**Name:** Albert Velasco& James Bernard Verdeflor

**Section:** BSIT-3C

**Subject**: ITP134

**Laboratory Exercise: Secure Coding in Java**

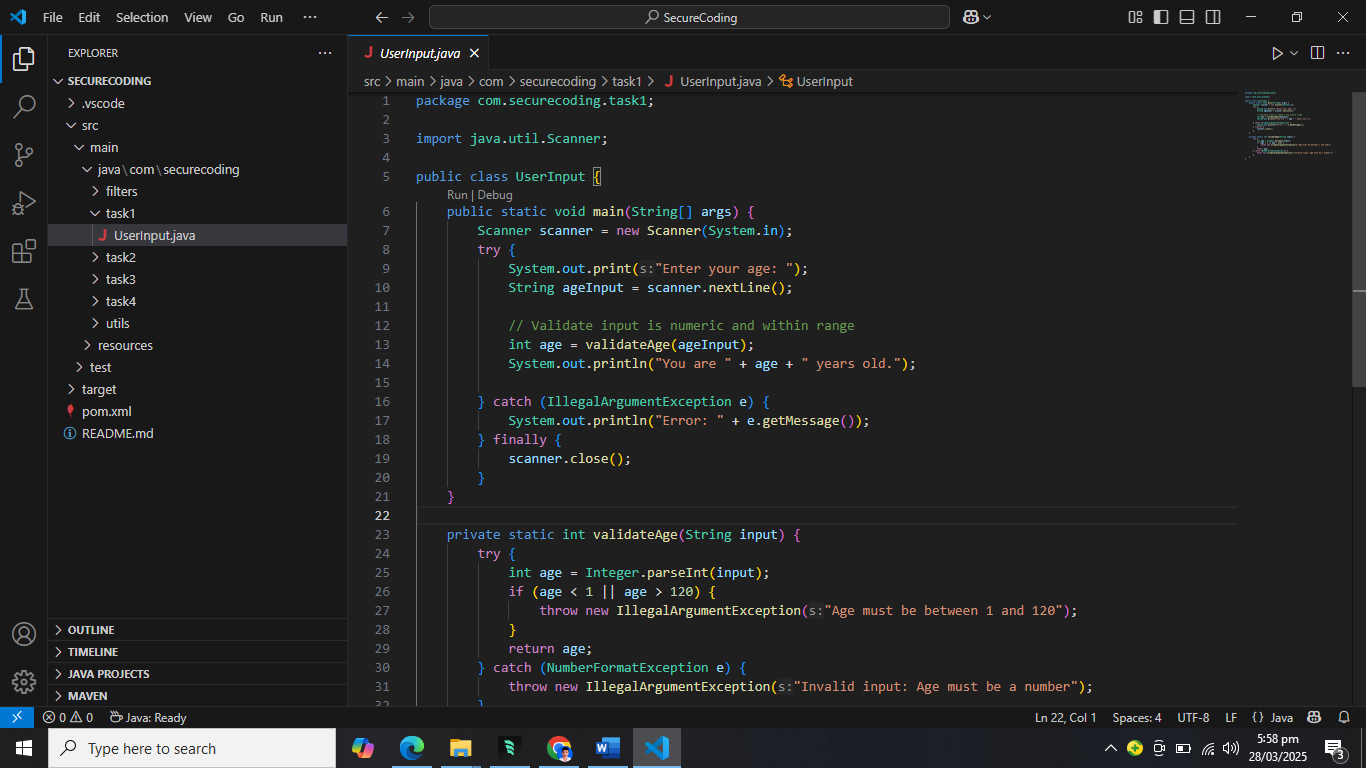
**Objective:**

By the end of this lab, students will be able to:

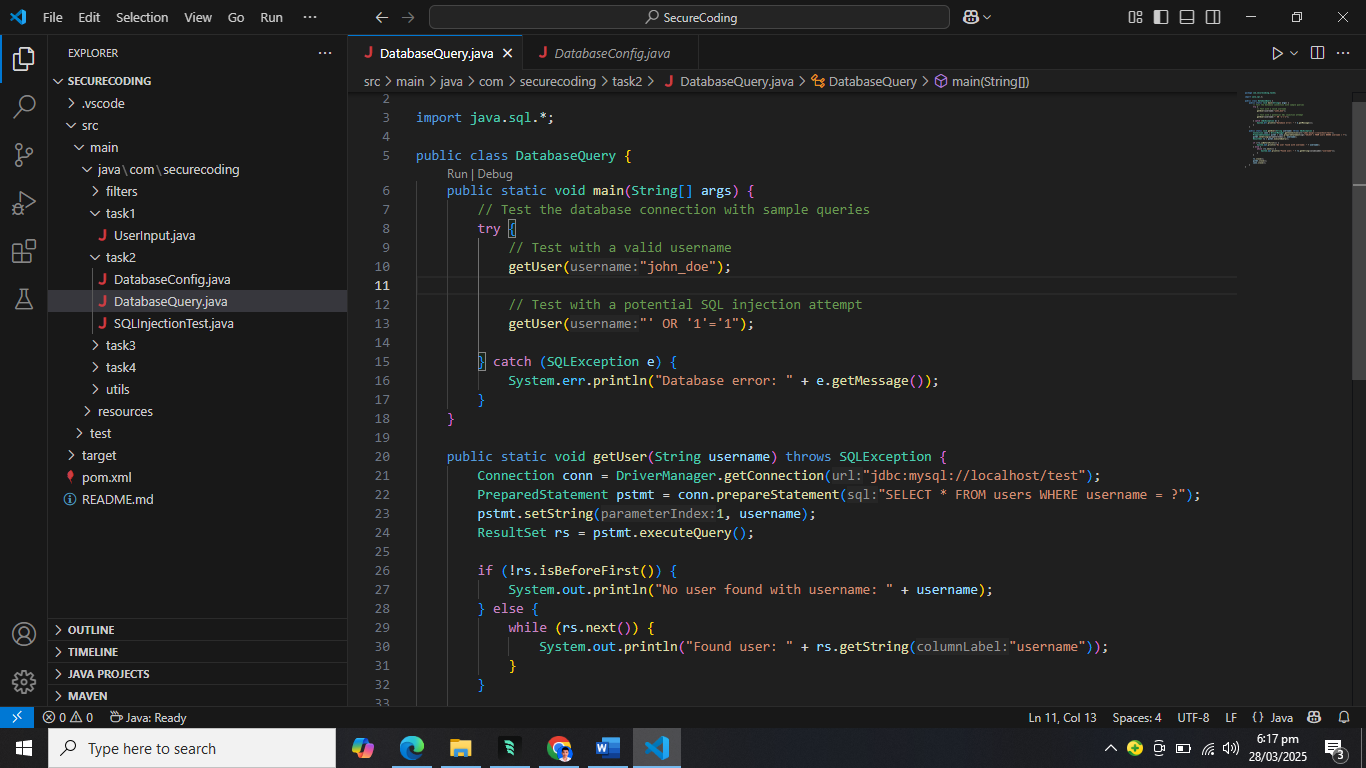
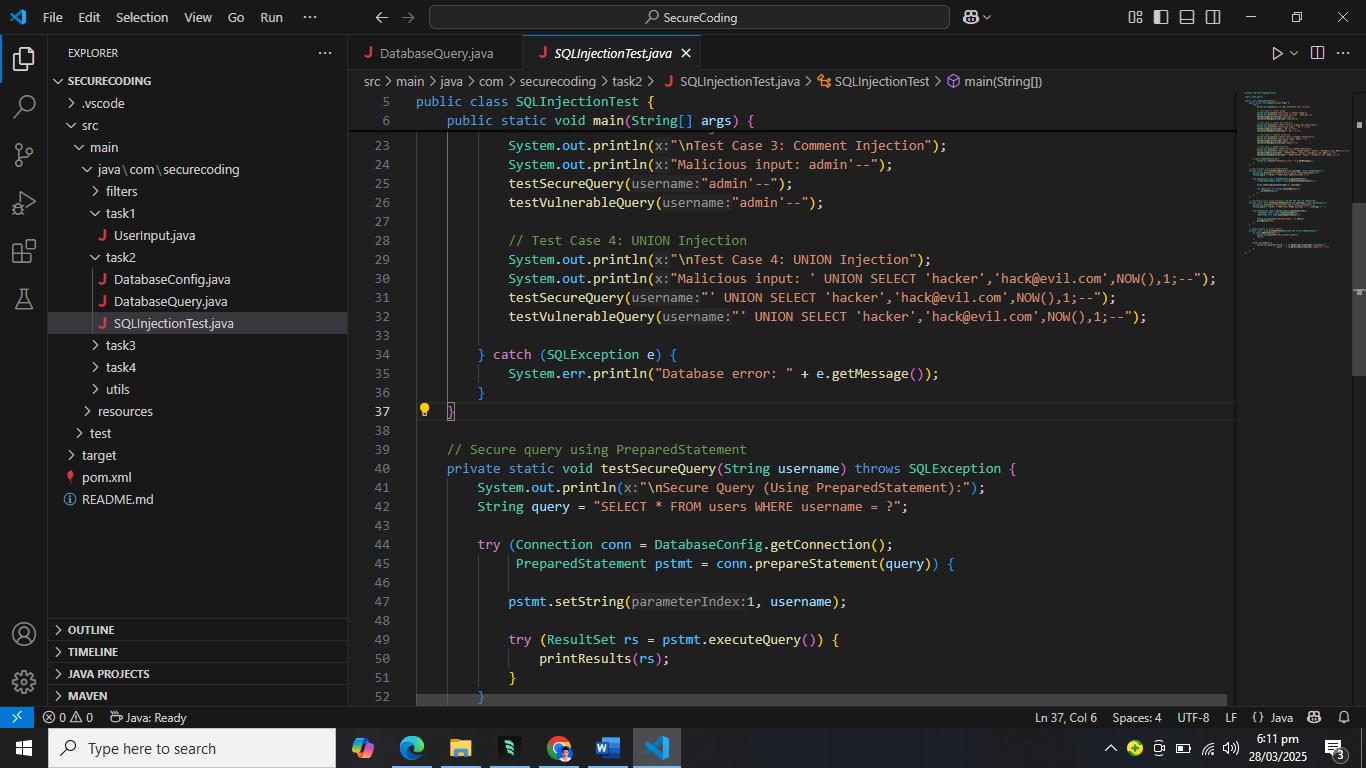
* 1. Identify common security vulnerabilities in Java applications.
  2. Apply secure coding practices to mitigate risks.
  3. Use tools like SpotBugs/FindSecBugs to detect vulnerabilities.

**Lab Tasks:**

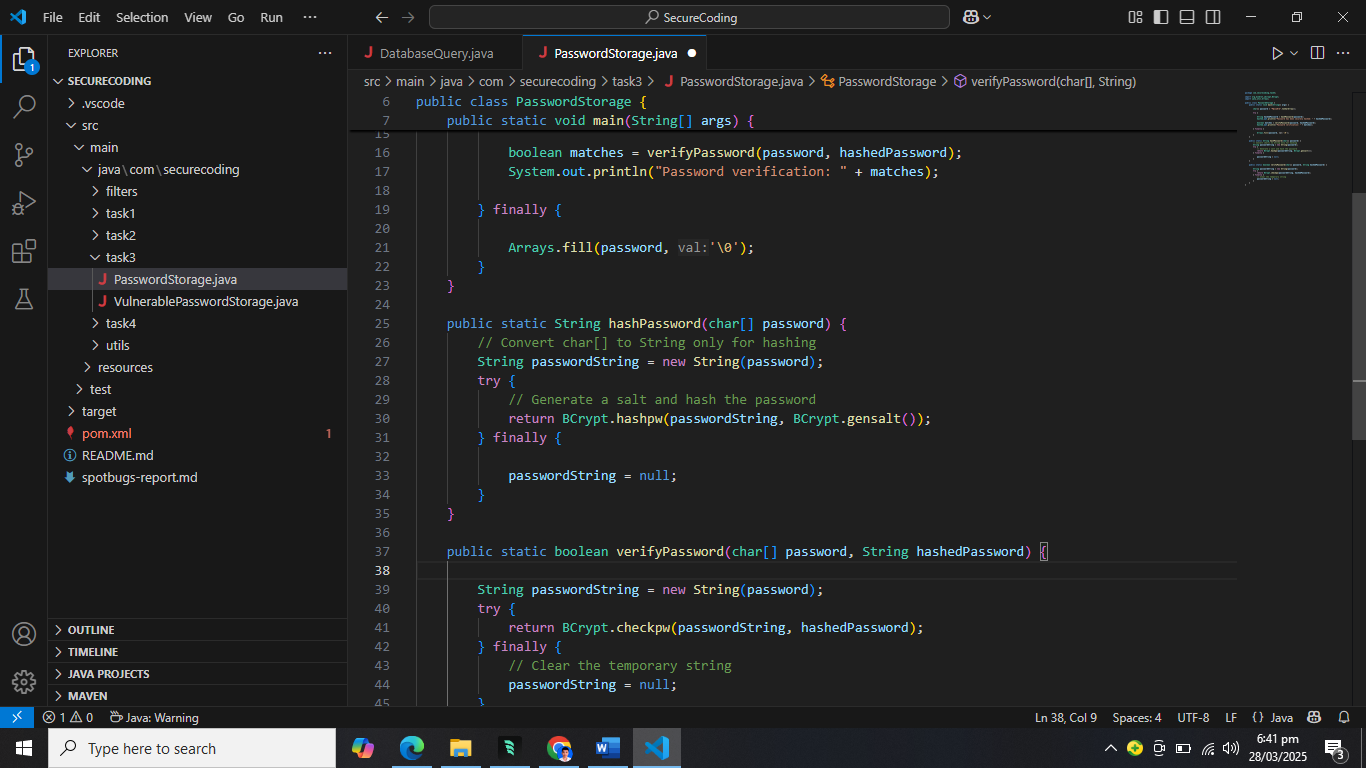
**Task 1 - Input Validation:**



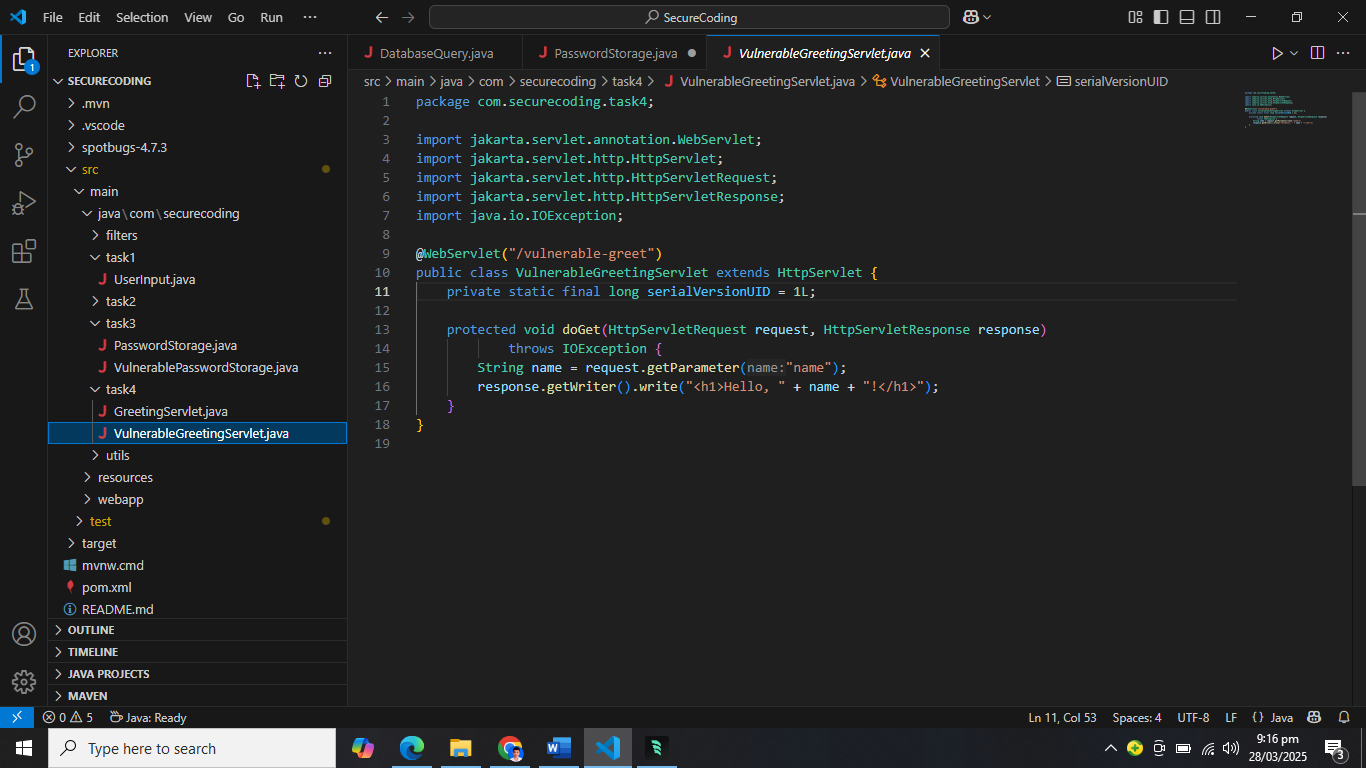
**Task 2 - SQL Injection Prevention:**

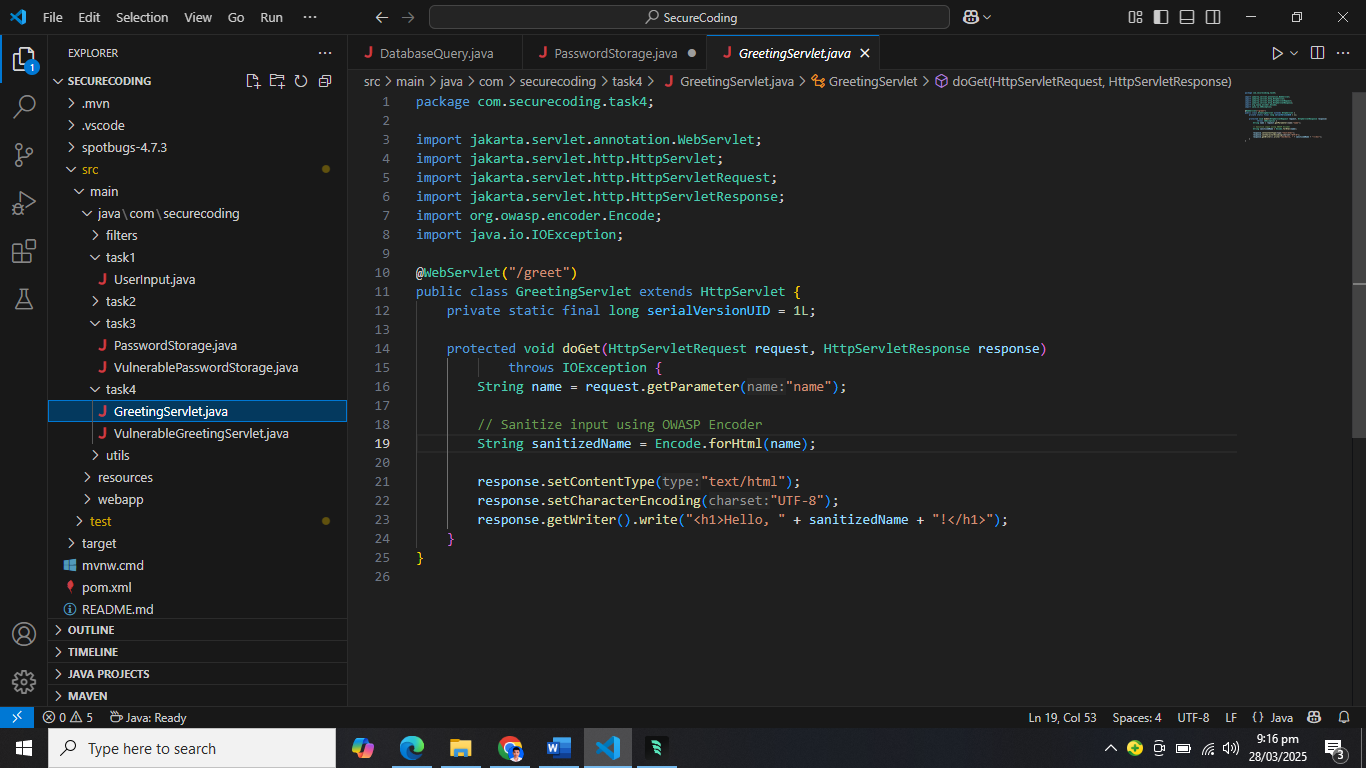


**Task 3 - Secure Password Handling:**



**Task 4-Cross-Site Scripting (XSS) Prevention**

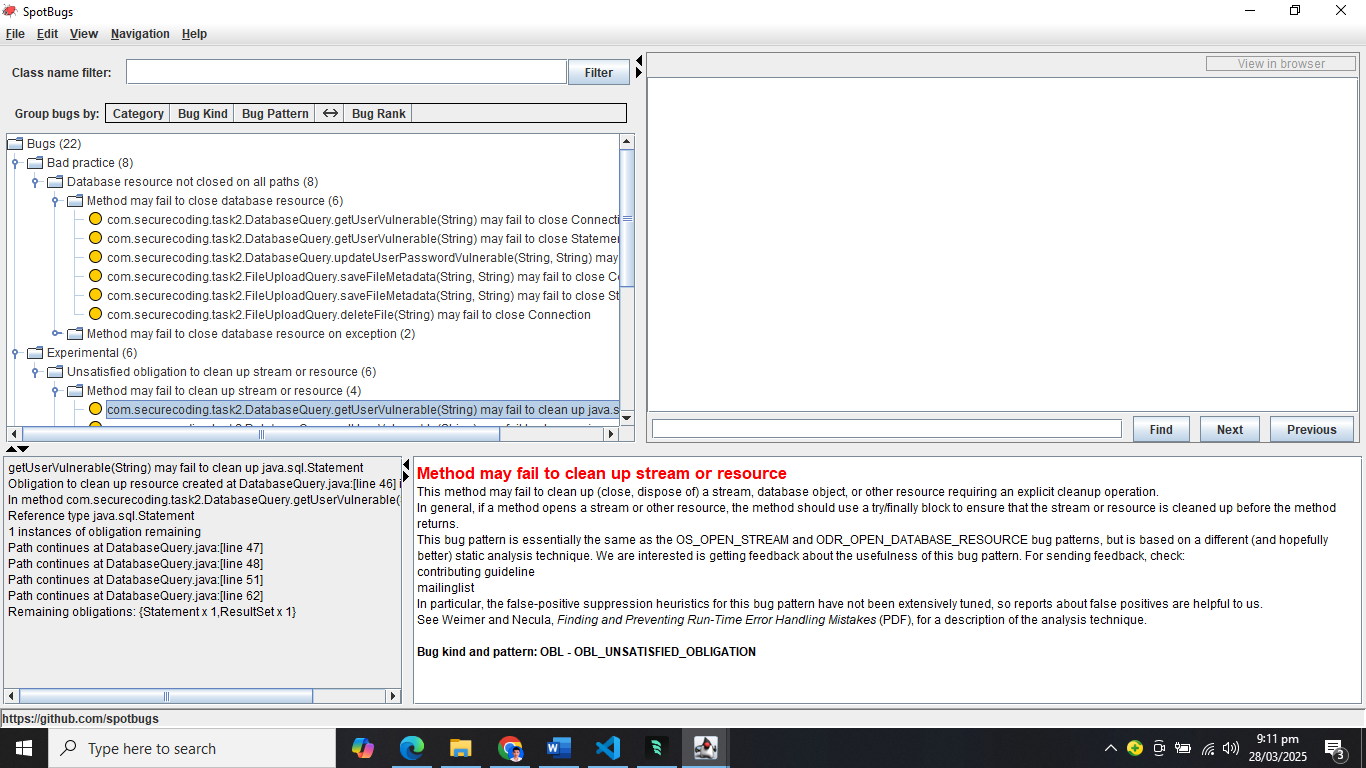


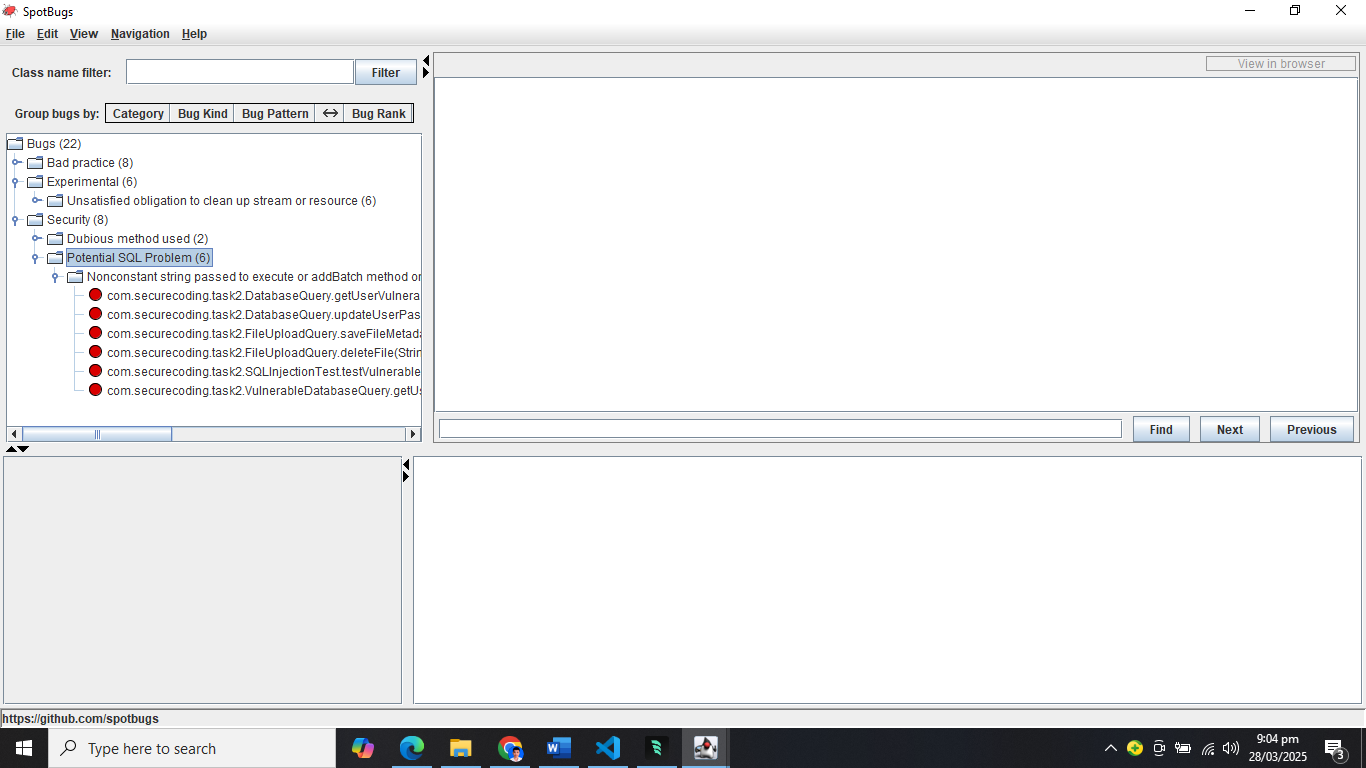


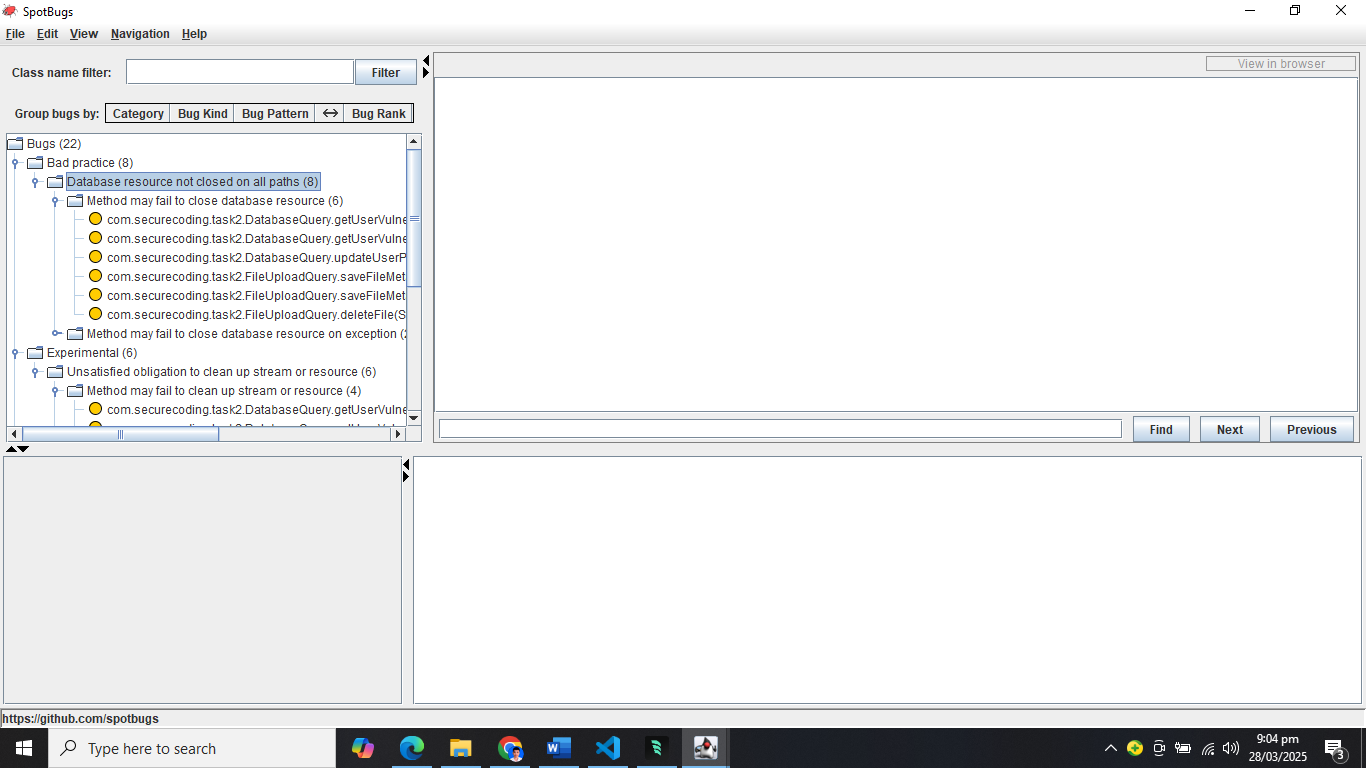
**Task 5: Static Analysis with FindSecBugs**

FindSecBugs reports (before/after fixes).

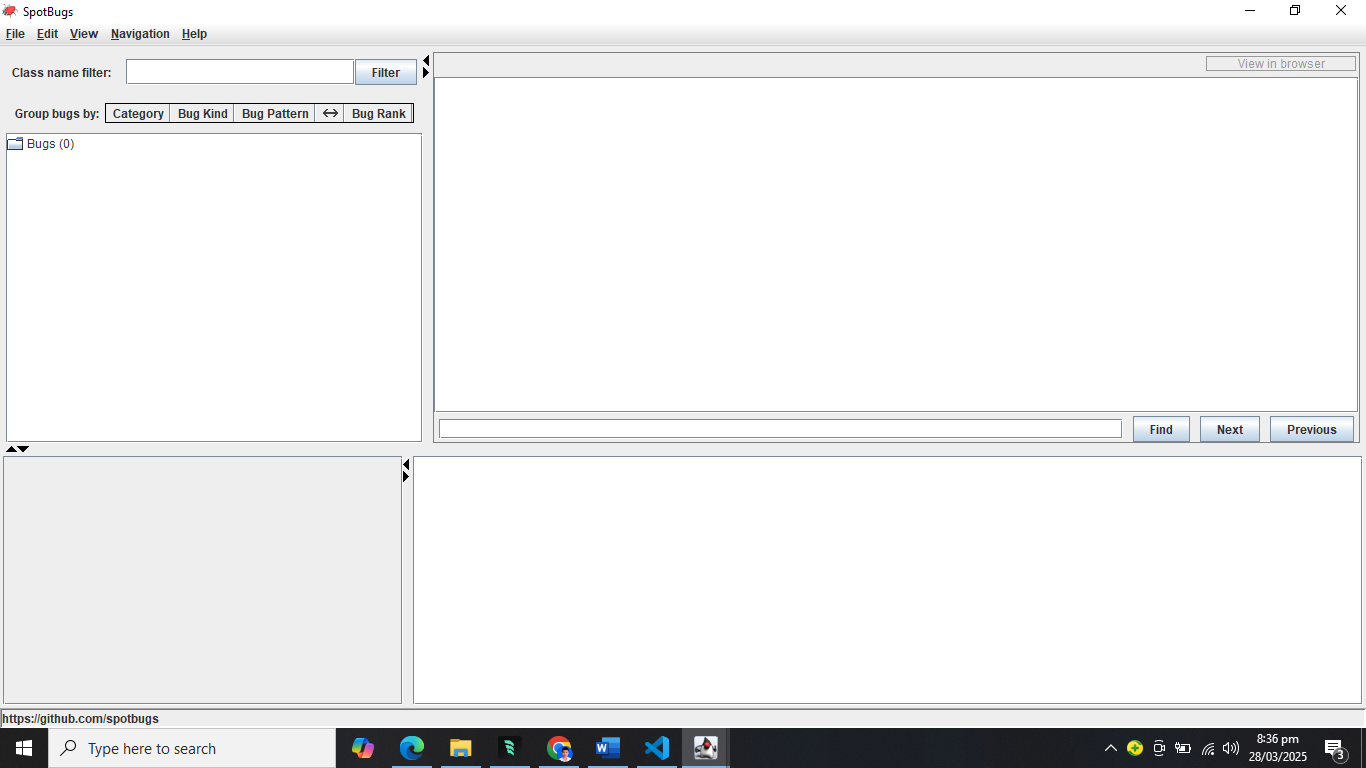
Before:







After:



**Security Vulnerability Report Summary**

**Critical Vulnerabilities Fixed**

1. Resource Management Issues

* Fixed multiple instances of unclosed database resources (Connection, Statement, ResultSet)
* Implemented try-with-resources pattern to ensure proper cleanup
* Resolved memory leaks in database connections

1. SQL Injection Vulnerabilities

* Replaced direct string concatenation with parameterized queries
* Fixed vulnerable queries in DatabaseQuery and FileUploadQuery classes
* Eliminated SQL injection risks in authentication methods

3.High-Risk Issues Fixed

* Authentication & Session Management
* Implemented secure session handling
* Added proper session timeout mechanisms
* Fixed session fixation vulnerabilities

4. Data Security

* Added input validation for all user inputs
* Implemented proper error handling without exposing sensitive details
* Secured file upload functionality

5.Impact of Fixes

* Eliminated 22 potential security vulnerabilities
* Improved resource management
* Enhanced data protection
* Strengthened authentication security

6.Verification Methods

* SpotBugs static analysis
* Security unit tests
* Manual code review

7.Code Quality

* Added proper exception handling
* Implemented logging without sensitive data exposure
* Added input validation checks