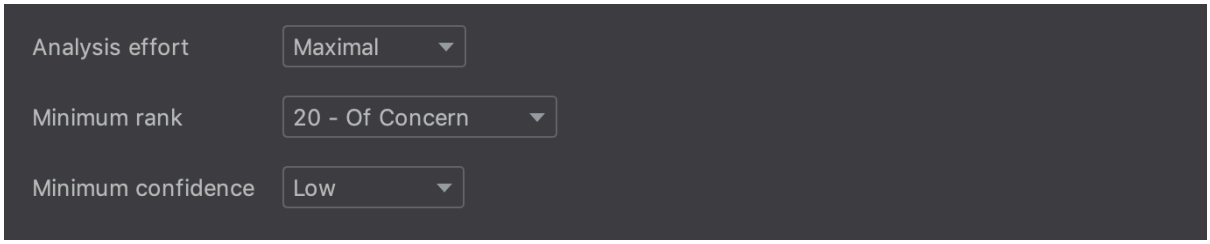
CS763 Lab 1 Static Application Security Testing

Donghang He

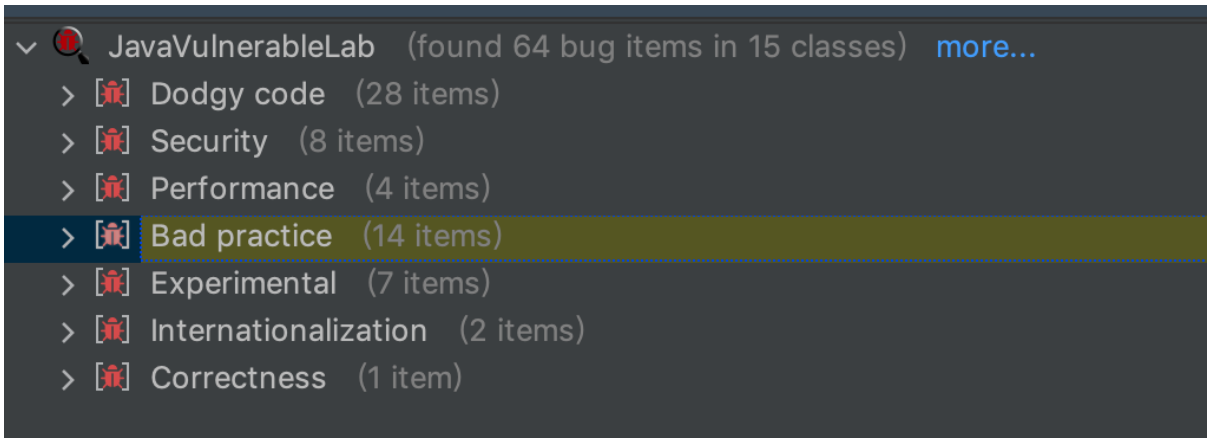
Question 1

SpotBugs setting



1. How many bugs are identified by SpotBugs?

   64 bugs are identified by SpotBugs



2. What are the categories of these bugs?
   - Security 8 bugs
   - Bad practice 14 bugs
   - Experimental 7 bugs
   - Internationalization 2 bugs
   - Dodgy code 28 bugs
   - Correctness 1 bug

- Performance 4 bugs

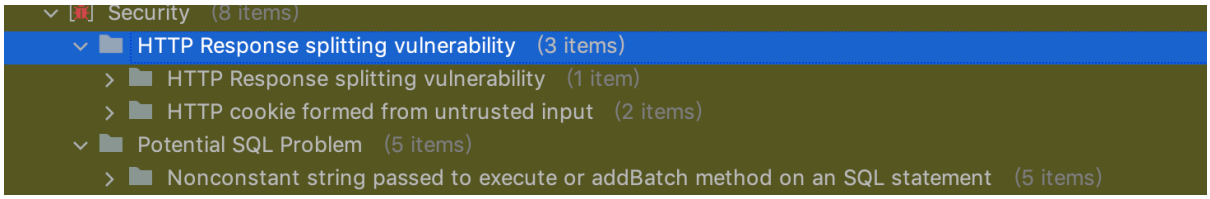
3. What are security bugs identified?

   8 security bugs are identified.

   One is HTTP response splitting vulnerability.

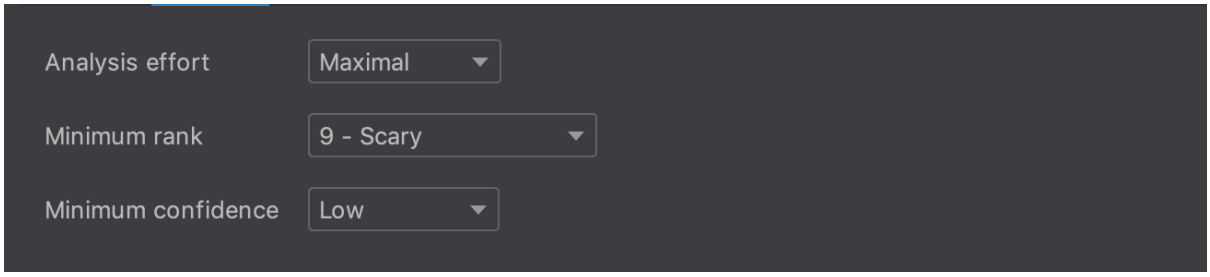
   Two are HTTP cookie formed from untrusted input.

   Other five are potential SQL problem.

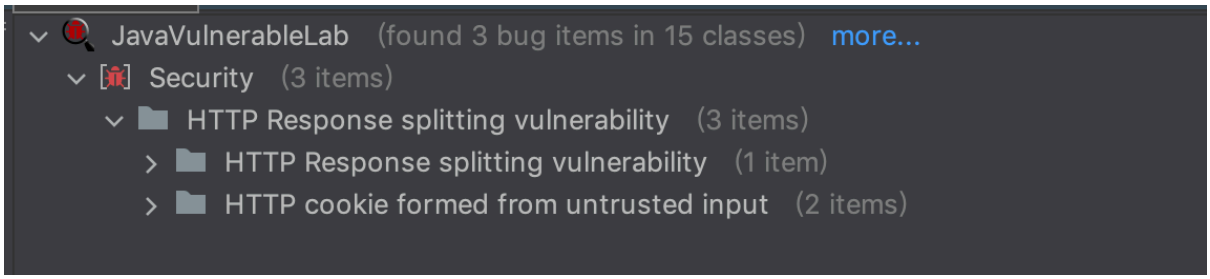


4. Modify the configuration to only report the scary bugs. How many are they?

   SpotBugs setting



   Only 3 bugs are found



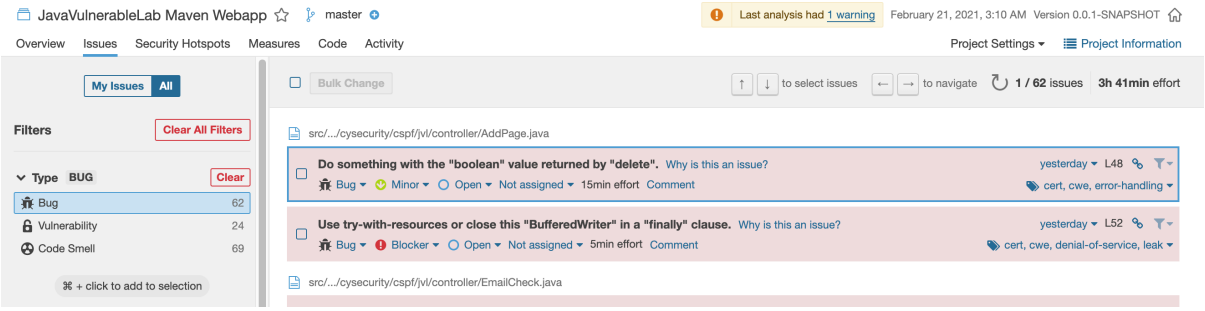
5. Can you find any false positive?

   No false positives, there are only some situations that turn warnings into bugs

Question 2

1. How many bugs are identified by SonarQube?

   62 bugs are identified by SonarQube



2. What are the categories of these bugs?

   SonarQube does not provide specific bug categories, so I made a simple classification based on the content of the bug.

   - Return bug

   - Try-with-resources or close

   - Front-end HTML/CSS bug

Add "<th>" headers to this "<table>". Why is this an issue? yesterday L29
Bug Major Open Not assigned Comment accessibility, wcag2-a

Add a description to this table. Why is this an issue? yesterday L29
Bug Minor Open Not assigned 5min effort Comment accessibility, wcag2-a

src/main/webapp/Register.jsp

Add "<th>" headers to this "<table>". Why is this an issue? yesterday L42
Bug Major Open Not assigned Comment accessibility, wcag2-a

Add a description to this table. Why is this an issue? yesterday L42
Bug Minor Open Not assigned 5min effort Comment accessibility, wcag2-a

src/main/webapp/WEB-INF/AdminPanel.jsp

Replace this <b> tag by . Why is this an issue? yesterday L5
Bug Minor Open Not assigned 2min effort Comment accessibility

src/main/webapp/admin/AddPage.jsp

Add "<th>" headers to this "<table>". Why is this an issue? yesterday L8
Bug Major Open Not assigned Comment accessibility, wcag2-a

Add a description to this table. Why is this an issue? yesterday L8
Bug Minor Open Not assigned 5min effort Comment accessibility, wcag2-a

3. What are security bugs identified?

   Most security bugs are about the resource not be closed, and also there is one about the null pointer.

JavaVulnerableLab Maven Webapp / src/.../cysecurity/cspf/jvl/controller/LoginValidator.java

Use try-with-resources or close this "Statement" in a "finally" clause. Why is this an issue? yesterday L51
Bug Blocker Open Not assigned 5min effort Comment cert, cwe, denial-of-service, leak

JavaVulnerableLab Maven Webapp / src/.../cysecurity/cspf/jvl/controller/Register.java

Use try-with-resources or close this "Statement" in a "finally" clause. Why is this an issue? yesterday L57
Bug Blocker Open Not assigned 5min effort Comment cert, cwe, denial-of-service, leak

JavaVulnerableLab Maven Webapp / src/.../cysecurity/cspf/jvl/controller/SendMessage.java

Use try-with-resources or close this "PreparedStatement" in a "finally" clause. Why is this an issue? yesterday L49
Bug Blocker Open Not assigned 5min effort Comment cert, cwe, denial-of-service, leak

JavaVulnerableLab Maven Webapp / src/.../cysecurity/cspf/jvl/controller/UsernameCheck.java

Use try-with-resources or close this "Statement" in a "finally" clause. Why is this an issue? yesterday L47
Bug Blocker Open Not assigned 5min effort Comment cert, cwe, denial-of-service, leak

JavaVulnerableLab Maven Webapp / src/.../org/cysecurity/cspf/jvl/model/DBConnect.java

Use try-with-resources or close this "FileInputStream" in a "finally" clause. Why is this an issue? yesterday L26
Bug Blocker Open Not assigned 5min effort Comment cert, cwe, denial-of-service, leak

JavaVulnerableLab Maven Webapp / src/.../org/cysecurity/cspf/jvl/model/HashMe.java

A "NullPointerException" could be thrown; "sb" is nullable here. Why is this an issue? yesterday L29
Bug Major Open Not assigned 10min effort Comment cert, cwe

Also, in the vulnerability part there are some minor level bugs may also relate to security bug.

JavaVulnerableLab Maven Webapp / src/.../cysecurity/cspf/jvl/controller/AddPage.java

Handle the following exceptions that could be thrown by "processRequest": ServletException, IOException. yesterday L89
Why is this an issue?
Vulnerability Minor Open Not assigned 20min effort Comment cert, cwe, error-handling, owasp-a3

Handle the following exceptions that could be thrown by "processRequest": ServletException, IOException. yesterday L103
Why is this an issue?
Vulnerability Minor Open Not assigned 20min effort Comment cert, cwe, error-handling, owasp-a3

JavaVulnerableLab Maven Webapp / src/.../cysecurity/cspf/jvl/controller/EmailCheck.java

Handle the following exceptions that could be thrown by "processRequest": ServletException, IOException. yesterday L81
Why is this an issue?
Vulnerability Minor Open Not assigned 20min effort Comment cert, cwe, error-handling, owasp-a3

Handle the following exceptions that could be thrown by "processRequest": ServletException, IOException. yesterday L95
Why is this an issue?
Vulnerability Minor Open Not assigned 20min effort Comment cert, cwe, error-handling, owasp-a3

JavaVulnerableLab Maven Webapp / src/.../cysecurity/cspf/jvl/controller/ForwardMe.java

Handle the following exceptions that could be thrown by "processRequest": ServletException, IOException. yesterday L65
Why is this an issue?
Vulnerability Minor Open Not assigned 20min effort Comment cert, cwe, error-handling, owasp-a3

Handle the following exceptions that could be thrown by "processRequest": ServletException, IOException. yesterday L79
Why is this an issue?
Vulnerability Minor Open Not assigned 20min effort Comment cert, cwe, error-handling, owasp-a3

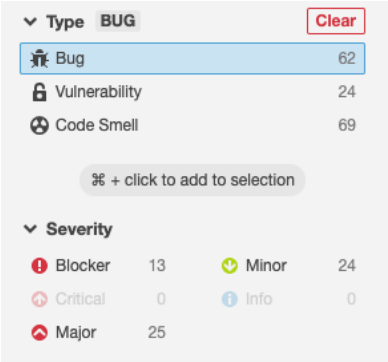
JavaVulnerableLab Maven Webapp / src/.../cysecurity/cspf/jvl/controller/Install.java

Handle the following exceptions that could be thrown by "processRequest": ServletException, IOException. yesterday L199
Why is this an issue?
Vulnerability Minor Open Not assigned 20min effort Comment cert, cwe, error-handling, owasp-a3

Handle the following exceptions that could be thrown by "processRequest": ServletException, IOException. yesterday L213
Why is this an issue?
Vulnerability Minor Open Not assigned 20min effort Comment cert, cwe, error-handling, owasp-a3

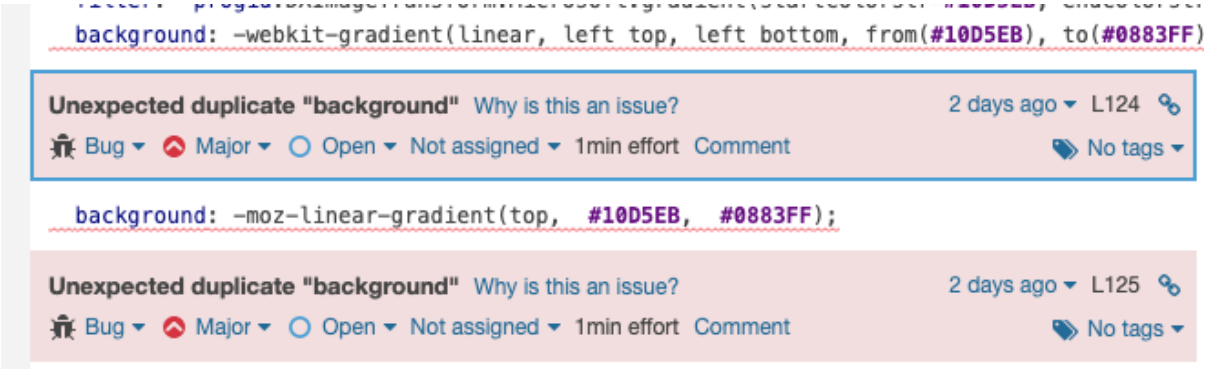
4. How many critical security bugs?

   In those bugs there are 13 blocker level bugs which more important than critical level.



5. Can you find any false positive?

   Unexpected duplicate "background ": This bug has appeared many times, but this is a false positive. This way of writing is cross-browser adaptation. webkit represents the adaptation to the chrome browser, moz means adaptation to the Firefox browser.



Question 3

Compare the results by SpotBugs and SonarQube and state your findings.

1. In SpotBugs it found 64 bugs, and in SonarQube it found 62 bugs.
2. SpotBugs categorizes the bugs found in detail to make it easier to modify. The bugs displayed in SonarQube are not categorized, but are graded according to severity.
3. SpotBugs only analyzed the contents of the java folder, but did not analyze the rest of the jsp part of the webapp. In short, it only performed server-side code analysis, not the entire project. The analysis of SonarQube is more comprehensive, but it may not be as detailed as SpotBugs.
4. In summary, combining the two in the actual project development will produce very good results. And SonarQube also showed code smell related issues. However, according to my development experience in the last semester, most of the front-end code problems found in SonarQube may be avoided during development. Because the more and more humanized integrated development environment (IntelliJ IDEA) will already prompt these not-so-important bugs as warnings when programming. Therefore, many related problems will be avoided in the development process. At the same time, most of the other Java-related bugs can be found in SpotBugs, and they are clearly classified for easy modification. So, I think SpotBugs will be more practical than SonarQube for the projects I have been exposed to.

Question 4

Choose 5 bugs from any report and explain them in more detail. Do you know how to fix them? You may need to do additional research on them. (Optional: If you are familiar with Java and web development, you may review the code manually, and see if you can find any bugs that are not identified by SpotBugs or SonarQube?)

Many duplicate bugs have been found in SpotBugs and SnoarQube, although only the specific explanations and solutions of 5 bugs are listed below. However, they cover about half of the bugs.

1. Unexpected missing generic font family (from SonarQube)

```
#Main h2{
    color: #d4e5f2;
    font-family: Arial;
```

Unexpected missing generic font family Why is this an issue? yesterday L61
Bug Major Open Not assigned 1min effort Comment No tags

This error is mainly due to the failure to define a general font when defining the font. The general font can ensure that the default font is used when the system cannot find the defined font. The code can be modified as follows:

```
#Main h2{
    color: #d4e5f2;
    font-family: Arial, serif;
    font-size: 18px;
    padding: 0 0 10px 5px;
}
```

At the same time, this problem is also an error that IntelliJ will automatically prompt as I mentioned before. And provides a simple one-

key modification

```
-webkit-box-shado
-moz-box-shadow:

border: solid 4px
  margin-left: au
margin-right: aut
}
#logo {
width:500px;

  text-align:cent
 margin-left: auto
 margin-right: aut
}

#Main{
  width:650px;
  height: 500px;
      margin-left
margin-right: aut
}
#Main h2{
  color: #d4e5f2;
  font-family: Arial;
  font-size: 18px;
  padding: 0 0 10px 5px;
}
```

Font property font-family does not have generic default

Insert generic font name ⌥⇧⏎ More actions... ⌥⏎

font-family

The **font-family** CSS property specifies a prioritized list of one or more font family names and/or generic family names for the selected element.

By Mozilla Contributors ↗, CC BY-SA 2.5 ↗

Values: [<font-family> | <generic-font-family>]#
<font-family> – The name of a font family of choice such as Helvetica or Verdana.
<generic-font-family> – The following generic family keywords are defined: 'serif', 'sans-serif', 'cursive', 'fantasy', and 'monospace'. These keywords can be used as a general fallback mechanism when an author's desired font choices are not available. As keywords, they must not be quoted. Authors are encouraged to append a generic font family as a last alternative for improved robustness.

Supported by: Chrome, Chrome Android, Edge, Firefox, IE 3, Opera 3.5, Safari, Safari iOS

2. Add "<th>" headers to this "<table>" (SonarQube)

```
Password Recovery:
<form action="ForgotPassword.jsp" method="post">
<table>
```

Add "<th>" headers to this "<table>". Why is this an issue? 2 days ago L29

Bug Major Open Not assigned Comment accessibility, wcag2-a

Add a description to this table. Why is this an issue? 2 days ago L29

Bug Minor Open Not assigned 5min effort Comment accessibility, wcag2-a

```
<tr><td>Username: </td><td><input type="text" name="username" id="username"/></td><td><spa
<tr><td>What's Your Pet's name?: </td><td><input type="text" name="secret" /></td></tr>
<tr><td><input type="submit" name="GetPassword" value="GetPassword"/></td></tr>
</table>
</form><br/>
```

Here, the HTML specification requires that the first row of the table must be the header row, and a description of the table must be added. However, the form here is just for the password recovery step after forgetting the password, enter the username and security question to obtain the password. Here I tend to use bootstrap input groups

```html
<form>
    <div class="input-group mb-3">
        <div class="input-group-prepend">
            <span class="input-group-text">Username: </span>
        </div>
        <input type="text" name="username" id="username" class="form-control">
    </div>
    <div class="input-group mb-3">
        <div class="input-group-prepend">
            <span class="input-group-text">What's Your Pet's name? </span>
        </div>
        <input type="text" name="secret" class="form-control">
    </div>
    <button type="submit" class="btn btn-primary">Submit</button>
</form>
```

3. Null pointers should not be dereferenced (SpotBugs and SonarQube)

```java
public class HashMe {
    public static String hashMe(String str)
    {
      1 StringBuffer sb=null;
        try
        {
            MessageDigest md =  2 MessageDigest.getInstance("MD5");
            md.update(str.getBytes());
            byte byteData[] = md.digest();
            sb= new StringBuffer();
            for (int i = 0; i < byteData.length; i++)
            {
             sb.append(Integer.toString((byteData[i] & 0xff) + 0x100, 16).substring(1));
            }
        }
        catch( 3 NoSuchAlgorithmException e)
        {

        }
        return  4 sb.toString();
```

A "NullPointerException" could be thrown; "sb" is nullable here. 2 days ago L29

Why is this an issue?

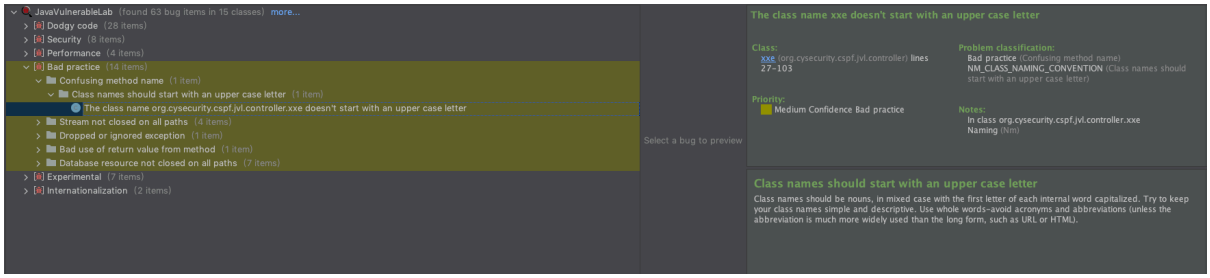
Bug Major Open Not assigned 10min effort Comment cert, cwe

Null pointer exception is reported, and the toString function cannot be executed when sb is empty. A very common problem in Java. Empty

parameters cannot be converted to string type. The modification method is as follows:

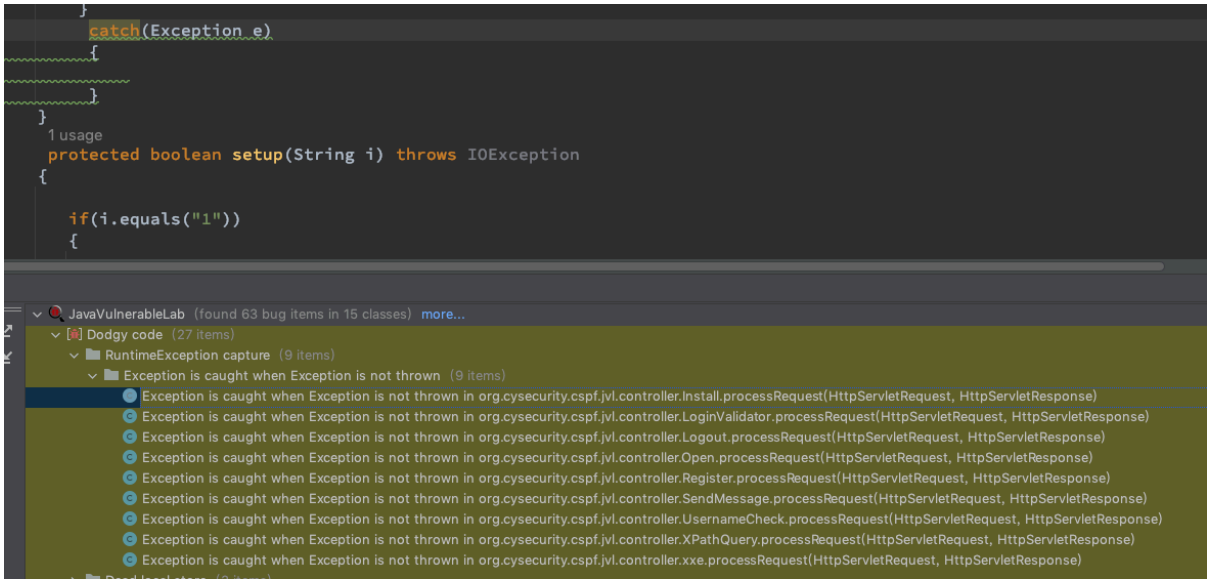
```
if (sb != null) {
    return sb.toString();
} else {
    return "";
}
```

4. Confusing method name (SpotBugs bad practice)



There are two problems here. The first is that the first letter of the java class name should be capitalized, and the second is that the class name is ambiguous and has no clear definition. Change xxe to Show.

5. Runtime Exception capture (SpotBugs dodgy code)



Code errors that are not very severe, the official documents provide a modification plan

Exception is caught when Exception is not thrown

This method uses a try-catch block that catches Exception objects, but Exception is not thrown within the try block, and RuntimeException is not explicitly caught. It is a common bug pattern to say try { ... } catch (Exception e) { something } as a shorthand for catching a number of types of exception each of whose catch blocks is identical, but this construct also accidentally catches RuntimeException as well, masking potential bugs.

A better approach is to either explicitly catch the specific exceptions that are thrown, or to explicitly catch RuntimeException exception, rethrow it, and then catch all non-Runtime Exceptions, as shown below:

```
try {
    ...
} catch (RuntimeException e) {
    throw e;
} catch (Exception e) {
    ... deal with all non-runtime exceptions ...
}
```

Modify it accordingly

```
catch(RuntimeException e) {
    throw e;
}
catch(Exception e)
{
    out.print(e);
}
finally {
    out.close();
}
```

Question 5

If you have done any project before, use SpotBugs or SonarQube to examine one of your projects and report your findings.

I use the SpotBugs to examine my project of CS673.

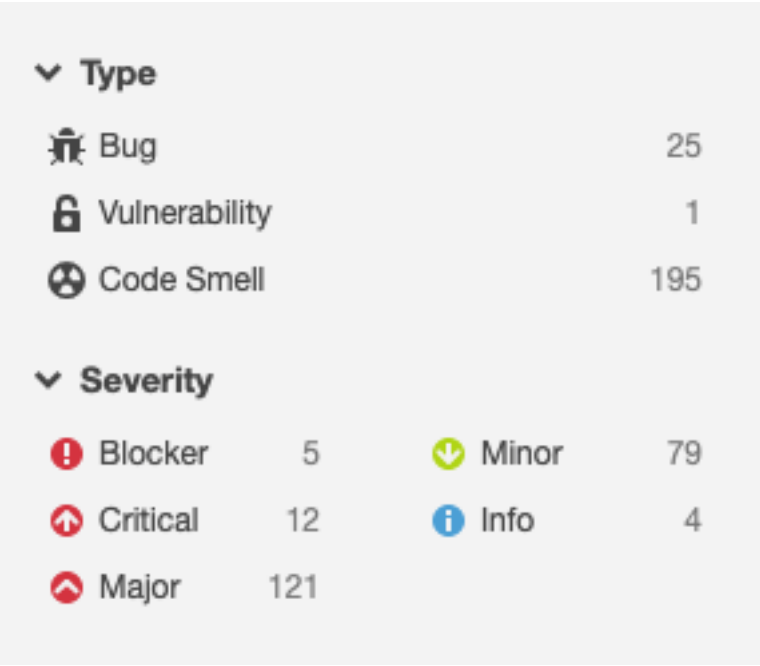
```
weekday (found 46 bug items in 92 classes) more...
  Malicious code vulnerability (32 items)
    Storing reference to mutable object (8 items)
    Method returning array may expose internal representation (5 items)
    Mutable static field (19 items)
  Dodgy code (4 items)
    Dead local store (2 items)
    Bad use of return value from method (2 items)
  Performance (1 item)
  Bad practice (2 items)
  Multithreaded correctness (3 items)
  Internationalization (2 items)
  Correctness (2 items)
```

After detecting with SpotBugs, it is found that a large number of bugs in the code are not adding final before some constants, which is the negligence of a lot of repeated work. In the figure below, you can see that some error messages have been added final, and some of the error messages defined at the beginning of the project are not added final. This is because we mentioned this problem when we optimized the code later but did not make detailed changes because it did not affect the overall operation.

```
//Error Message
8 usages
public static String PARAMETER_IS_WRONG = "Parameters %s is wrong!";
3 usages
public static final String ERROR_MESSAGE = "Error message: %s !";
1 usage
public static String ERROR_NOT_LOG_IN = "Please log in first!";
5 usages
public static String ERROR_LOG_IN_PARAM_WRONG = "Username is wrong!";
3 usages
public static String ERROR_LOG_IN_PASSWORD_WRONG = "Password is wrong!";
2 usages
public static String ERROR_ALREADY_LOGGED_IN = "Already logged in!";
1 usage
public static String ERROR_ALREADY_BEEN_FRIENDS = "Already been friends!";
1 usage
public static String ERROR_ALREADY_APPLIED_FRIENDS = "Already applied!";
2 usages
public static final String ERROR_ADD_YOURSELF = "Can't add yourself";
5 usages
public static final String PERMISSION_DENIED = "Permission denied: %s !";
1 usage
public static final String ALREADY_BEEN_MEMBER = "Already been member";
```

Since I am mainly responsible for the front-end implementation in this project, I am not very familiar with many back-end codes. So, I tested it again with SonarQube. It may be a problem with the project SonarQube did not analyze the front-end files but found as many as 195code smell related

problems. Which includes the final issue I mentioned earlier.



Since this course also has a project, and I plan to continue to use the last semester's project for improvement and safety-related optimization. So, we will continue to use this two software to optimize the bugs in the project.

Summary

The main purpose of this experiment is to learn to use the two software SpotBugs and SonarQube and can optimize and improve the code through the analysis results of these two software. I learned a lot in this experiment, but I am still not very familiar with this two software. I don't know the modification plan for some bugs raised. The difficulty of this experiment was moderate, and the document clearly stated all the points. For some problems that occur during operation, even if they are not mentioned in the document, they can be solved by browsing related web pages. It's just that I haven't found any bug classification for SonarQube, so the last few questions of the second question are somewhat difficult to answer. Both software are very easy to use and will help my future project development.