Secure Programming – Assignment 1

Rathna Sindura, Chikkam

Part 1

Manual Analysis

- On Line 22, PORT variable is initialized with a static value. Instead of using static values, the variable should be kept separately in a constants.java file and can be used in the SimpleWebServer class. Using hard-coded values within a class is not an acceptable practice.
- On line 29, Static object dServerSocket is instantiated separately, which is not an acceptable practice either, because static objects are supposed to be initialized only once.
- Exception handling is too generic in the run() method. Try, catch blocks are not present.
- End statement is not invoked for the while loop in run() method.
- In line 62, while parsing the HTTP request, StringTokenizer class constructor takes two string parameters, of which one is the http request and other is a space delimiter. Instead of sending a space directly through the constructor, a better approach would be to initialize the delimiter and then use the delimiter variable.
- Like run() method, try catch blocks are not added in this processRequest method, implementing generic exception handling is not an acceptable practice.
- serveFile method contains try catch blocks, but the catch block do not log the actual exception message "e.message" but only logs the generic exception. Apart from file not being present, exception can be that appropriate permissions are not provided on the specified location to read the file. Hence it is important to log the exception.
- FileReader object fr is not closed in this serveFile method, which is not an acceptable practice as it leads to memory leak.
- Main method too does not contain try catch blocks and exception handling is poorly implemented.

Tool Choices/ Versions

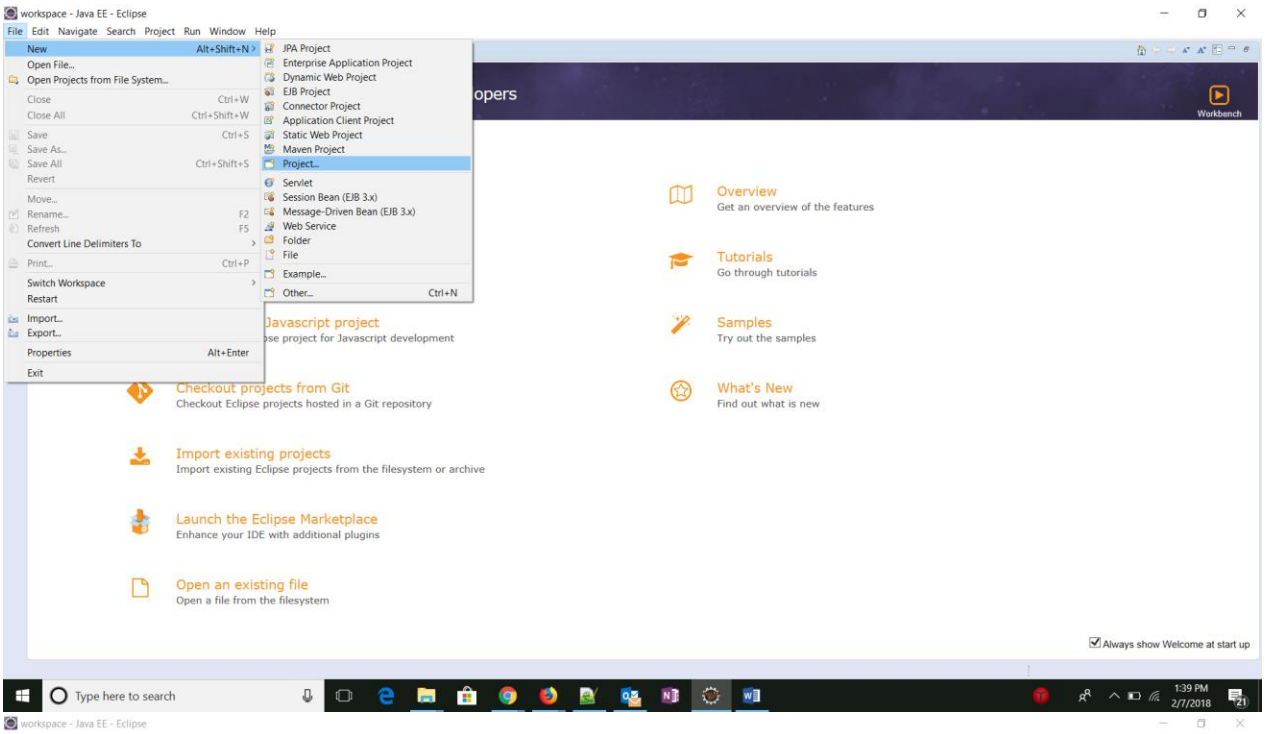
The tools I have used to test the code are:

- Eclipse Neon 3, Java JDK 8
- Findbugs – 3.0.1
- SonarLint – 3.3.1

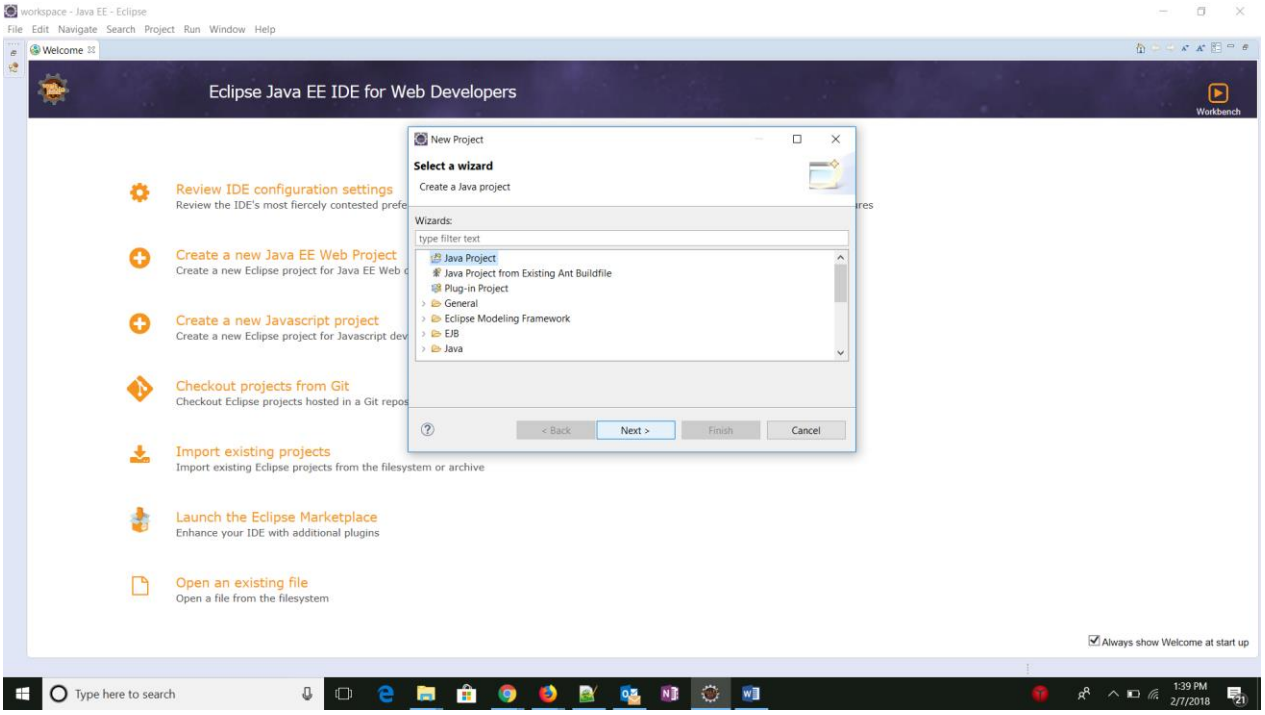
Tool Invocation Process

1. Using Eclipse, build a project and package named SimpleWebServer and add the SimpleWebServer class as shown in the steps from (a) to (h) below:
2.

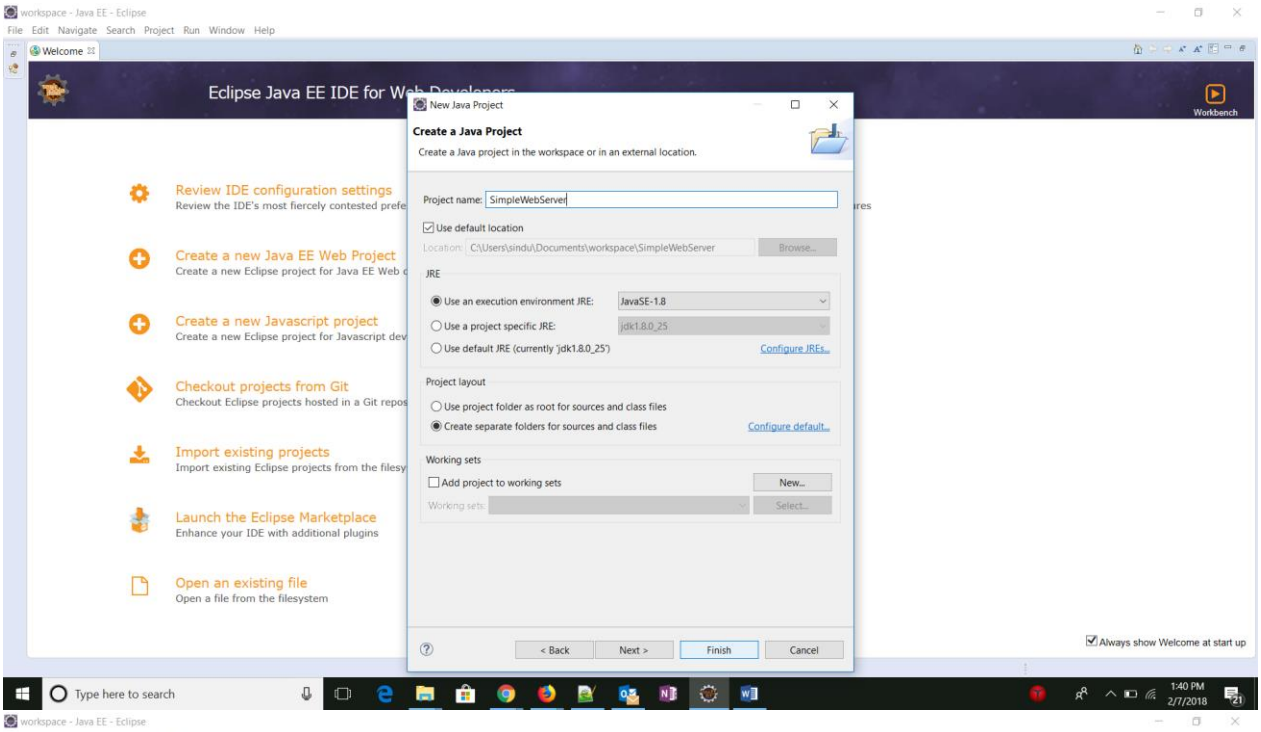
a.


workspace - Java EE - Eclipse
File Edit Navigate Search Project Run Window Help
New Alt+Shift+N
Open File...
Open Projects from File System...
Close Ctrl+W
Close All Ctrl+Shift+W
Save Ctrl+S
Save As...
Save All Ctrl+Shift+S
Revert
Move...
Rename... F2
Refresh F5
Convert Line Delimiters To
Print... Ctrl+P
Switch Workspace
Restart
Import...
Export...
Properties Alt+Enter
Exit
JPA Project
Enterprise Application Project
Dynamic Web Project
EJB Project
Connector Project
Application Client Project
Static Web Project
Maven Project
Project...
Servlet
Session Bean (EJB 3.x)
Message-Driven Bean (EJB 3.x)
Web Service
Folder
File
Example...
Other... Ctrl+N
opers
Workbench
Overview
Get an overview of the features
Tutorials
Go through tutorials
Samples
Try out the samples
What's New
Find out what is new
Javascript project
Checkout projects from Git
Checkout Eclipse projects hosted in a Git repository
Import existing projects
Import existing Eclipse projects from the filesystem or archive
Launch the Eclipse Marketplace
Enhance your IDE with additional plugins
Open an existing file
Open a file from the filesystem
Always show Welcome at start up
Type here to search
1:39 PM
2/7/2018

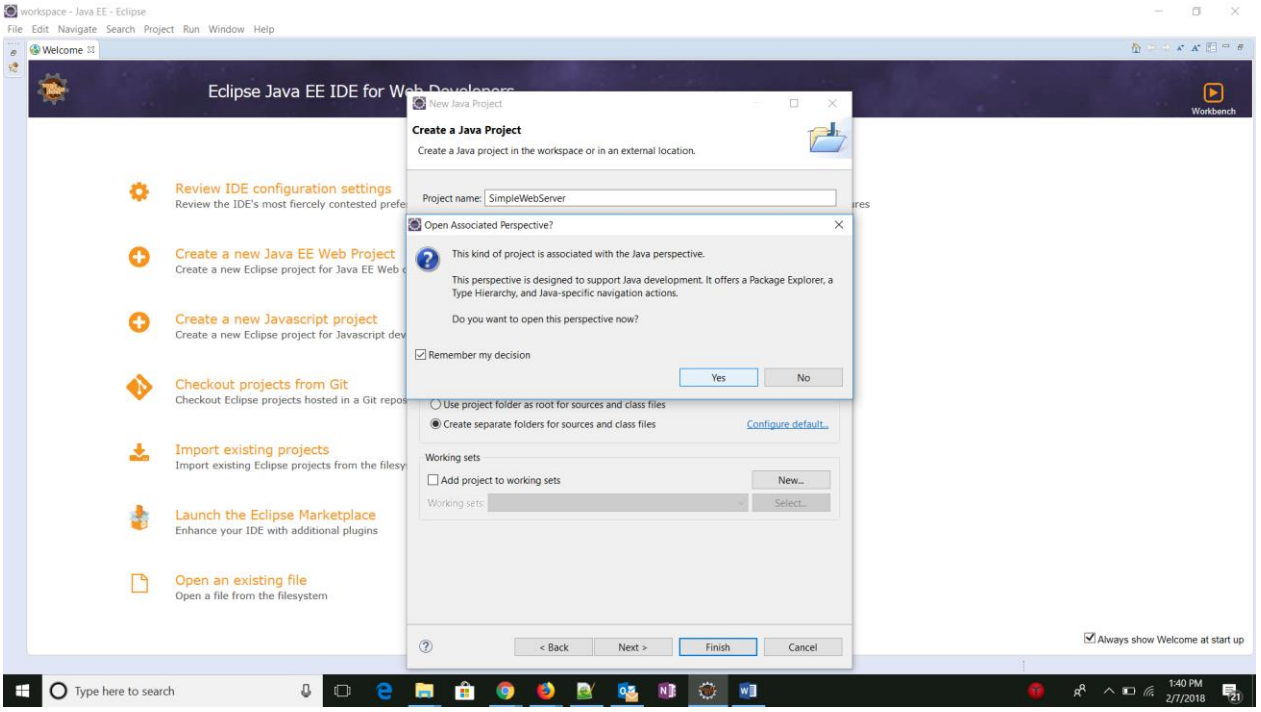
b.


workspace - Java EE - Eclipse
File Edit Navigate Search Project Run Window Help
Welcome
Eclipse Java EE IDE for Web Developers
Workbench
New Project
Select a wizard
Create a Java project
Wizards:
type filter text
Java Project
Java Project from Existing Ant Buildfile
Plug-in Project
General
Eclipse Modeling Framework
EJB
Java
< Back
Next >
Finish
Cancel
Review IDE configuration settings
Create a new Java EE Web Project
Create a new Eclipse project for Java EE Web
Create a new Javascript project
Create a new Eclipse project for Javascript dev
Checkout projects from Git
Checkout Eclipse projects hosted in a Git repos
Import existing projects
Import existing Eclipse projects from the filesystem or archive
Launch the Eclipse Marketplace
Enhance your IDE with additional plugins
Open an existing file
Open a file from the filesystem
Always show Welcome at start up
Type here to search
1:39 PM
2/7/2018

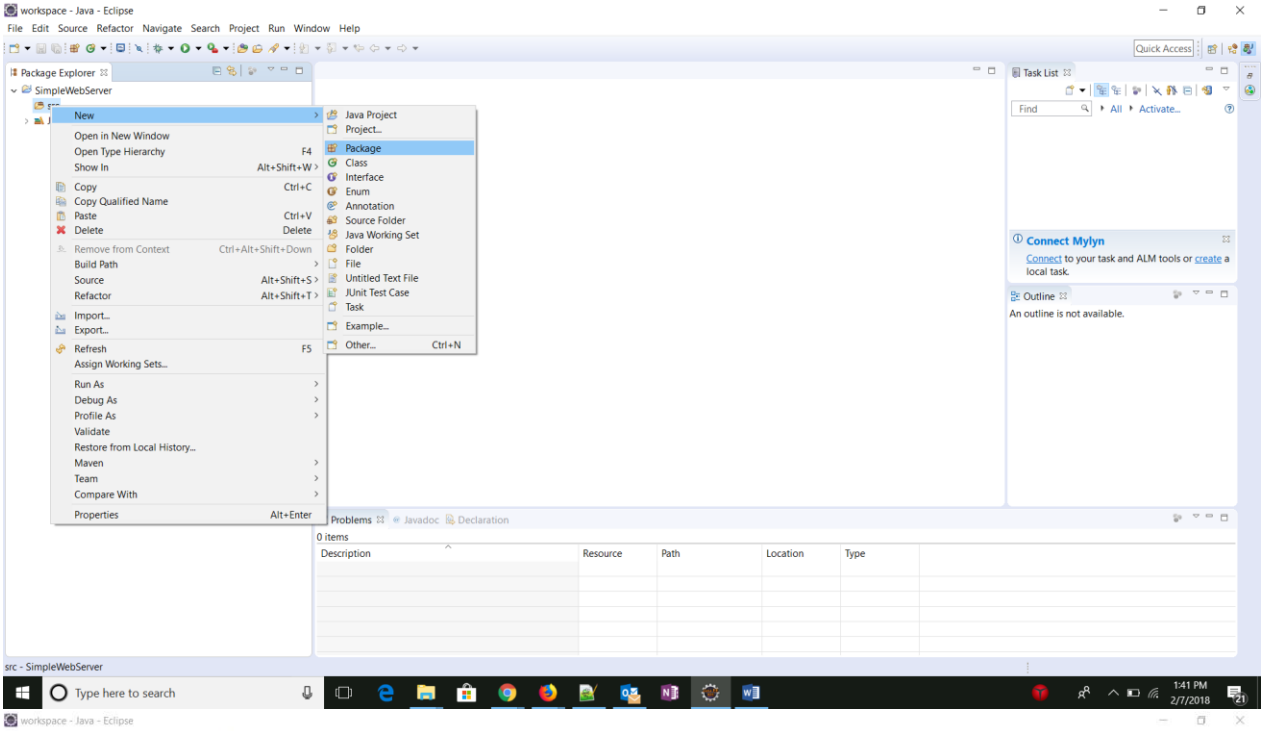
c.


workspace - Java EE - Eclipse
File Edit Navigate Search Project Run Window Help
Welcome
Eclipse Java EE IDE for Web Developers
Workbench
Review IDE configuration settings
Review the IDE's most fiercely contested prefe
Create a new Java EE Web Project
Create a new Eclipse project for Java EE Web
Create a new Javascript project
Create a new Eclipse project for Javascript dev
Checkout projects from Git
Checkout Eclipse projects hosted in a Git repos
Import existing projects
Import existing Eclipse projects from the filesy
Launch the Eclipse Marketplace
Enhance your IDE with additional plugins
Open an existing file
Open a file from the filesystem
New Java Project
Create a Java Project
Create a Java project in the workspace or in an external location.
Project name: SimpleWebServer
Use default location
Location: C:\Users\sindu\Documents\workspace\SimpleWebServer
Browse...
JRE
Use an execution environment JRE: JavaSE-1.8
Use a project specific JRE: jdk1.8.0_25
Use default JRE (currently 'jdk1.8.0_25')
Configure JREs...
Project layout
Use project folder as root for sources and class files
Create separate folders for sources and class files
Configure default...
Working sets
Add project to working sets
New...
Working sets:
Select...
< Back
Next >
Finish
Cancel
Always show Welcome at start up
Type here to search
1:40 PM
2/7/2018

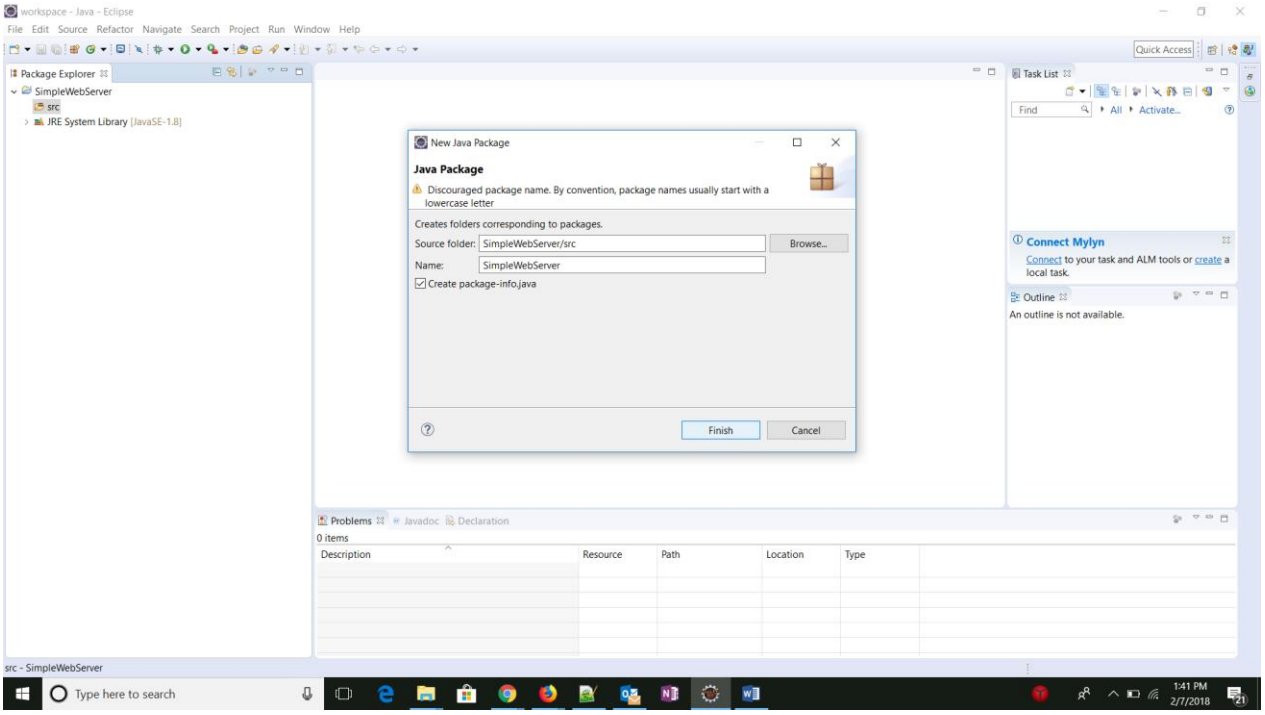
d.


workspace - Java EE - Eclipse
File Edit Navigate Search Project Run Window Help
Welcome
Eclipse Java EE IDE for Web Developers
Workbench
Review IDE configuration settings
Review the IDE's most fiercely contested prefe
Create a new Java EE Web Project
Create a new Eclipse project for Java EE Web
Create a new Javascript project
Create a new Eclipse project for Javascript dev
Checkout projects from Git
Checkout Eclipse projects hosted in a Git repos
Import existing projects
Import existing Eclipse projects from the filesy
Launch the Eclipse Marketplace
Enhance your IDE with additional plugins
Open an existing file
Open a file from the filesystem
New Java Project
Create a Java Project
Create a Java project in the workspace or in an external location.
Project name: SimpleWebServer
Open Associated Perspective?
This kind of project is associated with the Java perspective.
This perspective is designed to support Java development. It offers a Package Explorer, a Type Hierarchy, and Java-specific navigation actions.
Do you want to open this perspective now?
Remember my decision
Yes
No
Use project folder as root for sources and class files
Create separate folders for sources and class files
Configure default...
Working sets
Add project to working sets
New...
Working sets:
Select...
< Back
Next >
Finish
Cancel
Always show Welcome at start up
Type here to search
1:40 PM
2/7/2018

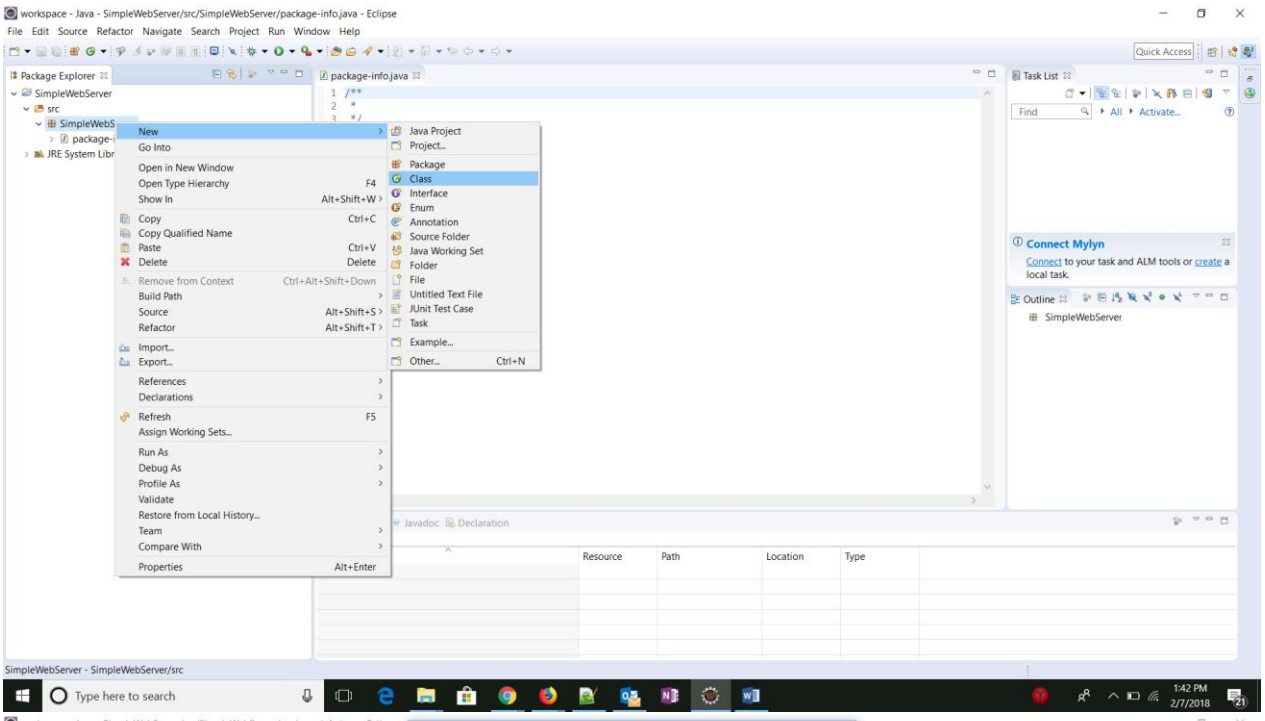
e.


workspace - Java - Eclipse
File Edit Source Refactor Navigate Search Project Run Window Help
Quick Access
Package Explorer
SimpleWebServer
New
Open in New Window
Open Type Hierarchy F4
Show In Alt+Shift+W
Copy Ctrl+C
Copy Qualified Name
Paste Ctrl+V
Delete Delete
Remove from Context Ctrl+Alt+Shift+Down
Build Path
Source Alt+Shift+S
Refactor Alt+Shift+T
Import...
Export...
Refresh F5
Assign Working Sets...
Run As
Debug As
Profile As
Validate
Restore from Local History...
Maven
Team
Compare With
Properties Alt+Enter
Java Project
Project...
Package
Class
Interface
Enum
Annotation
Source Folder
Java Working Set
Folder
File
Untitled Text File
JUnit Test Case
Task
Example...
Other... Ctrl+N
Task List
Find
All
Activate...
Connect Mylyn
Connect to your task and ALM tools or create a local task.
Outline
An outline is not available.
Problems
Javadoc
Declaration
0 items
Description
Resource
Path
Location
Type
src - SimpleWebServer
Type here to search
1:41 PM
2/7/2018

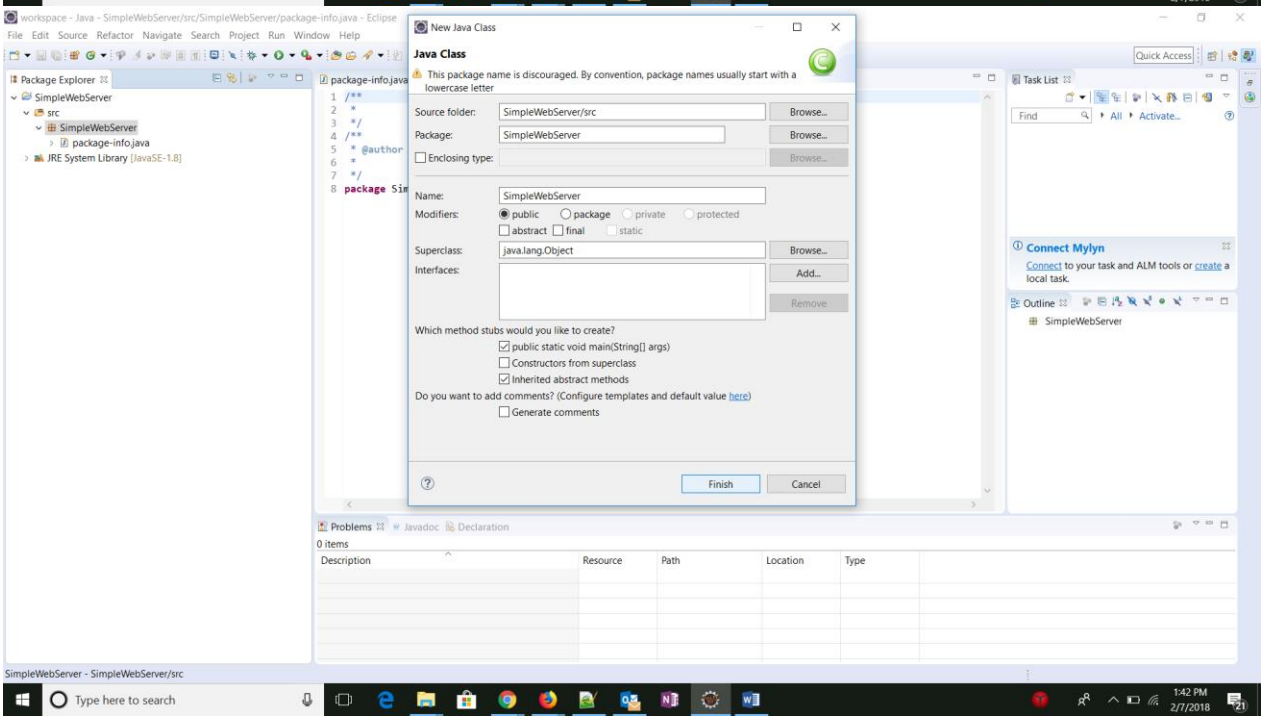
f.


workspace - Java - Eclipse
File Edit Source Refactor Navigate Search Project Run Window Help
Quick Access
Package Explorer
SimpleWebServer
src
JRE System Library [JavaSE-1.8]
New Java Package
Java Package
Discouraged package name. By convention, package names usually start with a lowercase letter
Creates folders corresponding to packages.
Source folder: SimpleWebServer/src
Browse...
Name: SimpleWebServer
Create package-info.java
Finish
Cancel
Task List
Find
All
Activate...
Connect Mylyn
Connect to your task and ALM tools or create a local task.
Outline
An outline is not available.
Problems
Javadoc
Declaration
0 items
Description
Resource
Path
Location
Type
src - SimpleWebServer
Type here to search
1:41 PM
2/7/2018

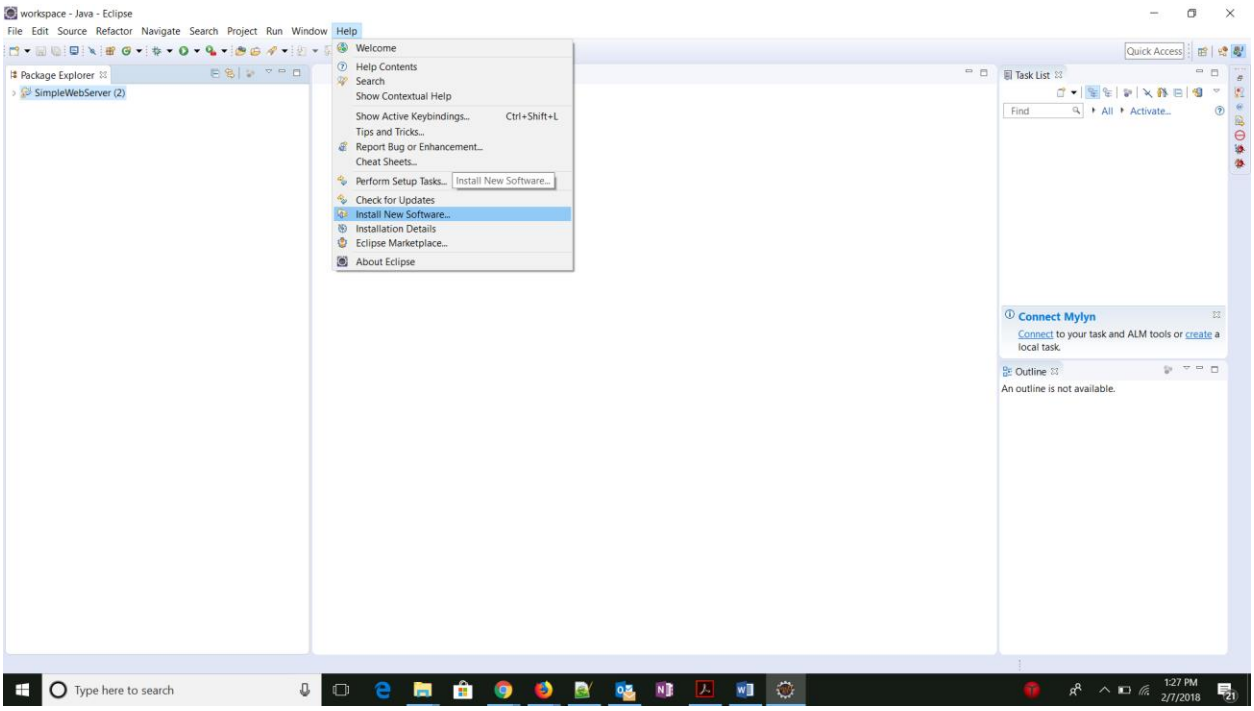
g.



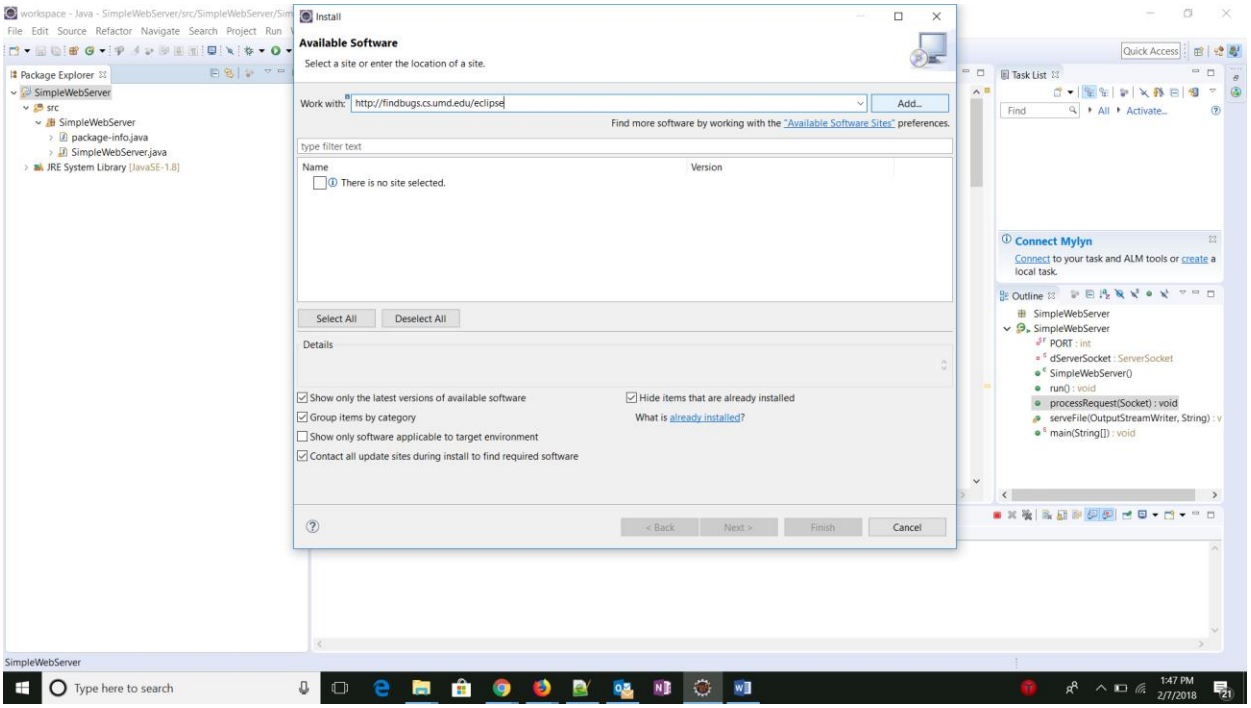
h.



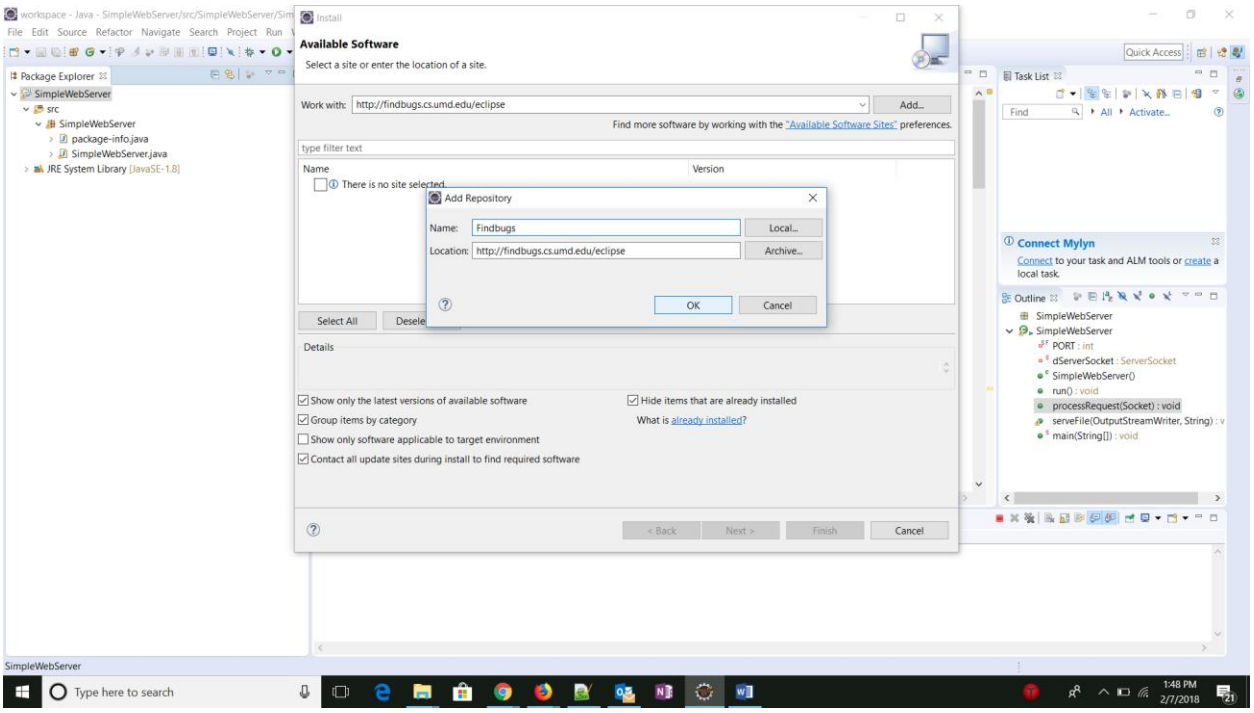
3. From Help tab, go to “Install New Software” to add the Findbugs plugin for eclipse as shown below:
    a. Click on “Install New Software”



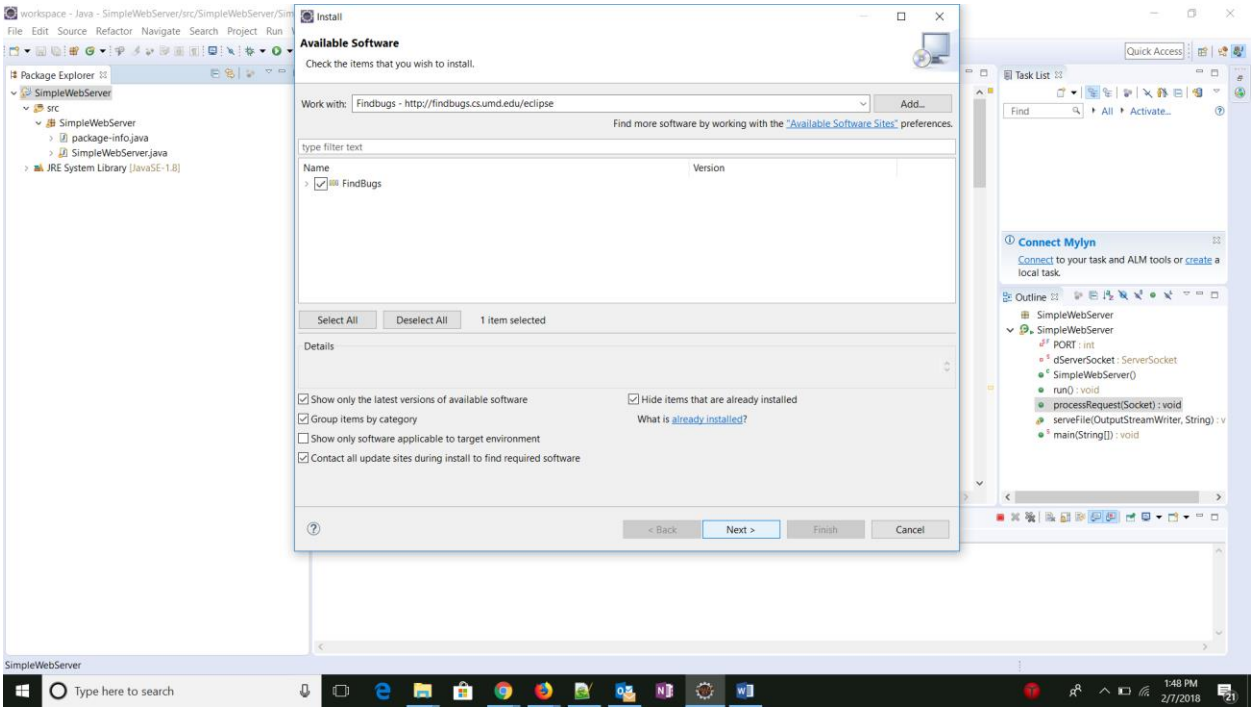
b. Give the url to get the findbugs plugin for eclipse as: http://findbugs.cs.umd.edu/eclipse and click on "Add"



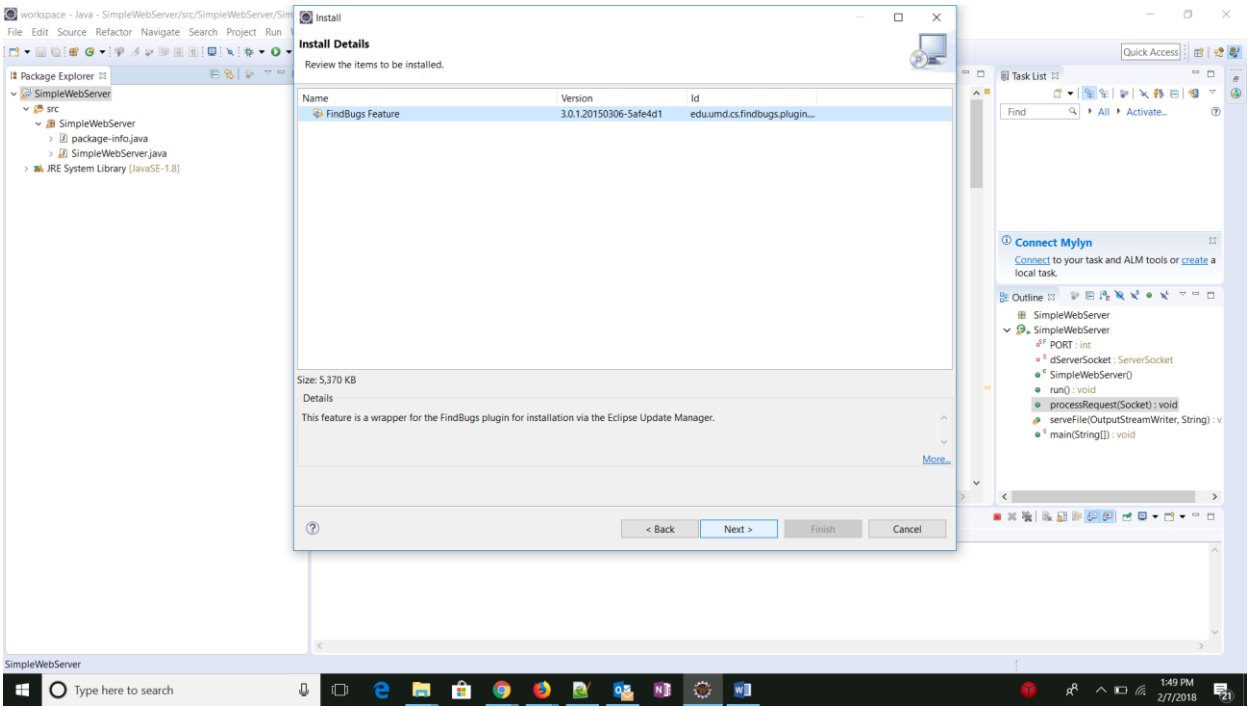
c. The below window pops up, give the name as 'Findbugs' and click 'ok':



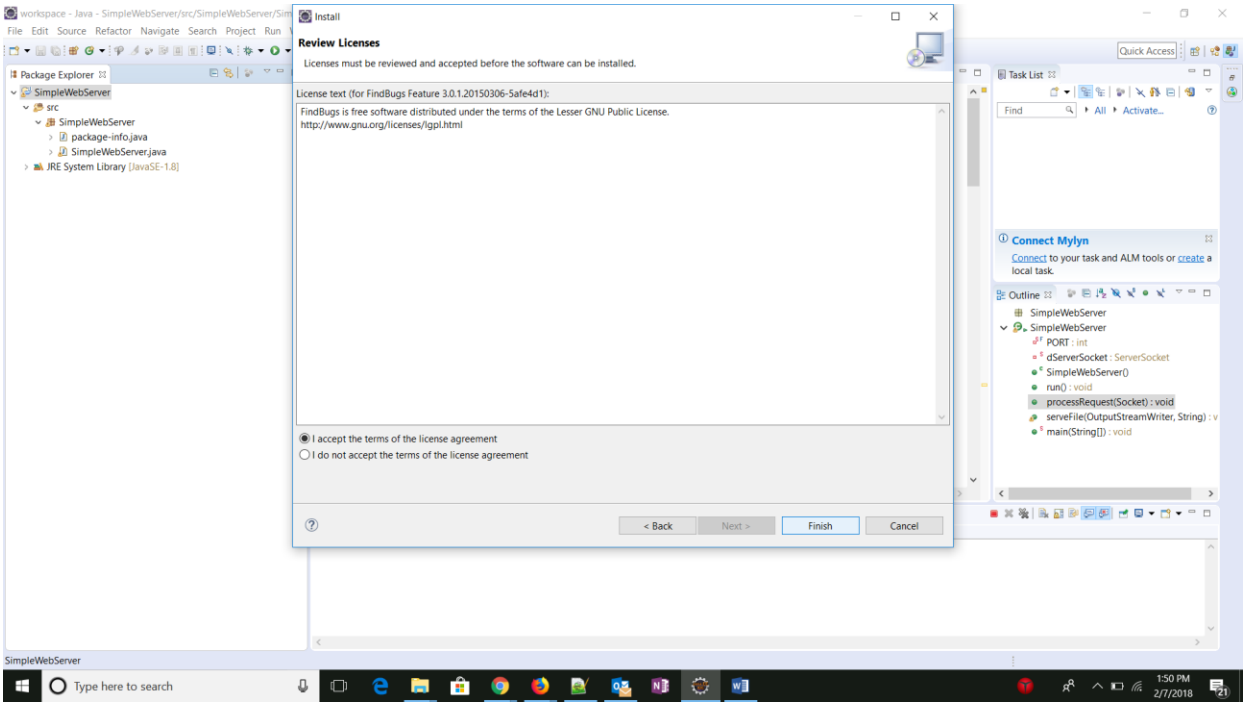
d. Select 'FindBugs' as shown in the window below and click 'Next':



e. Click 'Next' again as shown below:



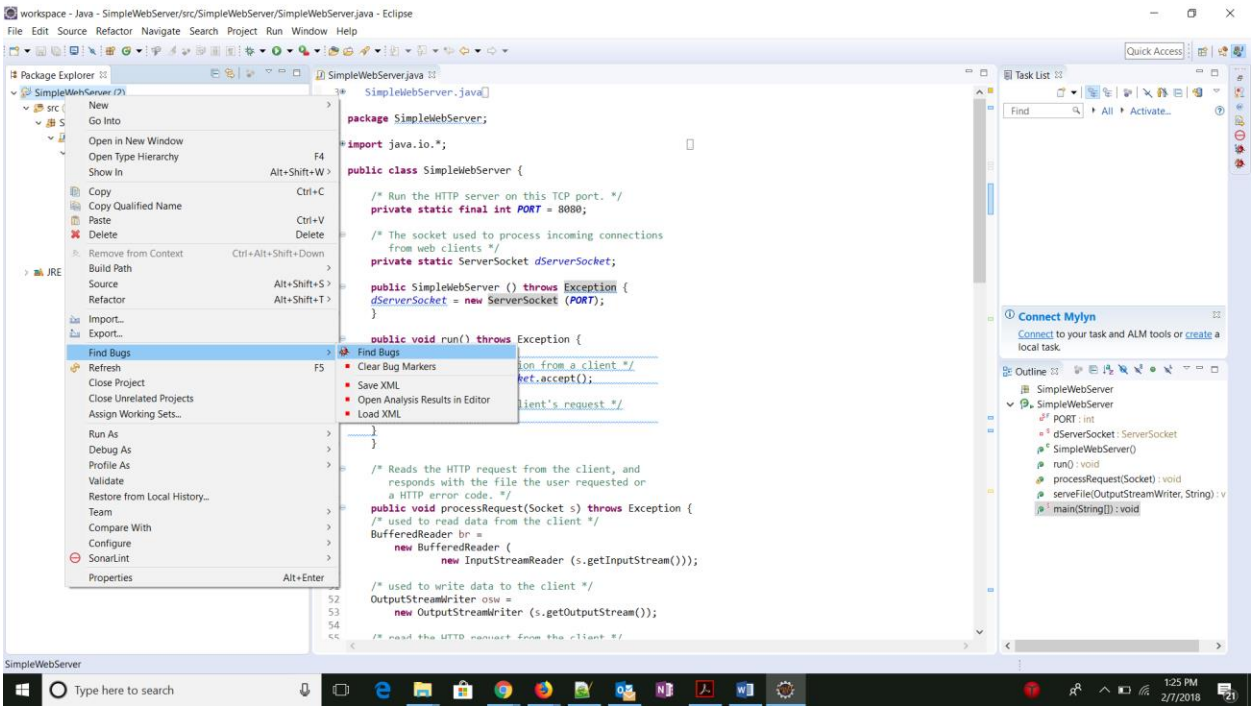
f. Select 'I accept' and click Finish to complete the installation Findbugs plugin for eclipse:



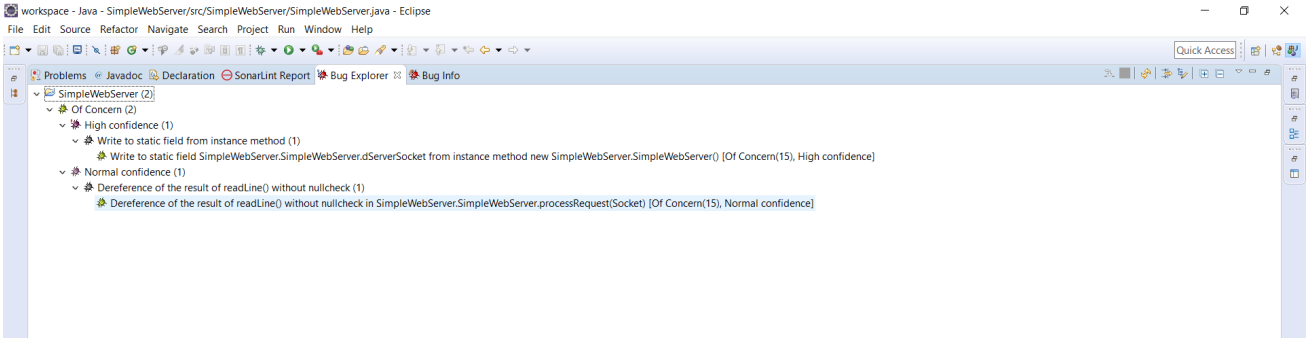
g.

h. It will ask you to restart eclipse, click ok to restart eclipse.

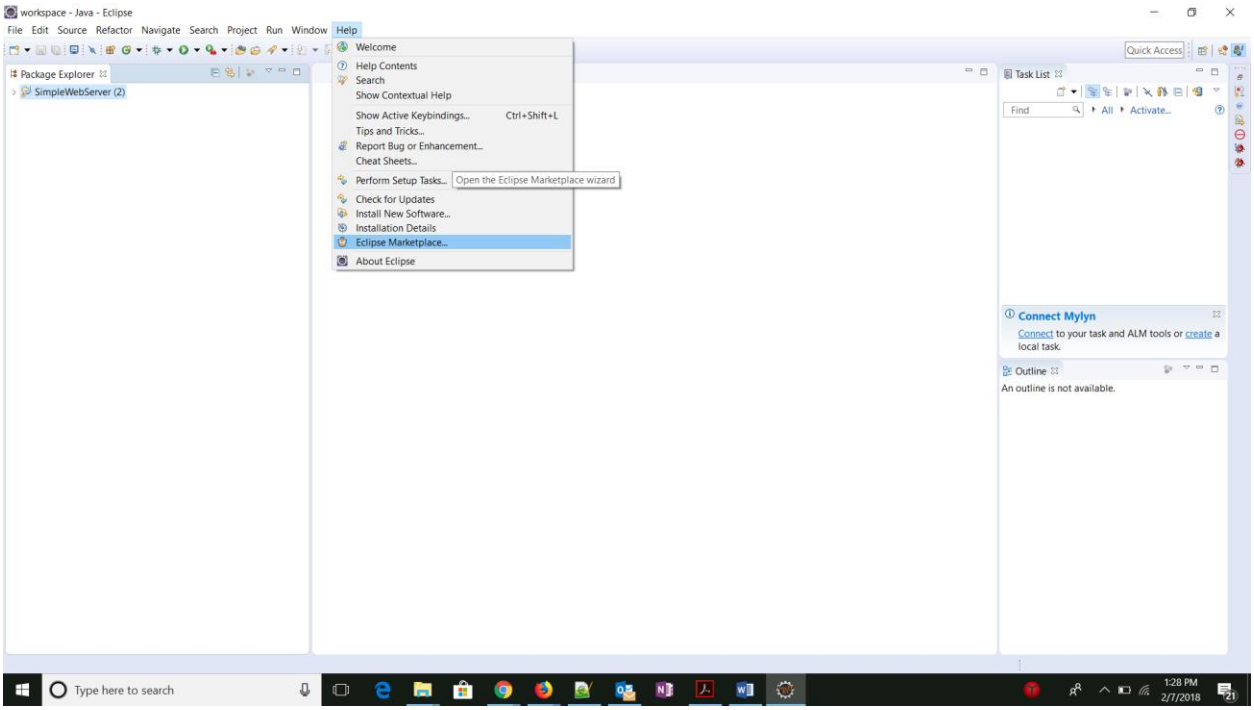
i. To run the tool, select the project in the package explorer and select Find Bugs and in the sub menu, select 'Find Bugs' again:



j. The below Find bugs explorer will display the bugs present in the code:

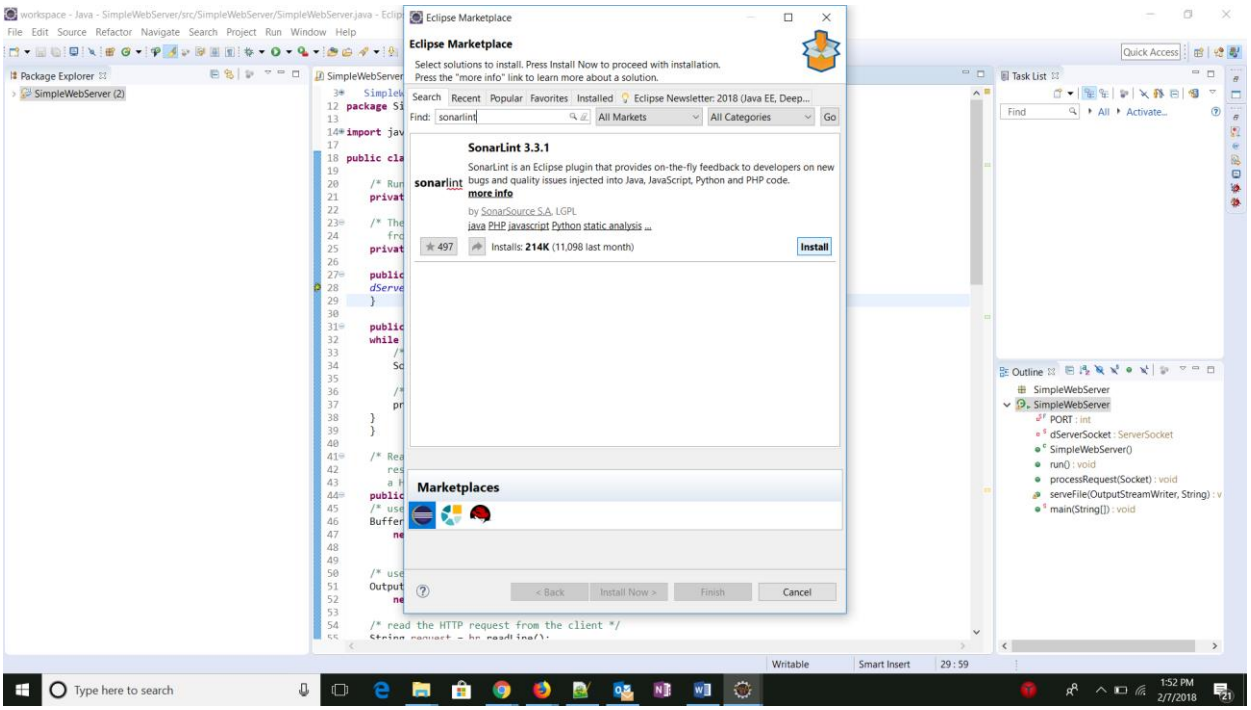


4. To install SonarLint plugin for eclipse, go to “Eclipse Market place” from the Help tab as shown below:

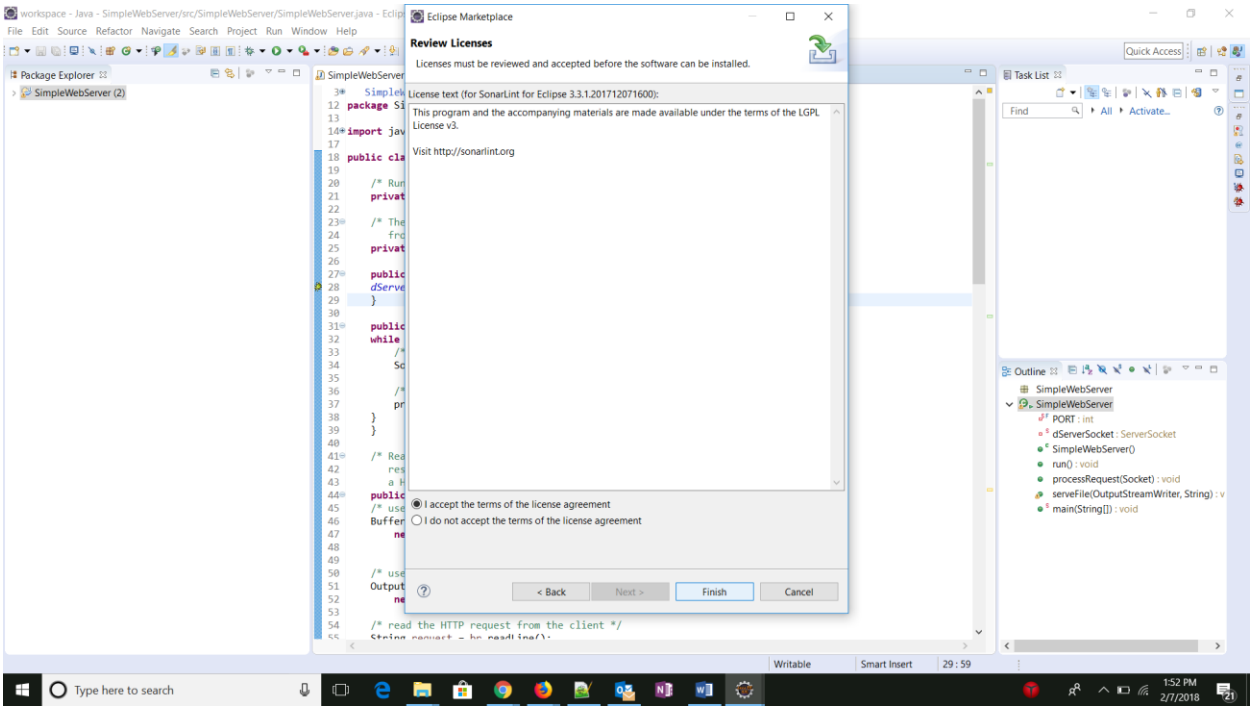


a.

b. Type in “sonarlint” as shown in below window and click install to install the SonarLint plugin for eclipse:

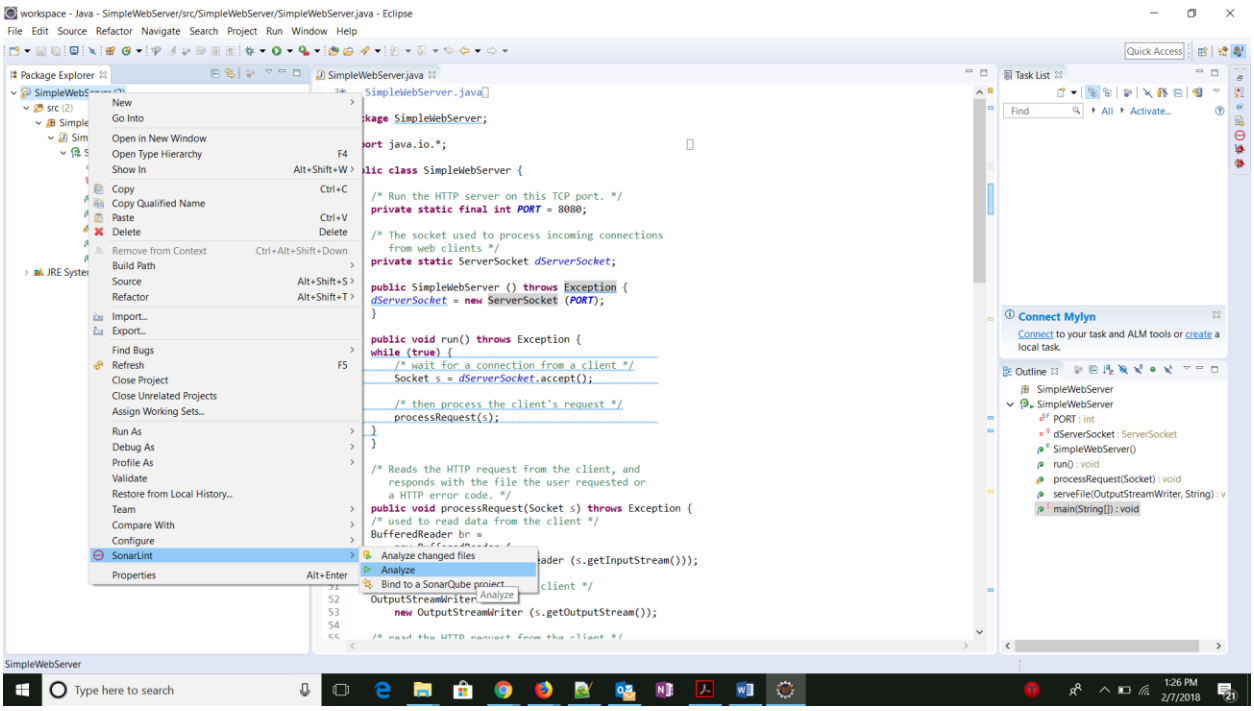


c. Select 'I Accept' and click "Finish" to install the plugin as shown in below window:



d. It will ask you to restart eclipse, click ok to restart eclipse.

e. To run the tool, select the project in the package explorer and select SonarLint, and in the sub menu, select 'Analyze' as shown in below window:



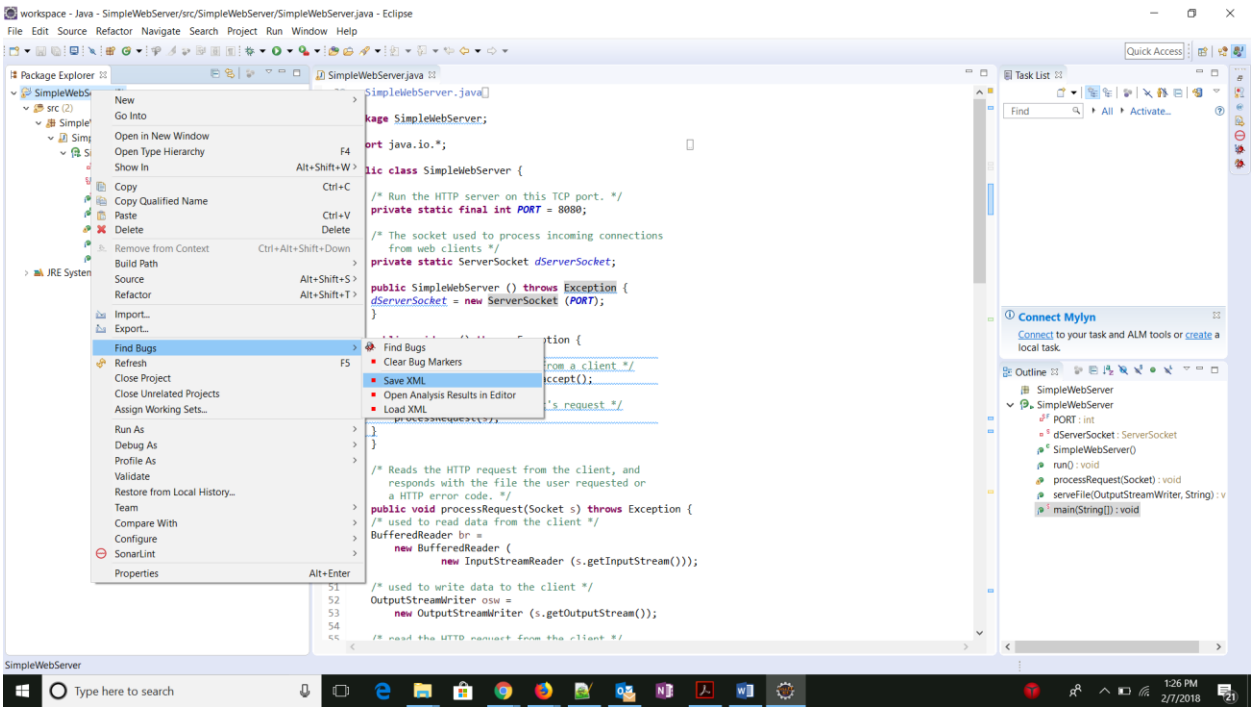
Comparison/ Contrast Tools

1. Does the tool analyze source or binary as input?
   - ✓Findbugs tool analyzes byte code which is why it is more prone to reporting false positives.
   - ✓SonarLint analyzes source code and provides much detailed information about the bugs it finds with a possible solution to fix the bug.
2. Which category of tools is it?
   a. Type checking
   b. Style checking
   c. Program understanding
   d. Program verification
   e. Property checking
   f. Bug finding
   g. Security review
   - ✓ Both the Findbugs and SonarLint are Bug finding tools.
3. Show an example (if one exists) of a finding that is reported by one tool and not others.
   - ✓In the method run(), end condition of the while loop is missing. This bug is reported by SonarLint tool but not by Findbugs tool.
4. Show an example (if one exists) of a finding reported by multiple tools.
   - ✓In Line 28, dServerSocket object is a static object and it is initialized in the constructor of the class which is not an acceptable practice. This bug is reported by both tools, Findbugs and SonarLint.
5. For the known flaw in the code used, document which tools reported it (true negative) and which tools did not (false positive).
   - ✓SonarLint reported that exception handling is generic in all the methods except serveFile of the SimpleWebServer class, whereas Findbugs tool did not report this obvious flaw in the code.

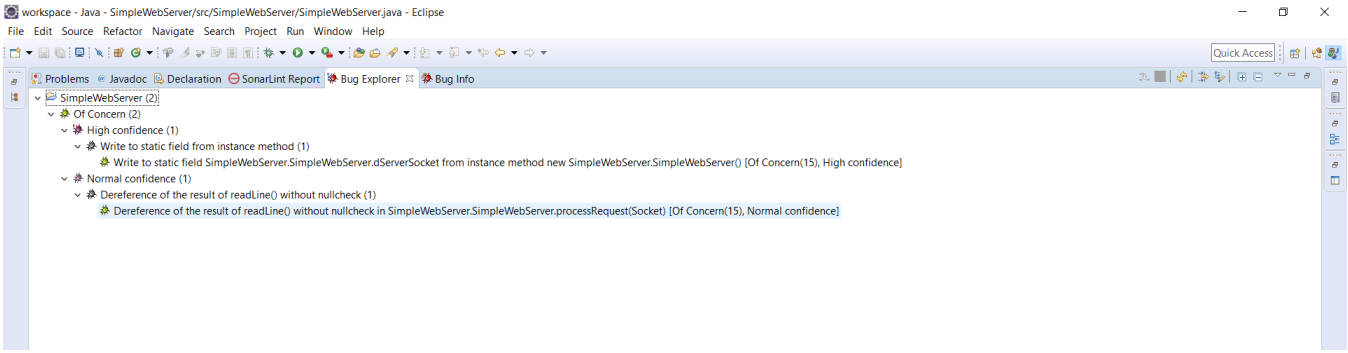
Results

Findbugs:

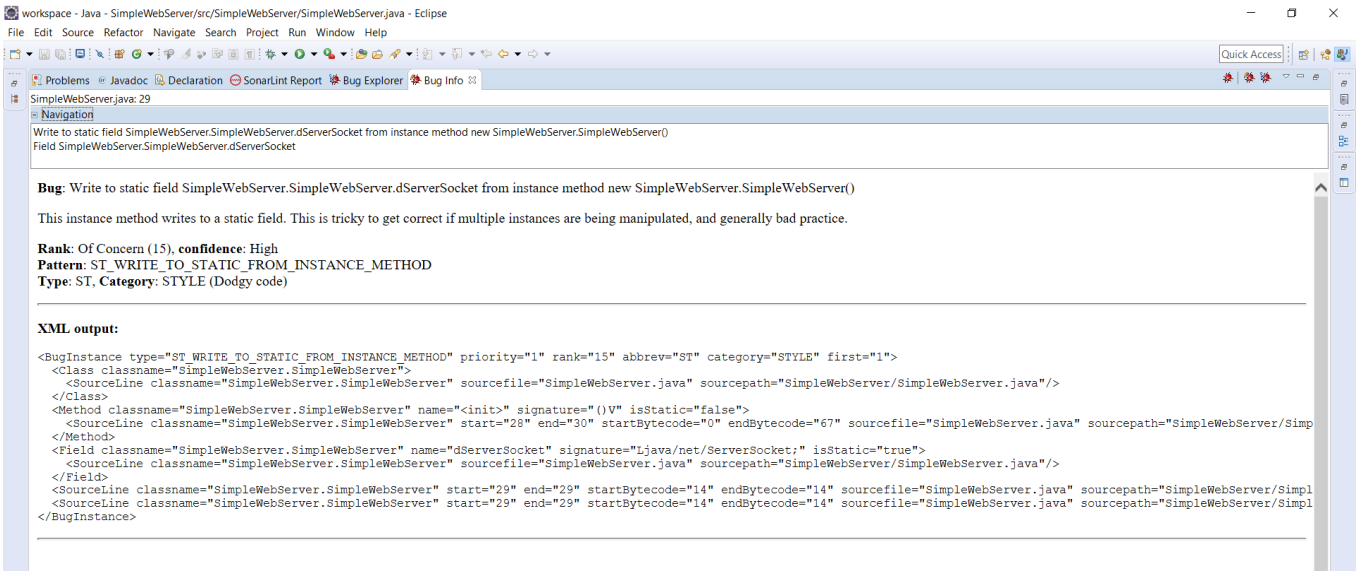
- To save the bug report given by the Findbugs tool, select the project in the package explorer and select Find Bugs and in the sub menu, select ‘Save XML’ to save the report in XML format as shown below:



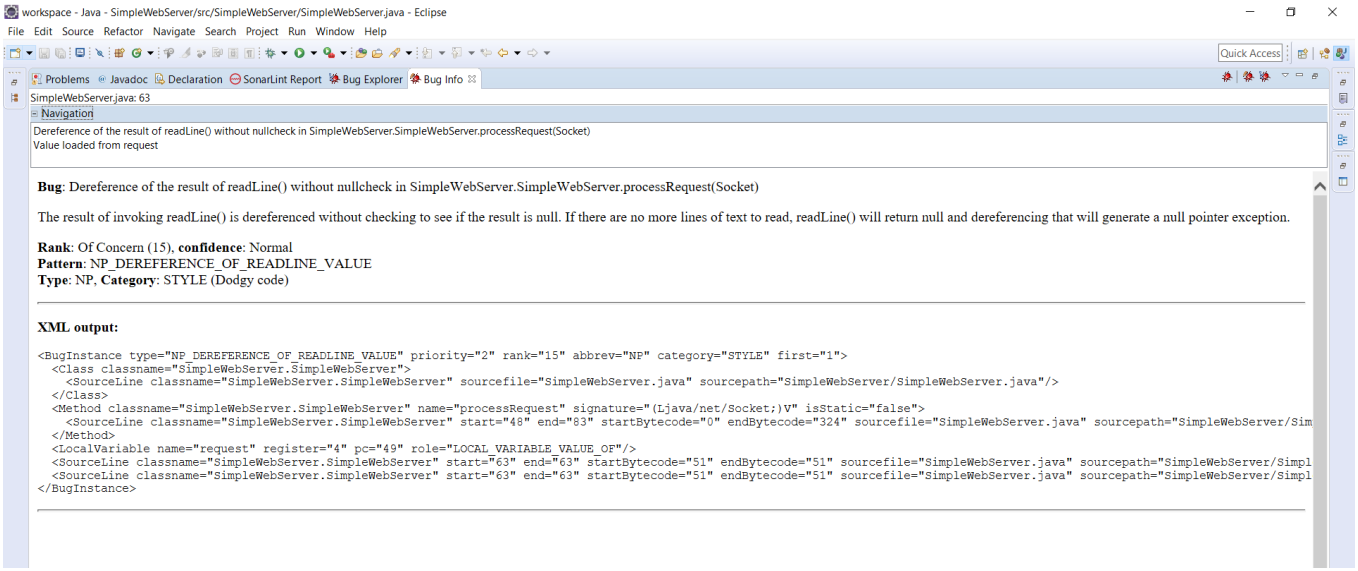
- Below are the screenshots of the bugs reported by the findbugs tool:



(a)



(b)



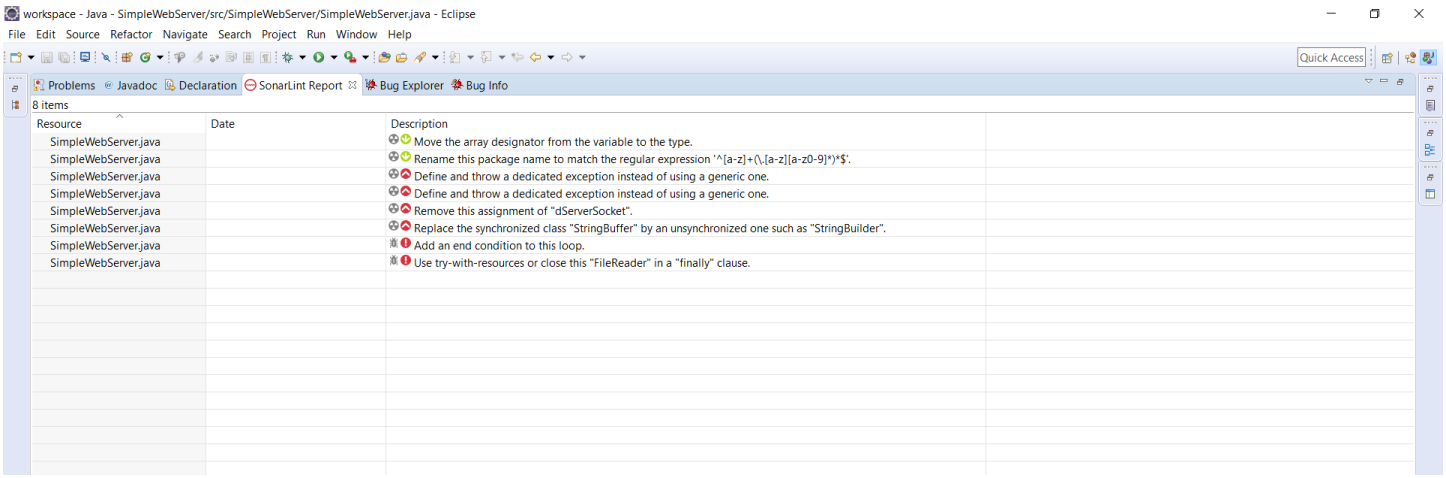
(c)

- Below is the XML report:

SimpleWebServer_FindBugs_Report.xml

SonarLint:

Below is the screenshot of the SonarLint report:



Part 2

Code Provided

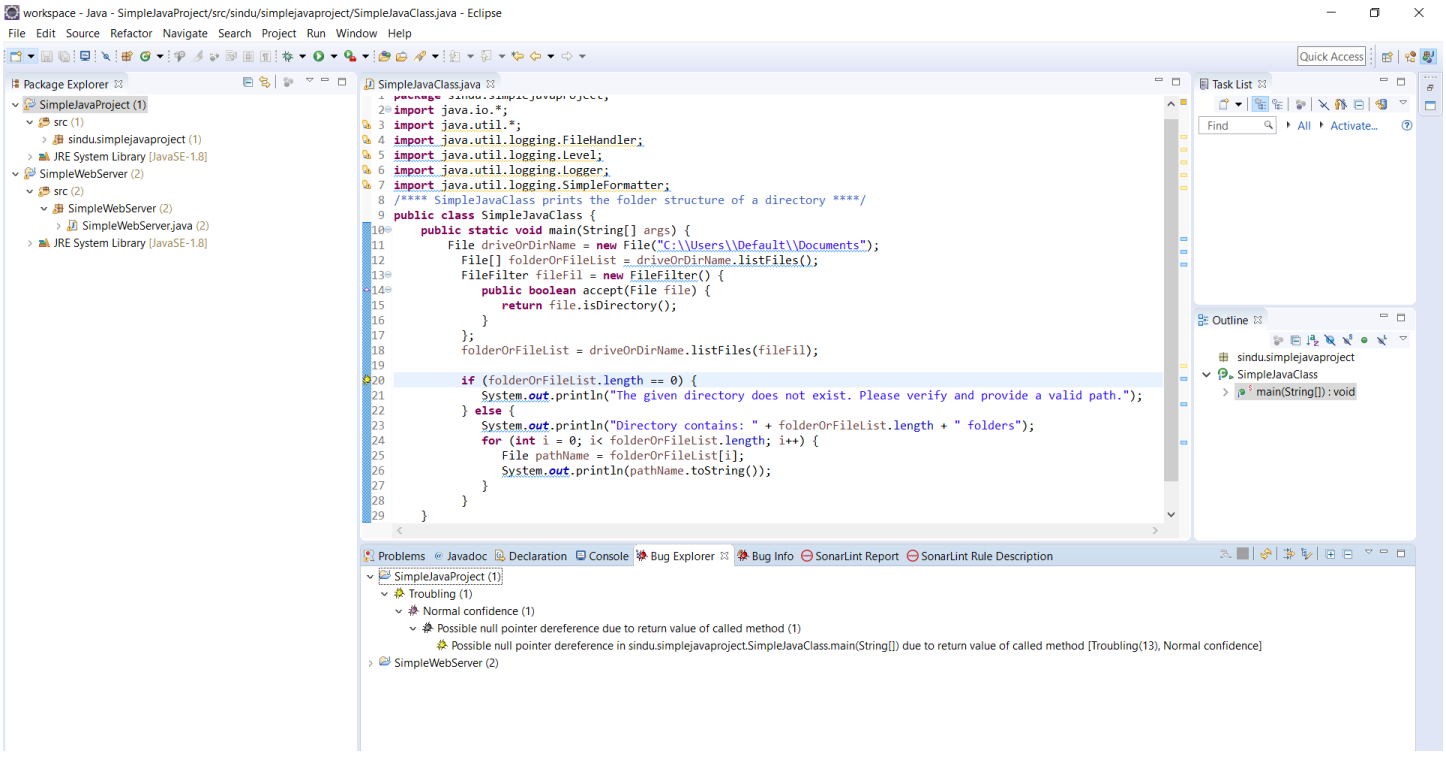
The code used for the part 2 of this project, returns the folder structure/ directory of a drive or a path.

Initial_SimpleJavaClass.java

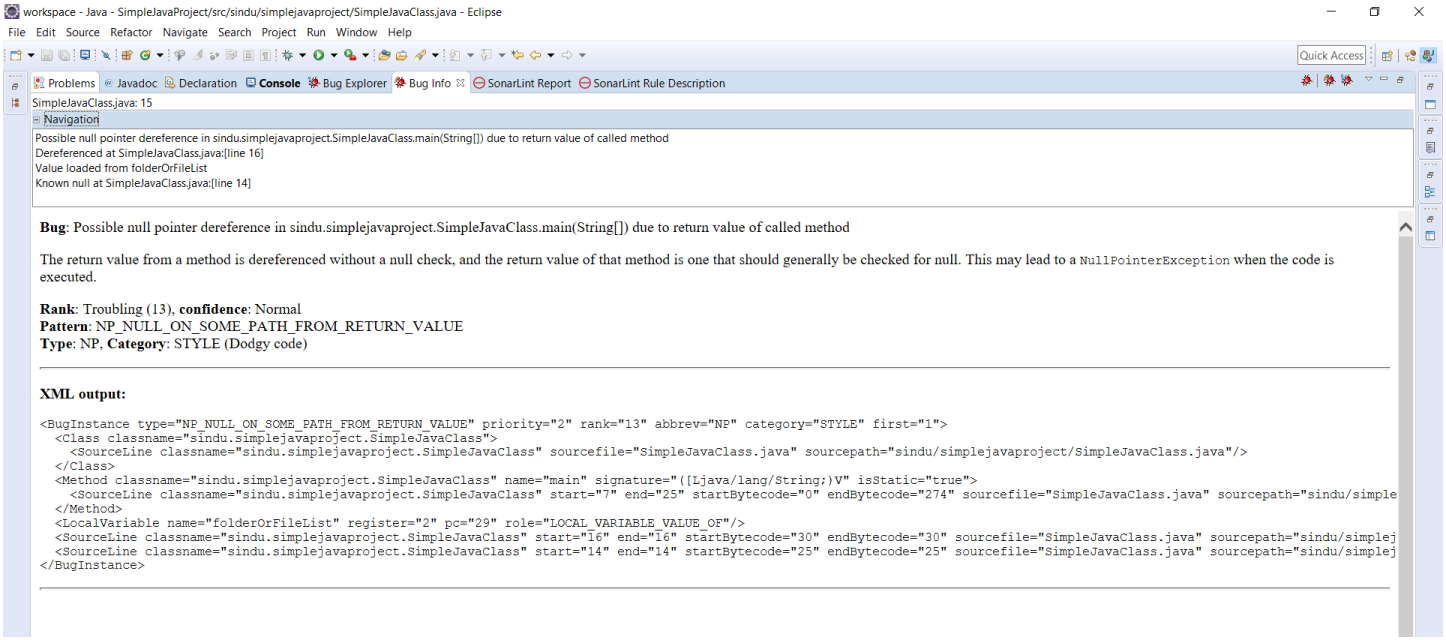
Results

Below are the results returned by Findbugs and SonarLint tools:

Findbugs:



(a)



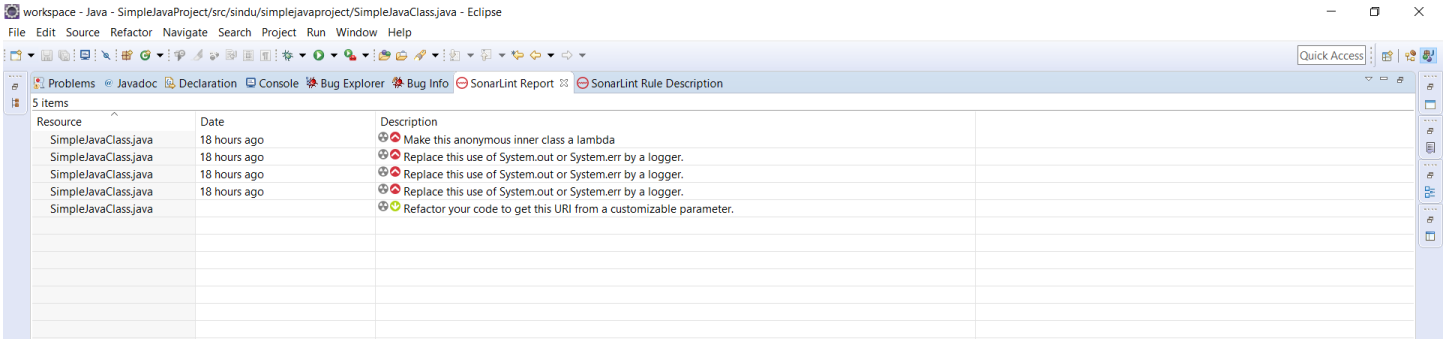
(b)

Below is the XML report:

SimpleJavaProject_Findbugs_Report.xml

SonarLint:

Below is the screenshot of the SonarLint report:



Fixes

Code after bug fixes:

SimpleJavaClass.java

Findbugs: 1 Normal Confidence bug - Fixed

“Possible null pointer dereference in sindu.simplejavaproject.SimpleJavaClass.main(String[]) due to return value of called method [Troubling(13), Normal confidence]”

As shown in the fig(a) in above section, the bug reported by the tool means that, on line 20, null check was not implemented for the folderOrFileList object. Once null check was added, no bugs were reported in the bug explorer.

SonarLint: 4 major bugs, 1 minor bug

Fixed:

3 of the major bugs as shown in the sonarlint report above are about using logger class instead writing the logs to console. Another major bug is about converting an inner class to lambda expression.

All the major bugs are fixed and the new report now has two minor bugs: