JAR file with Trivy..."
    trivy fs . --format json --output trivy_report.json
  displayName: 'Scan JAR File with Trivy'

# Publish the Trivy report as a build artifact
Settings
- task: PublishBuildArtifacts@1
  displayName: "Publish Trivy Scan Report"
  inputs:
    pathToPublish: 'trivy_report.json'
    artifactName: 'Trivy_Report'
```

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




```
},
"Results": [
  {
    "Target": "pom.xml",
    "Class": "lang-pkgs",
    "Type": "pom",
    "Vulnerabilities": [
      {
        "VulnerabilityID": "CVE-2023-6378",
        "PkgID": "ch.qos.logback:logback-classic:1.2.12",
        "PkgName": "ch.qos.logback:logback-classic",
        "PkgIdentifier": {
          "PURL": "pkg:maven/ch.qos.logback/logback-classic@1.2.12",
          "UID": "c159b17da5436c8b"
        },
        "InstalledVersion": "1.2.12",
        "FixedVersion": "1.3.12, 1.4.12, 1.2.13",
        "Status": "fixed",
        "Layer": {},
        "SeveritySource": "ghsa",
        "PrimaryURL": "https://avd.aquasec.com/nvd/cve-2023-6378",
        "DataSource": {
          "ID": "ghsa",
          "Name": "GitHub Security Advisory Maven",
          "URL": "https://github.com/advisories?query=type%3Areviewed+ecosystem%3Amaven"
        },
        "Title": "logback: serialization vulnerability in logback receiver",
        "Description": "A serialization vulnerability in logback receiver component part of \nlogback version 1.4
        "Severity": "HIGH",
        "CweIDs": [
          "CWE-502"
        ],
        "VendorSeverity": {
```


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

Refactor to use table

```
# Add Trivy scanning step for the JAR file
- script: |
    echo "Installing Trivy..."
    sudo apt-get install wget apt-transport-https gnupg lsb-release
    wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key
    echo deb https://aquasecurity.github.io/trivy-repo/deb $(lsb_releas
    sudo apt-get update
    sudo apt-get install trivy
    echo "Scanning JAR file with Trivy..."
    trivy fs . --format table
    trivy fs . --format json --output trivy_report.json
  displayName: 'Scan JAR File with Trivy'
```

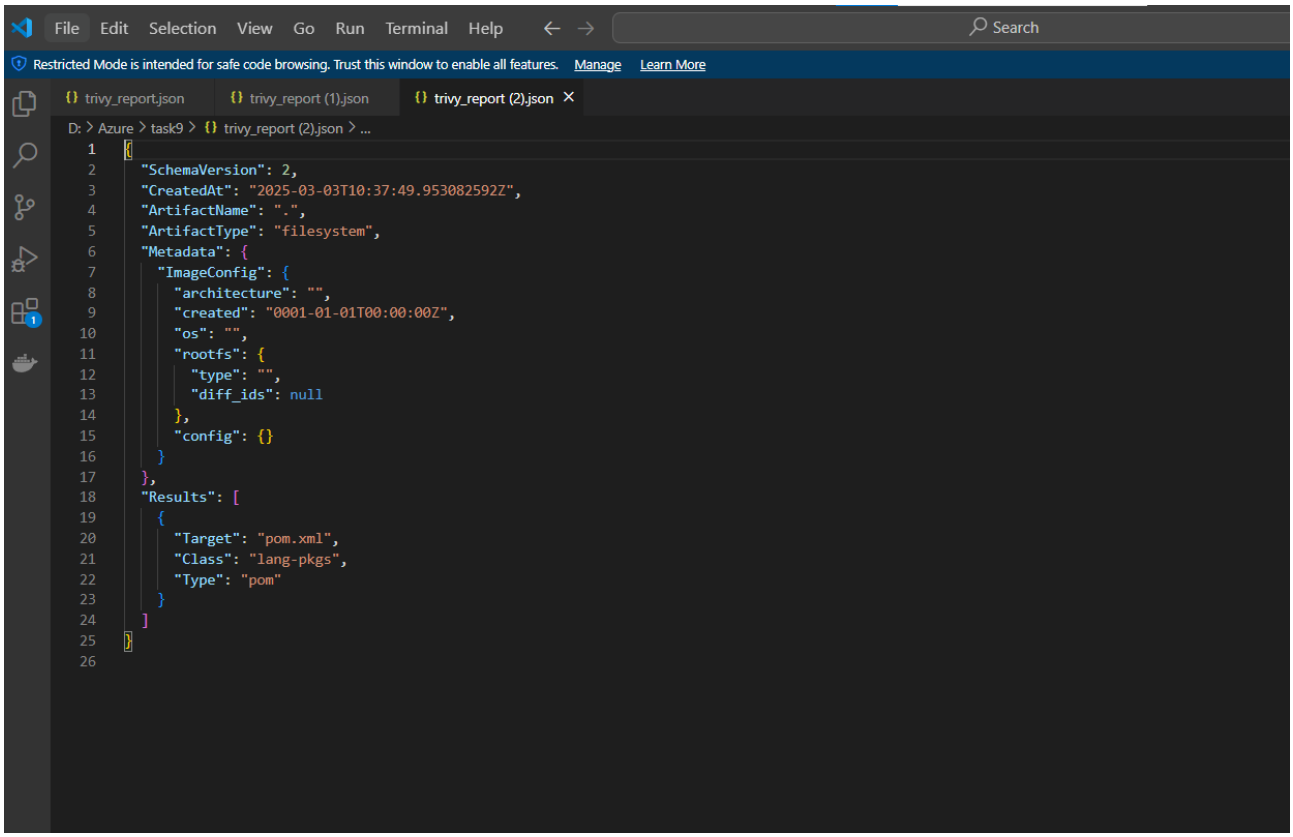
```
2025-03-03T08:29:30Z    INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-03-03T08:29:30Z    INFO    [secret] Please see also https://aquasecurity.github.io/trivy/v0.59/docs/scanner/secret#recommendation for faster secret detection
2025-03-03T08:29:30Z    INFO    Number of language-specific files       num=1
2025-03-03T08:29:30Z    INFO    [pom] Detecting vulnerabilities...

pom.xml (pom)
=============
Total: 32 (UNKNOWN: 0, LOW: 1, MEDIUM: 16, HIGH: 14, CRITICAL: 1)

┌──────────────────────────────────────┬────────────────┬──────────┬────────┬───────────────────┬──────────────────────────────┬──────────────────────────────────────────────────────────────┐
│               Library                │ Vulnerability  │ Severity │ Status │ Installed Version │        Fixed Version         │                            Title                             │
├──────────────────────────────────────┼────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│ ch.qos.logback:logback-classic       │ CVE-2023-6378  │ HIGH     │ fixed  │ 1.2.12            │ 1.3.12, 1.4.12, 1.2.13       │ logback: serialization vulnerability in logback receiver     │
│                                      │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2023-6378                    │
├──────────────────────────────────────┤                │          │        │                   │                              │                                                              │
│ ch.qos.logback:logback-core          │                │          │        │                   │                              │                                                              │
│                                      ├────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│                                      │ CVE-2023-6481  │          │        │                   │ 1.4.14, 1.3.14, 1.2.13       │ logback: A serialization vulnerability in logback receiver   │
│                                      │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2023-6481                    │
│                                      ├────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│                                      │ CVE-2024-12798 │ MEDIUM   │        │                   │ 1.5.13, 1.3.15               │ logback-core: arbitrary code execution via                   │
│                                      │                │          │        │                   │                              │ JaninoEventEvaluator                                         │
│                                      │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2024-12798                   │
│                                      ├────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│                                      │ CVE-2024-12801 │ LOW      │        │                   │                              │ logback-core: SaxEventRecorder vulnerable to Server-Side     │
│                                      │                │          │        │                   │                              │ Request Forgery (SSRF) attacks                               │
│                                      │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2024-12801                   │
├──────────────────────────────────────┼────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│ org.apache.tomcat.embed:tomcat-embed-core │ CVE-2023-46589 │ HIGH     │        │ 9.0.78            │ 11.0.0-M11, 10.1.16, 9.0.83, 8.5.96 │ tomcat: HTTP request smuggling via malformed trailer headers │
│                                      │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2023-46589                   │
│                                      ├────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│                                      │ CVE-2024-34750 │          │        │                   │ 11.0.0-M21, 10.1.25, 9.0.90  │ tomcat: Improper Handling of Exceptional Conditions          │
│                                      │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2024-34750                   │
│                                      ├────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│                                      │ CVE-2024-50379 │          │        │                   │ 11.0.2, 10.1.34, 9.0.98      │ tomcat: RCE due to TOCTOU issue in JSP compilation           │
│                                      │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2024-50379                   │
│                                      ├────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│                                      │ CVE-2024-56337 │          │        │                   │                              │ tomcat: Incomplete fix for CVE-2024-50379 - RCE due to       │
│                                      │                │          │        │                   │                              │ TOCTOU issue in...                                           │
│                                      │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2024-56337                   │
│                                      ├────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│                                      │ CVE-2023-41080 │ MEDIUM   │        │                   │ 8.5.93, 9.0.80, 10.1.13, 11.0.0-M11 │ tomcat: Open Redirect vulnerability in FORM authentication   │
│                                      │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2023-41080                   │
│                                      ├────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│                                      │ CVE-2023-42795 │          │        │                   │ 11.0.0-M12, 10.1.14, 9.0.81, 8.5.94 │ tomcat: improper cleaning of recycled objects could lead to  │
│                                      │                │          │        │                   │                              │ information leak                                             │
│                                      │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2023-42795                   │
│                                      ├────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│                                      │ CVE-2023-44487 │          │        │                   │                              │ HTTP/2: Multiple HTTP/2 enabled web servers are vulnerable   │
│                                      │                │          │        │                   │                              │ to a DDoS attack...                                          │
│                                      │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2023-44487                   │
│                                      ├────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│                                      │ CVE-2023-45648 │          │        │                   │                              │ tomcat: incorrectly parsed http trailer headers can cause    │
│                                      │                │          │        │                   │                              │ request smuggling                                            │
│                                      │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2023-45648                   │
└──────────────────────────────────────┴────────────────┴──────────┴────────┴───────────────────┴──────────────────────────────┴──────────────────────────────────────────────────────────────┘
```

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

Fixed java version to 21 and upgraded packages



```
2025-03-03T10:37:48.9386746Z W: Target DEP-11 (main/dep11/Components-amd64.yml) is configured multiple times in /etc/apt/sources.list.d/trivy.list:1 and /etc/apt/sources.list.d/trivy.list:10
2025-03-03T10:37:48.9387138Z W: Target DEP-11 (main/dep11/Components-all.yml) is configured multiple times in /etc/apt/sources.list.d/trivy.list:1 and /etc/apt/sources.list.d/trivy.list:10
2025-03-03T10:37:48.9387436Z W: Target CNF (main/cnf/Commands-amd64) is configured multiple times in /etc/apt/sources.list.d/trivy.list:1 and /etc/apt/sources.list.d/trivy.list:10
2025-03-03T10:37:48.9387730Z W: Target CNF (main/cnf/Commands-all) is configured multiple times in /etc/apt/sources.list.d/trivy.list:1 and /etc/apt/sources.list.d/trivy.list:10
2025-03-03T10:37:48.9802413Z Reading package lists...
2025-03-03T10:37:49.1475221Z Building dependency tree...
2025-03-03T10:37:49.1478443Z Reading state information...
2025-03-03T10:37:49.3526046Z trivy is already the newest version (0.59.1).
2025-03-03T10:37:49.3528078Z 0 upgraded, 0 newly installed, 0 to remove and 40 not upgraded.
2025-03-03T10:37:49.3546285Z Scanning Project file with Trivy...
2025-03-03T10:37:49.4260204Z 2025-03-03T10:37:49Z	INFO	[vuln] Vulnerability scanning is enabled
2025-03-03T10:37:49.4277506Z 2025-03-03T10:37:49Z	INFO	[secret] Secret scanning is enabled
2025-03-03T10:37:49.4277996Z 2025-03-03T10:37:49Z	INFO	[secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-03-03T10:37:49.4278982Z 2025-03-03T10:37:49Z	INFO	[secret] Please see also https://aquasecurity.github.io/trivy/v0.59/docs/scanner/secret#recommendation for faster secret detection
2025-03-03T10:37:49.6461891Z 2025-03-03T10:37:49Z	INFO	Number of language-specific files	num=1
2025-03-03T10:37:49.6462290Z 2025-03-03T10:37:49Z	INFO	[pom] Detecting vulnerabilities...
2025-03-03T10:37:49.7260026Z 2025-03-03T10:37:49Z	INFO	[vuln] Vulnerability scanning is enabled
2025-03-03T10:37:49.7260975Z 2025-03-03T10:37:49Z	INFO	[secret] Secret scanning is enabled
2025-03-03T10:37:49.7261204Z 2025-03-03T10:37:49Z	INFO	[secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-03-03T10:37:49.7261498Z 2025-03-03T10:37:49Z	INFO	[secret] Please see also https://aquasecurity.github.io/trivy/v0.59/docs/scanner/secret#recommendation for faster secret detection
2025-03-03T10:37:49.9491259Z 2025-03-03T10:37:49Z	INFO	Number of language-specific files	num=1
2025-03-03T10:37:49.9491953Z 2025-03-03T10:37:49Z	INFO	[pom] Detecting vulnerabilities...
2025-03-03T10:37:49.9574329Z
2025-03-03T10:37:49.9626451Z ##[section]Finishing: Scan Project with Trivy
```

No issues in packages founded after that

```xml
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 https://maven.apache.org/xsd/maven-4.0.0.xsd">
    <modelVersion>4.0.0</modelVersion>

    <parent>
        <groupId>org.springframework.boot</groupId>
        <artifactId>spring-boot-starter-parent</artifactId>
        <version>3.4.3</version> <!-- Оновлена версія Spring Boot -->
        <relativePath/>
    </parent>

    <groupId>com.example</groupId>
```

```xml
    </distributionManagement>

    <properties>
        <java.version>21</java.version>
        <maven.compiler.source>21</maven.compiler.source>
        <maven.compiler.target>21</maven.compiler.target>
    </properties>

    <dependencies>
        <!-- Spring Boot Starter для базової конфігурації -->
        <dependency>
            <groupId>org.springframework.boot</groupId>
            <artifactId>spring-boot-starter</artifactId>
        </dependency>

        <!-- Стартер для веб-додатків (MVC, REST) -->
        <dependency>
            <groupId>org.springframework.boot</groupId>
            <artifactId>spring-boot-starter-web</artifactId>
        </dependency>

        <!-- Snakeyaml для роботи з YAML файлами -->
        <dependency>
            <groupId>org.yaml</groupId>
```

```xml
    <!-- Spring Boot Test (JUnit 5) -->
    <dependency>
        <groupId>org.springframework.boot</groupId>
        <artifactId>spring-boot-starter-test</artifactId>
        <version>3.4.3</version> <!-- Оновлена версія Spring Boot -->
        <scope>test</scope>
    </dependency>

    <!-- JUnit 5 для тестів -->
    <dependency>
        <groupId>org.junit.jupiter</groupId>
        <artifactId>junit-jupiter</artifactId>
        <version>5.12.0</version>
    </dependency>

    <!-- Якщо ви використовуєте Tomcat Embed Websocket, оновіть його до версії без вразливостей -->
    <dependency>
        <groupId>org.apache.tomcat.embed</groupId>
        <artifactId>tomcat-embed-websocket</artifactId>
        <version>11.0.0-M17</version> <!-- Оновлена версія -->
    </dependency>

    <!-- Залежності для Spring Web та інших, якщо вони використовуються, також повинні бути оновлені -->
</dependencies>
```

```xml
    <build>
        <plugins>
            <!-- Compiler Plugin -->
            <plugin>
                <groupId>org.apache.maven.plugins</groupId>
                <artifactId>maven-compiler-plugin</artifactId>
                <version>3.11.0</version>
                <configuration>
                    <source>21</source>
                    <target>21</target>
                </configuration>
            </plugin>
        </plugins>
    </build>
</project>
```

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