

# CI Tools Task

## Step 1

Launch spot AWS EC2 instance with t2.medium instance type in Cybage AWS Account

## Step 2

Install below pre-requisite software to run the spring boot application

a) Java

Install java 17 application

```
$ sudo apt install openjdk-17-jdk openjdk-17-jre
```

check java version

```
$ java -version
```

```
System information as of Fri May 10 09:52:41 UTC 2024

System load:  0.0               Processes:    114
Usage of /:   18.6% of 28.89GB  Users logged in: 1
Memory usage: 21%              IPv4 address for eth0: 10.0.16.195
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

3 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

*** System restart required ***
Last login: Fri May 10 09:50:46 2024 from 18.206.107.27
ubuntu@ip-10-0-16-195:~$ ls
employee-management-main  employee-management-main.zip
ubuntu@ip-10-0-16-195:~$ cd employee-management-main/
ubuntu@ip-10-0-16-195:~/employee-management-main$ vav --version
Command 'vav' not found, did you mean:
  command 'vpv' from snap vpv (v0.8.2)
  command 'dav' from deb dav-text (0.9.0-2)
  command 'vam' from deb vim-addon-manager (0.5.10)
  command 'vax' from deb simh (3.8.1-6.1)
  command 'gav' from deb gav (0.9.0-3.1)
See 'snap info <snapname>' for additional versions.
ubuntu@ip-10-0-16-195:~/employee-management-main$ java --version
openjdk 17.0.10 2024-01-16
OpenJDK Runtime Environment (build 17.0.10+7-Ubuntu-122.04.1)
OpenJDK 64-Bit Server VM (build 17.0.10+7-Ubuntu-122.04.1, mixed mode, sharing)
ubuntu@ip-10-0-16-195:~/employee-management-main$
```

i-021c086616d99335a (snyk-rushikesh)

PublicIPs: 3.84.131.249 PrivateIPs: 10.0.16.195

## b) Maven

Install maven

\$ sudo apt install maven

Check maven version

\$ mvn -version

\$ mvn clean

to clean the project by deleting the target directory

```
No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ip-10-0-16-195:/home/ubuntu/employee-management-main# mvn clean
[INFO] Scanning for projects...
[WARNING]
[WARNING] Some problems were encountered while building the effective model for net.javaguides:springboot-backend:jar:0.0.1-SNAPSHOT
[WARNING] 'build.plugins.plugin.(groupId:artifactId)' must be unique but found duplicate declaration of plugin org.jacoco:jacoco-maven-plugin @ line 102,
[WARNING]
[WARNING] It is highly recommended to fix these problems because they threaten the stability of your build.
[WARNING]
[WARNING] For this reason, future Maven versions might no longer support building such malformed projects.
[WARNING]
[INFO] -----< net.javaguides:springboot-backend >-----
[INFO] Building springboot-backend 0.0.1-SNAPSHOT
[INFO] -----[ jar ]-----
[INFO]
[INFO] --- maven-clean-plugin:3.2.0:clean (default-clean) @ springboot-backend ---
[INFO] Deleting /home/ubuntu/employee-management-main/target
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
[INFO] Total time: 0.610 s
[INFO] Finished at: 2024-05-10T13:37:54Z
[INFO] -----
root@ip-10-0-16-195:/home/ubuntu/employee-management-main#
```

i-021c086616d99335a (snyk-rushikesh)

\$ mvn compile

to compile your code after cleaning

```
root@ip-10-0-16-195:/home/ubuntu/employee-management-main# mvn compile
[INFO] Scanning for projects...
[WARNING]
[WARNING] Some problems were encountered while building the effective model for net.javaguides:springboot-backend:jar:0.0.1-SNAPSHOT
[WARNING] 'build.plugins.plugin.(groupId:artifactId)' must be unique but found duplicate declaration of plugin org.jacoco:jacoco-maven-plugin @ line 102,
[WARNING]
[WARNING] It is highly recommended to fix these problems because they threaten the stability of your build.
[WARNING]
[WARNING] For this reason, future Maven versions might no longer support building such malformed projects.
[WARNING]
[INFO] -----< net.javaguides:springboot-backend >-----
[INFO] Building springboot-backend 0.0.1-SNAPSHOT
[INFO] -----[ jar ]-----
[INFO]
[INFO] --- jacoco-maven-plugin:0.8.7:prepare-agent (default) @ springboot-backend ---
[INFO] argLine set to -javaagent:/root/.m2/repository/org/jacoco/org.jacoco.agent/0.8.7/org.jacoco.agent-0.8.7-runtime.jar=destfile=/home/ubuntu/
[INFO]
[INFO] --- maven-resources-plugin:3.3.0:resources (default-resources) @ springboot-backend ---
[INFO] Copying 1 resource
[INFO] Copying 0 resource
[INFO]
[INFO] --- maven-compiler-plugin:3.10.1:compile (default-compile) @ springboot-backend ---
[INFO] Changes detected - recompiling the module!
[INFO] Compiling 5 source files to /home/ubuntu/employee-management-main/target/classes
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
[INFO] Total time: 3.158 s
[INFO] Finished at: 2024-05-10T13:40:10Z
[INFO] -----
root@ip-10-0-16-195:/home/ubuntu/employee-management-main#
```

i-021c086616d99335a (snyk-rushikesh)

Public IPs: 3.84.131.249 Private IPs: 10.0.16.195

\$ mvn package / \$ mvn jar  
package your project into a JAR file

```
root@ip-10-0-16-195:/home/ubuntu/employee-management-main# mvn compile
[INFO] Scanning for projects...
[WARNING]
[WARNING] Some problems were encountered while building the effective model for net.javaguides:springboot-backend:jar:0.0.1-SNAPSHOT
[WARNING] 'build.plugins.plugin.(groupId:artifactId)' must be unique but found duplicate declaration of plugin org.jacoco:jacoco-maven-plugin @ 1
[WARNING]
[WARNING] It is highly recommended to fix these problems because they threaten the stability of your build.
[WARNING]
[WARNING] For this reason, future Maven versions might no longer support building such malformed projects.
[WARNING]
[INFO] -----< net.javaguides:springboot-backend >-----
[INFO] Building springboot-backend 0.0.1-SNAPSHOT
[INFO] -----[ jar ]-----
[INFO]
[INFO] --- jacoco-maven-plugin:0.8.7:prepare-agent (default) @ springboot-backend ---
[INFO] argLine set to -javaagent:/root/.m2/repository/org/jacoco/org.jacoco.agent/0.8.7/org.jacoco.agent-0.8.7-runtime.jar=destfile=/home/ubuntu/
[INFO]
[INFO] --- maven-resources-plugin:3.3.0:resources (default-resources) @ springboot-backend ---
[INFO] Copying 1 resource
[INFO] Copying 0 resource
[INFO]
[INFO] --- maven-compiler-plugin:3.10.1:compile (default-compile) @ springboot-backend ---
[INFO] Changes detected - recompiling the module!
[INFO] Compiling 5 source files to /home/ubuntu/employee-management-main/target/classes
[INFO]
[INFO] BUILD SUCCESS
[INFO]
[INFO] -----
[INFO] Total time: 3.158 s
[INFO] Finished at: 2024-05-10T13:40:10Z
[INFO]
[INFO] -----
root@ip-10-0-16-195:/home/ubuntu/employee-management-main#
```

i-021c086616d99335a (snky-rushikesh)  
PublicIPs: 3.84.131.249 PrivateIPs: 10.0.16.195

\$ mvn install  
Maven installs the packaged artifacts into the local Maven repository (/root/.m2/repository)

```
[INFO] Analyzed bundle 'springboot-backend' with 4 classes
[INFO]
[INFO] --- maven-jar-plugin:3.3.0:jar (default-jar) @ springboot-backend ---
[INFO]
[INFO] --- spring-boot-maven-plugin:3.0.4:repackage (repackage) @ springboot-backend ---
[INFO] Replacing main artifact with repackaged archive
[INFO]
[INFO] --- jacoco-maven-plugin:0.8.7:check (jacoco-check) @ springboot-backend ---
[INFO] Loading execution data file /home/ubuntu/employee-management-main/target/jacoco.exec
[INFO] Analyzed bundle 'springboot-backend' with 4 classes
[INFO] All coverage checks have been met.
[INFO]
[INFO] --- maven-install-plugin:3.0.1:install (default-install) @ springboot-backend ---
Downloading from central: https://repo.maven.apache.org/maven2/org/eclipse/aether/aether-util/1.0.0.v20140518/aether-util-1.0.0.v20140518.pom
Downloaded from central: https://repo.maven.apache.org/maven2/org/eclipse/aether/aether-util/1.0.0.v20140518/aether-util-1.0.0.v20140518.pom (2.2 kB at 157 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/eclipse/aether/aether/1.0.0.v20140518/aether-1.0.0.v20140518.pom
Downloaded from central: https://repo.maven.apache.org/maven2/org/eclipse/aether/aether/1.0.0.v20140518/aether-1.0.0.v20140518.pom (30 kB at 914 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/eclipse/aether/aether-api/1.0.0.v20140518/aether-api-1.0.0.v20140518.pom
Downloaded from central: https://repo.maven.apache.org/maven2/org/eclipse/aether/aether-api/1.0.0.v20140518/aether-api-1.0.0.v20140518.pom (1.9 kB at 112 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/eclipse/aether/aether-util/1.0.0.v20140518/aether-util-1.0.0.v20140518.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/eclipse/aether/aether-api/1.0.0.v20140518/aether-api-1.0.0.v20140518.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/eclipse/aether/aether-util/1.0.0.v20140518/aether-util-1.0.0.v20140518.jar (146 kB at 1.4 MB/s)
Downloaded from central: https://repo.maven.apache.org/maven2/org/eclipse/aether/aether-api/1.0.0.v20140518/aether-api-1.0.0.v20140518.jar (136 kB at 1.1 MB/s)
[INFO] Installing /home/ubuntu/employee-management-main/pom.xml to /root/.m2/repository/net/javaguides/springboot-backend/0.0.1-SNAPSHOT/springboot-backend-0.0.1-SNAPSHOT.jar
[INFO] Installing /home/ubuntu/employee-management-main/target/springboot-backend-0.0.1-SNAPSHOT.jar to /root/.m2/repository/net/javaguides/springboot-backend/0.0.1-SNAPSHOT.jar
[INFO]
[INFO] BUILD SUCCESS
[INFO]
[INFO] -----
[INFO] Total time: 14.480 s
[INFO] Finished at: 2024-05-10T13:44:09Z
[INFO]
[INFO] -----
root@ip-10-0-16-195:/home/ubuntu/employee-management-main#
```

i-021c086616d99335a (snky-rushikesh)  
PublicIPs: 3.84.131.249 PrivateIPs: 10.0.16.195

\$ mvn clean test

first clean the project by removing the target directory and then compile the source code and execute all the tests in the project

```
aws Services Search [Alt+S]
[INFO] BUILD SUCCESS
[INFO] -----
[INFO] Total time: 15.712 s
[INFO] Finished at: 2024-05-10T08:21:43Z
[INFO] -----
ubuntu@ip-10-0-16-195:~/employee-management-main$ ls
Dockerfile LICENSE README.md contrib manifests pom.xml src target trivy_0.24.0_Linux-64bit.tar.gz
ubuntu@ip-10-0-16-195:~/employee-management-main$ vi pom.xml
ubuntu@ip-10-0-16-195:~/employee-management-main$ mvn clean test
[INFO] Scanning for projects...
[WARNING]
[WARNING] Some problems were encountered while building the effective model for net.javaguides:springboot-backend:jar:0.0.1-SNAPSHOT
[WARNING] 'build.plugins.plugin.(groupId:artifactId)' must be unique but found duplicate declaration of plugin org.jacoco:jacoco-maven-plugin @ line 102
[WARNING]
[WARNING] It is highly recommended to fix these problems because they threaten the stability of your build.
[WARNING]
[WARNING] For this reason, future Maven versions might no longer support building such malformed projects.
[WARNING]
[INFO] -----< net.javaguides:springboot-backend >-----
[INFO] Building springboot-backend 0.0.1-SNAPSHOT
[INFO] -----[ jar ]-----
Downloading from central: https://repo.maven.apache.org/maven2/org/jacoco/jacoco-maven-plugin/0.8.7/jacoco-maven-plugin-0.8.7.pom
Downloaded from central: https://repo.maven.apache.org/maven2/org/jacoco/jacoco-maven-plugin/0.8.7/jacoco-maven-plugin-0.8.7.pom (3.7 kB at 13 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/jacoco/org.jacoco.build/0.8.7/org.jacoco.build-0.8.7.pom
Downloaded from central: https://repo.maven.apache.org/maven2/org/jacoco/org.jacoco.build/0.8.7/org.jacoco.build-0.8.7.pom (43 kB at 763 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/jacoco/jacoco-maven-plugin/0.8.7/jacoco-maven-plugin-0.8.7.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/jacoco/jacoco-maven-plugin/0.8.7/jacoco-maven-plugin-0.8.7.jar (56 kB at 1.3 MB/s)
[INFO]
[INFO] --- maven-clean-plugin:3.2.0:clean (default-clean) @ springboot-backend ---
[INFO] Deleting /home/ubuntu/employee-management-main/target
[INFO]
[INFO] --- jacoco-maven-plugin:0.8.7:prepare-agent (default) @ springboot-backend ---
Downloading from central: https://repo.maven.apache.org/maven2/org/jacoco/org.jacoco.agent/0.8.7/org.jacoco.agent-0.8.7.pom
Downloaded from central: https://repo.maven.apache.org/maven2/org/jacoco/org.jacoco.agent/0.8.7/org.jacoco.agent-0.8.7.pom (3.5 kB at 184 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/jacoco/org.jacoco.core/0.8.7/org.jacoco.core-0.8.7.pom
Downloaded from central: https://repo.maven.apache.org/maven2/org/jacoco/org.jacoco.core/0.8.7/org.jacoco.core-0.8.7.pom (2.1 kB at 208 kB/s)
i-021c086616d99335a (snky-rushikesh)
```

\$ mvn clean verify

Maven will first clean the project by removing the target directory, then compile the source code, execute tests, package the application, and finally verify that it meets the specified quality criteria

```
ubuntu@ip-10-0-16-195:~/employee-management-main$ mvn clean verify
[INFO] Scanning for projects...
[WARNING]
[WARNING] Some problems were encountered while building the effective model for net.javaguides:springboot-backend:jar:0.0.1-SNAPSHOT
[WARNING] 'build.plugins.plugin.(groupId:artifactId)' must be unique but found duplicate declaration of plugin org.jacoco:jacoco-maven-plugin @ line 102
[WARNING]
[WARNING] It is highly recommended to fix these problems because they threaten the stability of your build.
[WARNING]
[WARNING] For this reason, future Maven versions might no longer support building such malformed projects.
[WARNING]
[INFO] -----< net.javaguides:springboot-backend >-----
[INFO] Building springboot-backend 0.0.1-SNAPSHOT
[INFO] -----[ jar ]-----
[INFO]
[INFO] --- maven-clean-plugin:3.2.0:clean (default-clean) @ springboot-backend ---
[INFO] Deleting /home/ubuntu/employee-management-main/target
[INFO]
[INFO] --- jacoco-maven-plugin:0.8.7:prepare-agent (default) @ springboot-backend ---
[INFO] argLine set to -javaagent:/home/ubuntu/.m2/repository/org/jacoco/org.jacoco.agent/0.8.7/org.jacoco.agent-0.8.7-runtime.jar
[INFO]
[INFO] --- maven-resources-plugin:3.3.0:resources (default-resources) @ springboot-backend ---
[INFO] Copying 1 resource
[INFO] Copying 0 resource
[INFO]
[INFO] --- maven-compiler-plugin:3.10.1:compile (default-compile) @ springboot-backend ---
[INFO] Changes detected - recompiling the module!
[INFO] Compiling 5 source files to /home/ubuntu/employee-management-main/target/classes
[INFO]
[INFO] --- maven-resources-plugin:3.3.0:testResources (default-testResources) @ springboot-backend ---
[INFO] skip non existing resourceDirectory /home/ubuntu/employee-management-main/src/test/resources
[INFO]
[INFO] --- maven-compiler-plugin:3.10.1:testCompile (default-testCompile) @ springboot-backend ---
[INFO] Changes detected - recompiling the module!
i-021c086616d99335a (snky-rushikesh)
PublicIPs: 3.84.131.249 PrivateIPs: 10.0.16.195
```

\$ mvn site  
to generate a project's site documentation

```
root@ip-172-31-36-251:/home# cd ubuntu/
root@ip-172-31-36-251:/home/ubuntu# cd employee-management/
root@ip-172-31-36-251:/home/ubuntu/employee-management# mvn site
[INFO] Scanning for projects...
[WARNING]
[WARNING] Some problems were encountered while building the effective model for net.javaguides:springboot-backend:jar:0.0.1-SNAPSHOT
[WARNING] 'build.plugins.plugin.(groupId:artifactId)' must be unique but found duplicate declaration of plugin org.jacoco:jacoco-maven-plugin @ line 101, column 10
[WARNING]
[WARNING] It is highly recommended to fix these problems because they threaten the stability of your build.
[WARNING]
[WARNING] For this reason, future Maven versions might no longer support building such malformed projects.
[WARNING]
[INFO]
[INFO] -----< net.javaguides:springboot-backend >-----
[INFO] Building springboot-backend 0.0.1-SNAPSHOT
[INFO] -----[ jar ]-----
[INFO]
[INFO] --- maven-site-plugin:3.3:site (default-site) @ springboot-backend ---
[WARNING] Report plugin org.apache.maven.plugins:maven-project-info-reports-plugin has an empty version.
[WARNING]
[WARNING] It is highly recommended to fix these problems because they threaten the stability of your build.
[WARNING]
[WARNING] For this reason, future Maven versions might no longer support building such malformed projects.
[INFO] configuring report plugin org.apache.maven.plugins:maven-project-info-reports-plugin:3.5.0
[WARNING] Error injecting: org.apache.maven.report.projectinfo.CiManagementReport
java.lang.NoClassDefFoundError: org/apache/maven/doxia/siterenderer/DocumentContent
    at java.lang.Class.getDeclaredConstructor0 (Native Method)
    at java.lang.Class.privateGetDeclaredConstructors (Class.java:3373)
    at java.lang.Class.getDeclaredConstructors (Class.java:2555)
    at com.google.inject.spi.InjectionPoint.forConstructorOf (InjectionPoint.java:243)
    at com.google.inject.internal.ConstructorBindingImpl.create (ConstructorBindingImpl.java:115)
    at com.google.inject.internal.InjectorImpl.createUninitializedBinding (InjectorImpl.java:717)
    at com.google.inject.internal.InjectorImpl.createJustInTimeBinding (InjectorImpl.java:941)
    at com.google.inject.internal.InjectorImpl.createJustInTimeBindingRecursive (InjectorImpl.java:863)
    at com.google.inject.internal.InjectorImpl.getJustInTimeBinding (InjectorImpl.java:300)
    at com.google.inject.internal.InjectorImpl.getBindingOrThrow (InjectorImpl.java:231)
    at com.google.inject.internal.InjectorImpl.getProviderOrThrow (InjectorImpl.java:1084)
    at com.google.inject.internal.InjectorImpl.getProvider (InjectorImpl.java:1116)
    at com.google.inject.internal.InjectorImpl.getProvider (InjectorImpl.java:1078)

i-046990c9f0c6f1e3f (rushikesh-snyk)
```

\$ mvn dependency:tree  
to generate a tree-like representation of your project's dependency hierarchy

```
root@ip-172-31-54-81:/home/ubuntu/employee-management# mvn dependency:tree
[INFO] Scanning for projects...
[WARNING]
[WARNING] Some problems were encountered while building the effective model for net.javaguides:springboot-backend:jar:0.0.1-SNAPSHOT
[WARNING] 'build.plugins.plugin.(groupId:artifactId)' must be unique but found duplicate declaration of plugin org.jacoco:jacoco-maven-plugin @ line 101, column 10
[WARNING]
[WARNING] It is highly recommended to fix these problems because they threaten the stability of your build.
[WARNING]
[WARNING] For this reason, future Maven versions might no longer support building such malformed projects.
[WARNING]
[INFO]
[INFO] -----< net.javaguides:springboot-backend >-----
[INFO] Building springboot-backend 0.0.1-SNAPSHOT
[INFO] -----[ jar ]-----
[INFO]
[INFO] --- maven-dependency-plugin:3.3:tree (default-cli) @ springboot-backend ---
[INFO] net.javaguides:springboot-backend:jar:0.0.1-SNAPSHOT
[INFO] +- org.springframework.boot:spring-boot-starter-data-jpa:jar:3.0.4:compile
[INFO] | +- org.springframework.boot:spring-boot-starter:jar:3.0.4:compile
[INFO] | | +- org.aspectj:aspectjweaver:jar:1.9.19:compile
[INFO] | +- org.springframework.boot:spring-boot-starter-jdbc:jar:3.0.4:compile
[INFO] | | +- com.zaxxer:HikariCP:jar:5.0.1:compile
[INFO] | | \- org.springframework:spring-jdbc:jar:6.0.6:compile
[INFO] +- org.hibernate.orm:hibernate-core:jar:6.1.7.Final:compile
[INFO] +- jakarta.persistence:jakarta.persistence-api:jar:3.1.0:compile
[INFO] +- jakarta.transaction:jakarta.transaction-api:jar:2.0.1:compile
[INFO] +- org.jboss.logging:jboss-logging:jar:3.5.0.Final:runtime
[INFO] +- org.hibernate.common:hibernate-commons-annotations:jar:6.0.6.Final:runtime
[INFO] +- org.jboss.jandex:jar:2.4.2.Final:runtime
[INFO] +- com.fasterxml:classmate:jar:1.5.1:runtime
[INFO] +- net.bytebuddy:byte-buddy:jar:1.12.23:runtime
[INFO] +- org.glassfish.jaxb:jaxb-runtime:jar:4.0.2:runtime
[INFO] | \- org.glassfish.jaxb:jaxb-core:jar:4.0.2:runtime
[INFO] |   +- org.eclipse.angus:angus-activation:jar:2.0.0:runtime
[INFO] |   +- org.glassfish.jaxb:txw2:jar:4.0.2:runtime
[INFO] |   \- com.sun.istack:istack-commons-runtime:jar:4.1.1:runtime
[INFO] +- jakarta.inject:jakarta.inject-api:jar:2.0.0:runtime
```

### c) Mysql

Install MySQL Server

```
sudo apt install mysql-server
```

To see secure MySQL Installation

```
sudo mysql_secure_installation
```

Access MySQL

```
sudo mysql
```

Configure Spring Boot Application

change the passwd in this file

```
vi src/main/resources/application.properties
```

Save and Exit vi

Restart Spring Boot Application

### d) Docker

Download and Install Docker

```
curl -fsSL https://get.docker.com -o get-docker.sh
```

This command downloads the Docker installation script from the official Docker website.

```
sh get-docker.sh
```

This command executes the downloaded script, which installs Docker on your system.

Check Docker Version

```
docker --version
```

Add User to Docker Group

```
sudo usermod -aG docker $USER
```

Check Docker Process

```
docker ps
```

Adjust Docker Socket Permissions

```
sudo chown ubuntu:docker /var/run/docker.sock
sudo chmod 600 /var/run/docker.sock
```

Check Docker Process Again  
docker ps

Npm  
Install Node.js and npm:  
sudo apt update  
sudo apt install nodejs npm

#### e) Snyk

Install Snyk globally  
npm install -g snyk

Authenticate Snyk  
snyk auth

Verify Installation  
snyk --version

snyk code

Snyk Code will scan your project's source code and analyze it for security vulnerabilities and code quality issues

```
Notifications about newly disclosed issues related to these dependencies will be emailed to you.

root@ip-172-31-54-81:/home/ubuntu/employee-management# snyk code test

Testing /home/ubuntu/employee-management ...

X [Low] Spring Cross-Site Request Forgery (CSRF)
  Path: src/main/java/net/javaguides/springboot/controller/EmployeeController.java, line 28
  Info: The employee parameter is vulnerable to Cross Site Request Forgery (CSRF) attacks due to not using Spring Security. This could allow an attacker to
  g Spring Security's CSRF protection within your application.

X [Low] Spring Cross-Site Request Forgery (CSRF)
  Path: src/main/java/net/javaguides/springboot/controller/EmployeeController.java, line 42
  Info: The employeeDetails parameter is vulnerable to Cross Site Request Forgery (CSRF) attacks due to not using Spring Security. This could allow an attac
  including Spring Security's CSRF protection within your application.

X [Medium] Origin Validation Error
  Path: src/main/java/net/javaguides/springboot/controller/EmployeeController.java, line 13
  Info: CORS policy "*" might be too permissive. This allows malicious code on other domains to communicate with the application, which is a security risk

✓ Test completed

Organization:    gaurav1222
Test type:      Static code analysis
Project path:    /home/ubuntu/employee-management

Summary:

3 Code issues found
1 [Medium] 2 [Low]
```

## \$ Snyk container

### To scan a container image with Snyk

```
Removing intermediate container 81d830ab0d9d
--> d7c3b402cfe3
Successfully built d7c3b402cfe3
Successfully tagged demo:latest
root@ip-172-31-54-81:/home/ubuntu/employee-management# snyk test

Testing /home/ubuntu/employee-management...

Tested 65 dependencies for known issues, found 24 issues, 24 vulnerable paths.

Issues to fix by upgrading:

Upgrade com.mysql:mysql-connector-j@8.0.32 to com.mysql:mysql-connector-j@8.2.0 to fix
  X Remote Code Execution (RCE) [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-COMMYSQJ-5441540] in com.mysql:mysql-connector-j@8.0.32
    introduced by com.mysql:mysql-connector-j@8.0.32
  X Access Control Bypass [High Severity] [https://security.snyk.io/vuln/SNYK-JAVA-COMMYSQJ-6075938] in com.mysql:mysql-connector-j@8.0.32
    introduced by com.mysql:mysql-connector-j@8.0.32

Upgrade org.springframework.boot:spring-boot-starter-web@3.0.4 to org.springframework.boot:spring-boot-starter-web@3.2.0 to fix
  X Arbitrary Code Execution [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGYAML-3152153] in org.yaml:snakeyaml@1.33
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework.boot:spring-boot-starter@3.0.4 > org.yaml:snakeyaml@1.33
  X Open Redirect (new) [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGSPRINGFRAMEWORK-6597980] in org.springframework:spring-web@6.0.6
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework:spring-web@6.0.6
  X Denial of Service (DoS) [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGSPRINGFRAMEWORK-6091650] in org.springframework:spring-web@6.0.6
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework:spring-web@6.0.6
  X Improper Input Validation [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHECATALYST-5959654] in org.apache.tomcat.embed:tomcat-embed-core@10.1.5
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework.boot:spring-boot-starter-tomcat@3.0.4 > org.apache.tomcat.embed:tomcat-embed-core@10.1.5
  X Incomplete Cleanup [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHECATALYST-5959972] in org.apache.tomcat.embed:tomcat-embed-core@10.1.5
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework.boot:spring-boot-starter-tomcat@3.0.4 > org.apache.tomcat.embed:tomcat-embed-core@10.1.5
  X Access Restriction Bypass [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHECATALYST-5862028] in org.apache.tomcat.embed:tomcat-embed-core@10.1.5
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework.boot:spring-boot-starter-tomcat@3.0.4 > org.apache.tomcat.embed:tomcat-embed-core@10.1.5
  X Denial of Service (DoS) [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHECATALYST-5596753] in org.apache.tomcat.embed:tomcat-embed-core@10.1.5
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework.boot:spring-boot-starter-tomcat@3.0.4 > org.apache.tomcat.embed:tomcat-embed-core@10.1.5
  X Allocation of Resources Without Limits or Throttling [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGSPRINGFRAMEWORK-5422217] in org.springframework:spring-expression@6.0
```

## \$ Snyk IaC

### To scan an infrastructure as code template with Snyk

```
Detected 0 dependencies (no project created)
root@ip-172-31-54-81:/home/ubuntu/employee-management# snyk iac test

Snyk Infrastructure as Code

✓ Test completed.

Issues

Low Severity Issues: 5

[Low] Container's or Pod's UID could clash with host's UID
Info: `runAsUser` value is set to low UID. UID of the container processes could clash with host's UIDs and lead to unintentional authorization bypass
Rule: https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
Path: [DocId: 0] > input > spec > template > spec > containers[employee-management] > securityContext > runAsUser
File: manifests/deployment.yaml
Resolve: Set `securityContext.runAsUser` value to greater or equal than 10'000. SecurityContext can be set on both `pod` and `container` level. If both are set, then the container level takes precedence

[Low] Container is running without memory limit
Info: Memory limit is not defined. Containers without memory limits are more likely to be terminated when the node runs out of memory
Rule: https://security.snyk.io/rules/cloud/SNYK-CC-K8S-4
Path: [DocId: 0] > input > spec > template > spec > containers[employee-management] > resources > limits > memory
File: manifests/deployment.yaml
```

## \$ snyk container test demo

docker image using snyk



## \$ snyk test

To test your project for vulnerabilities

```
Removing intermediate container 81d830ab0d9d
--> d7c3b402cfe3
Successfully built d7c3b402cfe3
Successfully tagged demo:latest
root@ip-172-31-54-81:/home/ubuntu/employee-management# snyk test

Testing /home/ubuntu/employee-management...

Tested 65 dependencies for known issues, found 24 issues, 24 vulnerable paths.

Issues to fix by upgrading:

Upgrade com.mysql:mysql-connector-j@8.0.32 to com.mysql:mysql-connector-j@8.2.0 to fix
  X Remote Code Execution (RCE) [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-COMMYSQL-5441540] in com.mysql:mysql-connector-j@8.0.32
    introduced by com.mysql:mysql-connector-j@8.0.32
  X Access Control Bypass [High Severity] [https://security.snyk.io/vuln/SNYK-JAVA-COMMYSQL-6075938] in com.mysql:mysql-connector-j@8.0.32
    introduced by com.mysql:mysql-connector-j@8.0.32

Upgrade org.springframework.boot:spring-boot-starter-web@3.0.4 to org.springframework.boot:spring-boot-starter-web@3.2.0 to fix
  X Arbitrary Code Execution [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGYAML-3152153] in org.yaml:snakeyaml@1.33
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework.boot:spring-boot-starter@3.0.4 > org.yaml:snakeyaml@1.33
  X Open Redirect (new) [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGSPRINGFRAMEWORK-6597980] in org.springframework:spring-web@6.0.6
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework:spring-web@6.0.6
  X Denial of Service (DoS) [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGSPRINGFRAMEWORK-6091650] in org.springframework:spring-web@6.0.6
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework:spring-web@6.0.6
  X Improper Input Validation [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHETOMCATEMBED-5959654] in org.apache.tomcat.embed:tomcat-embed-core@10.1.5
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework.boot:spring-boot-starter-tomcat@3.0.4 > org.apache.tomcat.embed:tomcat-embed-core@10.1.5
  X Incomplete Cleanup [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHETOMCATEMBED-595972] in org.apache.tomcat.embed:tomcat-embed-core@10.1.5
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework.boot:spring-boot-starter-tomcat@3.0.4 > org.apache.tomcat.embed:tomcat-embed-core@10.1.5
  X Access Restriction Bypass [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHETOMCATEMBED-5862028] in org.apache.tomcat.embed:tomcat-embed-core@10.1.5
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework.boot:spring-boot-starter-tomcat@3.0.4 > org.apache.tomcat.embed:tomcat-embed-core@10.1.5
  X Denial of Service (DoS) [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHETOMCATEMBED-5596753] in org.apache.tomcat.embed:tomcat-embed-core@10.1.5
    introduced by org.springframework.boot:spring-boot-starter-web@3.0.4 > org.springframework.boot:spring-boot-starter-tomcat@3.0.4 > org.apache.tomcat.embed:tomcat-embed-core@10.1.5
  X Allocation of Resources Without Limits or Throttling [Medium Severity] [https://security.snyk.io/vuln/SNYK-JAVA-ORGSPRINGFRAMEWORK-5422217] in org.springframework:spring-expression@6.0

i-06581b278a929e107 (gaurav-SYNK)
PublicIPs: 34.224.16.30 PrivateIPs: 172.31.54.81
```

## Snyk container test <image name>

```
root@ip-172-31-36-287:/opt/employee-management-main#
root@ip-172-31-36-287:/opt/employee-management-main# snyk container test test_image

Testing test_image...

X Low severity vulnerability found in shadow-utils
  Description: Improper Authentication
  Info: https://security.snyk.io/vuln/SNYK-ORACLE8-SHADOWUTILS-6082011
  Introduced through: shadow-utils@2:4.6-14.el8
  From: shadow-utils@2:4.6-14.el8
  Fixed in: 2:4.6-19.el8

X Low severity vulnerability found in libstdc++
  Description: Information Exposure
  Info: https://security.snyk.io/vuln/SNYK-ORACLE8-LIBSTDC-5893296
  Introduced through: libstdc++@8.5.0-4.0.2.el8_5
  From: libstdc++@8.5.0-4.0.2.el8_5
  Fixed in: 8:8.5.0-18.0.5.el8

X Low severity vulnerability found in libstdc++
  Description: CVE-2023-4039
  Info: https://security.snyk.io/vuln/SNYK-ORACLE8-LIBSTDC-5893315
  Introduced through: libstdc++@8.5.0-4.0.2.el8_5
  From: libstdc++@8.5.0-4.0.2.el8_5
  Fixed in: 8:8.5.0-18.0.5.el8

X Low severity vulnerability found in libssh-config
  Description: Out-of-bounds Write
  Info: https://security.snyk.io/vuln/SNYK-ORACLE8-LIBSSHCONFIG-2832422
  Introduced through: libssh-config@0.9.4-3.el8
  From: libssh-config@0.9.4-3.el8
  Fixed in: 0:0.9.6-3.el8

X Low severity vulnerability found in libssh
  Description: Out-of-bounds Write
  Info: https://security.snyk.io/vuln/SNYK-ORACLE8-LIBSSH-2832337
  Introduced through: libssh@0.9.4-3.el8
  From: libssh@0.9.4-3.el8
```

## f) Trivy

Add Trivy Repository

sudo apt-get update

sudo apt-get install -y 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.d/trivy.list
```

## Update Packages

```
sudo apt-get update
```

## Install Trivy

```
sudo apt-get install trivy
```

## Verify Installation

```
trivy --version
```

```
$ trivy image image name
```

```
scan docker images
```

```
ubuntu@ip-10-0-16-195:~/employee-management-main$ ls  
Dockerfile LICENSE README.md contrib manifests pom.xml src target trivy_0.24.0_Linux-64bit.tar.gz  
ubuntu@ip-10-0-16-195:~/employee-management-main$ docker ps  
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.45/containers/json": dial u  
er.sock: connect: permission denied  
ubuntu@ip-10-0-16-195:~/employee-management-main$ sudo usermod -s docker $USER  
ubuntu@ip-10-0-16-195:~/employee-management-main$ docker ps  
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.45/containers/json": dial u  
er.sock: connect: permission denied  
ubuntu@ip-10-0-16-195:~/employee-management-main$ srw-rw---- 1 ubuntu:docker 0 Jan 1 00:00 /var/run/docker.sock  
srw-rw----: command not found  
ubuntu@ip-10-0-16-195:~/employee-management-main$ sudo chown ubuntu:docker /var/run/docker.sock  
ubuntu@ip-10-0-16-195:~/employee-management-main$ sudo chmod 600 /var/run/docker.sock  
ubuntu@ip-10-0-16-195:~/employee-management-main$ docker ps  
CONTAINER ID   IMAGE      COMMAND                  CREATED    STATUS    PORTS    NAMES  
ubuntu@ip-10-0-16-195:~/employee-management-main$ trivy image demo  
2024-05-10T08:20:32.946Z      INFO    Detected OS: oracle  
2024-05-10T08:20:32.946Z      INFO    Detecting Oracle Linux vulnerabilities...  
2024-05-10T08:20:32.950Z      INFO    Number of language-specific files: 1  
2024-05-10T08:20:32.950Z      INFO    Detecting jar vulnerabilities...  
  
demo (oracle 8.5)  
=====
```

LIBRARY	VULNERABILITY ID	SEVERITY	INSTALLED VERSION	FIXED VERSION	TITLE
binutils	CVE-2022-4285	MEDIUM	2.30-108.0.2.el8_5.1	2.30-119.0.2.el8_8.2	binutils: NULL pointer dereference in bfd_elf_get_symbol_version_string leads to segfault -->avd.aquasec.com/nvd/cve-2022-4285
curl	CVE-2022-22576		7.61.1-22.el8	7.61.1-22.el8_6.3	curl: OAuth2 bearer bypass in connection re-use

```
i-021c086616d99335a (snky-rushikesh)
```

\$trivy filesystem /path of project

scanning filesystems for vulnerabilities

```
root@ip-172-31-54-81:/home/ubuntu/employee-management# trivy filesystem .
2024-05-11T07:03:51Z    INFO    Vulnerability scanning is enabled
2024-05-11T07:03:51Z    INFO    Secret scanning is enabled
2024-05-11T07:03:51Z    INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-05-11T07:03:51Z    INFO    Please see also https://aquasecurity.github.io/trivy/v0.51/docs/scanner/secret/#recommendation for faster secret detection
2024-05-11T07:03:52Z    INFO    Number of language-specific files      num=1
2024-05-11T07:03:52Z    INFO    [poc] Detecting vulnerabilities...
```

poc.xml (poc)

Total: 19 (UNKNOWN: 0, LOW: 0, MEDIUM: 8, HIGH: 11, CRITICAL: 0)

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
ch.qos.logback:logback-classic	CVE-2023-6378	HIGH	fixed	1.4.5	1.3.12, 1.4.12, 1.2.13	logback: serialization vulnerability in logback receiver <a href="https://avd.aquasec.com/nvd/cve-2023-6378">https://avd.aquasec.com/nvd/cve-2023-6378</a>
ch.qos.logback:logback-core						
org.apache.tomcat.embed:tomcat-embed-core	CVE-2023-28709			10.1.5	11.0.0-M5, 10.1.8, 9.0.74	tomcat: Fix for CVE-2023-24998 was incomplete <a href="https://avd.aquasec.com/nvd/cve-2023-28709">https://avd.aquasec.com/nvd/cve-2023-28709</a>
	CVE-2023-46589				11.0.0-M11, 10.1.16, 9.0.83, 8.5.96	tomcat: HTTP request smuggling via malformed trailer headers <a href="https://avd.aquasec.com/nvd/cve-2023-46589">https://avd.aquasec.com/nvd/cve-2023-46589</a>
	CVE-2023-41080	MEDIUM			8.5.93, 9.0.80, 10.1.13, 11.0.0-M11	tomcat: Open Redirect vulnerability in FORM authentication <a href="https://avd.aquasec.com/nvd/cve-2023-41080">https://avd.aquasec.com/nvd/cve-2023-41080</a>
	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 <a href="https://avd.aquasec.com/nvd/cve-2023-42795">https://avd.aquasec.com/nvd/cve-2023-42795</a>
	CVE-2023-44487					HTTP/2: Multiple HTTP/2 enabled web servers are vulnerable to a DoS attack... <a href="https://avd.aquasec.com/nvd/cve-2023-44487">https://avd.aquasec.com/nvd/cve-2023-44487</a>
	CVE-2023-45648					tomcat: Incorrectly parsed http trailer headers can cause request smuggling <a href="https://avd.aquasec.com/nvd/cve-2023-45648">https://avd.aquasec.com/nvd/cve-2023-45648</a>
	CVE-2024-24549				8.5.99, 9.0.86, 10.1.19, 11.0.0-M17	: Apache Tomcat: HTTP/2 header handling DoS <a href="https://avd.aquasec.com/nvd/cve-2024-24549">https://avd.aquasec.com/nvd/cve-2024-24549</a>

\$ trivy fs < folder name> ==== to scan the secrete

```
root@ip-172-31-36-207:/opt/employee-management-main# trivy fs src/
2024-05-11T14:06:21Z    INFO    Vulnerability scanning is enabled
2024-05-11T14:06:21Z    INFO    Secret scanning is enabled
2024-05-11T14:06:21Z    INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-05-11T14:06:21Z    INFO    Please see also https://aquasecurity.github.io/trivy/v0.51/docs/scanner/secret/#recommendation for faster secret detection
2024-05-11T14:06:21Z    INFO    Number of language-specific files      num=0
```

id\_rsa (secrets)

Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 1, CRITICAL: 0)

HIGH: AsymmetricPrivateKey (private-key)

Asymmetric Private Key

id\_rsa[]

1 [ -----BEGIN OPENSSH PRIVATE KEY-----

-----END OPENSSH PRIVATE KEY-----

2

root@ip-172-31-36-207:/opt/employee-management-main#

## Step 3

### Code coverage reports

To generate code coverage reports for the project, you can use tool like JaCoCo

Add the JaCoCo Maven plugin to the project's pom.xml file

Run Maven with the test and jacoco:report goals to generate code coverage reports:

```
mvn clean test jacoco:report
```

This will run the project's unit tests and generate a code coverage report in the target/site/jacoco directory.

Generating a sample JaCoCo code coverage report involves running tests against your codebase and then generating the report using the JaCoCo Maven plugin.

To install the Apache HTTP Server (httpd) on Ubuntu

```
sudo apt update
```

Install Apache HTTP Server

```
sudo apt install apache2
```

Start Apache Service

```
sudo systemctl start apache
```

Verify Apache Service Status

```
sudo systemctl status apache2
```

Enable Apache Service

```
sudo systemctl enable apache2
```

copy index.html file from /home/ubuntu/employee-management/target/site/jacoco/index.html  
TO /var/www/html

```
cp /home/ubuntu/employee-management/target/site/jacoco/index.html /var/www/html
```

Enable the http port in security group

Restart the apache2 server





`sudo systemctl restart apache2`

copy public IP and hit on browser we will get jacoco code coverage report

---

[Sessions](#)springboot-backend

## springboot-backend

Element	Missed Instructions	Cov.	Missed Branches	Cov.	Missed Cxty	Missed Lines	Missed Methods	Missed Classes				
<a href="#">net.javaguides.springboot</a>		44%	n/a	1	3	2	4	1	3	0	1	
<a href="#">net.javaguides.springboot.controller</a>		100%	n/a	0	9	0	17	0	9	0	1	
<a href="#">net.javaguides.springboot.model</a>		100%	n/a	0	10	0	7	0	10	0	1	
<a href="#">net.javaguides.springboot.exception</a>		100%	n/a	0	1	0	2	0	1	0	1	
Total	5 of 152	96%	0 of 0	n/a	1	23	2	30	1	23	0	4

Created with [JaCoCo](#) 0.8.7.202105040129