ATTACK DEFENSE

by PentesterAcademy

Name	Spotbugs: Finding Bugs in Java Code
URL	https://www.attackdefense.com/challengedetails?cid=2054
Type	DevSecOps Basics: Static Code Analysis

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Challenge Description

Spotbugs is a tool that is used to find bugs in Java source code using the static analysis.

A Kali CLI machine (kali-cli) is provided to the user. The source code for three web applications is provided in the home directory of the root user.

Objective: Find bugs in the source code of web applications using the Spotbugs tool.

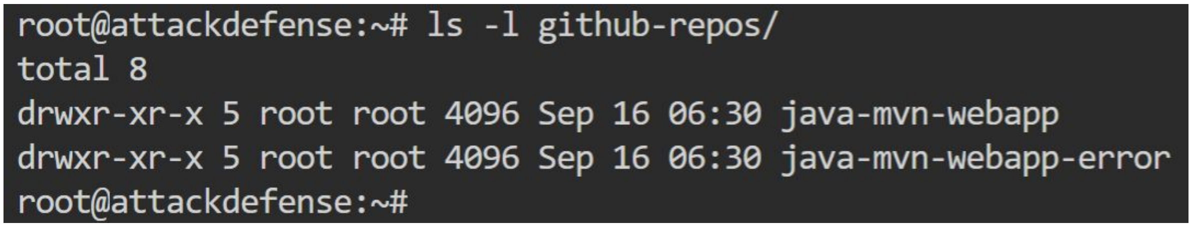
Instructions:

- The source code of web applications is provided at /root/github-repos

Solution

Step 1: Check the provided web applications.

Command: ls -l github-repos



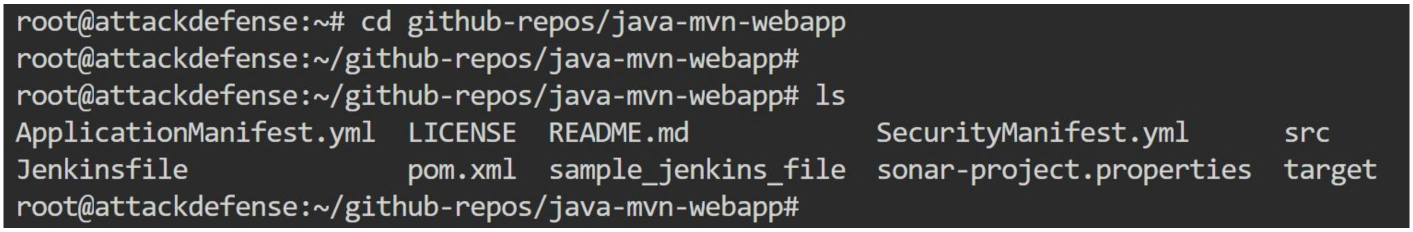
```
root@attackdefense:~# ls -l github-repos/
total 8
drwxr-xr-x 5 root root 4096 Sep 16 06:30 java-mvn-webapp
drwxr-xr-x 5 root root 4096 Sep 16 06:30 java-mvn-webapp-error
root@attackdefense:~#
```

We will take one example at a time and run the tool on that.

Example 1: Java Maven Webapp

Step 1: Change to the java-mvn-webapp directory and check its contents.

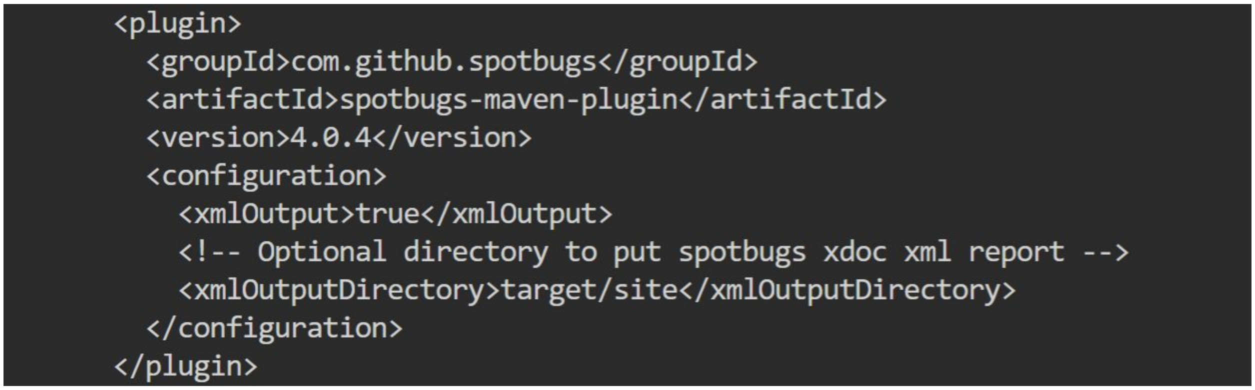
Commands:
cd github-repos/java-mvn-webapp
ls



```
root@attackdefense:~# cd github-repos/java-mvn-webapp
root@attackdefense:~/github-repos/java-mvn-webapp#
root@attackdefense:~/github-repos/java-mvn-webapp# ls
ApplicationManifest.yml  LICENSE  README.md          SecurityManifest.yml       src
Jenkinsfile              pom.xml  sample_jenkins_file  sonar-project.properties  target
root@attackdefense:~/github-repos/java-mvn-webapp#
```

Step 2: Check the contents of pom.xml of the application. The POM (Project Object Model) file contains the configuration information for the maven to build the project.

Command: cat pom.xml



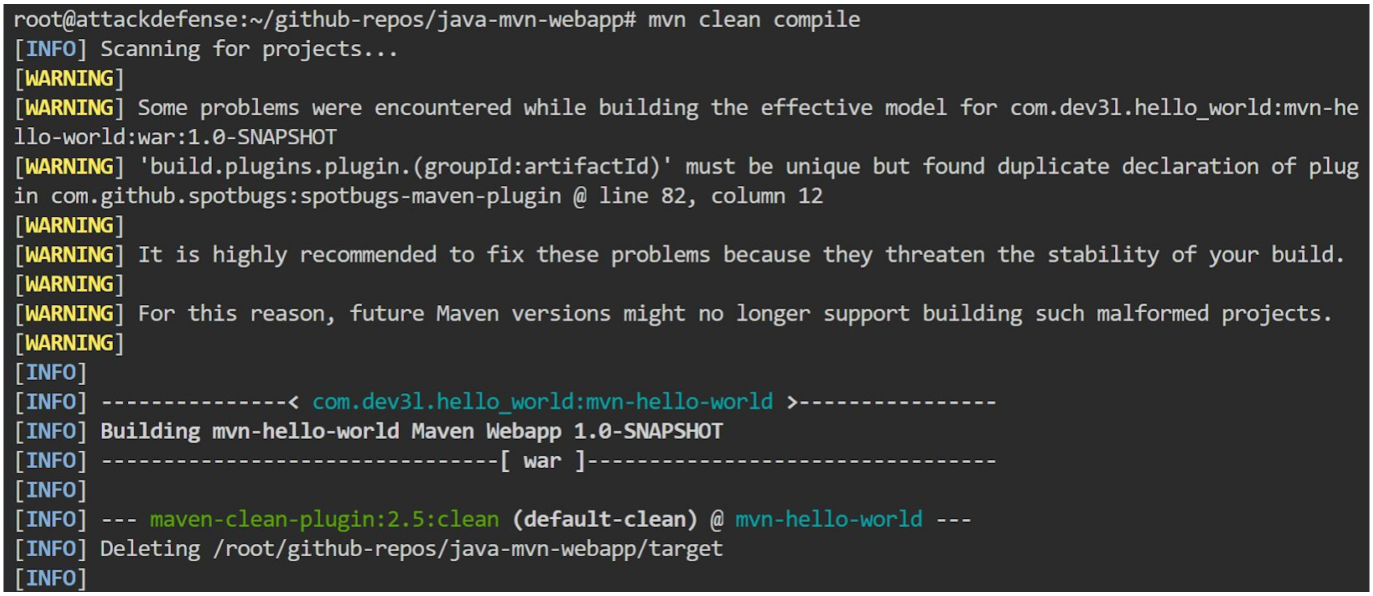
```
       <plugin>
         <groupId>com.github.spotbugs</groupId>
         <artifactId>spotbugs-maven-plugin</artifactId>
         <version>4.0.4</version>
         <configuration>
           <xmlOutput>true</xmlOutput>
           <!-- Optional directory to put spotbugs xdoc xml report -->
           <xmlOutputDirectory>target/site</xmlOutputDirectory>
         </configuration>
       </plugin>
```

The Spotbugs plugin is included in the application’s pom.xml file in the *compile* phase.

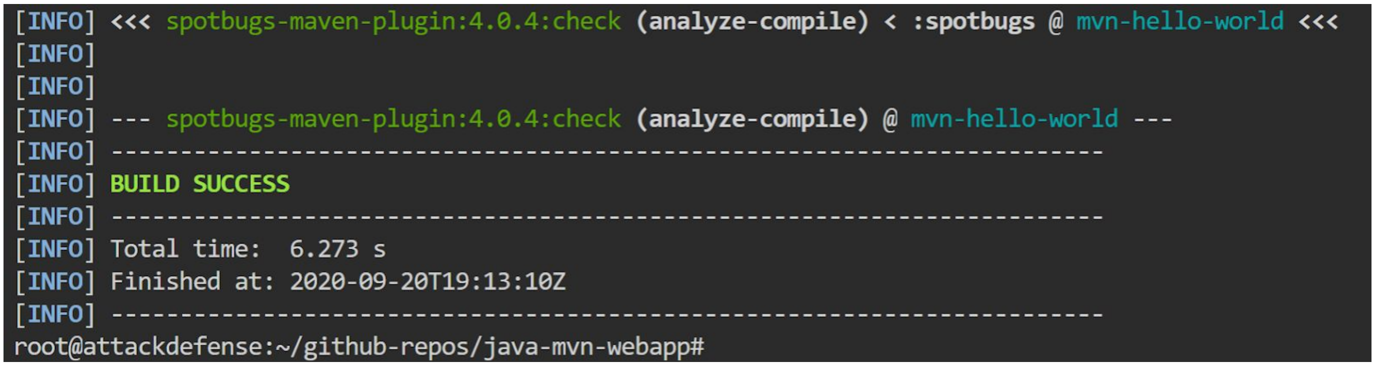
Compile phase is that stage in which maven compiles the source code. Hence, spotbugs will detect any errors that occurred during this phase.

Step 3: Build the project

Command: mvn clean compile



```
root@attackdefense:~/github-repos/java-mvn-webapp# mvn clean compile
[INFO] Scanning for projects...
[WARNING]
[WARNING] Some problems were encountered while building the effective model for com.dev3l.hello_world:mvn-he
llo-world:war:1.0-SNAPSHOT
[WARNING] 'build.plugins.plugin.(groupId:artifactId)' must be unique but found duplicate declaration of plug
in com.github.spotbugs:spotbugs-maven-plugin @ line 82, column 12
[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] --------------< com.dev3l.hello_world:mvn-hello-world >---------------
[INFO] Building mvn-hello-world Maven Webapp 1.0-SNAPSHOT
[INFO] --------------------------------[ war ]---------------------------------
[INFO]
[INFO] --- maven-clean-plugin:2.5:clean (default-clean) @ mvn-hello-world ---
[INFO] Deleting /root/github-repos/java-mvn-webapp/target
[INFO]
```



```
[INFO] <<< spotbugs-maven-plugin:4.0.4:check (analyze-compile) < :spotbugs @ mvn-hello-world <<<
[INFO]
[INFO]
[INFO] --- spotbugs-maven-plugin:4.0.4:check (analyze-compile) @ mvn-hello-world ---
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  6.273 s
[INFO] Finished at: 2020-09-20T19:13:10Z
[INFO] ------------------------------------------------------------------------
root@attackdefense:~/github-repos/java-mvn-webapp#
```

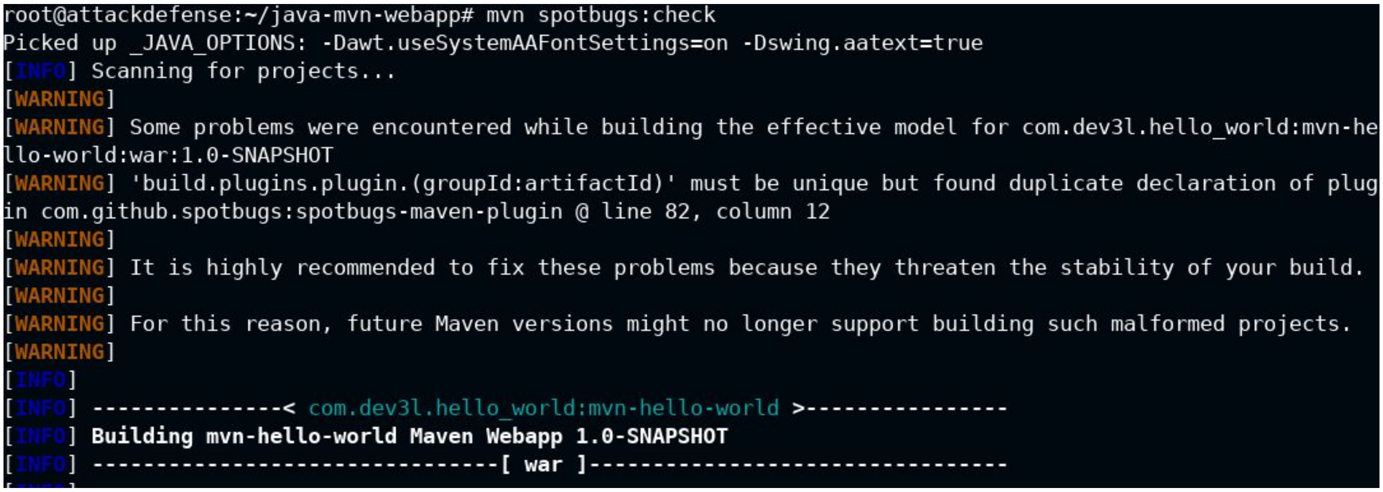
The build succeeded. The Spotbugs checked the code for issues and found no issues.

Another way to run the spotbugs plugin is to explicitly run it from CLI. The maven plugins support a group of goals. A specific goal can be executed by using following command:

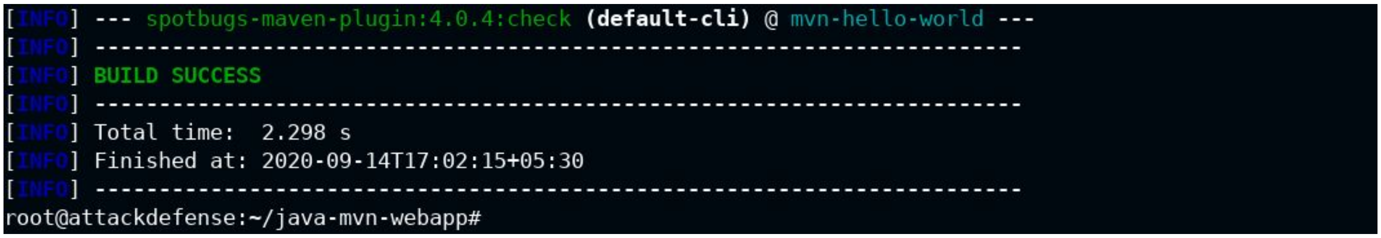
mvn plugin-prefix:goal

Step 4: Run the spotbugs plugin directly with the goal assigned to it in the pom.xml file.

Command: mvn spotbugs:check



```
root@attackdefense:~/java-mvn-webapp# mvn spotbugs:check
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[INFO] Scanning for projects...
[WARNING]
[WARNING] Some problems were encountered while building the effective model for com.dev3l.hello_world:mvn-he
llo-world:war:1.0-SNAPSHOT
[WARNING] 'build.plugins.plugin.(groupId:artifactId)' must be unique but found duplicate declaration of plug
in com.github.spotbugs:spotbugs-maven-plugin @ line 82, column 12
[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] ---------------< com.dev3l.hello_world:mvn-hello-world >----------------
[INFO] Building mvn-hello-world Maven Webapp 1.0-SNAPSHOT
[INFO] --------------------------------[ war ]---------------------------------
```



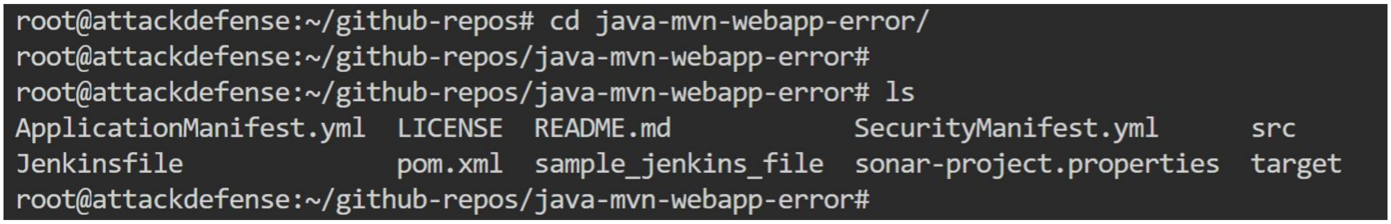
```
[INFO] --- spotbugs-maven-plugin:4.0.4:check (default-cli) @ mvn-hello-world ---
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  2.298 s
[INFO] Finished at: 2020-09-14T17:02:15+05:30
[INFO] ------------------------------------------------------------------------
root@attackdefense:~/java-mvn-webapp#
```

As expected, the spotbugs checked the application but found no bugs.

Example 2: Java Maven Webapp error

Step 1: Change to the java-mvn-webapp-error directory and check its contents.

Commands:
cd ~/github-repos/java-mvn-webapp-error
ls

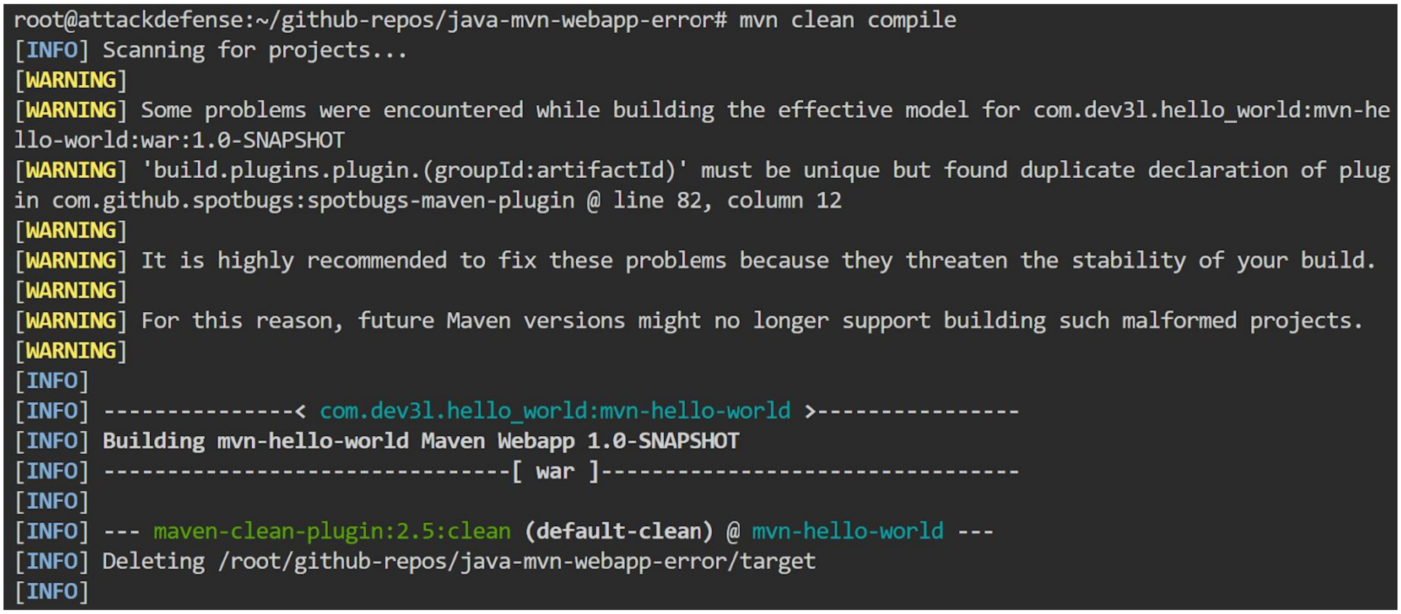


```
root@attackdefense:~/github-repos# cd java-mvn-webapp-error/
root@attackdefense:~/github-repos/java-mvn-webapp-error#
root@attackdefense:~/github-repos/java-mvn-webapp-error# ls
ApplicationManifest.yml  LICENSE  README.md          SecurityManifest.yml      src
Jenkinsfile              pom.xml  sample_jenkins_file  sonar-project.properties  target
root@attackdefense:~/github-repos/java-mvn-webapp-error#
```

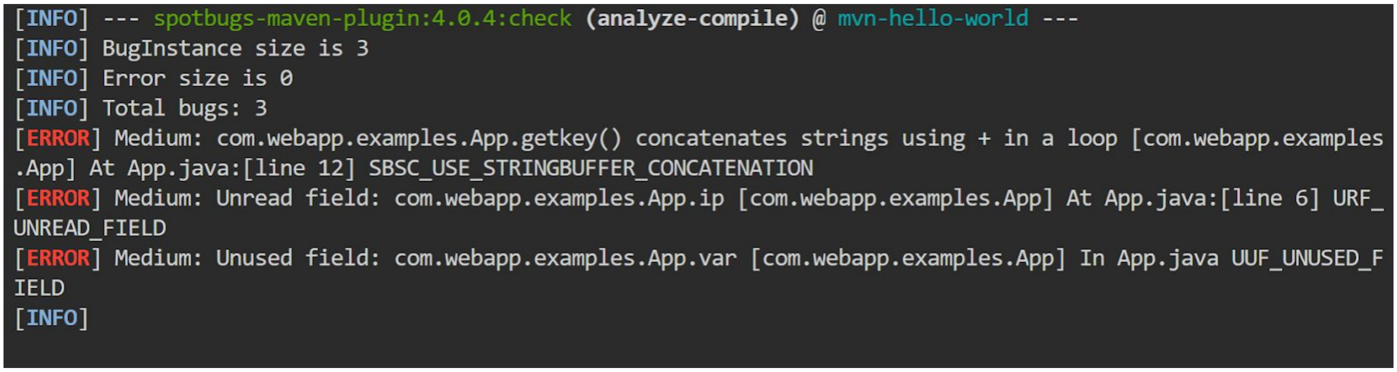
Note: This project is an exact copy of the previous project but we have introduced some issues to it.

Step 2: Build the project

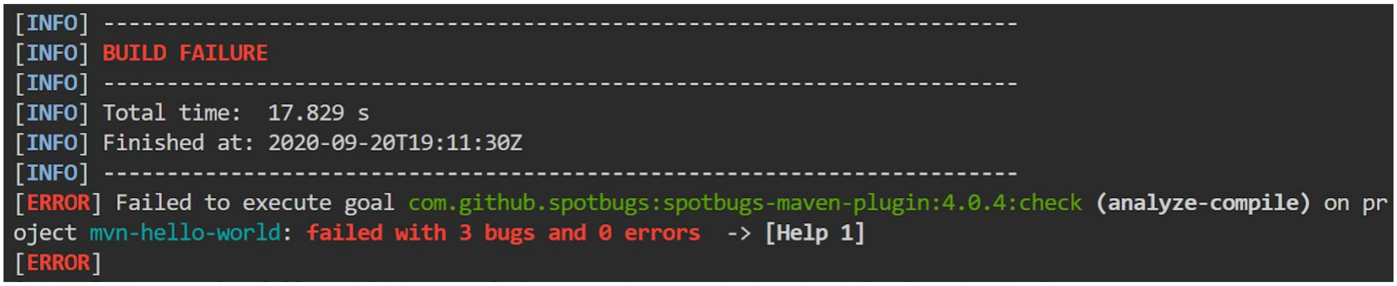
Command: mvn clean compile



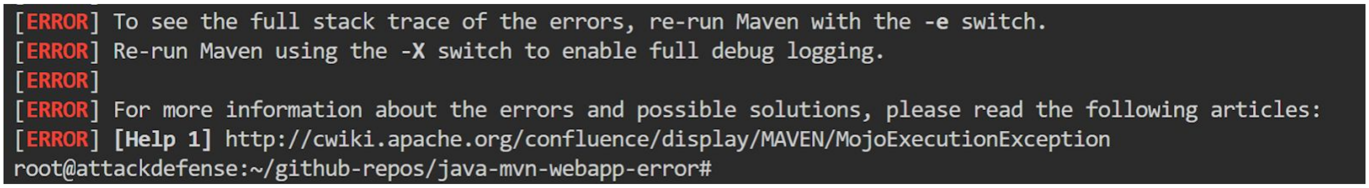
```
root@attackdefense:~/github-repos/java-mvn-webapp-error# mvn clean compile
[INFO] Scanning for projects...
[WARNING]
[WARNING] Some problems were encountered while building the effective model for com.dev3l.hello_world:mvn-he
llo-world:war:1.0-SNAPSHOT
[WARNING] 'build.plugins.plugin.(groupId:artifactId)' must be unique but found duplicate declaration of plug
in com.github.spotbugs:spotbugs-maven-plugin @ line 82, column 12
[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] ---------------< com.dev3l.hello_world:mvn-hello-world >----------------
[INFO] Building mvn-hello-world Maven Webapp 1.0-SNAPSHOT
[INFO] --------------------------------[ war ]---------------------------------
[INFO]
[INFO] --- maven-clean-plugin:2.5:clean (default-clean) @ mvn-hello-world ---
[INFO] Deleting /root/github-repos/java-mvn-webapp-error/target
[INFO]
```



```
[INFO] --- spotbugs-maven-plugin:4.0.4:check (analyze-compile) @ mvn-hello-world ---
[INFO] BugInstance size is 3
[INFO] Error size is 0
[INFO] Total bugs: 3
[ERROR] Medium: com.webapp.examples.App.getkey() concatenates strings using + in a loop [com.webapp.examples
.App] At App.java:[line 12] SBSC_USE_STRINGBUFFER_CONCATENATION
[ERROR] Medium: Unread field: com.webapp.examples.App.ip [com.webapp.examples.App] At App.java:[line 6] URF_
UNREAD_FIELD
[ERROR] Medium: Unused field: com.webapp.examples.App.var [com.webapp.examples.App] In App.java UUF_UNUSED_F
IELD
[INFO]
```



```
[INFO] ------------------------------------------------------------------------
[INFO] BUILD FAILURE
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  17.829 s
[INFO] Finished at: 2020-09-20T19:11:30Z
[INFO] ------------------------------------------------------------------------
[ERROR] Failed to execute goal com.github.spotbugs:spotbugs-maven-plugin:4.0.4:check (analyze-compile) on pr
oject mvn-hello-world: failed with 3 bugs and 0 errors  -> [Help 1]
[ERROR]
```



```
[ERROR] To see the full stack trace of the errors, re-run Maven with the -e switch.
[ERROR] Re-run Maven using the -X switch to enable full debug logging.
[ERROR]
[ERROR] For more information about the errors and possible solutions, please read the following articles:
[ERROR] [Help 1] http://cwiki.apache.org/confluence/display/MAVEN/MojoExecutionException
root@attackdefense:~/github-repos/java-mvn-webapp-error#
```

Issues Detected

- Plus (+) operator is used for concatenation
- Unread field
- Unused field

In this manner, Spotbugs can be used with Maven to find issues/bugs in an Java application.

Learnings

Perform static code analysis with Spotbugs.