**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

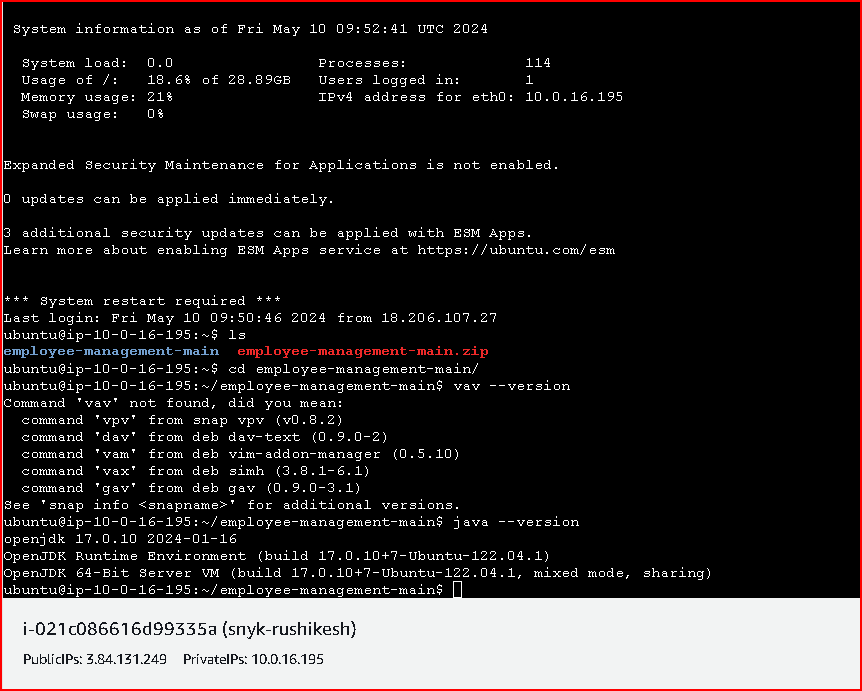
1. Java

Install java 17 application

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

check java version

$ java –version



1. Maven

Install maven

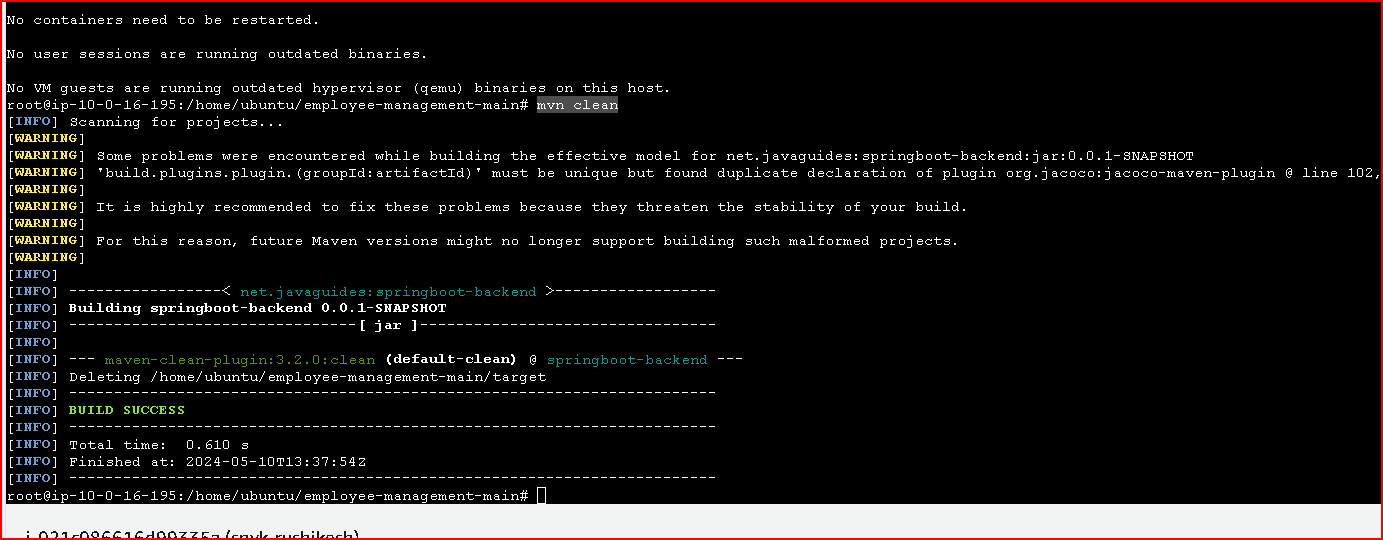
$ sudo apt install maven

Check maven version

$ mvn –version

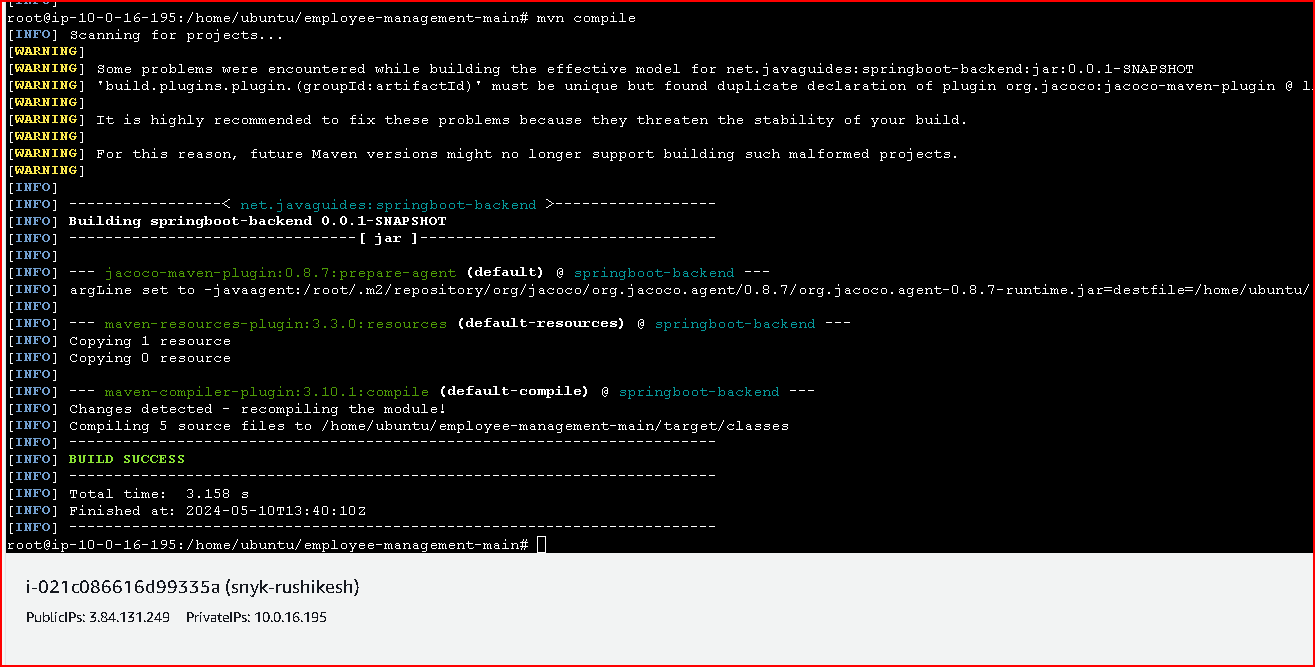
$ mvn clean

to clean the project by deleting the target directory



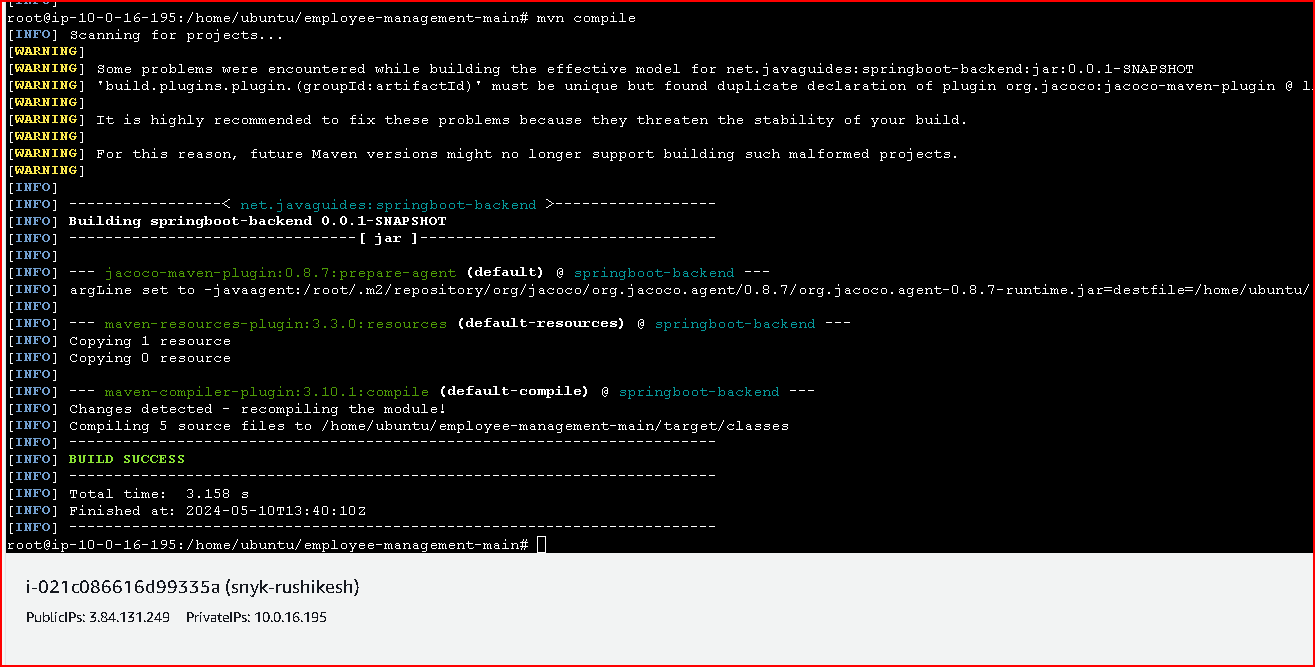
$ mvn compile

to compile your code after cleaning



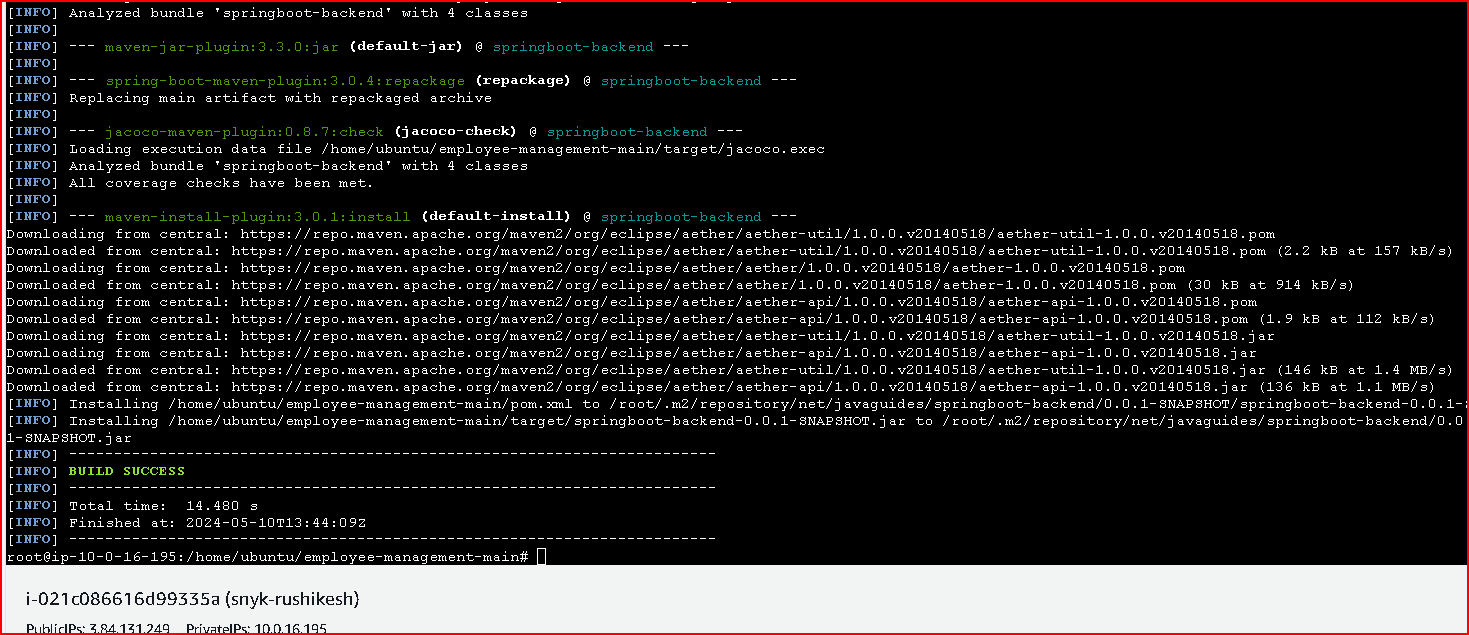
$ mvn package / $ mvn jar

package your project into a JAR file



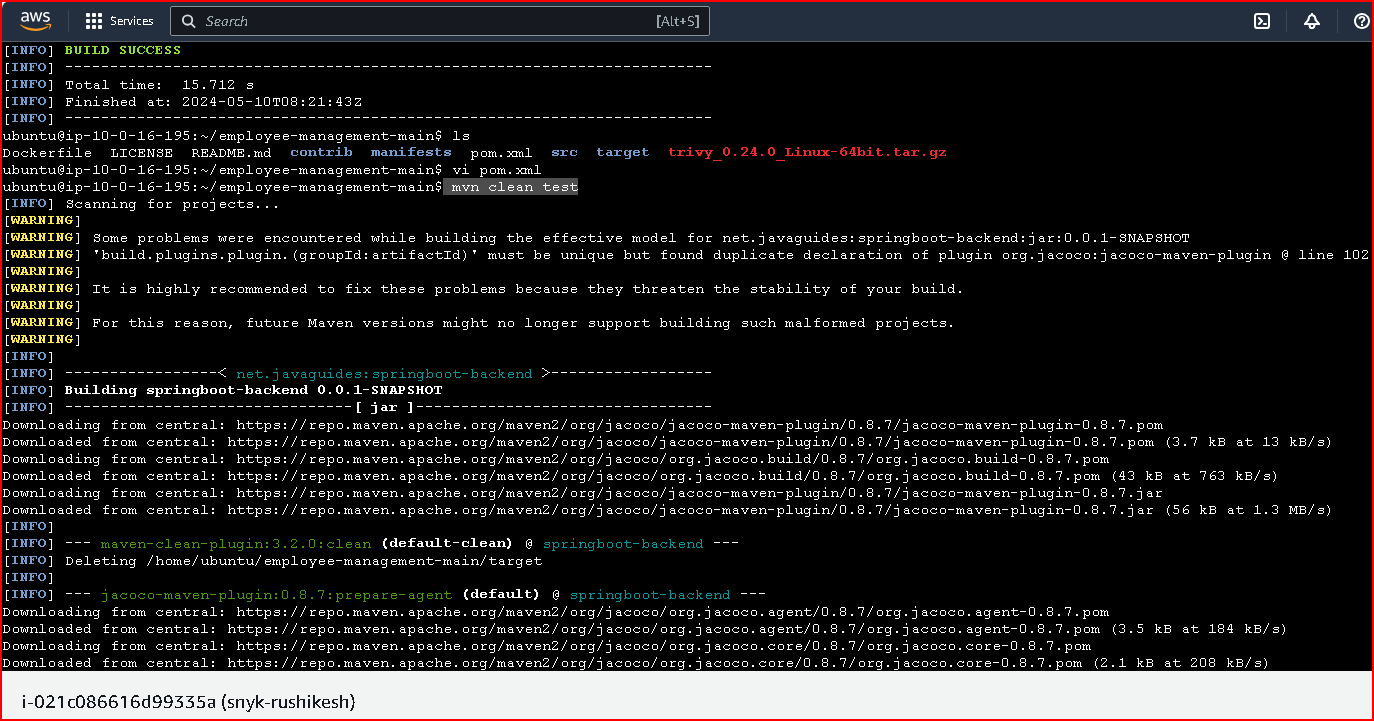
$ mvn install

Maven installs the packaged artifacts into the local Maven repository (/.m2/repository)



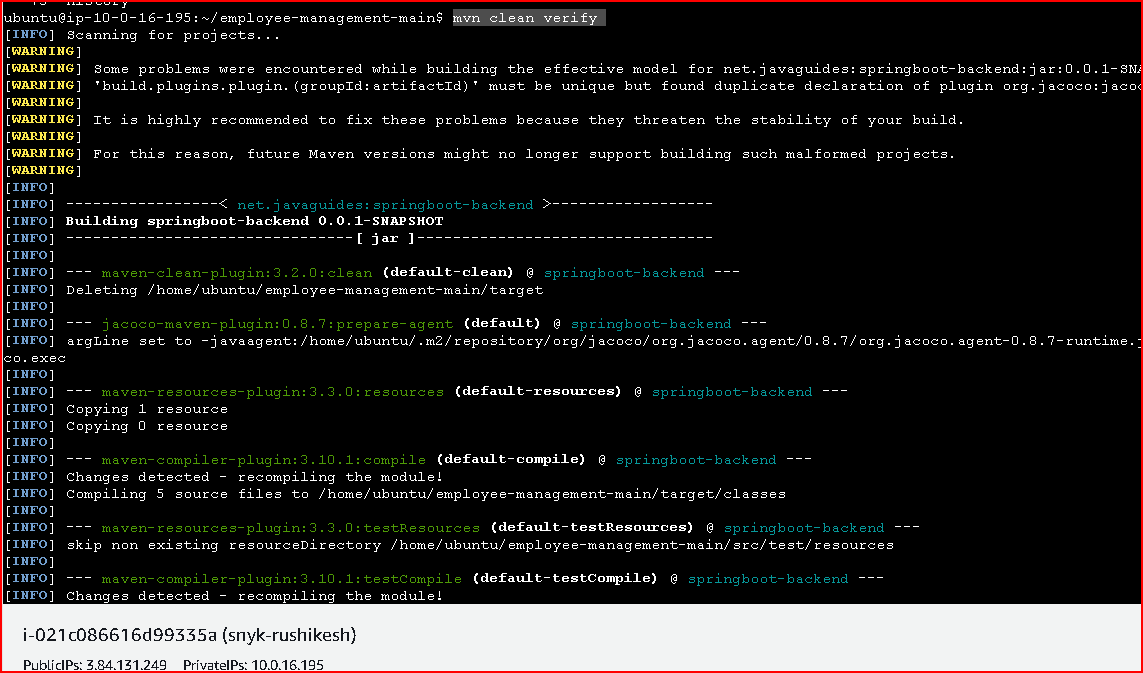
$ mvn clean test

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



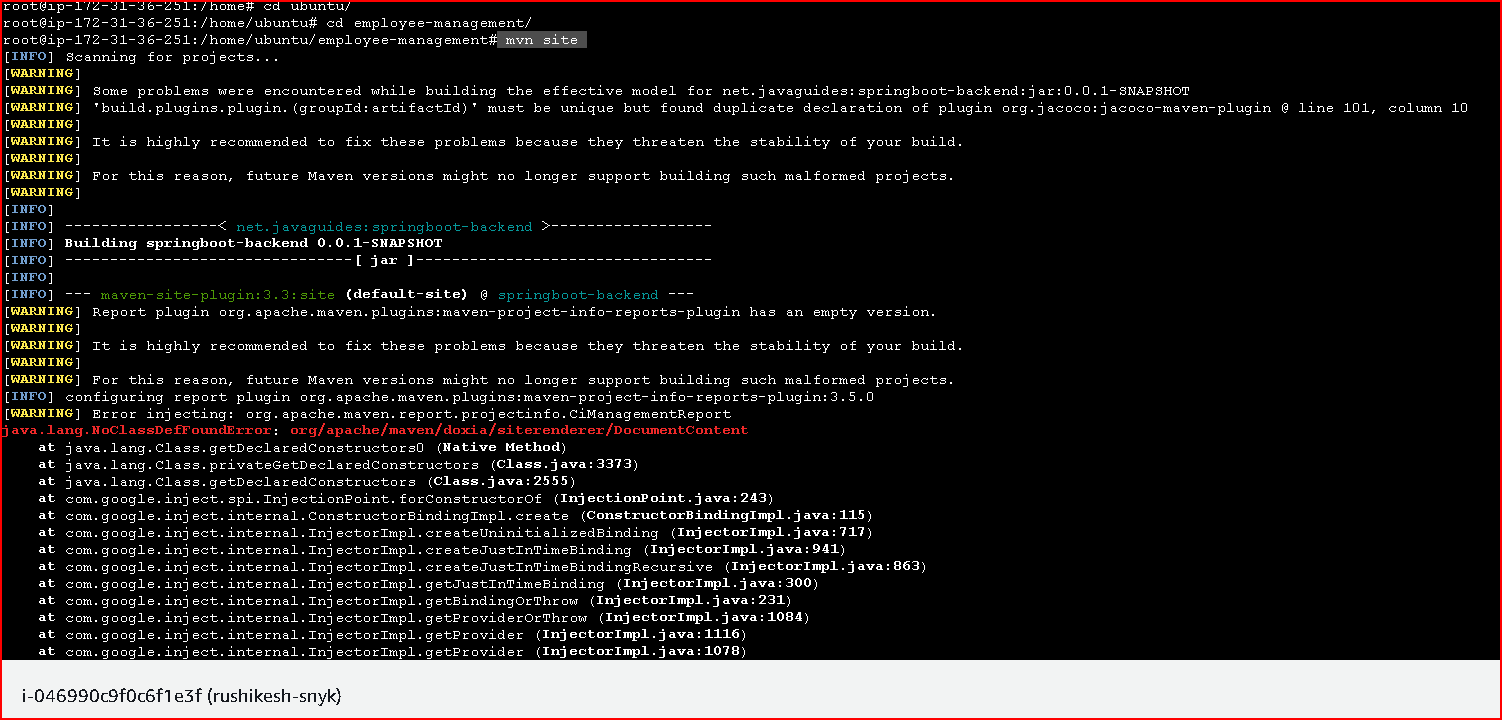
$ mvn clean verify

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



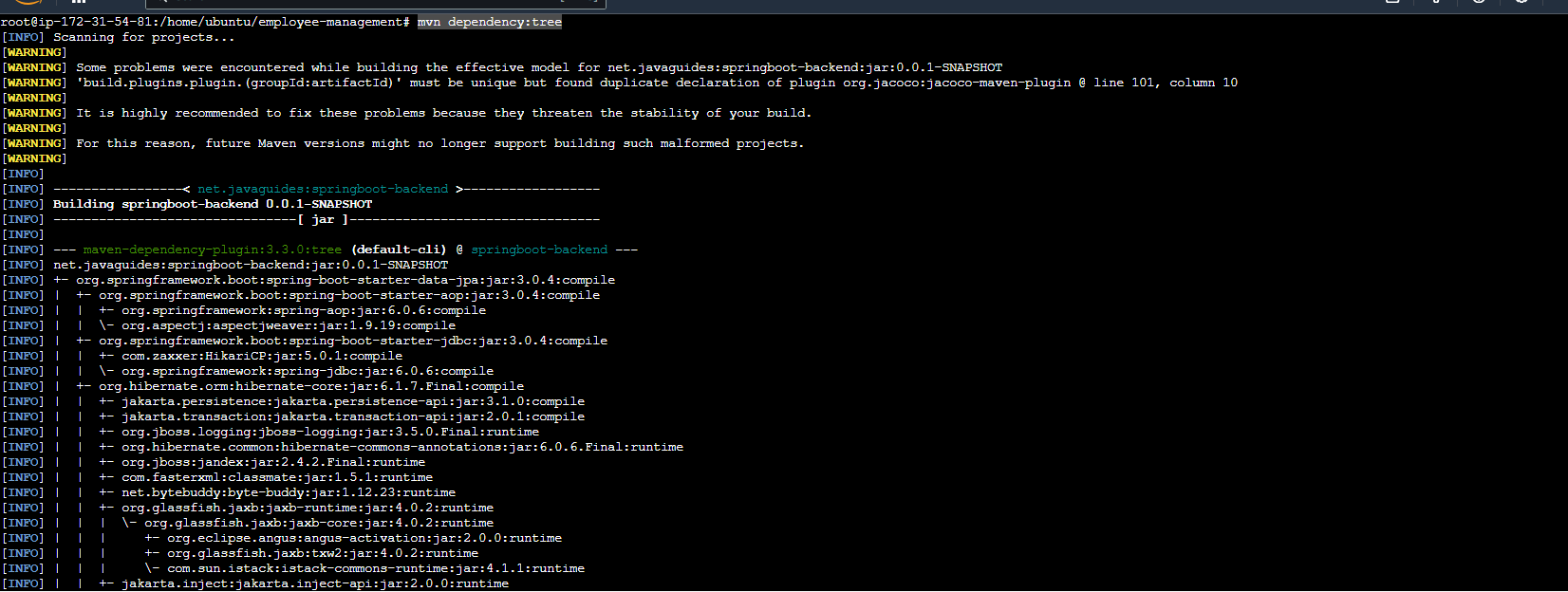
$ mvn site

to generate a project's site documentation



$ mvn dependency:tree

to generate a tree-like representation of your project's dependency hierarchy



1. **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 inthis file

vi src/main/resources/application.properties

Save and Exit vi

Restart Spring Boot Application

1. **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

1. **Snyk**

Install Snyk globally

npm install -g snyk

Authenticate Snyk

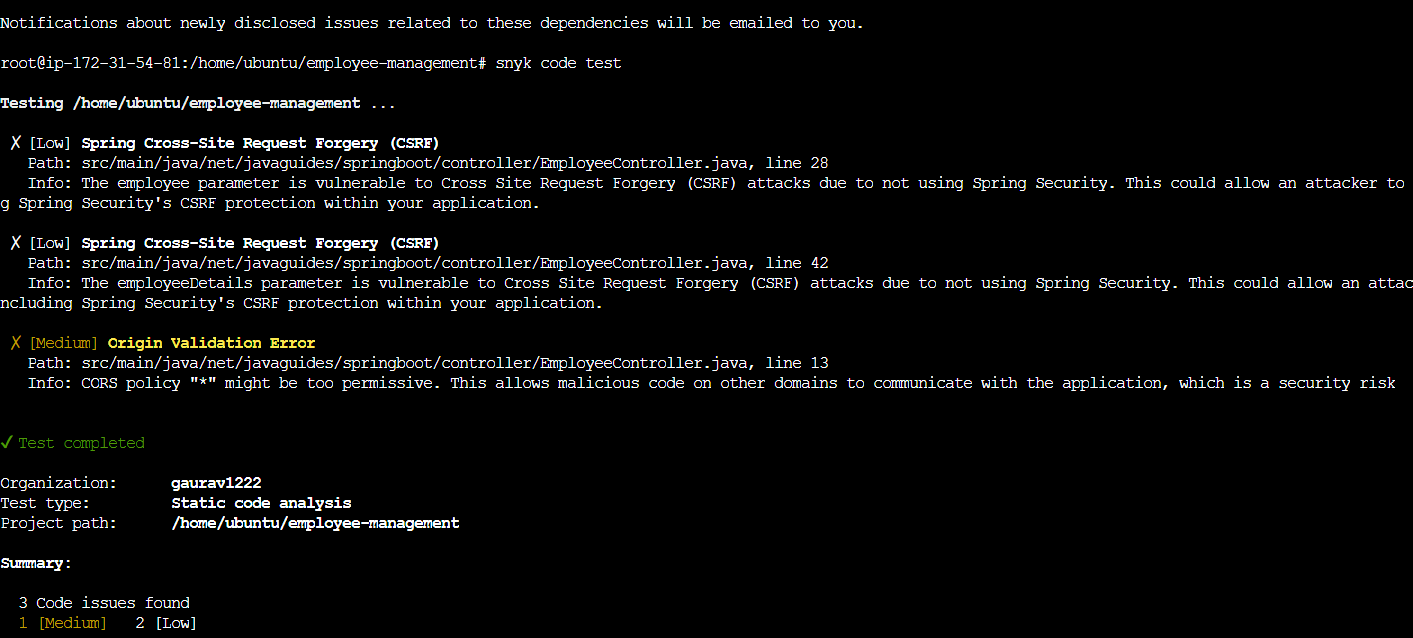
snyk auth

Verify Installation

snyk –version

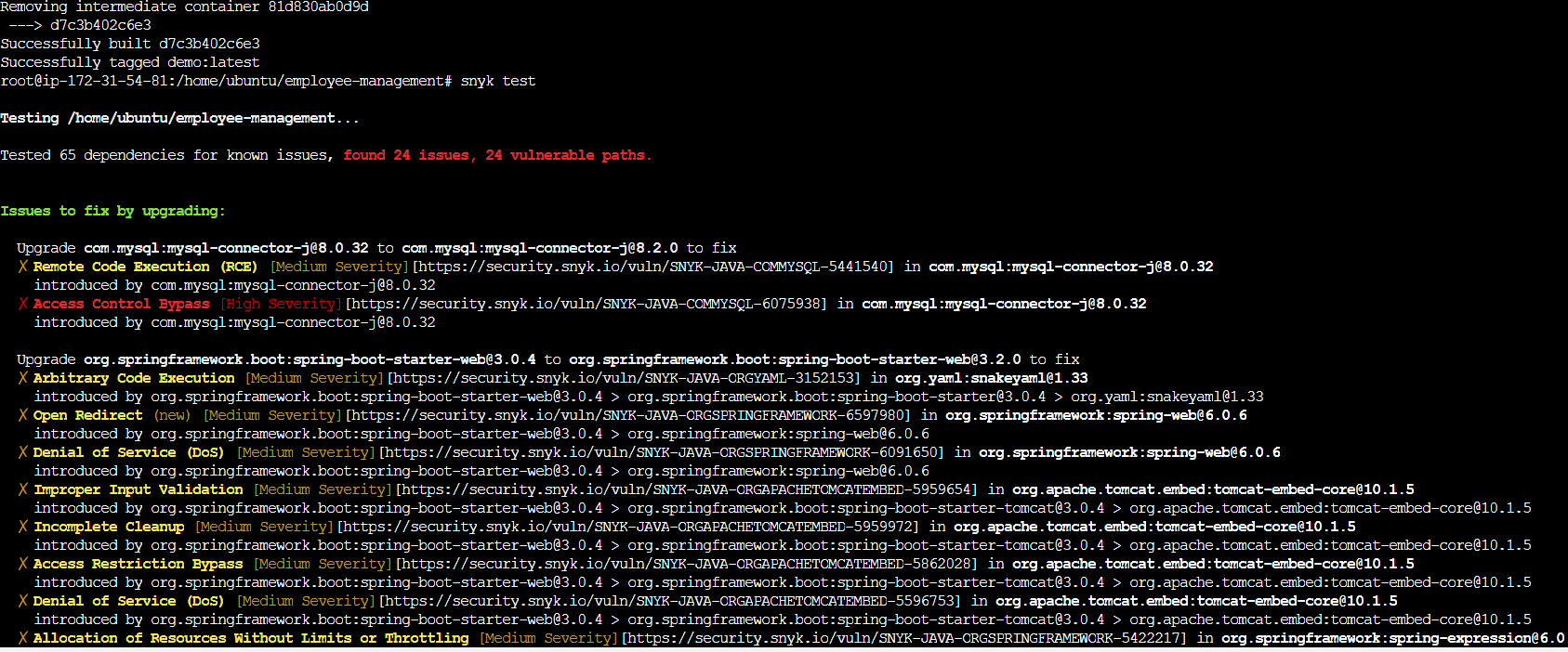
snyk code

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



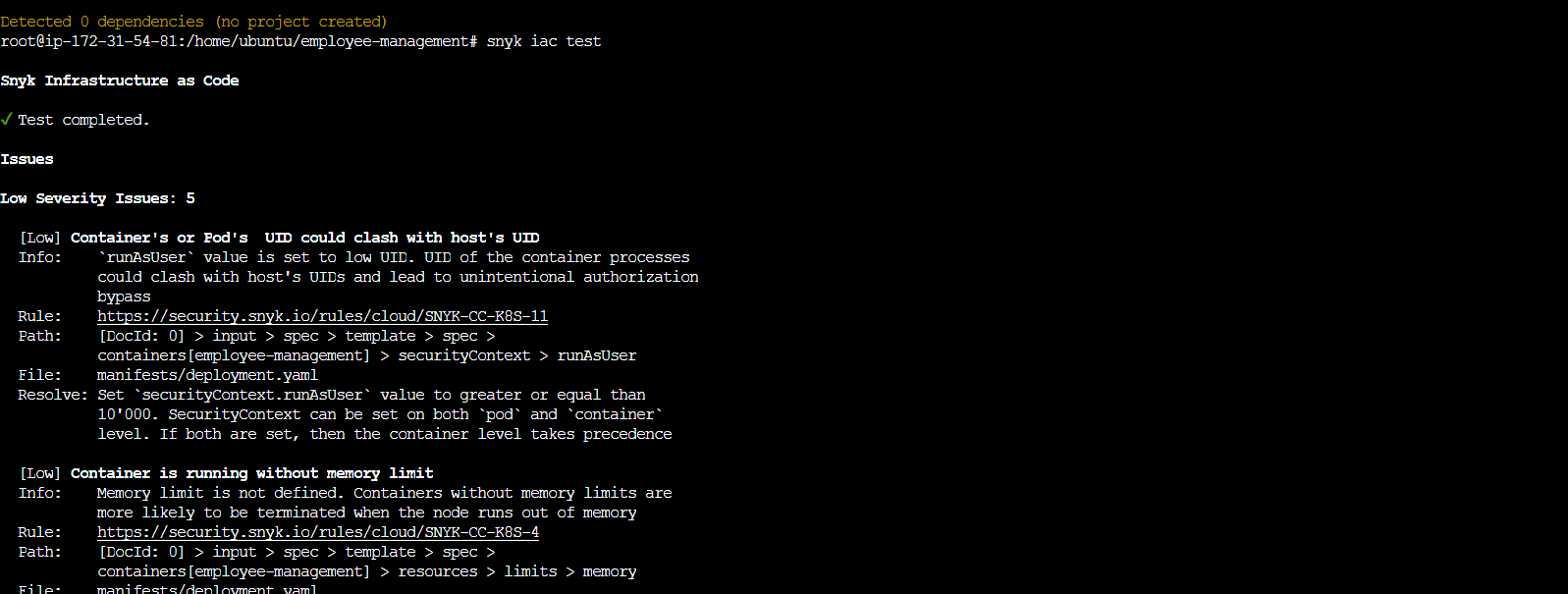
$ Snyk container

To scan a container image with Snyk



$ Snyk IaC

To scan an infrastructure as code template with Snyk

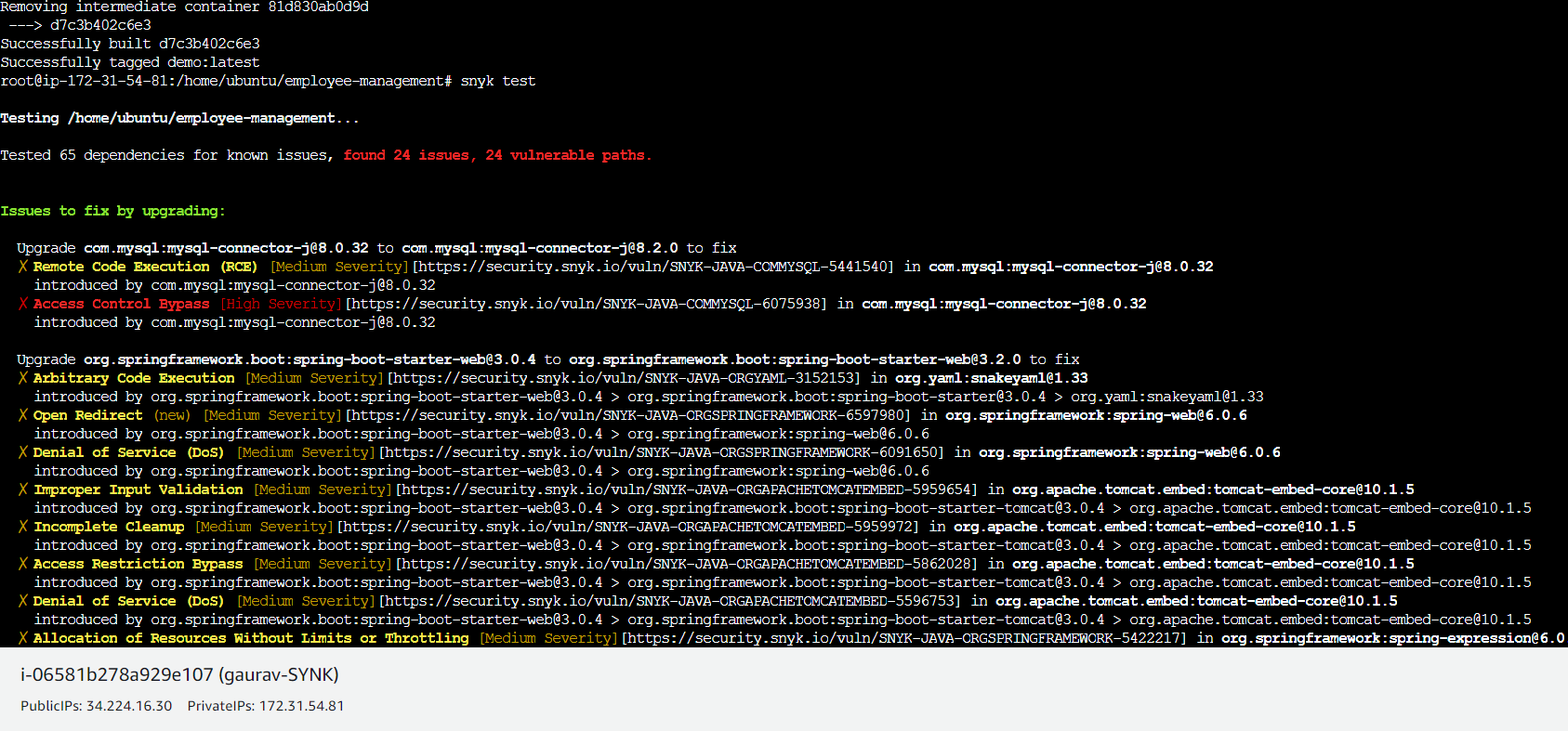


$ snyk container test demo

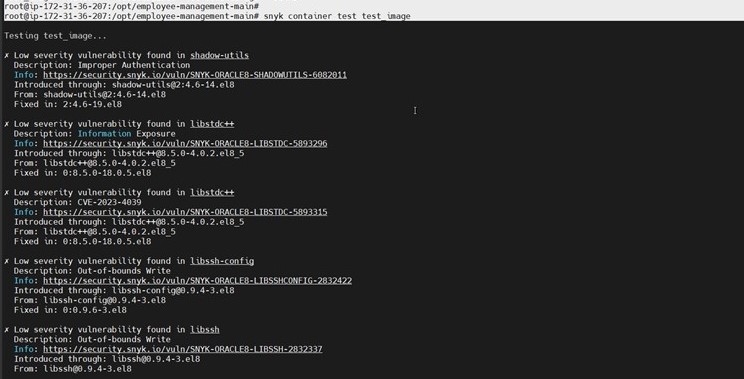
docker image using snyk

$ snyk test

To test your project for vulnerabilities



Snyk container test <image name>



1. **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

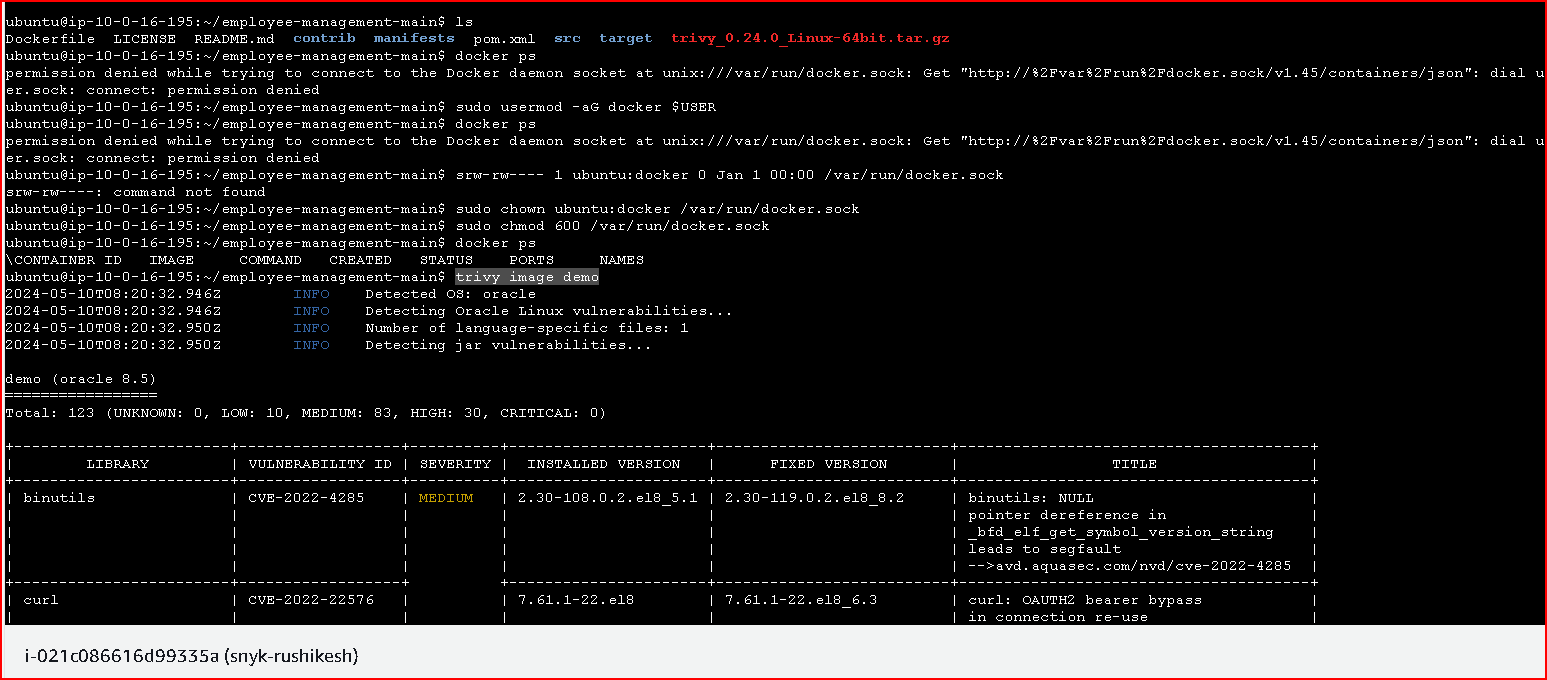
sudo apt-get install trivy

Verify Installation

trivy –version

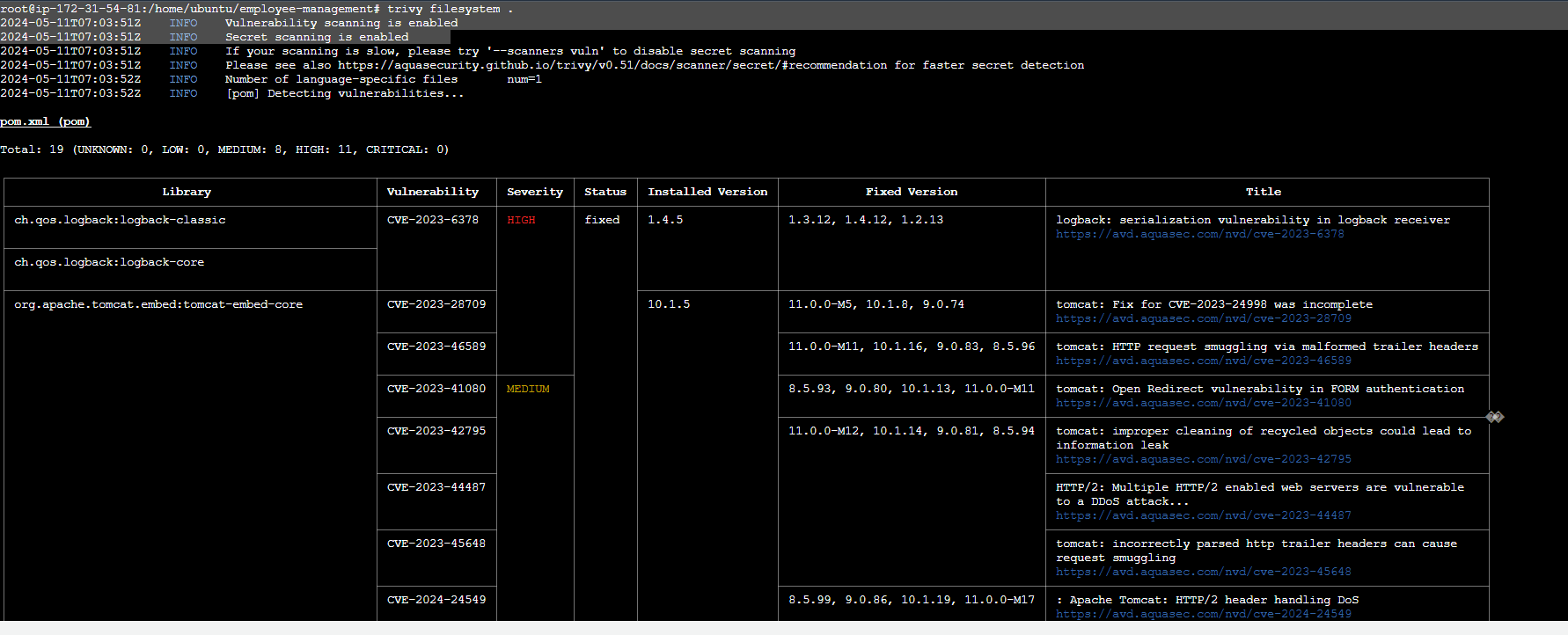
$ trivy image image name

scan docker images

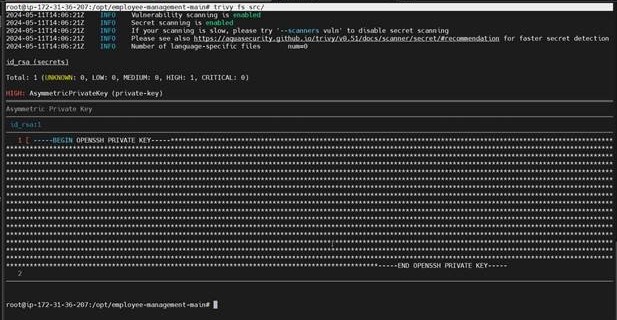


$trivy filesystem /path of project

scanning filesystems for vulnerabilities



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



**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

Enbale 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

