資訊人才軟體培育推廣計畫

Java安全程式設計

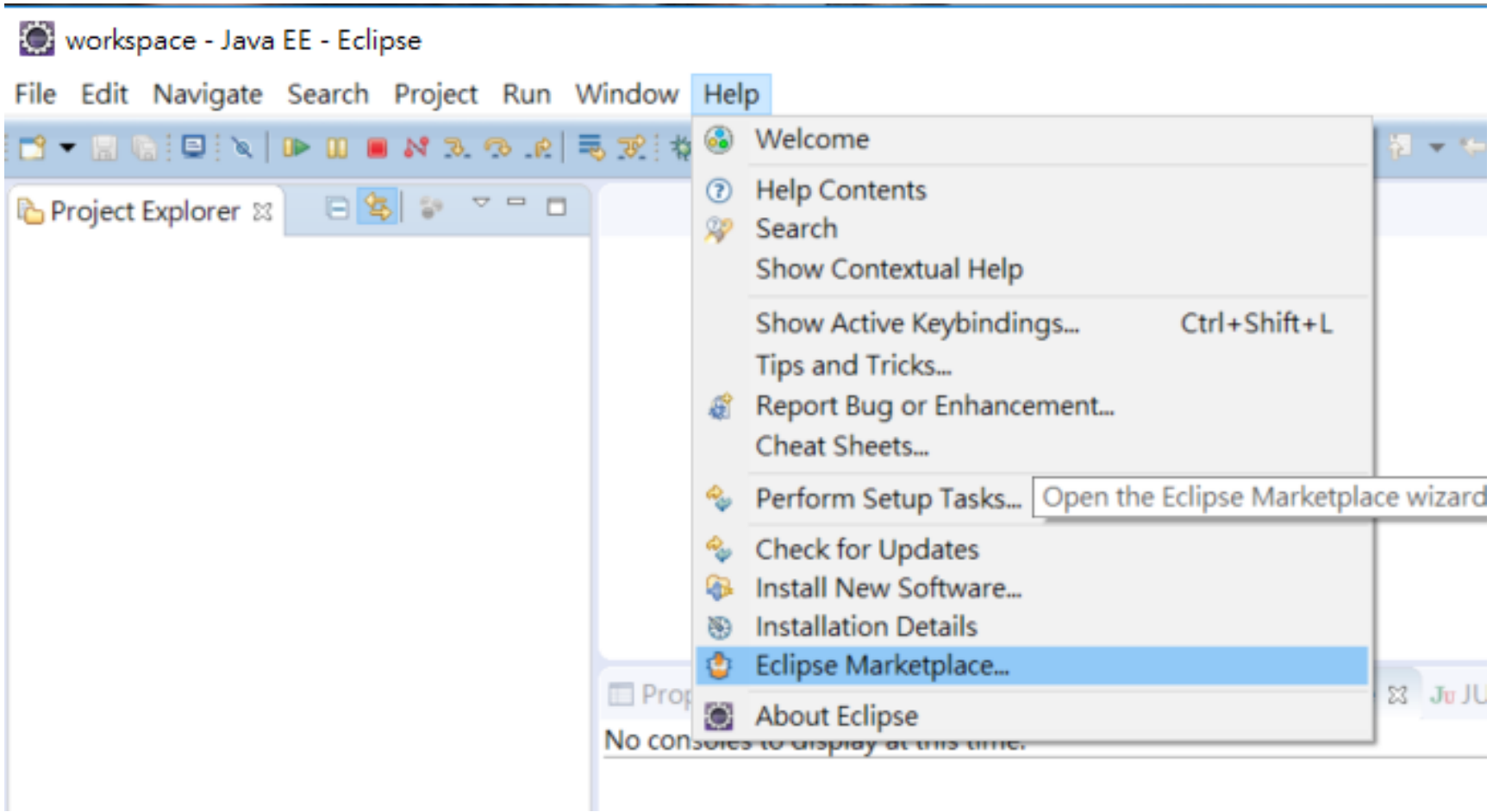
逢甲大學 資訊工程系
陳錫民 助理教授

2016年8月

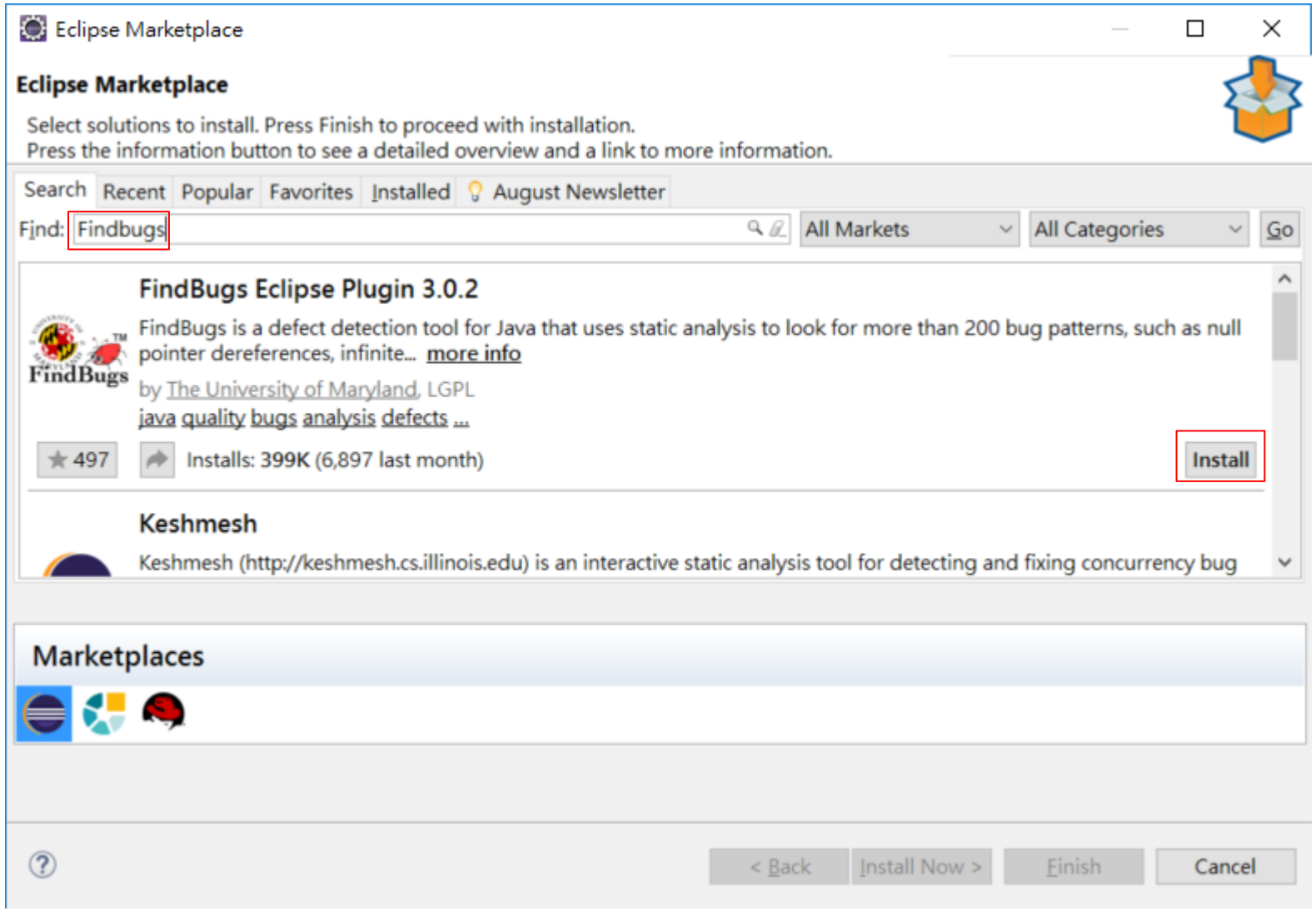
FindBugs for Eclipse

- 靜態程式碼分析工具
  - 偵測潛在的Bug、安全缺陷與不良的程式撰寫方式
- 支援Java
- Open-source Eclipse plugin
- 系統需求: Eclipse

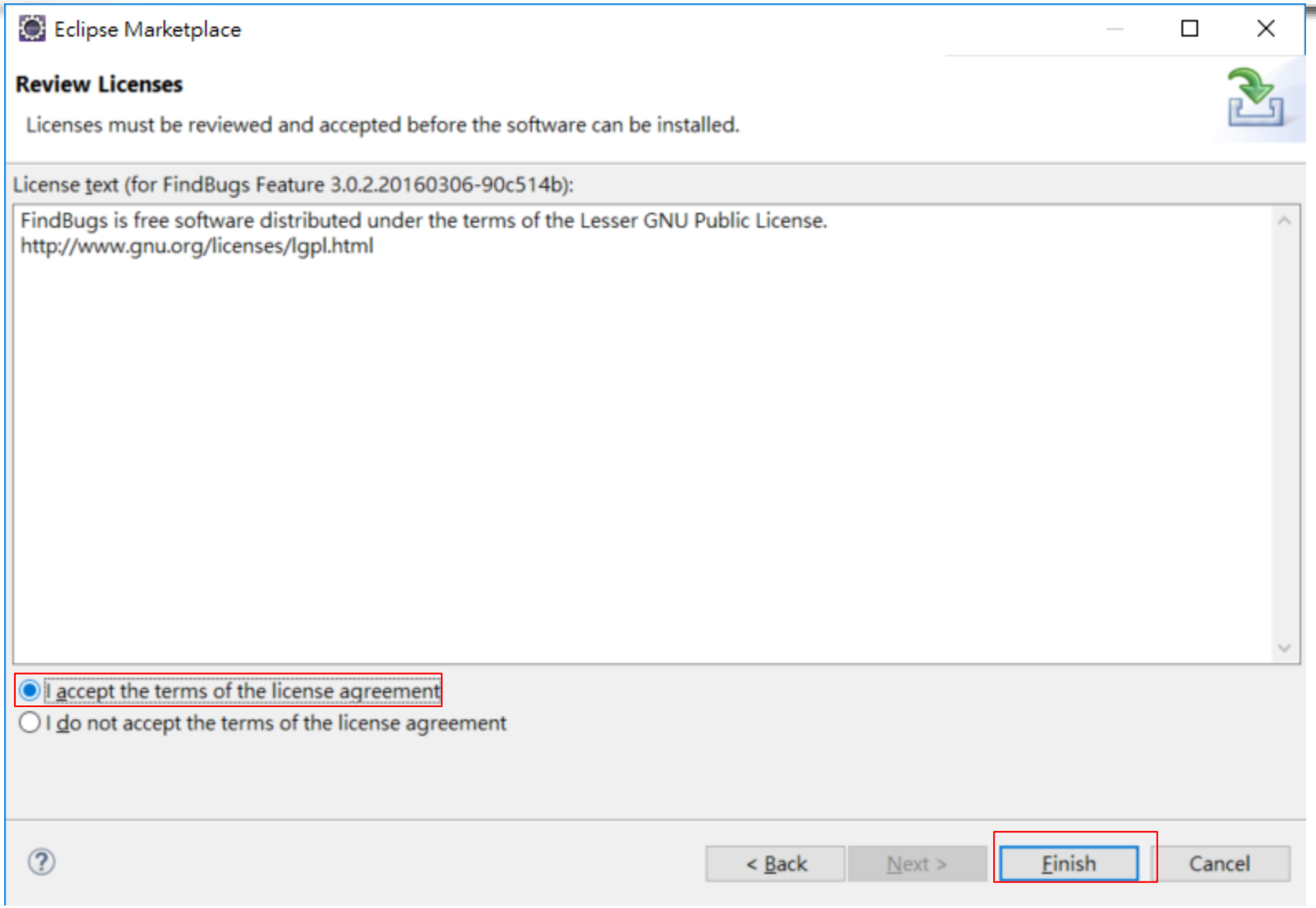
安裝FindBugs for Eclipse$_1$



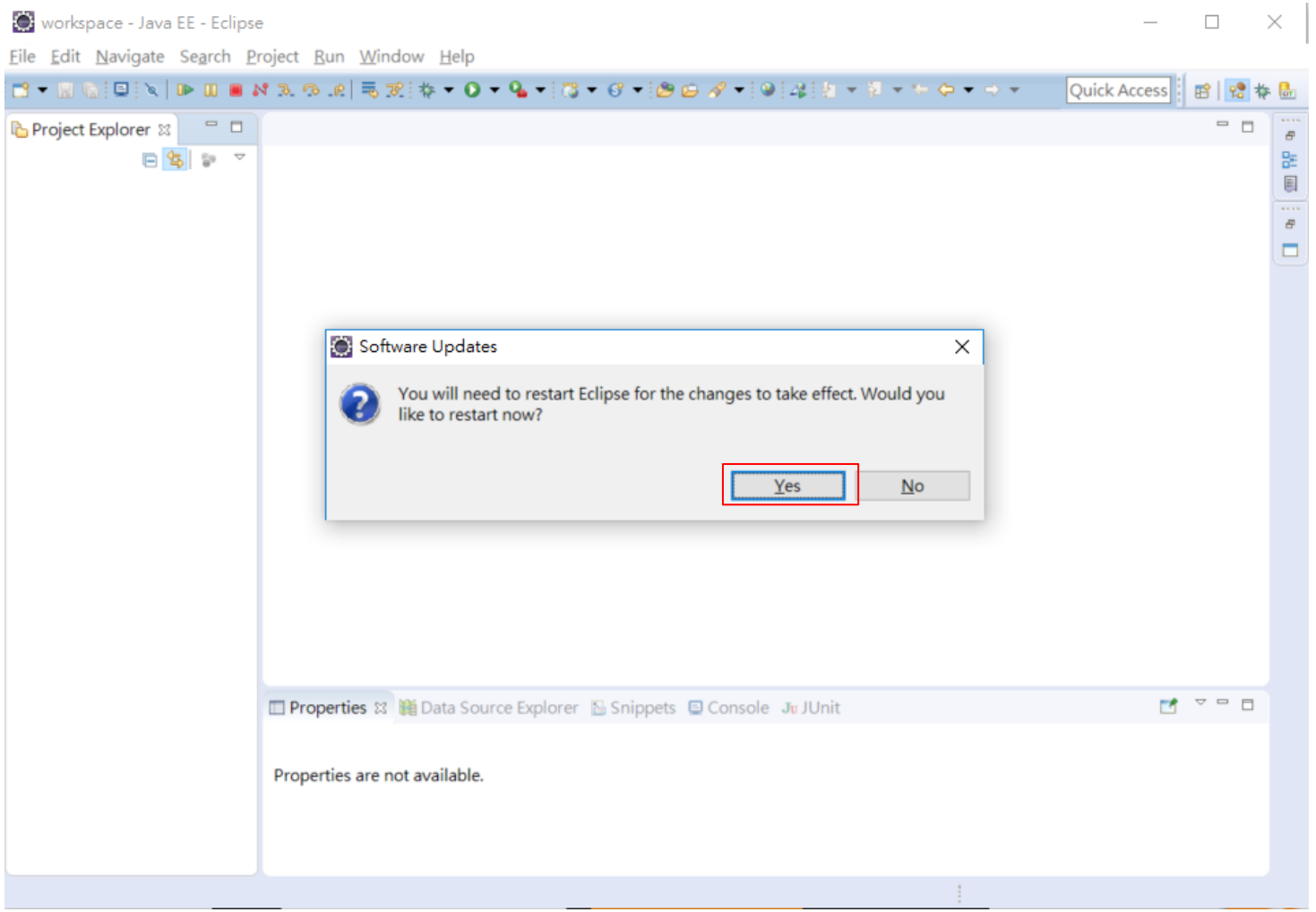
安裝FindBugs for Eclipse$_2$



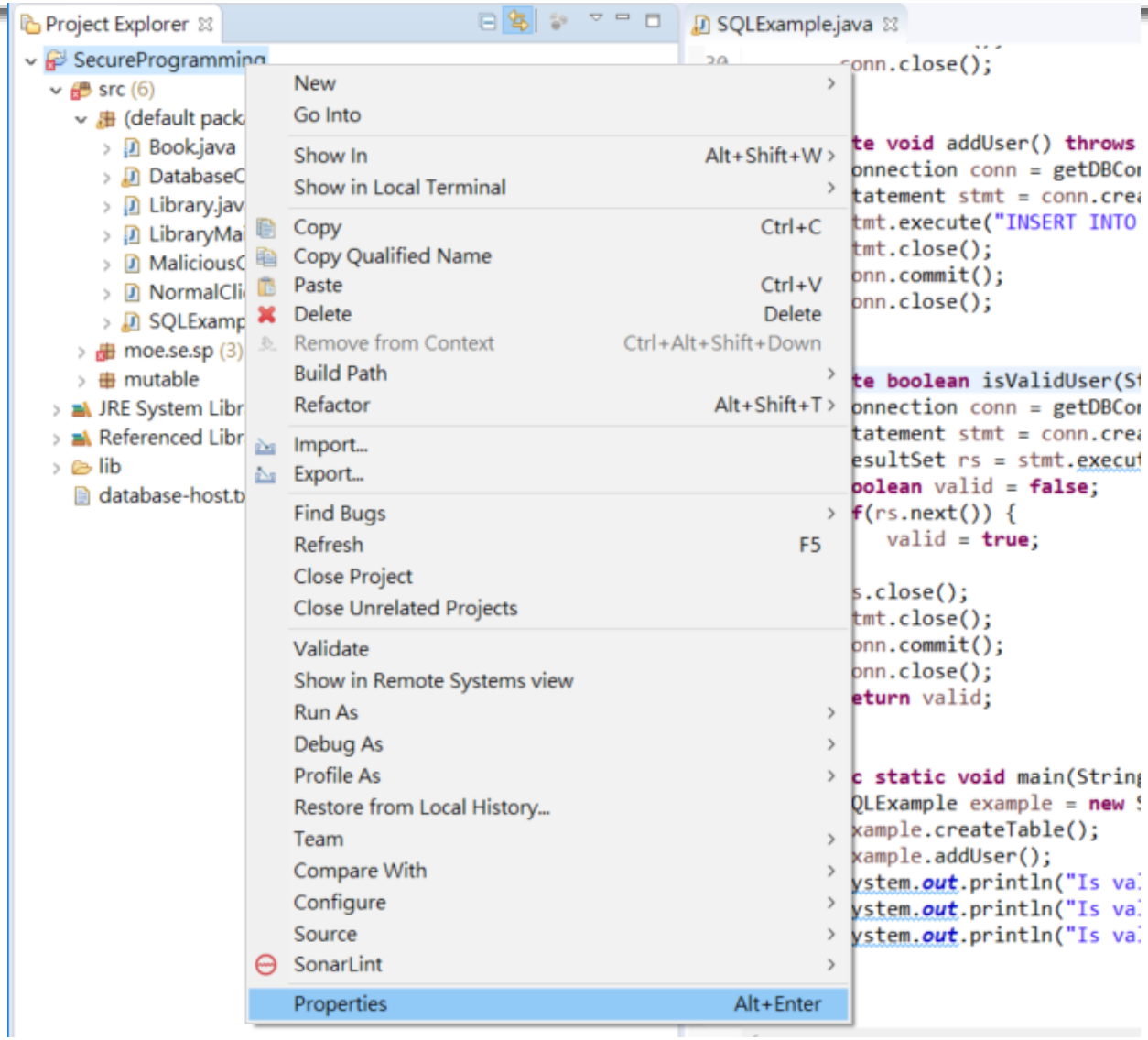
安裝FindBugs for Eclipse3



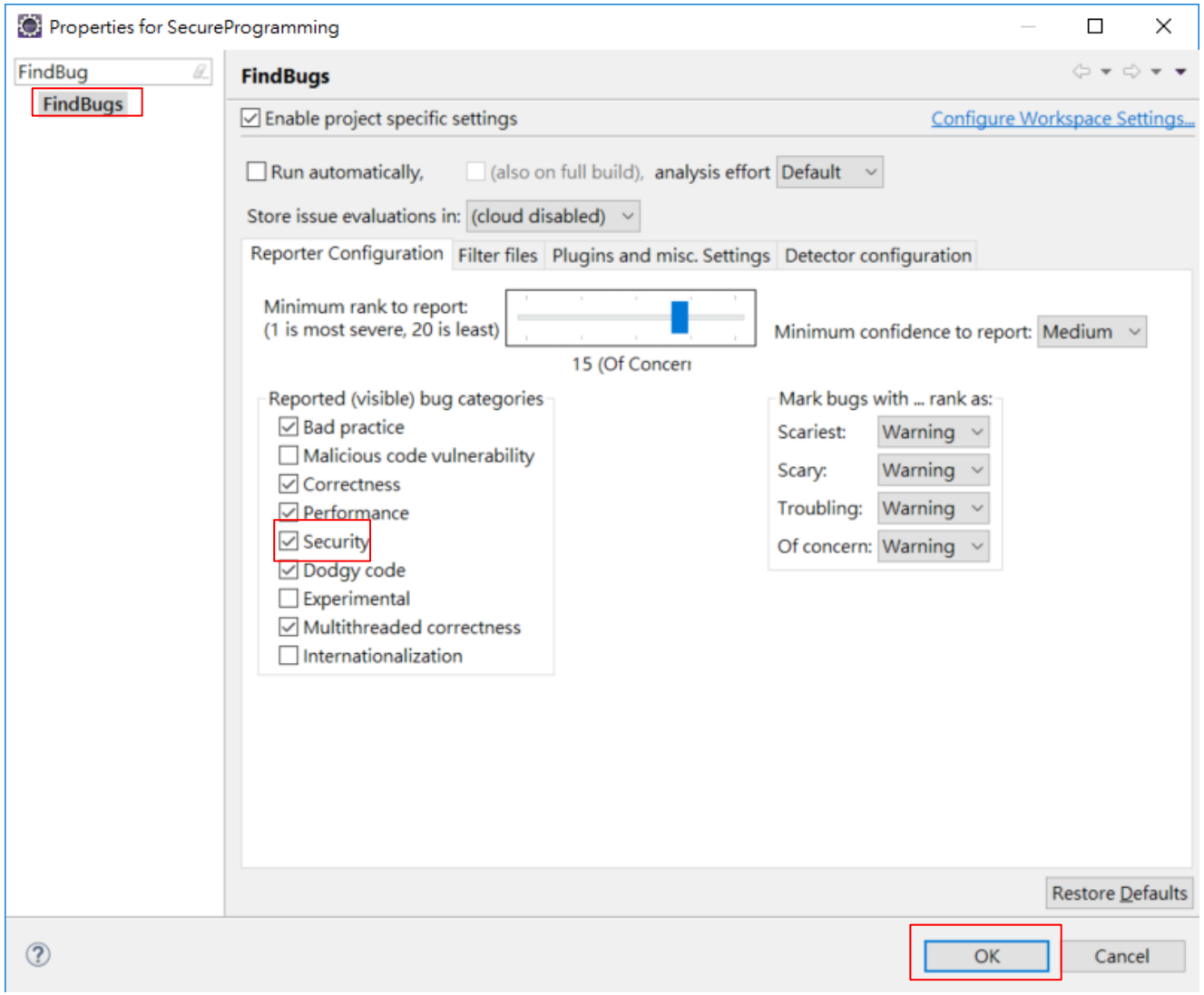
安裝FindBugs for Eclipse4



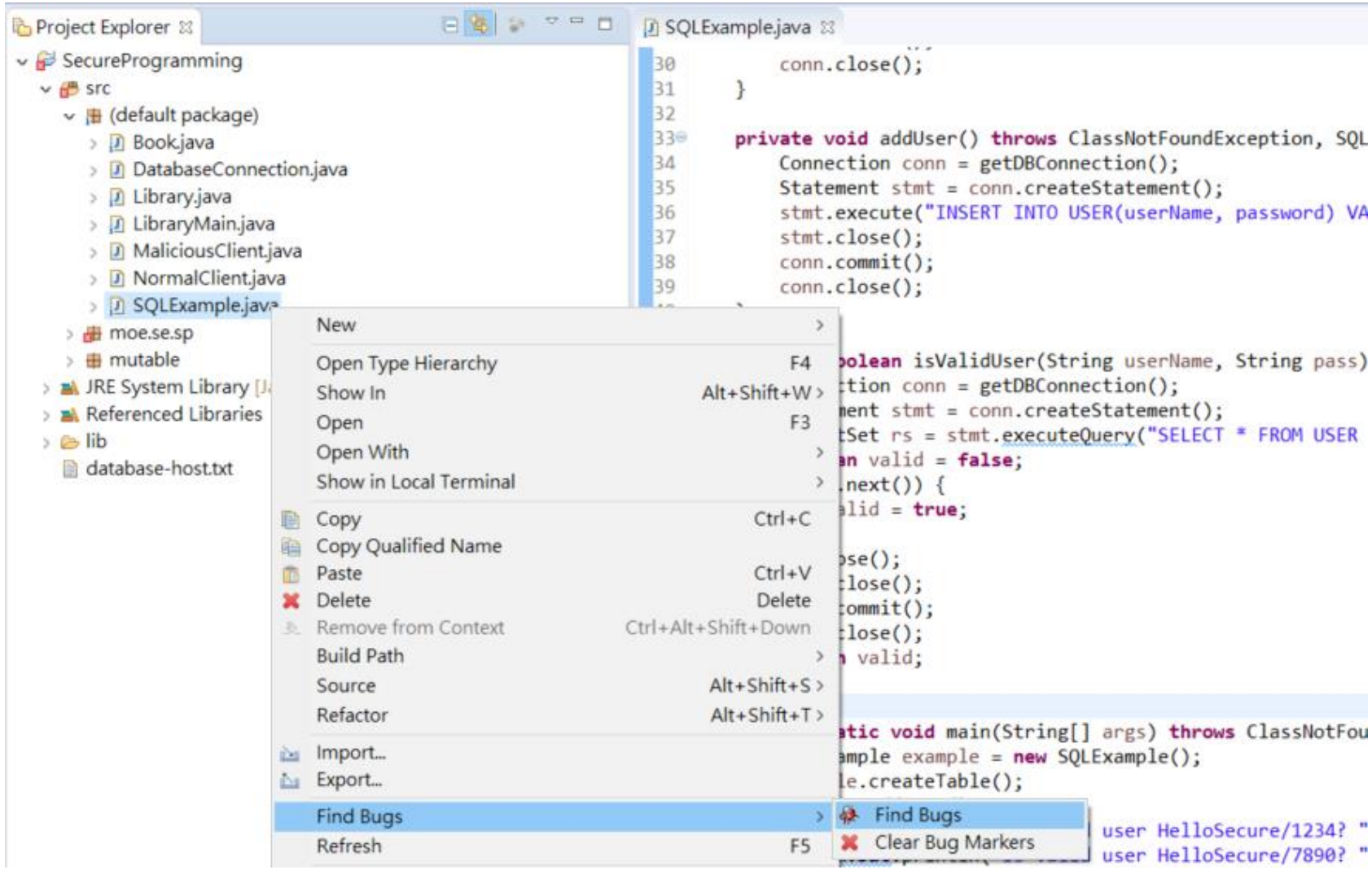
設定專案FindBugs$_1$



設定專案FindBugs2



執行程式碼分析

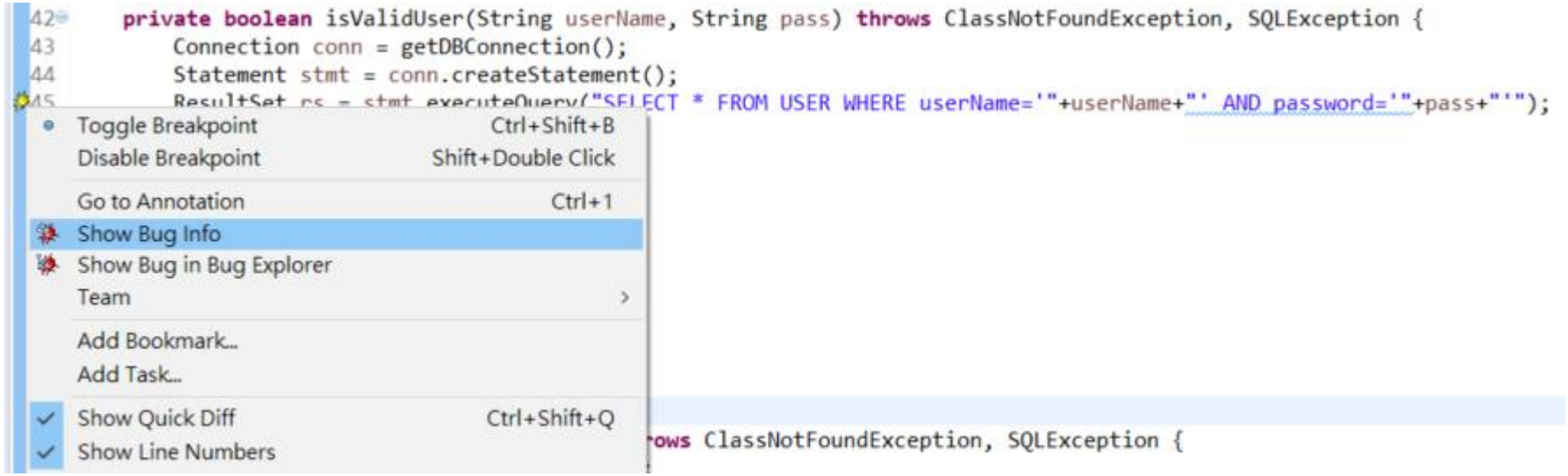


查看分析結果

SQLExample.java

```
30          conn.close();
31      }
32
33      private void addUser() throws ClassNotFoundException, SQLException {
34          Connection conn = getDBConnection();
35          Statement stmt = conn.createStatement();
36          stmt.execute("INSERT INTO USER(userName, password) VALUES ('"+TEST_USER+"', '"+TEST_PASS+"')");
37          stmt.close();
38          conn.commit();
39          conn.close();
40      }
41
42      private boolean isValidUser(String userName, String pass) throws ClassNotFoundException, SQLException {
43          Connection conn = getDBConnection();
44          Statement stmt = conn.createStatement();
45  Multiple markers at this line
      - SQLExample.isValidUser(String, String) passes a nonconstant String to an execute or addBatch method on an SQL statement [Troubling(10), High confidence]
      - Line breakpoint:SQLExample [line: 45] - isValidUser(String, String)
46
47
48              valid = true;
49          }
50          rs.close();
```

查看缺陷詳細資訊1



查看缺陷詳細資訊2

```
45        ResultSet rs = stmt.executeQuery("SELECT * FROM USER WHERE userName='"+userName+"' AND password='"+pass+"'");
46        boolean valid = false;
```

Properties | Data Source Explorer | Snippets | Console | JUnit | SonarLint Issues | Bug Info

SQLExample.java: 45

Navigation

SQLExample.isValidUser(String, String) passes a nonconstant String to an execute or addBatch method on an SQL statement

Bug: SQLExample.isValidUser(String, String) passes a nonconstant String to an execute or addBatch method on an SQL statement

The method invokes the execute or addBatch method on an SQL statement with a String that seems to be dynamically generated. Consider using a prepared statement instead. It is more efficient and less vulnerable to SQL injection attacks.

Rank: Troubling (10), **confidence**: High
Pattern: SQL_NONCONSTANT_STRING_PASSED_TO_EXECUTE
Type: SQL, **Category**: SECURITY (Security)