

---

# **spotbugs Documentation**

*Release 4.0.6*

**spotbugs community**

**Jul 06, 2020**



# CONTENTS

<b>1</b>	<b>Indices and tables</b>	<b>3</b>
<b>2</b>	<b>Contents</b>	<b>5</b>
2.1	Introduction . . . . .	5
2.2	Requirements . . . . .	5
2.3	Installing . . . . .	5
2.4	Running SpotBugs . . . . .	6
2.5	Using the SpotBugs GUI . . . . .	11
2.6	Using the SpotBugs Eclipse plugin . . . . .	13
2.7	Using the SpotBugs Ant task . . . . .	15
2.8	Using the SpotBugs Maven Plugin . . . . .	18
2.9	Using the SpotBugs Gradle Plugin . . . . .	19
2.10	Filter file . . . . .	20
2.11	Analysis Properties . . . . .	27
2.12	Effort . . . . .	28
2.13	Implement SpotBugs plugin . . . . .	29
2.14	Use SpotBugs Plugin on SonarQube . . . . .	32
2.15	SpotBugs FAQ . . . . .	33
2.16	SpotBugs Links . . . . .	35
2.17	Bug descriptions . . . . .	35
2.18	Guide for migration from SpotBugs 3.1 to 4.0 . . . . .	56
2.19	Guide for migration from FindBugs 3.0 to SpotBugs 3.1 . . . . .	56
2.20	Annotations . . . . .	59



This manual is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/1.0/> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

The name FindBugs and the FindBugs logo are trademarked by the University of Maryland.



## INDICES AND TABLES

- search



## CONTENTS

### 2.1 Introduction

SpotBugs is a program to find bugs in Java programs. It looks for instances of “bug patterns” — code instances that are likely to be errors.

This document describes version 4.0.6 of SpotBugs. We are very interested in getting your feedback on SpotBugs. Please visit the SpotBugs web page for the latest information on SpotBugs, contact information, and support resources such as information about the SpotBugs GitHub organization.

### 2.2 Requirements

To use SpotBugs, you need a runtime environment compatible with Java version 1.8 or later. SpotBugs is platform independent, and is known to run on GNU/Linux, Windows, and MacOS X platforms.

You should have at least 512 MB of memory to use SpotBugs. To analyze very large projects, more memory may be needed.

#### 2.2.1 Supported Java version

SpotBugs is built by JDK8, and run on JRE8 and newer versions.

SpotBugs can scan bytecode (class files) generated by JDK8 and newer versions. However, support for Java 11 and newer is still experimental. Visit [issue tracker](#) to find known problems.

SpotBugs does not support bytecode (class files) generated by outdated JDK such as 10, 9, 7 and older versions.

### 2.3 Installing

This chapter explains how to install SpotBugs.

### 2.3.1 Extracting the Distribution

The easiest way to install SpotBugs is to download a binary distribution. Binary distributions are available in [gzipped tar format](#) and [zip format](#). Once you have downloaded a binary distribution, extract it into a directory of your choice.

Extracting a gzipped tar format distribution:

```
$ gunzip -c spotbugs-4.0.6.tgz | tar xvf -
```

Extracting a zip format distribution:

```
C:\Software> unzip spotbugs-4.0.6.zip
```

Usually, extracting a binary distribution will create a directory ending in `spotbugs-4.0.6`. For example, if you extracted the binary distribution from the `C:\Software` directory, then the SpotBugs software will be extracted into the directory `C:\Software\spotbugs-4.0.6`. This directory is the SpotBugs home directory. We'll refer to it as `$SPOTBUGS_HOME` (or `%SPOTBUGS_HOME%` for Windows) throughout this manual.

## 2.4 Running SpotBugs

SpotBugs has two user interfaces: a graphical user interface (GUI) and a command line user interface. This chapter describes how to run each of these user interfaces.

### 2.4.1 Quick Start

If you are running SpotBugs on a Windows system, double-click on the file `%SPOTBUGS_HOME%\lib\spotbugs.jar` to start the SpotBugs GUI.

On a Unix, Linux, or macOS system, run the `$SPOTBUGS_HOME/bin/spotbugs` script, or run the command `java -jar $SPOTBUGS_HOME/lib/spotbugs.jar` to run the SpotBugs GUI.

Refer to *Using the SpotBugs GUI* for information on how to use the GUI.

### 2.4.2 Executing SpotBugs

This section describes how to invoke the SpotBugs program. There are two ways to invoke SpotBugs: directly, or using a wrapper script.

#### Direct invocation of SpotBugs

The preferred method of running SpotBugs is to directly execute `$SPOTBUGS_HOME/lib/spotbugs.jar` using the `-jar` command line switch of the JVM (java) executable. (Versions of SpotBugs prior to 1.3.5 required a wrapper script to invoke SpotBugs.)

The general syntax of invoking SpotBugs directly is the following:

```
java [JVM arguments] -jar $SPOTBUGS_HOME/lib/spotbugs.jar options...
```

## Choosing the User Interface

The first command line option chooses the SpotBugs user interface to execute. Possible values are:

- gui:** runs the graphical user interface (GUI)
- textui:** runs the command line user interface
- version:** displays the SpotBugs version number
- help:** displays help information for the SpotBugs command line user interface
- gui1:** executes the original (obsolete) SpotBugs graphical user interface

## Java Virtual Machine (JVM) arguments

Several Java Virtual Machine arguments are useful when invoking SpotBugs.

- XmxNNm:** Set the maximum Java heap size to NN megabytes. SpotBugs generally requires a large amount of memory. For a very large project, using 1500 megabytes is not unusual.
- Dname=value:** Set a Java system property. For example, you might use the argument `-Duser.language=ja` to display GUI messages in Japanese.

## Invocation of SpotBugs using a wrapper script

Another way to run SpotBugs is to use a wrapper script.

On Unix-like systems, use the following command to invoke the wrapper script:

```
$ $SPOTBUGS_HOME/bin/spotbugs options...
```

On Windows systems, the command to invoke the wrapper script is

```
C:\My Directory>%SPOTBUGS_HOME%\bin\spotbugs.bat options...
```

On both Unix-like and Windows systems, you can simply add the `$SPOTBUGS_HOME/bin` directory to your `PATH` environment variable and then invoke SpotBugs using the `spotbugs` command.

## Wrapper script command line options

The SpotBugs wrapper scripts support the following command-line options. Note that these command line options are not handled by the SpotBugs program per se; rather, they are handled by the wrapper script.

- jvmArgs args:** Specifies arguments to pass to the JVM. For example, you might want to set a JVM property:

```
$ spotbugs -textui -jvmArgs "-Duser.language=ja" myApp.jar
```

- javahome directory:** Specifies the directory containing the JRE (Java Runtime Environment) to use to execute FindBugs.
- maxHeap size:** Specifies the maximum Java heap size in megabytes. The default is 256. More memory may be required to analyze very large programs or libraries.
- debug:** Prints a trace of detectors run and classes analyzed to standard output. Useful for troubleshooting unexpected analysis failures.

**-property *name=value***: This option sets a system property. SpotBugs uses system properties to configure analysis options. See *Analysis Properties*. You can use this option multiple times in order to set multiple properties. Note: In most versions of Windows, the *name=value* string must be in quotes.

## 2.4.3 Command-line Options

This section describes the command line options supported by SpotBugs. These command line options may be used when invoking SpotBugs directly, or when using a wrapper script.

### Common command-line options

These options may be used with both the GUI and command-line interfaces.

- effort[:*min*|*less*|*default*|*more*|*max*]**: Set analysis effort level. The *-effort:min* disables several analyses that increase precision but also increase memory consumption. You may want to try this option if you find that SpotBugs with the *-effort:less* still runs out of memory, or takes an unusually long time to complete its analysis. The *-effort:less* disables some analyses that increase precision but also increase memory consumption. You may want to try this option if you find that SpotBugs with the *-effort:more*/*-effort:default* runs out of memory, or takes an unusually long time to complete its analysis. The *-effort:more* runs several analyses to find bugs, this is the *-effort:default*. The *-effort:max* enable analyses which increase precision and find more bugs, but which may require more memory and take more time to complete. See *Effort*.
- project *project***: Specify a project to be analyzed. The project file you specify should be one that was created using the GUI interface. It will typically end in the extension *.fb* or *.fbp*.
- pluginList <*jar1*[;*jar2*... ]>**: Specify list of plugin Jar files to load.
- home <*home directory*>**: Specify SpotBugs home directory.
- adjustExperimental**: Lower priority of experimental Bug Patterns.
- workHard**: Ensure analysis effort is at least 'default'.
- conserveSpace**: Same as *-effort:min* (for backward compatibility).

### GUI Options

These options are only accepted by the Graphical User Interface.

- look:plastic|gtk|native**: Set Swing look and feel.

### Text UI Options

These options are only accepted by the Text User Interface.

- sortByClass**: Sort reported bug instances by class name.
- include *filterFile.xml***: Only report bug instances that match the filter specified by *filterFile.xml*. See *Filter file*.
- exclude *filterFile.xml***: Report all bug instances except those matching the filter specified by *filterFile.xml*. See *Filter file*.
- onlyAnalyze *com.foobar.MyClass,com.foobar.mypkg.\****: Restrict analysis to find bugs to given comma-separated list of classes and packages. Unlike filtering, this option avoids running analysis on classes and packages that are not explicitly matched: for large projects, this may greatly reduce the amount of time needed to run the analysis. (However, some detectors may produce inaccurate results if they aren't run on the entire application.) Classes should be specified using their full classnames (including package), and packages should be specified in

the same way they would in a Java import statement to import all classes in the package (i.e., add `.*` to the full name of the package). Replace `.*` with `.-` to also analyze all subpackages.

- low:** Report all bugs.
- medium:** Report medium and high priority bugs. This is the default setting.
- high:** Report only high priority bugs.
- relaxed:** Relaxed reporting mode. For many detectors, this option suppresses the heuristics used to avoid reporting false positives.
- xml:** Produce the bug reports as XML. The XML data produced may be viewed in the GUI at a later time. You may also specify this option as `-xml:withMessages`; when this variant of the option is used, the XML output will contain human-readable messages describing the warnings contained in the file. XML files generated this way are easy to transform into reports.
- html:** Generate HTML output. By default, SpotBugs will use the `default.xml` XSLT stylesheet to generate the HTML: you can find this file in `spotbugs.jar`, or in the SpotBugs source or binary distributions. Variants of this option include `-html:plain.xml`, `-html:fancy.xml` and `-html:fancy-hist.xml`. The `plain.xml` stylesheet does not use Javascript or DOM, and may work better with older web browsers, or for printing. The `fancy.xml` stylesheet uses DOM and Javascript for navigation and CSS for visual presentation. The `fancy-hist.xml` an evolution of `fancy.xml` stylesheet. It makes an extensive use of DOM and Javascript for dynamically filtering the lists of bugs.  
  
If you want to specify your own XSLT stylesheet to perform the transformation to HTML, specify the option as `-html:myStylesheet.xml`, where `myStylesheet.xml` is the filename of the stylesheet you want to use.
- emacs:** Produce the bug reports in Emacs format.
- xdocs:** Produce the bug reports in xdoc XML format for use with Apache Maven.
- output *filename*:** Produce the output in the specified file.
- outputFile *filename*:** This argument is deprecated. Use `-output` instead.
- nested[:true|false]:** This option enables or disables scanning of nested jar and zip files found in the list of files and directories to be analyzed. By default, scanning of nested jar/zip files is enabled. To disable it, add `-nested:false` to the command line arguments.
- auxclasspath *classpath*:** Set the auxiliary classpath for analysis. This classpath should include all jar files and directories containing classes that are part of the program being analyzed but you do not want to have analyzed for bugs.
- auxclasspathFromInput:** Read the auxiliary classpath for analysis from standard input, each line adds new entry to the auxiliary classpath for analysis.
- auxclasspathFromFile *filepath*:** Read the auxiliary classpath for analysis from file, each line adds new entry to the auxiliary classpath for analysis.
- analyzeFromFile *filepath*:** Read the files to analyze from file, each line adds new entry to the classpath for analysis.
- userPrefs *edu.umd.cs.findbugs.core.prefs*:** Set the path of the user preferences file to use, which might override some of the options above. Specifying `userPrefs` as first argument would mean some later options will override them, as last argument would mean they will override some previous options). This rationale behind this option is to reuse SpotBugs Eclipse project settings for command line execution.
- showPlugins:** Show list of available detector plugins.

## Output options

- timestampNow:** Set timestamp of results to be current time.
- quiet:** Suppress error messages.
- longBugCodes:** Report long bug codes.
- progress:** Display progress in terminal window.
- release <release name>:** Set the release name of the analyzed application.
- maxRank <rank>:** Only report issues with a bug rank at least as scary as that provided.
- dontCombineWarnings:** Don't combine warnings that differ only in line number.
- train[:outputDir]:** Save training data (experimental); output dir defaults to '.'.
- useTraining[:inputDir]:** Use training data (experimental); input dir defaults to '.'.
- redoAnalysis <filename>:** Redo analysis using configuration from previous analysis.
- sourceInfo <filename>:** Specify source info file (line numbers for fields/classes).
- projectName <project name>:** Descriptive name of project.
- reanalyze <filename>:** Redo analysis in provided file.

## Output filtering options

- bugCategories <cat1[,cat2...]>:** Only report bugs in given categories.
- excludeBugs <baseline bugs>:** Exclude bugs that are also reported in the baseline xml output.
- applySuppression:** Exclude any bugs that match suppression filter loaded from fbp file.

## Detector (visitor) configuration options

- visitors <v1[,v2...]>:** Run only named visitors.
- omitVisitors <v1[,v2...]>:** Omit named visitors.
- chooseVisitors <+v1,-v2,...>:** Selectively enable/disable detectors.
- choosePlugins <+p1,-p2,...>:** Selectively enable/disable plugins.
- adjustPriority <v1=(raiselower)[,..]>:** Raise/lower priority of warnings for given visitor(s)

## Project configuration options

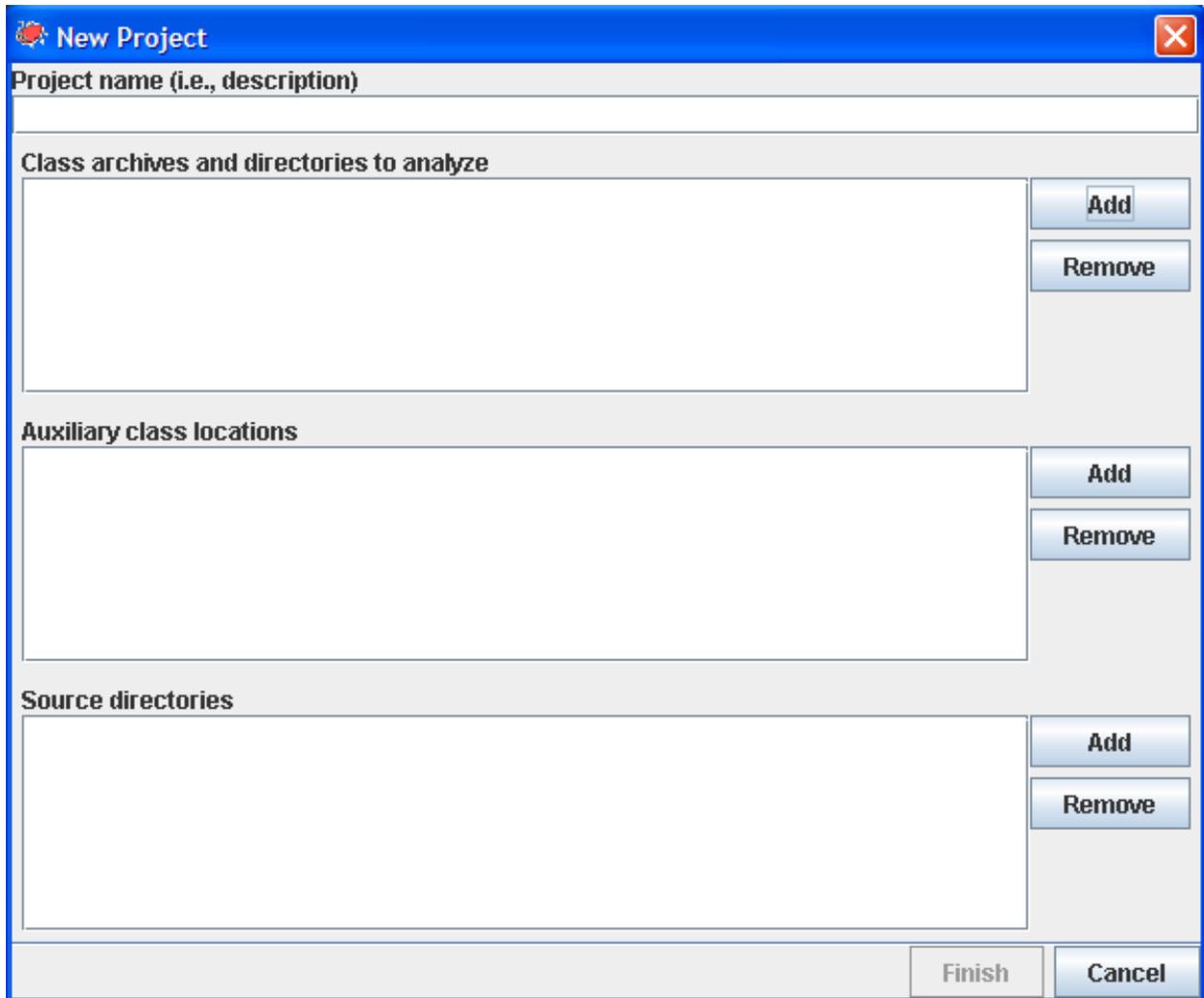
- sourcepath <source path>:** Set source path for analyzed classes.
- exitcode:** Set exit code of process.
- noClassOk:** Output empty warning file if no classes are specified.
- xargs:** Get list of classfiles/jarfiles from standard input rather than command line.
- bugReporters <name,name2,-name3>:** Bug reporter decorators to explicitly enable/disable.
- printConfiguration:** Print configuration and exit, without running analysis.

## 2.5 Using the SpotBugs GUI

This chapter describes how to use the SpotBugs graphical user interface (GUI).

### 2.5.1 Creating a Project

After you have started SpotBugs using the `spotbugs` command, choose the `File` → `New Project` menu item. You will see a dialog which looks like this:



Use the “Add” button next to “Classpath to analyze” to select a Java archive file (zip, jar, ear, or war file) or directory containing java classes to analyze for bugs. You may add multiple archives/directories.

You can also add the source directories which contain the source code for the Java archives you are analyzing. This will enable SpotBugs to highlight the source code which contains a possible error. The source directories you add should be the roots of the Java package hierarchy. For example, if your application is contained in the `org.foo.bar.myapplication` package, you should add the parent directory of the `org` directory to the source directory list for the project.

Another optional step is to add additional Jar files or directories as “Auxiliary classpath locations” entries. You should do this if the archives and directories you are analyzing have references to other classes which are not included in the analyzed archives/directories and are not in the standard runtime classpath. Some of the bug pattern detectors in

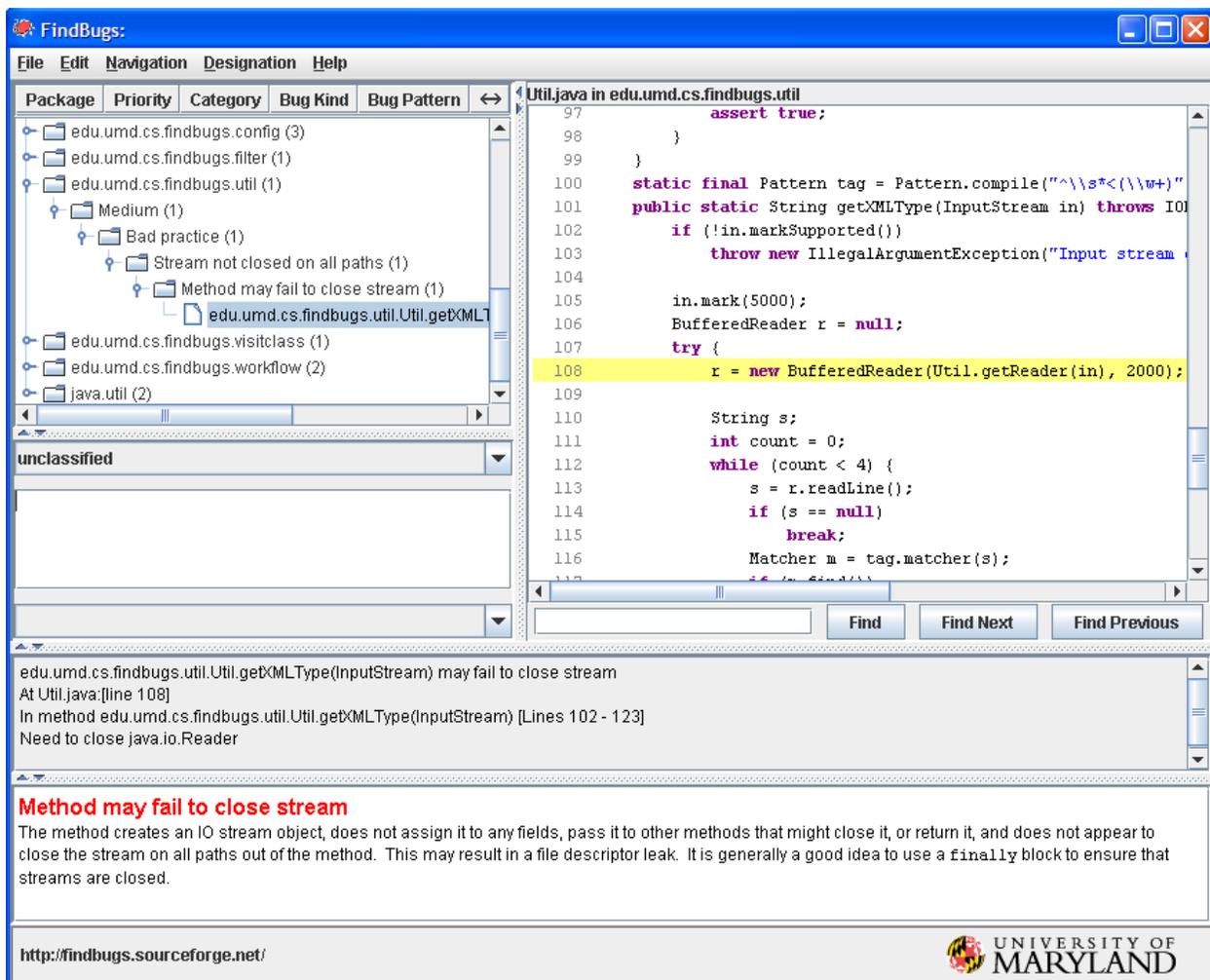
FindBugs make use of class hierarchy information, so you will get more accurate results if the entire class hierarchy is available which FindBugs performs its analysis.

## 2.5.2 Running the Analysis

Once you have added all of the archives, directories, and source directories, click the “Analyze” button to analyze the classes contained in the Jar files. Note that for a very large program on an older computer, this may take quite a while (tens of minutes). A recent computer with ample memory will typically be able to analyze a large program in only a few minutes.

## 2.5.3 Browsing Results

When the analysis completes, you will see a screen like the following:



The upper left-hand pane of the window shows the bug tree; this is a hierarchical representation of all of the potential bugs detected in the analyzed Jar files.

When you select a particular bug instance in the top pane, you will see a description of the bug in the “Details” tab of the bottom pane. In addition, the source code pane on the upper-right will show the program source code where the potential bug occurs, if source is available. In the above example, the bug is a stream object that is not closed. The source code window highlights the line where the stream object is created.

You may add a textual annotations to bug instances. To do so, type them into the text box just below the hierarchical view. You can type any information which you would like to record. When you load and save bug results files, the annotations are preserved.

## 2.5.4 Saving and Opening

You may use the `File` → `Save as...` menu option to save your work. To save your work, including the jar file lists you specified and all bug results, choose “FindBugs analysis results (.xml)” from the drop-down list in the “Save as...” dialog. There are also options for saving just the jar file lists (“FindBugs project file (.fbp)”) or just the results (“FindBugs analysis file (.fba)”). A saved file may be loaded with the `File` → `Open...` menu option.

## 2.6 Using the SpotBugs Eclipse plugin

The SpotBugs Eclipse plugin allows SpotBugs to be used within the Eclipse IDE. The SpotBugs Eclipse plugin was generously contributed by Peter Friese. Phil Crosby and Andrey Loskutov contributed major improvements to the plugin.

### 2.6.1 Requirements

To use the SpotBugs Plugin for Eclipse, you need Eclipse Neon (4.6) or later.

### 2.6.2 Installation

We provide update sites that allow you to automatically install SpotBugs into Eclipse and also query and install updates. There are three different update sites:

<https://spotbugs.github.io/eclipse/> Only provides official releases of SpotBugs Eclipse plugin.

<https://spotbugs.github.io/eclipse-candidate/> Provides official releases and release candidates of SpotBugs Eclipse plugin.

<https://spotbugs.github.io/eclipse-latest/> Provides latest SpotBugs Eclipse plugin built from master branch.

<https://spotbugs.github.io/eclipse-stable-latest/> Provides latest SpotBugs Eclipse plugin built from release-3.1 branch.

Or just use [Eclipse marketplace](#) to install SpotBugs Eclipse plugin.

### 2.6.3 Using the Plugin

To get started, right click on a Java project in Package Explorer, and select the option labeled “Spot Bugs”. SpotBugs will run, and problem markers (displayed in source windows, and also in the Eclipse Problems view) will point to locations in your code which have been identified as potential instances of bug patterns.

You can also run SpotBugs on existing java archives (jar, ear, zip, war etc). Simply create an empty Java project and attach archives to the project classpath. Having that, you can now right click the archive node in Package Explorer and select the option labeled “Spot Bugs”. If you additionally configure the source code locations for the binaries, SpotBugs will also link the generated warnings to the right source files.

You may customize how SpotBugs runs by opening the Properties dialog for a Java project, and choosing the “SpotBugs” property page. Options you may choose include:

- Enable or disable the “Run SpotBugs Automatically” checkbox. When enabled, SpotBugs will run every time you modify a Java class within the project.
- Choose minimum warning priority and enabled bug categories. These options will choose which warnings are shown. For example, if you select the “Medium” warning priority, only Medium and High priority warnings will be shown. Similarly, if you uncheck the “Style” checkbox, no warnings in the Style category will be displayed.
- Select detectors. The table allows you to select which detectors you want to enable for your project.

### 2.6.4 Extending the Eclipse Plugin (since 2.0.0)

Eclipse plugin supports contribution of custom SpotBugs detectors (see also `AddingDetectors.txt` for more information). There are two ways to contribute custom plugins to the Eclipse:

- Existing standard SpotBugs detector packages can be configured via `Window → Preferences → Java → FindBugs → Misc. Settings → Custom Detectors`. Simply specify there locations of any additional plugin libraries. The benefit of this solution is that already existing detector packages can be used “as is”, and that you can quickly verify the quality of third party detectors. The drawback is that you have to apply this settings in each new Eclipse workspace, and this settings can’t be shared between team members.
- It is possible to contribute custom detectors via standard Eclipse extensions mechanism.

Please check the documentation of the `eclipsePlugin/schema/detectorPlugins.exsd` extension point how to update the `plugin.xml`. Existing FindBugs detector plugins can be easily “extended” to be full featured SpotBugs AND Eclipse detector plugins. Usually you only need to add `META-INF/MANIFEST.MF` and `plugin.xml` to the jar and update your build scripts to not to override the `MANIFEST.MF` during the build.

The benefit of this solution is that for given (shared) Eclipse installation each team member has exactly same detectors set, and there is no need to configure anything anymore. The (really small) precondition is that you have to convert your existing detectors package to the valid Eclipse plugin. You can do this even for third-party detector packages. Another major differentiator is the ability to extend the default SpotBugs classpath at runtime with required third party libraries (see `AddingDetectors.txt` for more information).

### 2.6.5 Troubleshooting

This section lists common problems with the plugin and (if known) how to resolve them.

- If you see `OutOfMemory` error dialogs after starting SpotBugs analysis in Eclipse, please increase JVM available memory: change `eclipse.ini` and add the lines below to the end of the file:

```
-vmargs  
-Xmx1000m
```

Important: the configuration arguments starting with the line `-vmargs` must be last lines in the `eclipse.ini` file, and only one argument per line is allowed!

- If you do not see any SpotBugs problem markers (in your source windows or in the Problems View), you may need to change your `Problems View` filter settings. See [FAQ](#) for more information.

## 2.7 Using the SpotBugs Ant task

This chapter describes how to integrate SpotBugs into a build script for Ant, which is a popular Java build and deployment tool. Using the SpotBugs Ant task, your build script can automatically run SpotBugs on your Java code.

The Ant task was generously contributed by Mike Fagan.

### 2.7.1 Installing the Ant task

To install the Ant task, simply copy `$SPOTBUGS_HOME/lib/spotbugs-ant.jar` into the `lib` subdirectory of your Ant installation.

**Note:** It is strongly recommended that you use the Ant task with the version of SpotBugs it was included with. We do not guarantee that the Ant task Jar file will work with any version of SpotBugs other than the one it was included with.

### 2.7.2 Modifying build.xml

To incorporate SpotBugs into `build.xml` (the build script for Ant), you first need to add a task definition. This should appear as follows:

```
<taskdef
  resource="edu/umd/cs/findbugs/anttask/tasks.properties"
  classpath="path/to/spotbugs-ant.jar" />
```

The task definition specifies that when a `spotbugs` element is seen in `build.xml`, it should use the indicated class to execute the task.

After you have added the task definition, you can define a target which uses the `spotbugs` task. Here is an example which could be added to the `build.xml` for the Apache BCEL library.

```
<property name="spotbugs.home" value="/export/home/daveho/work/spotbugs" />

<target name="spotbugs" depends="jar">
  <spotbugs home="{spotbugs.home}"
    output="xml"
    outputFile="bcel-sb.xml" >
    <auxClasspath path="{basedir}/lib/Regex.jar" />
    <sourcePath path="{basedir}/src/java" />
    <class location="{basedir}/bin/bcel.jar" />
  </spotbugs>
</target>
```

The `spotbugs` element must have the `home` attribute set to the directory in which SpotBugs is installed; in other words, `$SPOTBUGS_HOME`. See *Installing*.

This target will execute SpotBugs on `bcel.jar`, which is the Jar file produced by BCEL's build script. (By making it depend on the "jar" target, we ensure that the library is fully compiled before running SpotBugs on it.) The output of SpotBugs will be saved in XML format to a file called `bcel-sb.xml`. An auxiliary Jar file, `Regex.jar`, is added to the aux classpath, because it is referenced by the main BCEL library. A source path is specified so that the saved bug data will have accurate references to the BCEL source code.

### 2.7.3 Executing the task

Here is an example of invoking Ant from the command line, using the spotbugs target defined above.

```
[daveho@noir]$ ant spotbugs
Buildfile: build.xml

init:

compile:

examples:

jar:

spotbugs:
 [spotbugs] Running SpotBugs...
 [spotbugs] Bugs were found
 [spotbugs] Output saved to bcel-sb.xml

BUILD SUCCESSFUL
Total time: 35 seconds
```

In this case, because we saved the bug results in an XML file, we can use the SpotBugs GUI to view the results; see *Running SpotBugs*.

### 2.7.4 Parameters

This section describes the parameters that may be specified when using the FindBugs task.

**class** A optional nested element specifying which classes to analyze. The class element must specify a location attribute which names the archive file (jar, zip, etc.), directory, or class file to be analyzed. Multiple class elements may be specified as children of a single spotbugs element.

In addition to or instead of specifying a class element, the SpotBugs task can contain one or more fileset element(s) that specify files to be analyzed. For example, you might use a fileset to specify that all of the jar files in a directory should be analyzed.

**auxClasspath** An optional nested element which specifies a classpath (Jar files or directories) containing classes used by the analyzed library or application, but which you don't want to analyze. It is specified the same way as Ant's classpath element for the Java task.

**sourcePath** An optional nested element which specifies a source directory path containing source files used to compile the Java code being analyzed. By specifying a source path, any generated XML bug output will have complete source information, which allows later viewing in the GUI.

**home** A required attribute. It must be set to the name of the directory where SpotBugs is installed.

**quietErrors** An optional boolean attribute. If true, reports of serious analysis errors and missing classes will be suppressed in the SpotBugs output. Default is false.

**reportLevel** An optional attribute. It specifies the confidence/priority threshold for reporting issues. If set to `low`, confidence is not used to filter bugs. If set to `medium` (the default), low confidence issues are suppressed. If set to `high`, only high confidence bugs are reported.

**output** Optional attribute. It specifies the output format. If set to `xml` (the default), output is in XML format. If set to `"xml:withMessages"`, output is in XML format augmented with human-readable messages. (You should use this format if you plan to generate a report using an XSL stylesheet.) If set to `"html"`, output is in HTML formatted

(default stylesheet is default.xml). If set to `text`, output is in ad-hoc text format. If set to `emacs`, output is in Emacs error message format. If set to `xdocs`, output is xdoc XML for use with Apache Maven.

**stylesheet** Optional attribute. It specifies the stylesheet to use to generate html output when the output is set to `html`. Stylesheets included in the FindBugs distribution include `default.xml`, `fancy.xml`, `fancy-hist.xml`, `plain.xml`, and `summary.xml`. The default value, if no `stylesheet` attribute is provided, is `default.xml`.

**sort** Optional attribute. If the output attribute is set to `text`, then the sort attribute specifies whether or not reported bugs are sorted by class. Default is `true`.

**outputFile** Optional attribute. If specified, names the output file in which the FindBugs output will be saved. By default, the output is displayed directly by Ant.

**debug** Optional boolean attribute. If set to `true`, SpotBugs prints diagnostic information about which classes are being analyzed, and which bug pattern detectors are being run. Default is `false`.

**effort** Set the analysis effort level. The value specified should be one of `min`, `default`, or `max`. See *Command-line Options <running.html#command-line-options>*: for more information about setting the analysis level.

**conserveSpace** Synonym for `effort="min"`.

**workHard** Synonym for `effort="max"`.

**visitors** Optional attribute. It specifies a comma-separated list of bug detectors which should be run. The bug detectors are specified by their class names, without any package qualification. By default, all detectors which are not disabled by default are run.

**omitVisitors** Optional attribute. It specifies a comma-separated list of bug detectors. It is like the `visitors` attribute, except it specifies detectors which will not be run.

**chooseVisitors** Optional attribute. It specifies a comma-separated list of bug detectors prefixed with "+" or "-" to selectively enable/disable them.

**excludeFilter** Optional attribute. It specifies the filename of a filter specifying bugs to exclude from being reported. See *Filter file*.

**excludePath** An optional nested element. It specifies a path containing filters specifying bugs to exclude from being reported. See *Filter file*.

**includeFilter** Optional attribute. It specifies the filename of a filter specifying which bugs are reported. See *Filter file*.

**includePath** An optional nested element. It specifies a path containing filters specifying which bugs are reported. See *Filter file*.

**projectFile** Optional attribute. It specifies the name of a project file. Project files are created by the FindBugs GUI, and specify classes, aux classpath entries, and source directories. By naming a project, you don't need to specify any class elements, nor do you need to specify `auxClasspath` or `sourcePath` attributes. See *Running SpotBugs* for how to create a project.

**jvmargs** Optional attribute. It specifies any arguments that should be passed to the Java virtual machine used to run SpotBugs. You may need to use this attribute to specify flags to increase the amount of memory the JVM may use if you are analyzing a very large program.

**systemProperty** Optional nested element. If specified, defines a system property. The name attribute specifies the name of the system property, and the value attribute specifies the value of the system property.

**timeout** Optional attribute. It specifies the amount of time, in milliseconds, that the Java process executing SpotBugs may run before it is assumed to be hung and is terminated. The default is 600,000 milliseconds, which is ten minutes. Note that for very large programs, SpotBugs may require more than ten minutes to complete its analysis.

**failOnError** Optional boolean attribute. Whether to abort the build process if there is an error running SpotBugs. Defaults to `false`.

**errorProperty** Optional attribute which specifies the name of a property that will be set to `true` if an error occurs while running SpotBugs.

**warningsProperty** Optional attribute which specifies the name of a property that will be set to `true` if any warnings are reported by SpotBugs on the analyzed program.

**userPreferencesFile** Optional attribute. Set the path of the user preferences file to use, which might override some of the options above. Specifying `userPreferencesFile` as first argument would mean some later options will override them, as last argument would mean they will override some previous options). This rationale behind this option is to reuse SpotBugs Eclipse project settings for command line execution.

**nested** Optional attribute which enables or disables scanning of nested jar and zip files found in the list of files and directories to be analyzed. By default, scanning of nested jar/zip files is enabled.

**setExitCode** Optional boolean attribute. Whether the exit code will be returned to the main ant job. Defaults to `true`.

## 2.8 Using the SpotBugs Maven Plugin

This chapter describes how to integrate SpotBugs into a Maven project.

### 2.8.1 Add spotbugs-maven-plugin to your pom.xml

Add `<plugin>` into your `pom.xml` like below:

```
<plugin>
  <groupId>com.github.spotbugs</groupId>
  <artifactId>spotbugs-maven-plugin</artifactId>
  <version>4.0.4</version>
  <dependencies>
    <!-- overwrite dependency on spotbugs if you want to specify the version of
    ↪spotbugs -->
    <dependency>
      <groupId>com.github.spotbugs</groupId>
      <artifactId>spotbugs</artifactId>
      <version>4.0.6</version>
    </dependency>
  </dependencies>
</plugin>
```

### 2.8.2 Goals of spotbugs-maven-plugin

#### spotbugs goal

`spotbugs` goal analyses target project by SpotBugs. For detail, please refer `spotbugs` goal description in maven site.

### check goal

`check` goal runs analysis like `spotbugs` goal, and make the build failed if it found any bugs. For detail, please refer [check goal description in maven site](#).

### gui goal

`gui` goal launches SpotBugs GUI to check analysis result. For detail, please refer [gui goal description in maven site](#).

### help goal

`help` goal displays usage of this Maven plugin.

## 2.9 Using the SpotBugs Gradle Plugin

This chapter describes how to integrate SpotBugs into a build script for Gradle.

### 2.9.1 Use SpotBugs Gradle Plugin

Please follow instruction found on [official Gradle Plugin page](#).

Note that SpotBugs Gradle Plugin does not support Gradle v4, you need to use v5.6 or later.

### 2.9.2 Tasks introduced by this Gradle Plugin

This Gradle Plugin generates task for each sourceSet generated by Gradle Java Plugin. For instance, if you have two sourceSets `main` and `test`, this plugin will generates two tasks: `spotbugsMain` and `spotbugsTest`.

Generated tasks uses compiled `.class` files as input, so it will run after java compilation runs (e.g. `classes` task). SpotBugs Gradle Plugin adds task dependency from `check` to these generated tasks, so you can simply run `./gradlew check` to run SpotBugs.

If you do not want to generate tasks automatically, use the [SpotBugs Base Plugin](#) instead. This plugin does not generate tasks so you can configure from scratch.

### 2.9.3 Configure Gradle Plugin

This plugin uses the Extension to configure. Please check the document for [SpotBugsExtension](#).

For instance, to specify the version of SpotBugs, you can configure like below:

```
spotbugs {
    toolVersion = '4.0.6'
}
```

## 2.9.4 Introduce SpotBugs Plugin

To introduce SpotBugs Plugin, please declare dependency in dependencies like below:

```
dependencies {
  spotbugsPlugins 'com.h3xstream.findseccbugs:findseccbugs-plugin:1.10.1'
}
```

## 2.9.5 Other usage

Visit the [official README](#) for detail.

## 2.10 Filter file

Filter files may be used to include or exclude bug reports for particular classes and methods. This chapter explains how to use filter files.

### 2.10.1 Introduction to Filter Files

Conceptually, a filter matches bug instances against a set of criteria. By defining a filter, you can select bug instances for special treatment; for example, to exclude or include them in a report.

A filter file is an XML document with a top-level `FindBugsFilter` element which has some number of `Match` elements as children. Each `Match` element represents a predicate which is applied to generated bug instances. Usually, a filter will be used to exclude bug instances. For example:

```
$ spotbugs -textui -exclude myExcludeFilter.xml myApp.jar
```

However, a filter could also be used to select bug instances to specifically report:

```
$ spotbugs -textui -include myIncludeFilter.xml myApp.jar
```

`Match` elements contain children, which are conjuncts of the predicate. In other words, each of the children must be `true` for the predicate to be `true`.

### 2.10.2 Types of Match clauses

#### <Bug>

This element specifies a particular bug pattern or patterns to match. The `pattern` attribute is a comma-separated list of bug pattern types. You can find the bug pattern types for particular warnings by looking at the output produced by the `-xml` output option (the `type` attribute of `BugInstance` elements), or from the *Bug descriptions*.

For more coarse-grained matching, use `code` attribute. It takes a comma-separated list of bug abbreviations. For most-coarse grained matching use `category` attribute, that takes a comma separated list of bug category names: `CORRECTNESS`, `MT_CORRECTNESS`, `BAD_PRACTICICE`, `PERFORMANCE`, `STYLE`.

If more than one of the attributes mentioned above are specified on the same `<Bug>` element, all bug patterns that match either one of specified pattern names, or abbreviations, or categories will be matched.

As a backwards compatibility measure, `<BugPattern>` and `<BugCode>` elements may be used instead of `<Bug>` element. Each of these uses a `name` attribute for specifying accepted values list. Support for these elements may be removed in a future release.

### **<Confidence>**

This element matches warnings with a particular bug confidence. The `value` attribute should be an integer value: 1 to match high-confidence warnings, 2 to match normal-confidence warnings, or 3 to match low-confidence warnings. `<Confidence>` replaced `<Priority>` in 2.0.0 release.

### **<Priority>**

Same as `<Confidence>`, exists for backward compatibility.

### **<Rank>**

This element matches warnings with a particular bug rank. The `value` attribute should be an integer value between 1 and 20, where 1 to 4 are scariest, 5 to 9 scary, 10 to 14 troubling, and 15 to 20 of concern bugs.

### **<Package>**

This element matches warnings associated with classes within the package specified using `name` attribute. Nested packages are not included (along the lines of Java import statement). However matching multiple packages can be achieved easily using regex name match.

### **<Class>**

This element matches warnings associated with a particular class. The `name` attribute is used to specify the exact or regex match pattern for the class name. The `role` attribute is the class role.

As a backward compatibility measure, instead of element of this type, you can use `class` attribute on a `Match` element to specify exact an class name or `classregex` attribute to specify a regular expression to match the class name against.

If the `Match` element contains neither a `Class` element, nor a `class` / `classregex` attribute, the predicate will apply to all classes. Such predicate is likely to match more bug instances than you want, unless it is refined further down with appropriate method or field predicates.

### **<Source>**

This element matches warnings associated with a particular source file. The `name` attribute is used to specify the exact or regex match pattern for the source file name.

### <Method>

This element specifies a method. The `name` attribute is used to specify the exact or regex match pattern for the method name. The `params` attribute is a comma-separated list of the types of the method's parameters. The `returns` attribute is the method's return type. The `role` attribute is the method role. In `params` and `returns`, class names must be fully qualified. (E.g., `"java.lang.String"` instead of just `"String"`.) If one of the latter attributes is specified the other is required for creating a method signature. Note that you can provide either `name` attribute or `params` and `returns` attributes or all three of them. This way you can provide various kinds of name and signature based matches.

### <Field>

This element specifies a field. The `name` attribute is used to specify the exact or regex match pattern for the field name. You can also filter fields according to their signature - use `type` attribute to specify fully qualified type of the field. You can specify either or both of these attributes in order to perform name / signature based matches. The `role` attribute is the field role.

### <Local>

This element specifies a local variable. The `name` attribute is used to specify the exact or regex match pattern for the local variable name. Local variables are variables defined within a method.

### <Type>

This element matches warnings associated with a particular type. The `descriptor` attribute is used to specify the exact or regex match pattern for type descriptor. If the descriptor starts with the `~` character the rest of attribute content is interpreted as a Java regular expression. The `role` attribute is the class role, and the `typeParameters` is the type parameters. Both of `role` and `typeParameters` are optional attributes.

### <Or>

This element combines `Match` clauses as disjuncts. I.e., you can put two `Method` elements in an `Or` clause in order to match either method.

### <And>

This element combines `Match` clauses which both must evaluate to `true`. I.e., you can put `Bug` and `Confidence` elements in an `And` clause in order to match specific bugs with given confidence only.

### <Not>

This element inverts the included child `Match`. I.e., you can put a `Bug` element in a `Not` clause in order to match any bug excluding the given one.

### 2.10.3 Java element name matching

If the name attribute of `Class`, `Source`, `Method` or `Field` starts with the `~` character the rest of attribute content is interpreted as a Java regular expression that is matched against the names of the Java element in question.

Note that the pattern is matched against whole element name and therefore `.*` clauses need to be used at pattern beginning and/or end to perform substring matching.

See [java.util.regex.Pattern](#) documentation for pattern syntax.

### 2.10.4 Caveats

`Match` clauses can only match information that is actually contained in the bug instances. Every bug instance has a class, so in general, excluding bugs by class will work.

Some bug instances have two (or more) classes. For example, the DE (dropped exception) bugs report both the class containing the method where the dropped exception happens, and the class which represents the type of the dropped exception. Only the *first* (primary) class is matched against `Match` clauses. So, for example, if you want to suppress IC (initialization circularity) reports for classes “com.foobar.A” and “com.foobar.B”, you would use two `Match` clauses:

```
<Match>
  <Class name="com.foobar.A" />
  <Bug code="IC" />
</Match>
<Match>
  <Class name="com.foobar.B" />
  <Bug code="IC" />
</Match>
```

By explicitly matching both classes, you ensure that the IC bug instance will be matched regardless of which class involved in the circularity happens to be listed first in the bug instance. (Of course, this approach might accidentally suppress circularities involving “com.foobar.A” or “com.foobar.B” and a third class.)

Many kinds of bugs report what method they occur in. For those bug instances, you can put `Method` clauses in the `Match` element and they should work as expected.

### 2.10.5 Examples

#### Match all bug reports for a class

```
<Match>
  <Class name="com.foobar.MyClass" />
</Match>
```

#### Match certain tests from a class by specifying their abbreviations

```
<Match>
  <Class name="com.foobar.MyClass" / >
  <Bug code="DE,UrF,SIC" />
</Match>
```

### Match certain tests from all classes by specifying their abbreviations

```
<Match>
  <Bug code="DE,UrF,SIC" />
</Match>
```

### Match certain tests from all classes by specifying their category

```
<Match>
  <Bug category="PERFORMANCE" />
</Match>
```

### Match bug types from specified methods of a class by their abbreviations

```
<Match>
  <Class name="com.foobar.MyClass" />
  <Or>
    <Method name="frob" params="int,java.lang.String" returns="void" />
    <Method name="blat" params="" returns="boolean" />
  </Or>
  <Bug code="DC" />
</Match>
```

### Match a particular bug pattern in a particular method

```
<!-- A method with an open stream false positive. -->
<Match>
  <Class name="com.foobar.MyClass" />
  <Method name="writeDataToFile" />
  <Bug pattern="OS_OPEN_STREAM" />
</Match>
```

### Match a particular bug pattern with a given priority in a particular method

```
<!-- A method with a dead local store false positive (medium priority). -->
<Match>
  <Class name="com.foobar.MyClass" />
  <Method name="someMethod" />
  <Bug pattern="DLS_DEAD_LOCAL_STORE" />
  <Priority value="2" />
</Match>
```

**Match minor bugs introduced by AspectJ compiler (you are probably not interested in these unless you are an AspectJ developer)**

```
<Match>
  <Class name="~.*\$AjcClosure\d+" />
  <Bug pattern="DLS_DEAD_LOCAL_STORE" />
  <Method name="run" />
</Match>
<Match>
  <Bug pattern="UUF_UNUSED_FIELD" />
  <Field name="~ajc\$.*" />
</Match>
```

**Match bugs in specific parts of the code base**

```
<!-- match unused fields warnings in Messages classes in all packages -->
<Match>
  <Class name="~.*\.Messages" />
  <Bug code="UUF" />
</Match>
<!-- match mutable statics warnings in all internal packages -->
<Match>
  <Package name="~.*\.internal" />
  <Bug code="MS" />
</Match>
<!-- match anonymous inner classes warnings in ui package hierarchy -->
<Match>
  <Package name="~com\.foobar\.fooproject\.ui.*" />
  <Bug pattern="SIC_INNER_SHOULD_BE_STATIC_ANON" />
</Match>
```

**Match bugs on fields or methods with specific signatures**

```
<!-- match System.exit(...) usage warnings in void main(String[]) methods in all_
↳classes -->
<Match>
  <Method returns="void" name="main" params="java.lang.String[]" />
  <Bug pattern="DM_EXIT" />
</Match>
<!-- match UuF warnings on fields of type com.foobar.DebugInfo on all classes -->
<Match>
  <Field type="com.foobar.DebugInfo" />
  <Bug code="UuF" />
</Match>
```

## Match bugs using the Not filter operator

```

<!-- ignore all bugs in test classes, except for those bugs specifically relating to
↳JUnit tests -->
<!-- i.e. filter bug if ( classIsJUnitTest && ! bugIsRelatedToJUnit ) -->
<Match>
  <!-- the Match filter is equivalent to a logical 'And' -->

  <Class name="~.*\.*Test" />
  <!-- test classes are suffixed by 'Test' -->

  <Not>
    <Bug code="IJU" /> <!-- 'IJU' is the code for bugs related to JUnit test code --
↳>
  </Not>
</Match>

```

## Full exclusion filter file to match all classes generated from Groovy source files

```

<?xml version="1.0" encoding="UTF-8"?>
<FindBugsFilter>
  <Match>
    <Source name="~.*\.*groovy" />
  </Match>
</FindBugsFilter>

```

## 2.10.6 Complete Example

```

<?xml version="1.0" encoding="UTF-8"?>
<FindBugsFilter
  xmlns="https://github.com/spotbugs/filter/3.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="https://github.com/spotbugs/filter/3.0.0 https://
↳raw.githubusercontent.com/spotbugs/spotbugs/3.1.0/spotbugs/etc/findbugsfilter.xsd">
  <Match>
    <Class name="com.foobar.ClassNotToBeAnalyzed" />
  </Match>

  <Match>
    <Class name="com.foobar.ClassWithSomeBugsMatched" />
    <Bug code="DE,UrF,SIC" />
  </Match>

  <!-- Match all XYZ violations. -->
  <Match>
    <Bug code="XYZ" />
  </Match>

  <!-- Match all doublecheck violations in these methods of "AnotherClass". -->
  <Match>
    <Class name="com.foobar.AnotherClass" />
    <Or>
      <Method name="nonOverloadedMethod" />

```

(continues on next page)

(continued from previous page)

```

    <Method name="frob" params="int,java.lang.String" returns="void" />
    <Method name="blat" params="" returns="boolean" />
  </Or>
  <Bug code="DC" />
</Match>

<!-- A method with a dead local store false positive (medium priority). -->
<Match>
  <Class name="com.foobar.MyClass" />
  <Method name="someMethod" />
  <Bug pattern="DLS_DEAD_LOCAL_STORE" />
  <Priority value="2" />
</Match>

<!-- All bugs in test classes, except for JUnit-specific bugs -->
<Match>
  <Class name="~.*\.*Test" />
  <Not>
    <Bug code="IJU" />
  </Not>
</Match>
</FindBugsFilter>

```

## 2.11 Analysis Properties

SpotBugs allows several aspects of the analyses it performs to be customized. System properties are used to configure these options. This chapter describes the configurable analysis options.

The analysis options have two main purposes. First, they allow you to inform SpotBugs about the meaning of methods in your application, so that it can produce more accurate results, or produce fewer false warnings. Second, they allow you to configure the precision of the analysis performed. Reducing analysis precision can save memory and analysis time, at the expense of missing some real bugs, or producing more false warnings.

The analysis options are set using the `-property` command line option. For example:

```
$ spotbugs -textui -property "cfg.noprune=true" myApp.jar
```

The list of configurable analysis properties is shown in following table:

Property Name	Value	Meaning
find-bugs.assertion.methods	Comma-separated list of fully qualified method names: e.g., "com.foo.MyClass.checkAssertion"	This property specifies the names of methods that are used to check program assertions. Specifying these methods allows the null pointer dereference bug detector to avoid reporting false warnings for values which are checked by "Assertion" methods.
find-bugs.decomment	true or false	If true, the DroppedException detector scans source code for empty catch blocks for a comment, and if one is found, does not report a warning.
find-bugs.maskedfields.locals	true or false	If true, emit low priority warnings for local variables which obscure fields. Default is false.
find-bugs.null.deref.assumensp	true or false	not used (intention: If true, the null dereference detector assumes that any reference value returned from a method or passed to a method in a parameter might be null. Default is false. Note that enabling this property will very likely cause a large number of false warnings to be produced.)
find-bugs.refcomp.reportAll	true or false	If true, all suspicious reference comparisons using the == and != operators are reported.,If false, only one such warning is issued per method.,Default is false.
find-bugs.sf.comment	true or false	If true, the SwitchFallthrough detector will only report warnings for cases where the source code does not have a comment containing the words "fall" or "nobreak". (An accurate source path must be used for this feature to work correctly.) This helps find cases where the switch fallthrough is likely to be unintentional.

## 2.12 Effort

Effort value adjusts internal flags of SpotBugs, to reduce computation cost by lowering the prediction.

The default effort configuration is same with `more`.

Flags in Find-Bugs.java	Description	Effort Level			
		min	less	more	max
Accurate Exceptions	Determine (1) what exceptions can be thrown on exception edges, (2) which catch blocks are reachable, and (3) which exception edges carry only, “implicit” runtime exceptions.		✓	✓	✓
Model Instanceof	Model the effect of instanceof checks in type analysis		✓	✓	✓
Track Guaranteed Value Derefs in Null Pointer Analysis	In the null pointer analysis, track null values that are guaranteed to be, dereferenced on some (non-implicit-exception) path.			✓	✓
Track Value Numbers in Null Pointer Analysis	In the null pointer analysis, track value numbers that are known to be, null. This allows us to not lose track of null values that are not, currently in the stack frame but might be in a heap location where the, value is recoverable by redundant load elimination or forward, substitution.			✓	✓
Interprocedural Analysis	Enable interprocedural analysis for application classes.			✓	✓
Interprocedural Analysis of Referenced Classes	Enable interprocedural analysis for referenced classes (non-application classes).				✓
Conserve Space	Try to conserve space at the expense of precision. e.g. Prune unconditional exception thrower edges for control flow graph analysis, to reduce memory footprint.	✓			
Skip Huge Methods	Skip method analysis if length of its bytecode is too long (6,000).	✓	✓	✓	

## 2.13 Implement SpotBugs plugin

### 2.13.1 Create Maven project

Use `spotbugs-archetype` to create Maven project. Then Maven archetype plugin will ask you to decide plugin’s `groupId`, `artifactId`, `package` and `initial version`.

```
$ mvn archetype:generate \
  -DarchetypeArtifactId=spotbugs-archetype \
  -DarchetypeGroupId=com.github.spotbugs \
  -DarchetypeVersion=0.2.3
```

### 2.13.2 Write java code to represent bug to find

In generated project, you can find a file named as `BadCase.java`. Update this file to represent the target bug to find. If you have multiple patterns to represent, add more classes into `src/test/java` directory.

### 2.13.3 Write test case to ensure your detector can find bug

In generated project, you can find another file named as `MyDetectorTest.java`. The `spotbugs.performAnalysis(Path)` in this test runs SpotBugs with your plugin, and return all found bugs (here 1st argument of this method is a path of class file compiled from `BadCase.java`).

You can use `BugInstanceMatcher` to verify that your plugin can find bug as expected.

Currently this test should fail, because we've not updated detector itself yet.

### 2.13.4 Write java code to avoid false-positive

To avoid false-positive, it is good to ensure that in which case detector should NOT find bug.

Update `GoodCase.java` in your project, and represent such cases. After that, add a test method into `MyDetectorTest.java` which verify that no bug found from this `GoodCase` class.

If you have multiple patterns to represent, add more classes into `src/test/java` directory.

### 2.13.5 Update detector to pass all unit tests

Now you have tests to ensure that your detector can work as expected.

---

**Note:** TBU

---

#### Which super class you should choose

**AnnotationDetector** Base detector which analyzes annotations on classes, fields, methods, and method parameters.

**BytecodeScanningDetector** Base detector which analyzes java bytecode in class files.

**OpcodesStackDetector** Sub class of `BytecodeScanningDetector`, which can scan the bytecode of a method and use an operand stack.

### 2.13.6 Update findbugs.xml

SpotBugs reads `findbugs.xml` in each plugin to find detectors and bugs. So when you add new detector, you need to add new `<Detector>` element like below:

```
<Detector class="com.github.plugin.MyDetector" reports="MY_BUG" speed="fast" />
```

It is also necessary to add `<BugPattern>`, to describe type and category of your bug pattern.

```
<BugPattern type="MY_BUG" category="CORRECTNESS" />
```

You can find `findbugs.xml` in `src/main/resources` directory of generated Maven project.

## 2.13.7 Update messages.xml

SpotBugs reads `messages.xml` in each plugin to construct human readable message to report detected bug. It also supports reading localized messages from `messages_ja.xml`, `messages_fr.xml` and so on.

You can find `messages.xml` in `src/main/resources` directory of generated Maven project.

### Update message of Detector

In `<Detector>` element, you can add detector's description message. Note that it should be plain text, HTML is not supported.

```
<Detector class="com.github.plugin.MyDetector">
  <Details>
    Original detector to detect MY_BUG bug pattern.
  </Details>
</Detector>
```

### Update message of Bug Pattern

In `<BugPattern>` element, you can add bug pattern's description message. There are three kinds of messages:

**ShortDescription** Short description for bug pattern. Useful to tell its intent and character for users. It should be plain text, HTML is not supported.

**LongDescription** Longer description for bug pattern. You can use placeholder like `{0}` (0-indexed), then added data into `BugInstance` will be inserted at there. So this `LongDescription` is useful to tell detailed information about detected bug.

It should be plain text, HTML is not supported.

**Details** Detailed description for bug pattern. It should be HTML format, so this is useful to tell detailed specs/examples with table, list and code snippets.

```
<BugPattern type="MY_BUG">
  <ShortDescription>Explain bug pattern shortly.</ShortDescription>
  <LongDescription>
    Explain existing problem in code, and how developer should improve their_
    ↪implementation.
  </LongDescription>
  <Details>
    <![CDATA[
      <p>Explain existing problem in code, and how developer should improve their_
      ↪implementation.</p>
    ]]>
  </Details>
</BugPattern>
```

## 2.14 Use SpotBugs Plugin on SonarQube

The SpotBugs SonarQube Plugin uses major SpotBugs plugins such as `fb-contrib` and `Find Security Bugs`. However, if you want to use another SpotBugs plugin, you need to build your own SonarQube plugin. For detailed requirements on SonarQube plugins, see the [SonarQube official guidelines](#).

### 2.14.1 Create Maven Project

Follow the interaction in the [SonarQube official guidelines](#). It is recommended to use sub-modules, to manage both the SpotBugs plugin and the SonarQube plugin in one project. You can refer to [this module](#) as an example.

You also need to configure the `sonar-packaging-maven-plugin`, to make your plugin depend on the [SpotBugs SonarQube Plugin](#). For instance, if you're using SonarQube 6.7 LTS, your plugin requires SpotBugs SonarQube Plugin version 3.7, so your configuration should be like below:

```
<configuration>
  <basePlugin>findbugs</basePlugin>
  <requirePlugins>findbugs:3.7</requirePlugins>
  ...
</configuration>
```

### 2.14.2 Generate rules.xml

SonarQube doesn't understand the Bug Pattern metadata provided for SpotBugs, so we need to convert `findbugs.xml` and `messages.xml` to the SonarQube format named `rules.xml`.

If your SpotBugs plugin isn't complex, you can simply introduce the [SonarQube rule xml generator Maven Plugin](#) to generate `rules.xml`. Follow the interaction described in its [README](#).

### 2.14.3 Update RulesDefinition.java

Your `SonarQubeRulesDefinition.java` should load the generated `rules.xml` to the `FindBugs` repository.

When you create a `NewRepository` instance, use `FindbugsRulesDefinition.REPOSITORY_KEY` as the repository key, and do not rename it by calling `NewRepository#setName(String)`. It is necessary to fulfill the requirement from [SonarQube API](#). Here is an example:

```
@Override
public void define(Context context) {
    NewRepository repository =
        context.createRepository(FindbugsRulesDefinition.REPOSITORY_KEY, Java.KEY);

    RulesDefinitionXMLLoader ruleLoader = new RulesDefinitionXMLLoader();
    ruleLoader.load(
        repository,
        getClass().getResourceAsStream(
            "/path/to/rules.xml"),
        "UTF-8");
    repository.done();
}
```

## 2.14.4 Update Plugin.java

Plugin.java should be a simple implementation that just loads your RulesDefinition class. Here is an example:

```
@Override
public void define(Context context) {
    context.addExtensions(Arrays.asList(SonarQubeRulesDefinition.class));
}
```

## 2.14.5 Deploy onto SonarQube

mvn package will generate a .jar file that works as a SonarQube plugin. Follow the [SonarQube official guidelines](#) to deploy it onto SonarQube.

Note that you need to enable new rules manually in your SonarQube profile, or newly added rules will not be used at analysis.

## 2.15 SpotBugs FAQ

This document contains answers to frequently asked questions about SpotBugs. If you just want general information about SpotBugs, have a look at the manual.

### 2.15.1 Q1: I'm getting java.lang.UnsupportedClassVersionError when I try to run SpotBugs

SpotBugs requires JRE8 or later to run. If you use an earlier version, you will see an exception error message similar to the following:

```
Exception in thread "main" java.lang.UnsupportedClassVersionError:
edu/umd/cs/findbugs/gui/FindBugsFrame (Unsupported major.minor version 52.0)
```

The solution is to upgrade to JRE8 or later.

### 2.15.2 Q2: SpotBugs is running out of memory, or is taking a long time to finish

In general, SpotBugs requires lots of memory and a relatively fast CPU. For large applications, 1024M or more of heap space may be required.

By default, SpotBugs allocates 768M of heap space. You can increase this using the `-maxHeap n` option, where `n` is the number of megabytes of heap space to allocate.

### 2.15.3 Q3: What is the “auxiliary classpath”? Why should I specify it?

Many important facts about a Java class require information about the classes that it references. For example:

- What other classes and interfaces the class inherits from
- What exceptions can be thrown by methods in external classes and interfaces

The “auxiliary classpath” is a list of Jar files, directories, and class files containing classes that are used by the code you want SpotBugs to analyze, but should not themselves be analyzed by SpotBugs.

If SpotBugs doesn’t have complete information about referenced classes, it will not be able to produce results that are as accurate as possible. For example, having a complete repository of referenced classes allows SpotBugs to prune control flow information so it can concentrate on paths through methods that are most likely to be feasible at runtime. Also, some bug detectors (such as the suspicious reference comparison detector) rely on being able to perform type inference, which requires complete type hierarchy information.

For these reasons, we strongly recommend that you completely specify the auxiliary classpath when you run SpotBugs. You can do this by using the `-auxclasspath` command line option, or the “Classpath entries” list in the GUI project editor dialog.

If SpotBugs cannot find a class referenced by your application, it will print out a message when the analysis completes, specifying the classes that were missing. You should modify the auxiliary classpath to specify how to find the missing classes, and then run SpotBugs again.

### 2.15.4 Q4: The Eclipse plugin doesn’t load

The symptom of this problem is that Eclipse fails to load the SpotBugs UI plugin with the message:

```
Plug-in “edu.umd.cs.findbugs.plugin.eclipse” was disabled due to missing or disabled prerequisite plug-in “org.eclipse.ui.ide”
```

The reason for this problem is that the Eclipse plugin distributed with SpotBugs does not work with older 3.x versions of Eclipse. Please use Eclipse Neon (version 4.6) or newer.

### 2.15.5 Q5: I’m getting a lot of false “OS” and “ODR” warnings

By default, SpotBugs assumes that any method invocation can throw an unchecked runtime exception. As a result, it may assume that an unchecked exception thrown out of the method could bypass a call to a `close()` method for a stream or database resource.

You can use the `-workHard` command line argument or the `findbugs.workHard` boolean analysis property to make SpotBugs work harder to prune unlikely exception edges. This generally reduces the number of false warnings, at the expense of slowing down the analysis.

### 2.15.6 Q6: The Eclipse plugin loads, but doesn’t work correctly

- Make sure the Java code you trying to analyze is built properly and has no classpath or compile errors.
- Make sure the project and workspace SpotBugs settings are valid - in doubt, revert them to defaults.
- Make sure the Error log view does not show errors.

### 2.15.7 Q7: Where is the Maven plugin for SpotBugs?

The Maven Plugin for SpotBugs may be found [here](#).

## 2.16 SpotBugs Links

This page contains links to related projects, including tools that are similar to SpotBugs.

### 2.16.1 IDE Integration

**m2e-code-quality** An Eclipse plugin which configures the FindBugs/SpotBugs Eclipse plugin to match the FindBugs/SpotBugs Maven plugin.

### 2.16.2 SpotBugs Plugins

**fb-contrib** A FindBugs/SpotBugs plugin for doing static code analysis on java byte code.

**Find Security Bugs** A FindBugs/SpotBugs plugin for security audits of Java web applications.

**findbugs-slf4j** A FindBugs/SpotBugs plugin to verify usage of SLF4J.

### 2.16.3 Similar/Related Tools

**FindBugs-IDEA** The FindBugs plugin for IntelliJ IDEA.

**sonar-findbugs** A SonarQube plugin which provides rules based on SpotBugs and its major plugins.

**Checkstyle** A style checker for Java.

**PMD** An extensible cross-language static code analyzer.

**huntbugs** New Java bytecode static analyzer tool based on [Procyon Compiler Tools](#) aimed to supersede the FindBugs.

**Google Error Prone** A static analysis tool for Java that catches common programming mistakes at compile-time.

**Checker Framework** A pluggable type-checking for Java.

## 2.17 Bug descriptions

This document lists the standard bug patterns reported by SpotBugs.

### 2.17.1 Bad practice (BAD\_PRACTICE)

Violations of recommended and essential coding practice. Examples include hash code and equals problems, cloneable idiom, dropped exceptions, Serializable problems, and misuse of finalize. We strive to make this analysis accurate, although some groups may not care about some of the bad practices.

CNT: Rough value of known constant found (CNT\_ROUGH\_CONSTANT\_VALUE)

NP: Method with Boolean return type returns explicit null (NP\_BOOLEAN\_RETURN\_NULL)

SW: Certain swing methods needs to be invoked in Swing thread (SW\_SWING\_METHODS\_INVOKED\_IN\_SWING\_THREAD)

FI: Finalizer only nulls fields (FI\_FINALIZER\_ONLY\_NULLS\_FIELDS)

FI: Finalizer nulls fields (FI\_FINALIZER\_NULLS\_FIELDS)

UI: Usage of GetResource may be unsafe if class is extended (UI\_INHERITANCE\_UNSAFE\_GETRESOURCE)

AM: Creates an empty zip file entry (AM\_CREATES\_EMPTY\_ZIP\_FILE\_ENTRY)

AM: Creates an empty jar file entry (AM\_CREATES\_EMPTY\_JAR\_FILE\_ENTRY)

IMSE: Dubious catching of IllegalMonitorStateException (IMSE\_DONT\_CATCH\_IMSE)

CN: Class defines clone() but doesn't implement Cloneable (CN\_IMPLEMENTES\_CLONE\_BUT\_NOT\_CLONEABLE)

CN: Class implements Cloneable but does not define or use clone method (CN\_IDIOM)

CN: clone method does not call super.clone() (CN\_IDIOM\_NO\_SUPER\_CALL)

DE: Method might drop exception (DE\_MIGHT\_DROP)

DE: Method might ignore exception (DE\_MIGHT\_IGNORE)

Dm: Method invokes System.exit(...) (DM\_EXIT)

Nm: Use of identifier that is a keyword in later versions of Java (NM\_FUTURE\_KEYWORD\_USED\_AS\_IDENTIFIER)

Nm: Use of identifier that is a keyword in later versions of Java (NM\_FUTURE\_KEYWORD\_USED\_AS\_MEMBER\_IDENTIFIER)

JCIP: Fields of immutable classes should be final (JCIP\_FIELD\_ISNT\_FINAL\_IN\_IMMUTABLE\_CLASS)

Dm: Method invokes dangerous method runFinalizersOnExit (DM\_RUN\_FINALIZERS\_ON\_EXIT)

NP: equals() method does not check for null argument (NP\_EQUALS\_SHOULD\_HANDLE\_NULL\_ARGUMENT)

FI: Empty finalizer should be deleted (FI\_EMPTY)

FI: Finalizer nullifies superclass finalizer (FI\_NULLIFY\_SUPER)

FI: Finalizer does nothing but call superclass finalizer (FI\_USELESS)

FI: Finalizer does not call superclass finalizer (FI\_MISSING\_SUPER\_CALL)

**FI:** Explicit invocation of finalizer (FI\_EXPLICIT\_INVOCATION)

**Eq:** Equals checks for incompatible operand (EQ\_CHECK\_FOR\_OPERAND\_NOT\_COMPATIBLE\_WITH\_THIS)

**Eq:** equals method fails for subtypes (EQ\_GETCLASS\_AND\_CLASS\_CONSTANT)

**Eq:** Covariant equals() method defined (EQ\_SELF\_NO\_OBJECT)

**Co:** Covariant compareTo() method defined (CO\_SELF\_NO\_OBJECT)

**Co:** compareTo()/compare() returns Integer.MIN\_VALUE (CO\_COMPARETO\_RESULTS\_MIN\_VALUE)

**Co:** compareTo()/compare() incorrectly handles float or double value (CO\_COMPARETO\_INCORRECT\_FLOATING)

**RV:** Negating the result of compareTo()/compare() (RV\_NEGATING\_RESULT\_OF\_COMPARETO)

**ES:** Comparison of String objects using == or != (ES\_COMPARING\_STRINGS\_WITH\_EQ)

**ES:** Comparison of String parameter using == or != (ES\_COMPARING\_PARAMETER\_STRING\_WITH\_EQ)

**Eq:** Class defines compareTo(...) and uses Object.equals() (EQ\_COMPARETO\_USE\_OBJECT\_EQUALS)

**HE:** Class defines hashCode() and uses Object.equals() (HE\_HASHCODE\_USE\_OBJECT\_EQUALS)

**HE:** Class defines hashCode() but not equals() (HE\_HASHCODE\_NO\_EQUALS)

**HE:** Class defines equals() and uses Object.hashCode() (HE\_EQUALS\_USE\_HASHCODE)

**HE:** Class inherits equals() and uses Object.hashCode() (HE\_INHERITS\_EQUALS\_USE\_HASHCODE)

**HE:** Class defines equals() but not hashCode() (HE\_EQUALS\_NO\_HASHCODE)

**Eq:** Abstract class defines covariant equals() method (EQ\_ABSTRACT\_SELF)

**Co:** Abstract class defines covariant compareTo() method (CO\_ABSTRACT\_SELF)

**IC:** Superclass uses subclass during initialization (IC\_SUPERCLASS\_USES\_SUBCLASS\_DURING\_INITIALIZATION)

**SI:** Static initializer creates instance before all static final fields assigned (SI\_INSTANCE\_BEFORE\_FINALS\_ASSIGNED)

**It:** Iterator next() method can't throw NoSuchElementException (IT\_NO\_SUCH\_ELEMENT)

**ME:** Enum field is public and mutable (ME\_MUTABLE\_ENUM\_FIELD)

**ME:** Public enum method unconditionally sets its field (ME\_ENUM\_FIELD\_SETTER)

**Nm:** Method names should start with a lower case letter (NM\_METHOD\_NAMING\_CONVENTION)

**Nm:** Field names should start with a lower case letter (NM\_FIELD\_NAMING\_CONVENTION)

Nm: Class names shouldn't shadow simple name of implemented interface (NM\_SAME\_SIMPLE\_NAME\_AS\_INTERFACE)

Nm: Class names shouldn't shadow simple name of superclass (NM\_SAME\_SIMPLE\_NAME\_AS\_SUPERCLASS)

Nm: Class names should start with an upper case letter (NM\_CLASS\_NAMING\_CONVENTION)

Nm: Very confusing method names (but perhaps intentional) (NM\_VERY\_CONFUSING\_INTENTIONAL)

Nm: Method doesn't override method in superclass due to wrong package for parameter (NM\_WRONG\_PACKAGE\_INTENTIONAL)

Nm: Confusing method names (NM\_CONFUSING)

Nm: Class is not derived from an Exception, even though it is named as such (NM\_CLASS\_NOT\_EXCEPTION)

RR: Method ignores results of `InputStream.read()` (RR\_NOT\_CHECKED)

RR: Method ignores results of `InputStream.skip()` (SR\_NOT\_CHECKED)

Se: Class is `Serializable` but its superclass doesn't define a void constructor (SE\_NO\_SUITABLE\_CONSTRUCTOR)

Se: Class is `Externalizable` but doesn't define a void constructor (SE\_NO\_SUITABLE\_CONSTRUCTOR\_FOR\_EXTERNALIZATION)

Se: `Comparator` doesn't implement `Serializable` (SE\_COMPARATOR\_SHOULD\_BE\_SERIALIZABLE)

SnVI: Class is `Serializable`, but doesn't define `serialVersionUID` (SE\_NO\_SERIALVERSIONID)

Se: The `readResolve` method must be declared with a return type of `Object`. (SE\_READ\_RESOLVE\_MUST\_RETURN\_OBJECT)

Se: Transient field that isn't set by deserialization. (SE\_TRANSIENT\_FIELD\_NOT\_RESTORED)

Se: `serialVersionUID` isn't final (SE\_NONFINAL\_SERIALVERSIONID)

Se: `serialVersionUID` isn't static (SE\_NONSTATIC\_SERIALVERSIONID)

Se: `serialVersionUID` isn't long (SE\_NONLONG\_SERIALVERSIONID)

Se: Non-transient non-serializable instance field in serializable class (SE\_BAD\_FIELD)

Se: `Serializable` inner class (SE\_INNER\_CLASS)

Se: Non-serializable class has a serializable inner class (SE\_BAD\_FIELD\_INNER\_CLASS)

Se: Non-serializable value stored into instance field of a serializable class (SE\_BAD\_FIELD\_STORE)

RV: Method ignores exceptional return value (RV\_RETURN\_VALUE\_IGNORED\_BAD\_PRACTICE)

NP: toString method may return null (NP\_TOSTRING\_COULD\_RETURN\_NULL)

NP: Clone method may return null (NP\_CLONE\_COULD\_RETURN\_NULL)

OS: Method may fail to close stream (OS\_OPEN\_STREAM)

OS: Method may fail to close stream on exception (OS\_OPEN\_STREAM\_EXCEPTION\_PATH)

RC: Suspicious reference comparison to constant (RC\_REF\_COMPARISON\_BAD\_PRACTICE)

RC: Suspicious reference comparison of Boolean values (RC\_REF\_COMPARISON\_BAD\_PRACTICE\_BOOLEAN)

FS: Format string should use %n rather than n (VA\_FORMAT\_STRING\_USES\_NEWLINE)

BIT: Check for sign of bitwise operation (BIT\_SIGNED\_CHECK)

ODR: Method may fail to close database resource (ODR\_OPEN\_DATABASE\_RESOURCE)

ODR: Method may fail to close database resource on exception (ODR\_OPEN\_DATABASE\_RESOURCE\_EXCEPTION\_PATH)

ISC: Needless instantiation of class that only supplies static methods (ISC\_INSTANTIATE\_STATIC\_CLASS)

DMI: Random object created and used only once (DMI\_RANDOM\_USED\_ONLY\_ONCE)

BC: Equals method should not assume anything about the type of its argument (BC\_EQUALS\_METHOD\_SHOULD\_WORK\_FOR\_ALL\_OBJECTS)

J2EE: Store of non serializable object into HttpSession (J2EE\_STORE\_OF\_NON\_SERIALIZABLE\_OBJECT\_INTO\_SESSION)

GC: Unchecked type in generic call (GC\_UNCHECKED\_TYPE\_IN\_GENERIC\_CALL)

PZ: Don't reuse entry objects in iterators (PZ\_DONT\_REUSE\_ENTRY\_OBJECTS\_IN\_ITERATORS)

DMI: Adding elements of an entry set may fail due to reuse of Entry objects (DMI\_ENTRY\_SETS\_MAY\_REUSE\_ENTRY\_OBJECTS)

DMI: Don't use removeAll to clear a collection (DMI\_USING\_REMOVEALL\_TO\_CLEAR\_COLLECTION)

### 2.17.2 Correctness (CORRECTNESS)

Probable bug - an apparent coding mistake resulting in code that was probably not what the developer intended. We strive for a low false positive rate.

CN: Super method is annotated with `@OverridingMethodsMustInvokeSuper`, but the overriding method isn't calling the super method. (OVERRIDING\_METHODS\_MUST\_INVOKE\_SUPER)

NP: Method with Optional return type returns explicit null (NP\_OPTIONAL\_RETURN\_NULL)

NP: Non-null field is not initialized (NP\_NONNULL\_FIELD\_NOT\_INITIALIZED\_IN\_CONSTRUCTOR)

VR: Class makes reference to unresolvable class or method (VR\_UNRESOLVABLE\_REFERENCE)

IL: An apparent infinite loop (IL\_INFINITE\_LOOP)

IO: Doomed attempt to append to an object output stream (IO\_APPENDING\_TO\_OBJECT\_OUTPUT\_STREAM)

IL: An apparent infinite recursive loop (IL\_INFINITE\_RECURSIVE\_LOOP)

IL: A collection is added to itself (IL\_CONTAINER\_ADDED\_TO\_ITSELF)

RpC: Repeated conditional tests (RpC\_REPEATED\_CONDITIONAL\_TEST)

FL: Method performs math using floating point precision (FL\_MATH\_USING\_FLOAT\_PRECISION)

CAA: Possibly incompatible element is stored in covariant array (CAA\_COVARIANT\_ARRAY\_ELEMENT\_STORE)

Dm: Useless/vacuous call to EasyMock method (DMI\_VACUOUS\_CALL\_TO\_EASYMOCK\_METHOD)

Dm: Futile attempt to change max pool size of ScheduledThreadPoolExecutor (DMI\_FUTILE\_ATTEMPT\_TO\_CHANGE\_MAXPOOL\_SIZE\_OF\_SCHEDULED\_THREAD\_POOL\_EXECUTOR)

DMI: BigDecimal constructed from double that isn't represented precisely (DMI\_BIGDECIMAL\_CONSTRUCTED\_FROM\_DOUBLE)

Dm: Creation of ScheduledThreadPoolExecutor with zero core threads (DMI\_SCHEDULED\_THREAD\_POOL\_EXECUTOR\_WITH\_ZERO\_CORE\_THREADS)

Dm: Can't use reflection to check for presence of annotation without runtime retention (DMI\_ANNOTATION\_IS\_NOT\_VISIBLE\_TO\_REFLECTION)

NP: Method does not check for null argument (NP\_ARGUMENT\_MIGHT\_BE\_NULL)

RV: Bad attempt to compute absolute value of signed random integer (RV\_ABSOLUTE\_VALUE\_OF\_RANDOM\_INT)

RV: Bad attempt to compute absolute value of signed 32-bit hashCode (RV\_ABSOLUTE\_VALUE\_OF\_HASHCODE)

RV: Random value from 0 to 1 is coerced to the integer 0 (RV\_01\_TO\_INT)

Dm: Incorrect combination of Math.max and Math.min (DM\_INVALID\_MIN\_MAX)

**Eq:** equals method compares class names rather than class objects (EQ\_COMPARING\_CLASS\_NAMES)

**Eq:** equals method always returns true (EQ\_ALWAYS\_TRUE)

**Eq:** equals method always returns false (EQ\_ALWAYS\_FALSE)

**Eq:** equals method overrides equals in superclass and may not be symmetric (EQ\_OVERRIDING\_EQUALS\_NOT\_SYMMETRIC)

**Eq:** Covariant equals() method defined for enum (EQ\_DONT\_DEFINE\_EQUALS\_FOR\_ENUM)

**Eq:** Covariant equals() method defined, Object.equals(Object) inherited (EQ\_SELF\_USE\_OBJECT)

**Eq:** equals() method defined that doesn't override Object.equals(Object) (EQ\_OTHER\_USE\_OBJECT)

**Eq:** equals() method defined that doesn't override equals(Object) (EQ\_OTHER\_NO\_OBJECT)

**HE:** Signature declares use of unhashable class in hashed construct (HE\_SIGNATURE\_DECLARES\_HASHING\_OF\_UNHASHABLE\_CLASS)

**HE:** Use of class without a hashCode() method in a hashed data structure (HE\_USE\_OF\_UNHASHABLE\_CLASS)

**UR:** Uninitialized read of field in constructor (UR\_UNINIT\_READ)

**UR:** Uninitialized read of field method called from constructor of superclass (UR\_UNINIT\_READ\_CALLED\_FROM\_SUPER\_CONSTRUCTOR)

**Nm:** Very confusing method names (NM\_VERY\_CONFUSING)

**Nm:** Method doesn't override method in superclass due to wrong package for parameter (NM\_WRONG\_PACKAGE)

**Nm:** Apparent method/constructor confusion (NM\_METHOD\_CONSTRUCTOR\_CONFUSION)

**Nm:** Class defines hashCode(); should it be hashCode()? (NM\_LCASE\_HASHCODE)

**Nm:** Class defines toString(); should it be toString()? (NM\_LCASE\_TOSTRING)

**Nm:** Class defines equal(Object); should it be equals(Object)? (NM\_BAD\_EQUAL)

**Se:** The readResolve method must not be declared as a static method. (SE\_READ\_RESOLVE\_IS\_STATIC)

**Se:** Method must be private in order for serialization to work (SE\_METHOD\_MUST\_BE\_PRIVATE)

**SF:** Dead store due to switch statement fall through (SF\_DEAD\_STORE\_DUE\_TO\_SWITCH\_FALLTHROUGH)

**SF:** Dead store due to switch statement fall through to throw (SF\_DEAD\_STORE\_DUE\_TO\_SWITCH\_FALLTHROUGH\_TO\_THROW)

NP: Read of unwritten field (NP\_UNWRITTEN\_FIELD)

UwF: Field only ever set to null (UWF\_NULL\_FIELD)

UwF: Unwritten field (UWF\_UNWRITTEN\_FIELD)

SIC: Deadly embrace of non-static inner class and thread local (SIC\_THREADLOCAL\_DEADLY\_EMBRACE)

RANGE: Array index is out of bounds (RANGE\_ARRAY\_INDEX)

RANGE: Array offset is out of bounds (RANGE\_ARRAY\_OFFSET)

RANGE: Array length is out of bounds (RANGE\_ARRAY\_LENGTH)

RANGE: String index is out of bounds (RANGE\_STRING\_INDEX)

RV: Method ignores return value (RV\_RETURN\_VALUE\_IGNORED)

RV: Exception created and dropped rather than thrown (RV\_EXCEPTION\_NOT\_THROWN)

RV: Code checks for specific values returned by compareTo (RV\_CHECK\_COMPARETO\_FOR\_SPECIFIC\_RETURN\_VALUE)

NP: Null pointer dereference (NP\_ALWAYS\_NULL)

NP: close() invoked on a value that is always null (NP\_CLOSING\_NULL)

NP: Store of null value into field annotated @Nonnull (NP\_STORE\_INTO\_NONNULL\_FIELD)

NP: Null pointer dereference in method on exception path (NP\_ALWAYS\_NULL\_EXCEPTION)

NP: Possible null pointer dereference (NP\_NULL\_ON\_SOME\_PATH)

NP: Possible null pointer dereference in method on exception path (NP\_NULL\_ON\_SOME\_PATH\_EXCEPTION)

NP: Method call passes null for non-null parameter (NP\_NULL\_PARAM\_DEREF)

NP: Non-virtual method call passes null for non-null parameter (NP\_NULL\_PARAM\_DEREF\_NONVIRTUAL)

NP: Method call passes null for non-null parameter (NP\_NULL\_PARAM\_DEREF\_ALL\_TARGETS\_DANGEROUS)

NP: Method call passes null to a non-null parameter (NP\_NONNULL\_PARAM\_VIOLATION)

NP: Method may return null, but is declared @Nonnull (NP\_NONNULL\_RETURN\_VIOLATION)

NP: Null value is guaranteed to be dereferenced (NP\_GUARANTEED\_DEREF)

NP: Value is null and guaranteed to be dereferenced on exception path (NP\_GUARANTEED\_DEREF\_ON\_EXCEPTION\_PATH)

DMI: Reversed method arguments (DMI\_ARGUMENTS\_WRONG\_ORDER)

RCN: Nullcheck of value previously dereferenced (RCN\_REDUNDANT\_NULLCHECK\_WOULD\_HAVE\_BEEN\_A\_NPE)

RC: Suspicious reference comparison (RC\_REF\_COMPARISON)

VA: Primitive array passed to function expecting a variable number of object arguments (VA\_PRIMITIVE\_ARRAY\_PASSED\_TO\_OBJECT\_VARARG)

EC: Using pointer equality to compare different types (EC\_UNRELATED\_TYPES\_USING\_POINTER\_EQUALITY)

EC: Call to equals() comparing different types (EC\_UNRELATED\_TYPES)

EC: equals() used to compare array and nonarray (EC\_ARRAY\_AND\_NONARRAY)

EC: Call to equals(null) (EC\_NULL\_ARG)

EC: Call to equals() comparing different interface types (EC\_UNRELATED\_INTERFACES)

EC: Call to equals() comparing unrelated class and interface (EC\_UNRELATED\_CLASS\_AND\_INTERFACE)

SA: Self assignment of local rather than assignment to field (SA\_LOCAL\_SELF\_ASSIGNMENT\_INSTEAD\_OF\_FIELD)

INT: Bad comparison of int value with long constant (INT\_BAD\_COMPARISON\_WITH\_INT\_VALUE)

INT: Bad comparison of signed byte (INT\_BAD\_COMPARISON\_WITH\_SIGNED\_BYTE)

INT: Bad comparison of nonnegative value with negative constant or zero (INT\_BAD\_COMPARISON\_WITH\_NONNEGATIVE\_VALUE)

BIT: Bitwise add of signed byte value (BIT\_ADD\_OF\_SIGNED\_BYTE)

BIT: Bitwise OR of signed byte value (BIT\_IOR\_OF\_SIGNED\_BYTE)

BIT: Check for sign of bitwise operation involving negative number (BIT\_SIGNED\_CHECK\_HIGH\_BIT)

BIT: Incompatible bit masks (BIT\_AND)

BIT: Check to see if ((...) & 0) == 0 (BIT\_AND\_ZZ)

BIT: Incompatible bit masks (BIT\_IOR)

SA: Self assignment of field (SA\_FIELD\_SELF\_ASSIGNMENT)

SA: Nonsensical self computation involving a field (e.g., x & x) (SA\_FIELD\_SELF\_COMPUTATION)

SA: Nonsensical self computation involving a variable (e.g., x & x) (SA\_LOCAL\_SELF\_COMPUTATION)

SA: Self comparison of field with itself (SA\_FIELD\_SELF\_COMPARISON)

SA: Self comparison of value with itself (SA\_LOCAL\_SELF\_COMPARISON)

UMAC: Uncallible method defined in anonymous class (UMAC\_UNCALLABLE\_METHOD\_OF\_ANONYMOUS\_CLASS)

IJU: JUnit assertion in run method will not be noticed by JUnit (IJU\_ASSERT\_METHOD\_INVOKED\_FROM\_RUN\_METHOD)

IJU: TestCase declares a bad suite method (IJU\_BAD\_SUITE\_METHOD)

IJU: TestCase defines setUp that doesn't call super.setUp() (IJU\_SETUP\_NO\_SUPER)

IJU: TestCase defines tearDown that doesn't call super.tearDown() (IJU\_TEARDOWN\_NO\_SUPER)

IJU: TestCase implements a non-static suite method (IJU\_SUITE\_NOT\_STATIC)

IJU: TestCase has no tests (IJU\_NO\_TESTS)

BOA: Class overrides a method implemented in super class Adapter wrongly (BOA\_BADLY\_OVERRIDDEN\_ADAPTER)

SQL: Method attempts to access a result set field with index 0 (SQL\_BAD\_RESULTSET\_ACCESS)

SQL: Method attempts to access a prepared statement parameter with index 0 (SQL\_BAD\_PREPARED\_STATEMENT\_ACCESS)

SIO: Unnecessary type check done using instanceof operator (SIO\_SUPERFLUOUS\_INSTANCEOF)

BAC: Bad Applet Constructor relies on uninitialized AppletStub (BAC\_BAD\_APPLET\_CONSTRUCTOR)

EC: equals(...) used to compare incompatible arrays (EC\_INCOMPATIBLE\_ARRAY\_COMPARE)

EC: Invocation of equals() on an array, which is equivalent to == (EC\_BAD\_ARRAY\_COMPARE)

STI: Unneeded use of currentThread() call, to call interrupted() (STI\_INTERRUPTED\_ON\_CURRENTTHREAD)

STI: Static Thread.interrupted() method invoked on thread instance (STI\_INTERRUPTED\_ON\_UNKNOWNTHREAD)

DLS: Useless increment in return statement (DLS\_DEAD\_LOCAL\_INCREMENT\_IN\_RETURN)

DLS: Dead store of class literal (DLS\_DEAD\_STORE\_OF\_CLASS\_LITERAL)

IP: A parameter is dead upon entry to a method but overwritten (IP\_PARAMETER\_IS\_DEAD\_BUT\_OVERWRITTEN)

MF: Method defines a variable that obscures a field (MF\_METHOD\_MASKS\_FIELD)

MF: Class defines field that masks a superclass field (MF\_CLASS\_MASKS\_FIELD)

FE: Doomed test for equality to NaN (FE\_TEST\_IF\_EQUAL\_TO\_NOT\_A\_NUMBER)

ICAST: int value converted to long and used as absolute time (ICAST\_INT\_2\_LONG\_AS\_INSTANT)

ICAST: Integral value cast to double and then passed to Math.ceil (ICAST\_INT\_CAST\_TO\_DOUBLE\_PASSED\_TO\_CEIL)

ICAST: int value cast to float and then passed to Math.round (ICAST\_INT\_CAST\_TO\_FLOAT\_PASSED\_TO\_ROUND)

NP: A known null value is checked to see if it is an instance of a type (NP\_NULL\_INSTANCEOF)

DMI: Double.longBitsToDouble invoked on an int (DMI\_LONG\_BITS\_TO\_DOUBLE\_INVOKED\_ON\_INT)

BC: Impossible cast (BC\_IMPOSSIBLE\_CAST)

BC: Impossible downcast (BC\_IMPOSSIBLE\_DOWNCAST)

BC: Impossible downcast of toArray() result (BC\_IMPOSSIBLE\_DOWNCAST\_OF\_TOARRAY)

BC: instanceof will always return false (BC\_IMPOSSIBLE\_INSTANCEOF)

RE: "." or "|" used for regular expression (RE\_POSSIBLE\_UNINTENDED\_PATTERN)

RE: Invalid syntax for regular expression (RE\_BAD\_SYNTAX\_FOR\_REGULAR\_EXPRESSION)

RE: File.separator used for regular expression (RE\_CANT\_USE\_FILE\_SEPARATOR\_AS\_REGULAR\_EXPRESSION)

DLS: Overwritten increment (DLS\_OVERWRITTEN\_INCREMENT)

BSHIFT: 32 bit int shifted by an amount not in the range -31..31 (ICAST\_BAD\_SHIFT\_AMOUNT)

BSHIFT: Possible bad parsing of shift operation (BSHIFT\_WRONG\_ADD\_PRIORITY)

IM: Integer multiply of result of integer remainder (IM\_MULTIPLYING\_RESULT\_OF\_IREM)

DMI: Invocation of hashCode on an array (DMI\_INVOKING\_HASHCODE\_ON\_ARRAY)

USELESS\_STRING: Invocation of toString on an array (DMI\_INVOKING\_TOSTRING\_ON\_ARRAY)

USELESS\_STRING: Invocation of toString on an unnamed array (DMI\_INVOKING\_TOSTRING\_ON\_ANONYMOUS\_ARRAY)

DMI: Bad constant value for month (DMI\_BAD\_MONTH)

DMI: hasNext method invokes next (DMI\_CALLING\_NEXT\_FROM\_HASNEXT)

QBA: Method assigns boolean literal in boolean expression (QBA\_QUESTIONABLE\_BOOLEAN\_ASSIGNMENT)

GC: No relationship between generic parameter and method argument (GC\_UNRELATED\_TYPES)

DMI: Vacuous call to collections (DMI\_VACUOUS\_SELF\_COLLECTION\_CALL)

**DMI: D'oh! A nonsensical method invocation (DMI\_DOH)**

**DMI: Collections should not contain themselves (DMI\_COLLECTIONS\_SHOULD\_NOT\_CONTAIN\_THEMSELVES)**

**TQ: Value without a type qualifier used where a value is required to have that qualifier (TQ\_UNKNOWN\_VALUE\_USED\_WHERE\_ALWAYS\_STRICTLY\_REQUIRED)**

**TQ: Comparing values with incompatible type qualifiers (TQ\_COMPARING\_VALUES\_WITH\_INCOMPATIBLE\_TYPE\_QUALIFIERS)**

**TQ: Value annotated as carrying a type qualifier used where a value that must not carry that qualifier is required (TQ\_ALWAYS\_VALUE\_USED\_WHERE\_NEVER\_REQUIRED)**

**TQ: Value annotated as never carrying a type qualifier used where value carrying that qualifier is required (TQ\_NEVER\_VALUE\_USED\_WHERE\_ALWAYS\_REQUIRED)**

**TQ: Value that might not carry a type qualifier is always used in a way requires that type qualifier (TQ\_MAYBE\_SOURCE\_VALUE\_REACHES\_ALWAYS\_SINK)**

**TQ: Value that might carry a type qualifier is always used in a way prohibits it from having that type qualifier (TQ\_MAYBE\_SOURCE\_VALUE\_REACHES\_NEVER\_SINK)**

**FB: Unexpected/undesired warning from SpotBugs (FB\_UNEXPECTED\_WARNING)**

**FB: Missing expected or desired warning from SpotBugs (FB\_MISSING\_EXPECTED\_WARNING)**

### 2.17.3 Experimental (EXPERIMENTAL)

Experimental and not fully vetted bug patterns

**SKIPPED: Class too big for analysis (SKIPPED\_CLASS\_TOO\_BIG)**

**TEST: Unknown bug pattern (UNKNOWN)**

**TEST: Testing (TESTING)**

**TEST: Testing 1 (TESTING1)**

**TEST: Testing 2 (TESTING2)**

**TEST: Testing 3 (TESTING3)**

**OBL: Method may fail to clean up stream or resource (OBL\_UNSATISFIED\_OBLIGATION)**

**OBL: Method may fail to clean up stream or resource on checked exception (OBL\_UNSATISFIED\_OBLIGATION\_EXCEPTION\_EDGE)**

**LG: Potential lost logger changes due to weak reference in OpenJDK (LG\_LOST\_LOGGER\_DUE\_TO\_WEAK\_REFERENCE)**

### 2.17.4 Internationalization (I18N)

code flaws having to do with internationalization and locale

Dm: Consider using Locale parameterized version of invoked method (DM\_CONVERT\_CASE)

Dm: Reliance on default encoding (DM\_DEFAULT\_ENCODING)

### 2.17.5 Malicious code vulnerability (MALICIOUS\_CODE)

code that is vulnerable to attacks from untrusted code

DP: Method invoked that should be only be invoked inside a doPrivileged block (DP\_DO\_INSIDE\_DO\_PRIVILEGED)

DP: Classloaders should only be created inside doPrivileged block (DP\_CREATE\_CLASSLOADER\_INSIDE\_DO\_PRIVILEGED)

FI: Finalizer should be protected, not public (FI\_PUBLIC\_SHOULD\_BE\_PROTECTED)

MS: Public static method may expose internal representation by returning array (MS\_EXPOSE\_REP)

EI: May expose internal representation by returning reference to mutable object (EI\_EXPOSE\_REP)

EI2: May expose internal representation by incorporating reference to mutable object (EI\_EXPOSE\_REP2)

MS: May expose internal static state by storing a mutable object into a static field (EI\_EXPOSE\_STATIC\_REP2)

MS: Field should be moved out of an interface and made package protected (MS\_OOI\_PKGPROTECT)

MS: Field should be both final and package protected (MS\_FINAL\_PKGPROTECT)

MS: Field isn't final but should be (MS\_SHOULD\_BE\_FINAL)

MS: Field isn't final but should be refactored to be so (MS\_SHOULD\_BE\_REFACTORED\_TO\_BE\_FINAL)

MS: Field should be package protected (MS\_PKGPROTECT)

MS: Field is a mutable Hashtable (MS\_MUTABLE\_HASHTABLE)

MS: Field is a mutable array (MS\_MUTABLE\_ARRAY)

MS: Field is a mutable collection (MS\_MUTABLE\_COLLECTION)

MS: Field is a mutable collection which should be package protected (MS\_MUTABLE\_COLLECTION\_PKGPROTECT)

MS: Field isn't final and can't be protected from malicious code (MS\_CANNOT\_BE\_FINAL)

### 2.17.6 Multithreaded correctness (MT\_CORRECTNESS)

code flaws having to do with threads, locks, and volatiles

**AT:** Sequence of calls to concurrent abstraction may not be atomic (AT\_OPERATION\_SEQUENCE\_ON\_CONCURRENT\_ABSTRACTION)

**STCAL:** Static Calendar field (STCAL\_STATIC\_CALENDAR\_INSTANCE)

**STCAL:** Static DateFormat (STCAL\_STATIC\_SIMPLE\_DATE\_FORMAT\_INSTANCE)

**STCAL:** Call to static Calendar (STCAL\_INVOKE\_ON\_STATIC\_CALENDAR\_INSTANCE)

**STCAL:** Call to static DateFormat (STCAL\_INVOKE\_ON\_STATIC\_DATE\_FORMAT\_INSTANCE)

**NP:** Synchronize and null check on the same field. (NP\_SYNC\_AND\_NULL\_CHECK\_FIELD)

**VO:** A volatile reference to an array doesn't treat the array elements as volatile (VO\_VOLATILE\_REFERENCE\_TO\_ARRAY)

**VO:** An increment to a volatile field isn't atomic (VO\_VOLATILE\_INCREMENT)

**Dm:** Monitor wait() called on Condition (DM\_MONITOR\_WAIT\_ON\_CONDITION)

**Dm:** A thread was created using the default empty run method (DM\_USELESS\_THREAD)

**DC:** Possible double check of field (DC\_DOUBLECHECK)

**DC:** Possible exposure of partially initialized object (DC\_PARTIALLY\_CONSTRUCTED)

**DL:** Synchronization on interned String (DL\_SYNCHRONIZATION\_ON\_SHARED\_CONSTANT)

**DL:** Synchronization on Boolean (DL\_SYNCHRONIZATION\_ON\_BOOLEAN)

**DL:** Synchronization on boxed primitive (DL\_SYNCHRONIZATION\_ON\_BOXED\_PRIMITIVE)

**DL:** Synchronization on boxed primitive values (DL\_SYNCHRONIZATION\_ON\_UNSHARED\_BOXED\_PRIMITIVE)

**WL:** Synchronization on getClass rather than class literal (WL\_USING\_GETCLASS\_RATHER\_THAN\_CLASS\_LITERAL)

**ESync:** Empty synchronized block (ESync\_EMPTY\_SYNC)

**MSF:** Mutable servlet field (MSF\_MUTABLE\_SERVLET\_FIELD)

**IS:** Inconsistent synchronization (IS2\_INCONSISTENT\_SYNC)

**NN:** Naked notify (NN\_NAKED\_NOTIFY)

**Ru:** Invokes run on a thread (did you mean to start it instead?) (RU\_INVOKE\_RUN)

**SP:** Method spins on field (SP\_SPIN\_ON\_FIELD)

**TLW:** Wait with two locks held (TLW\_TWO\_LOCK\_WAIT)

**UW:** Unconditional wait (UW\_UNCOND\_WAIT)

**UG:** Unsynchronized get method, synchronized set method (UG\_SYNC\_SET\_UNSYNC\_GET)

**IS:** Field not guarded against concurrent access (IS\_FIELD\_NOT\_GUARDED)

**ML:** Synchronization on field in futile attempt to guard that field (ML\_SYNC\_ON\_FIELD\_TO\_GUARD\_CHANGING\_THAT\_FIELD)

**ML:** Method synchronizes on an updated field (ML\_SYNC\_ON\_UPDATED\_FIELD)

**WS:** Class's writeObject() method is synchronized but nothing else is (WS\_WRITEOBJECT\_SYNC)

**RS:** Class's readObject() method is synchronized (RS\_READOBJECT\_SYNC)

**SC:** Constructor invokes Thread.start() (SC\_START\_IN\_CTOR)

**Wa:** Wait not in loop (WA\_NOT\_IN\_LOOP)

**Wa:** Condition.await() not in loop (WA\_AWAIT\_NOT\_IN\_LOOP)

**No:** Using notify() rather than notifyAll() (NO\_NOTIFY\_NOT\_NOTIFYALL)

**UL:** Method does not release lock on all paths (UL\_UNRELEASED\_LOCK)

**UL:** Method does not release lock on all exception paths (UL\_UNRELEASED\_LOCK\_EXCEPTION\_PATH)

**MWN:** Mismatched wait() (MWN\_MISMATCHED\_WAIT)

**MWN:** Mismatched notify() (MWN\_MISMATCHED\_NOTIFY)

**LI:** Incorrect lazy initialization of static field (LI\_LAZY\_INIT\_STATIC)

**LI:** Incorrect lazy initialization and update of static field (LI\_LAZY\_INIT\_UPDATE\_STATIC)

**JLM:** Synchronization performed on util.concurrent instance (JLM\_JSR166\_UTILCONCURRENT\_MONITORENTER)

**JLM:** Using monitor style wait methods on util.concurrent abstraction (JML\_JSR166\_CALLING\_WAIT\_RATHER\_THAN\_AWAIT)

**JLM:** Synchronization performed on Lock (JLM\_JSR166\_LOCK\_MONITORENTER)

**SWL:** Method calls Thread.sleep() with a lock held (SWL\_SLEEP\_WITH\_LOCK\_HELD)

**RV:** Return value of putIfAbsent ignored, value passed to putIfAbsent reused (RV\_RETURN\_VALUE\_OF\_PUTIFABSENT\_IGNORED)

### 2.17.7 Bogus random noise (NOISE)

Bogus random noise: intended to be useful as a control in data mining experiments, not in finding actual bugs in software

**NOISE: Bogus warning about a null pointer dereference (NOISE\_NULL\_DEREFERENCE)**

**NOISE: Bogus warning about a method call (NOISE\_METHOD\_CALL)**

**NOISE: Bogus warning about a field reference (NOISE\_FIELD\_REFERENCE)**

**NOISE: Bogus warning about an operation (NOISE\_OPERATION)**

## 2.17.8 Performance (PERFORMANCE)

code that is not necessarily incorrect but may be inefficient

**HSC: Huge string constants is duplicated across multiple class files (HSC\_HUGE\_SHARED\_STRING\_CONSTANT)**

**Dm: The equals and hashCode methods of URL are blocking (DMI\_BLOCKING\_METHODS\_ON\_URL)**

**Dm: Maps and sets of URLs can be performance hogs (DMI\_COLLECTION\_OF\_URLS)**

**Dm: Method invokes inefficient new String(String) constructor (DM\_STRING\_CTOR)**

**Dm: Method invokes inefficient new String() constructor (DM\_STRING\_VOID\_CTOR)**

**Dm: Method invokes toString() method on a String (DM\_STRING\_TOSTRING)**

**Dm: Explicit garbage collection; extremely dubious except in benchmarking code (DM\_GC)**

**Dm: Method invokes inefficient Boolean constructor; use Boolean.valueOf(...) instead (DM\_BOOLEAN\_CTOR)**

**Bx: Method invokes inefficient Number constructor; use static valueOf instead (DM\_NUMBER\_CTOR)**

**Bx: Method invokes inefficient floating-point Number constructor; use static valueOf instead (DM\_FP\_NUMBER\_CTOR)**

**Bx: Method allocates a boxed primitive just to call toString (DM\_BOXED\_PRIMITIVE\_TOSTRING)**

**Bx: Boxing/unboxing to parse a primitive (DM\_BOXED\_PRIMITIVE\_FOR\_PARSING)**

**Bx: Boxing a primitive to compare (DM\_BOXED\_PRIMITIVE\_FOR\_COMPARE)**

**Bx: Primitive value is unboxed and coerced for ternary operator (BX\_UNBOXED\_AND\_COERCED\_FOR\_TERNARY\_OPERATOR)**

**Bx: Boxed value is unboxed and then immediately reboxed (BX\_UNBOXING\_IMMEDIATELY\_REBOXED)**

**Bx: Primitive value is boxed and then immediately unboxed (BX\_BOXING\_IMMEDIATELY\_UNBOXED)**

**Bx:** Primitive value is boxed then unboxed to perform primitive coercion (BX\_BOXING\_IMMEDIATELY\_UNBOXED\_TO\_PERFORM\_COERCION)

**Dm:** Method allocates an object, only to get the class object (DM\_NEW\_FOR\_GETCLASS)

**Dm:** Use the nextInt method of Random rather than nextDouble to generate a random integer (DM\_NEXTINT\_VIA\_NEXTDOUBLE)

**SS:** Unread field: should this field be static? (SS\_SHOULD\_BE\_STATIC)

**UuF:** Unused field (UUF\_UNUSED\_FIELD)

**UrF:** Unread field (URF\_UNREAD\_FIELD)

**SIC:** Should be a static inner class (SIC\_INNER\_SHOULD\_BE\_STATIC)

**SIC:** Could be refactored into a static inner class (SIC\_INNER\_SHOULD\_BE\_STATIC\_NEEDS\_THIS)

**SIC:** Could be refactored into a named static inner class (SIC\_INNER\_SHOULD\_BE\_STATIC\_ANON)

**UPM:** Private method is never called (UPM\_UNCALLED\_PRIVATE\_METHOD)

**SBSC:** Method concatenates strings using + in a loop (SBSC\_USE\_STRINGBUFFER\_CONCATENATION)

**IIL:** NodeList.getLength() called in a loop (IIL\_ELEMENTS\_GET\_LENGTH\_IN\_LOOP)

**IIL:** Method calls prepareStatement in a loop (IIL\_PREPARE\_STATEMENT\_IN\_LOOP)

**IIL:** Method calls Pattern.compile in a loop (IIL\_PATTERN\_COMPILE\_IN\_LOOP)

**IIL:** Method compiles the regular expression in a loop (IIL\_PATTERN\_COMPILE\_IN\_LOOP\_INDIRECT)

**IIO:** Inefficient use of String.indexOf(String) (IIO\_INEFFICIENT\_INDEX\_OF)

**IIO:** Inefficient use of String.lastIndexOf(String) (IIO\_INEFFICIENT\_LAST\_INDEX\_OF)

**ITA:** Method uses toArray() with zero-length array argument (ITA\_INEFFICIENT\_TO\_ARRAY)

**WMI:** Inefficient use of keySet iterator instead of entrySet iterator (WMI\_WRONG\_MAP\_ITERATOR)

**UM:** Method calls static Math class method on a constant value (UM\_UNNECESSARY\_MATH)

**IMA:** Method accesses a private member variable of owning class (IMA\_INEFFICIENT\_MEMBER\_ACCESS)

## 2.17.9 Security (SECURITY)

A use of untrusted input in a way that could create a remotely exploitable security vulnerability.

XSS: Servlet reflected cross site scripting vulnerability in error page (XSS\_REQUEST\_PARAMETER\_TO\_SEND\_ERROR)

XSS: Servlet reflected cross site scripting vulnerability (XSS\_REQUEST\_PARAMETER\_TO\_SERVLET\_WRITER)

XSS: JSP reflected cross site scripting vulnerability (XSS\_REQUEST\_PARAMETER\_TO\_JSP\_WRITER)

HRS: HTTP Response splitting vulnerability (HRS\_REQUEST\_PARAMETER\_TO\_HTTP\_HEADER)

HRS: HTTP cookie formed from untrusted input (HRS\_REQUEST\_PARAMETER\_TO\_COOKIE)

PT: Absolute path traversal in servlet (PT\_ABSOLUTE\_PATH\_TRAVERSAL)

PT: Relative path traversal in servlet (PT\_RELATIVE\_PATH\_TRAVERSAL)

Dm: Hardcoded constant database password (DMI\_CONSTANT\_DB\_PASSWORD)

Dm: Empty database password (DMI\_EMPTY\_DB\_PASSWORD)

SQL: Nonconstant string passed to execute or addBatch method on an SQL statement (SQL\_NONCONSTANT\_STRING\_PASSED\_TO\_EXECUTE)

SQL: A prepared statement is generated from a nonconstant String (SQL\_PREPARED\_STATEMENT\_GENERATED\_FROM\_NONCONSTANT\_STRING)

### 2.17.10 Dodgy code (STYLE)

code that is confusing, anomalous, or written in a way that leads itself to errors. Examples include dead local stores, switch fall through, unconfirmed casts, and redundant null check of value known to be null. More false positives accepted. In previous versions of SpotBugs, this category was known as Style.

CAA: Covariant array assignment to a field (CAA\_COVARIANT\_ARRAY\_FIELD)

CAA: Covariant array is returned from the method (CAA\_COVARIANT\_ARRAY\_RETURN)

CAA: Covariant array assignment to a local variable (CAA\_COVARIANT\_ARRAY\_LOCAL)

Dm: Call to unsupported method (DMI\_UNSUPPORTED\_METHOD)

Dm: Thread passed where Runnable expected (DMI\_THREAD\_PASSED\_WHERE\_RUNNABLE\_EXPECTED)

NP: Dereference of the result of readLine() without nullcheck (NP\_DEREFERENCE\_OF\_READLINE\_VALUE)

NP: Immediate dereference of the result of readLine() (NP\_IMMEDIATE\_DEREFERENCE\_OF\_READLINE)

RV: Remainder of 32-bit signed random integer (RV\_REM\_OF\_RANDOM\_INT)

RV: Remainder of hashCode could be negative (RV\_REM\_OF\_HASHCODE)

Eq: Unusual equals method (EQ\_UNUSUAL)

Eq: Class doesn't override equals in superclass (EQ\_DOESNT\_OVERRIDE\_EQUALS)

NS: Questionable use of non-short-circuit logic (NS\_NON\_SHORT\_CIRCUIT)

NS: Potentially dangerous use of non-short-circuit logic (NS\_DANGEROUS\_NON\_SHORT\_CIRCUIT)

IC: Initialization circularity (IC\_INIT\_CIRCULARITY)

IA: Potentially ambiguous invocation of either an inherited or outer method (IA\_AMBIGUOUS\_INVOCATION\_OF\_INHERITED\_OR\_OUTER\_METHOD)

Se: Private readResolve method not inherited by subclasses (SE\_PRIVATE\_READ\_RESOLVE\_NOT\_INHERITED)

Se: Transient field of class that isn't Serializable. (SE\_TRANSIENT\_FIELD\_OF\_NONSERIALIZABLE\_CLASS)

SF: Switch statement found where one case falls through to the next case (SF\_SWITCH\_FALLTHROUGH)

SF: Switch statement found where default case is missing (SF\_SWITCH\_NO\_DEFAULT)

UuF: Unused public or protected field (UUF\_UNUSED\_PUBLIC\_OR\_PROTECTED\_FIELD)

Urf: Unread public/protected field (URF\_UNREAD\_PUBLIC\_OR\_PROTECTED\_FIELD)

QF: Complicated, subtle or wrong increment in for-loop (QF\_QUESTIONABLE\_FOR\_LOOP)

NP: Read of unwritten public or protected field (NP\_UNWRITTEN\_PUBLIC\_OR\_PROTECTED\_FIELD)

UwF: Field not initialized in constructor but dereferenced without null check (UWF\_FIELD\_NOT\_INITIALIZED\_IN\_CONSTRUCTOR)

UwF: Unwritten public or protected field (UWF\_UNWRITTEN\_PUBLIC\_OR\_PROTECTED\_FIELD)

UC: Useless non-empty void method (UC\_USELESS\_VOID\_METHOD)

UC: Condition has no effect (UC\_USELESS\_CONDITION)

UC: Condition has no effect due to the variable type (UC\_USELESS\_CONDITION\_TYPE)

UC: Useless object created (UC\_USELESS\_OBJECT)

UC: Useless object created on stack (UC\_USELESS\_OBJECT\_STACK)

RV: Method ignores return value, is this OK? (RV\_RETURN\_VALUE\_IGNORED\_INFERRED)

RV: Return value of method without side effect is ignored (RV\_RETURN\_VALUE\_IGNORED\_NO\_SIDE\_EFFECT)

RV: Method checks to see if result of String.indexOf is positive (RV\_CHECK\_FOR\_POSITIVE\_INDEXOF)

RV: Method discards result of readLine after checking if it is non-null (RV\_DONT\_JUST\_NULL\_CHECK\_READLINE)

NP: Parameter must be non-null but is marked as nullable (NP\_PARAMETER\_MUST\_BE\_NONNULL\_BUT\_MARKED\_NULLABLE)

NP: Possible null pointer dereference due to return value of called method (NP\_NULL\_ON\_SOME\_PATH\_FROM\_RETURN\_VALUE)

NP: Possible null pointer dereference on branch that might be infeasible (NP\_NULL\_ON\_SOME\_PATH\_MIGHT\_BE\_INFEASIBLE)

NP: Load of known null value (NP\_LOAD\_OF\_KNOWN\_NULL\_VALUE)

PZLA: Consider returning a zero length array rather than null (PZLA\_PREFER\_ZERO\_LENGTH\_ARRAYS)

UCF: Useless control flow (UCF\_USELESS\_CONTROL\_FLOW)

UCF: Useless control flow to next line (UCF\_USELESS\_CONTROL\_FLOW\_NEXT\_LINE)

RCN: Redundant nullcheck of value known to be null (RCN\_REDUNDANT\_NULLCHECK\_OF\_NULL\_VALUE)

RCN: Redundant nullcheck of value known to be non-null (RCN\_REDUNDANT\_NULLCHECK\_OF\_NONNULL\_VALUE)

RCN: Redundant comparison of two null values (RCN\_REDUNDANT\_COMPARISON\_TWO\_NULL\_VALUES)

RCN: Redundant comparison of non-null value to null (RCN\_REDUNDANT\_COMPARISON\_OF\_NULL\_AND\_NONNULL\_VALUE)

SA: Self assignment of local variable (SA\_LOCAL\_SELF\_ASSIGNMENT)

INT: Integer remainder modulo 1 (INT\_BAD\_REM\_BY\_1)

INT: Vacuous comparison of integer value (INT\_VACUOUS\_COMPARISON)

INT: Vacuous bit mask operation on integer value (INT\_VACUOUS\_BIT\_OPERATION)

SA: Double assignment of local variable (SA\_LOCAL\_DOUBLE\_ASSIGNMENT)

SA: Double assignment of field (SA\_FIELD\_DOUBLE\_ASSIGNMENT)

DLS: Useless assignment in return statement (DLS\_DEAD\_LOCAL\_STORE\_IN\_RETURN)

DLS: Dead store to local variable (DLS\_DEAD\_LOCAL\_STORE)

DLS: Dead store to local variable that shadows field (DLS\_DEAD\_LOCAL\_STORE\_SHADOWS\_FIELD)

DLS: Dead store of null to local variable (DLS\_DEAD\_LOCAL\_STORE\_OF\_NULL)

REC: Exception is caught when Exception is not thrown (REC\_CATCH\_EXCEPTION)

FE: Test for floating point equality (FE\_FLOATING\_POINT\_EQUALITY)

CD: Test for circular dependencies among classes (CD\_CIRCULAR\_DEPENDENCY)

RI: Class implements same interface as superclass (RI\_REDUNDANT\_INTERFACES)

MTIA: Class extends Struts Action class and uses instance variables (MTIA\_SUSPECT\_STRUTS\_INSTANCE\_FIELD)

MTIA: Class extends Servlet class and uses instance variables (MTIA\_SUSPECT\_SERVLET\_INSTANCE\_FIELD)

PS: Class exposes synchronization and semaphores in its public interface (PS\_PUBLIC\_SEMAPHORES)

ICAST: Result of integer multiplication cast to long (ICAST\_INTEGER\_MULTIPLY\_CAST\_TO\_LONG)

ICAST: Integral division result cast to double or float (ICAST\_IDIV\_CAST\_TO\_DOUBLE)

BC: Questionable cast to concrete collection (BC\_BAD\_CAST\_TO\_CONCRETE\_COLLECTION)

BC: Unchecked/unconfirmed cast (BC\_UNCONFIRMED\_CAST)

BC: Unchecked/unconfirmed cast of return value from method (BC\_UNCONFIRMED\_CAST\_OF\_RETURN\_VALUE)

BC: instanceof will always return true (BC\_VACUOUS\_INSTANCEOF)

BC: Questionable cast to abstract collection (BC\_BAD\_CAST\_TO\_ABSTRACT\_COLLECTION)

IM: Check for oddness that won't work for negative numbers (IM\_BAD\_CHECK\_FOR\_ODD)

IM: Computation of average could overflow (IM\_AVERAGE\_COMPUTATION\_COULD\_OVERFLOW)

BSHIFT: Unsigned right shift cast to short/byte (ICAST\_QUESTIONABLE\_UNSIGNED\_RIGHT\_SHIFT)

DMI: Code contains a hard coded reference to an absolute pathname (DMI\_HARDCODED\_ABSOLUTE\_FILENAME)

DMI: Invocation of substring(0), which returns the original value (DMI\_USELESS\_SUBSTRING)

ST: Write to static field from instance method (ST\_WRITE\_TO\_STATIC\_FROM\_INSTANCE\_METHOD)

DMI: Non serializable object written to ObjectOutputStream (DMI\_NONSERIALIZABLE\_OBJECT\_WRITTEN)

DB: Method uses the same code for two branches (DB\_DUPLICATE\_BRANCHES)

DB: Method uses the same code for two switch clauses (DB\_DUPLICATE\_SWITCH\_CLAUSES)

XFB: Method directly allocates a specific implementation of xml interfaces (XFB\_XML\_FACTORY\_BYPASS)

USM: Method superfluously delegates to parent class method (USM\_USELESS\_SUBCLASS\_METHOD)

USM: Abstract Method is already defined in implemented interface (USM\_USELESS\_ABSTRACT\_METHOD)

CI: Class is final but declares protected field (CI\_CONFUSED\_INHERITANCE)

TQ: Value required to not have type qualifier, but marked as unknown (TQ\_EXPLICIT\_UNKNOWN\_SOURCE\_VALUE\_REACHES\_NEVER\_SINK)

TQ: Value required to have type qualifier, but marked as unknown (TQ\_EXPLICIT\_UNKNOWN\_SOURCE\_VALUE\_REACHES\_ALWAYS\_SINK)

NP: Method relaxes nullness annotation on return value (NP\_METHOD\_RETURN\_RELAXING\_ANNOTATION)

NP: Method tightens nullness annotation on parameter (NP\_METHOD\_PARAMETER\_TIGHTENS\_ANNOTATION)

## 2.18 Guide for migration from SpotBugs 3.1 to 4.0

### 2.18.1 for SpotBugs Users

- SpotBugs now use SLF4J instead of calling STDERR/STDOUT directly. So when you run SpotBugs, it is recommended to have a SLF4J binding in classpath.
- SQL files in SpotBugs project are dropped. Generally it does not affect your usage.
- JNLP (Applet) support is dropped.

### 2.18.2 for Plugin Developers

- The *speed* attribute of *Detector* element in *findbugs.xml* is deprecated.
- The dependency on *jaxen* has been changed to *runtime* scope. Generally it does not affect your project because SpotBugs does not depend on it directly.
- The dependency on *Saxon-HE* has added as a *runtime* scope dependency.
- Some deprecated APIs have been removed, refer the javadoc and migrate to preferred API before you migrate to SpotBugs 4.0.

## 2.19 Guide for migration from FindBugs 3.0 to SpotBugs 3.1

### 2.19.1 com.google.code.findbugs:findbugs

Simply replace `com.google.code.findbugs:findbugs` with `com.github.spotbugs:spotbugs`.

```
<!-- for Maven -->
<dependency>
  <groupId>com.github.spotbugs</groupId>
  <artifactId>spotbugs</artifactId>
  <version>4.0.6</version>
</dependency>
```

```
// for Gradle
compile 'com.github.spotbugs:spotbugs:4.0.6'
```

## 2.19.2 com.google.code.findbugs:jsr305

JSR305 is already Dormant status, so SpotBugs does not release jsr305 jar file. Please continue using findbugs' one.

## 2.19.3 com.google.code.findbugs:findbugs-annotations

Please depend on spotbugs-annotations instead.

```
<!-- for Maven -->
<dependency>
  <groupId>com.github.spotbugs</groupId>
  <artifactId>spotbugs-annotations</artifactId>
  <version>4.0.6</version>
  <optional>true</optional>
</dependency>
```

```
// for Gradle
compileOnly 'com.github.spotbugs:spotbugs-annotations:4.0.6'
```

## 2.19.4 com.google.code.findbugs:annotations

Please depend on both of spotbugs-annotations and net.jcip:jcip-annotations:1.0 instead.

```
<!-- for Maven -->
<dependency>
  <groupId>net.jcip</groupId>
  <artifactId>jcip-annotations</artifactId>
  <version>1.0</version>
  <optional>true</optional>
</dependency>
<dependency>
  <groupId>com.github.spotbugs</groupId>
  <artifactId>spotbugs-annotations</artifactId>
  <version>4.0.6</version>
  <optional>true</optional>
</dependency>
```

```
// for Gradle
compileOnly 'net.jcip:jcip-annotations:1.0'
compileOnly 'com.github.spotbugs:spotbugs-annotations:4.0.6'
```

## 2.19.5 FindBugs Ant task

Please replace `findbugs-ant.jar` with `spotbugs-ant.jar`.

```
<taskdef
  resource="edu/umd/cs/findbugs/anttask/tasks.properties"
  classpath="path/to/spotbugs-ant.jar" />
<property name="spotbugs.home" value="/path/to/spotbugs/home" />

<target name="spotbugs" depends="jar">
  <spotbugs home="${spotbugs.home}"
    output="xml"
    outputFile="bcel-fb.xml" >
    <auxClasspath path="${basedir}/lib/Regex.jar" />
    <sourcePath path="${basedir}/src/java" />
    <class location="${basedir}/bin/bcel.jar" />
  </spotbugs>
</target>
```

## 2.19.6 FindBugs Maven plugin

Please use `com.github.spotbugs:spotbugs-maven-plugin` instead of `org.codehaus.mojo:findbugs-maven-plugin`.

```
<plugin>
  <groupId>com.github.spotbugs</groupId>
  <artifactId>spotbugs-maven-plugin</artifactId>
  <version>4.0.4</version>
  <dependencies>
    <!-- overwrite dependency on spotbugs if you want to specify the version of
    ↪ spotbugs -->
    <dependency>
      <groupId>com.github.spotbugs</groupId>
      <artifactId>spotbugs</artifactId>
      <version>4.0.6</version>
    </dependency>
  </dependencies>
</plugin>
```

## 2.19.7 FindBugs Gradle plugin

Please use spotbugs plugin found on <https://plugins.gradle.org/plugin/com.github.spotbugs>

```
plugins {
  id 'com.github.spotbugs' version '4.4.1'
}
spotbugs {
  toolVersion = '4.0.6'
}

// To generate an HTML report instead of XML
tasks.withType(com.github.spotbugs.snom.SpotBugsTask) {
  reports.xml.enabled = false
  reports.html.enabled = true
}
```

## 2.19.8 FindBugs Eclipse plugin

Please use following update site instead.

- <https://spotbugs.github.io/eclipse/> (to use stable version)
- <https://spotbugs.github.io/eclipse-candidate/> (to use candidate version)
- <https://spotbugs.github.io/eclipse-latest/> (to use latest build)

## 2.20 Annotations

SpotBugs supports several annotations to express the developer's intent so that SpotBugs can issue warnings more appropriately. Annotations for SpotBugs (mostly deprecated except for SuppressFBWarnings).

### 2.20.1 edu.umd.cs.findbugs.annotations.CheckForNull

The annotated element might be null, and uses of the element should check for null.

### 2.20.2 edu.umd.cs.findbugs.annotations.CheckReturnValue

This annotation is used to denote a method whose return value should always be checked when invoking the method.

### 2.20.3 edu.umd.cs.findbugs.annotations.CleanupObligation

Mark a class or interface as a resource type requiring cleanup.

### 2.20.4 edu.umd.cs.findbugs.annotations.CreatesObligation

Mark a constructor or method as creating a resource which requires cleanup.

### 2.20.5 edu.umd.cs.findbugs.annotations.DefaultAnnotation

Indicates that all members of the class or package should be annotated with the default value of the supplied annotation class.

### 2.20.6 edu.umd.cs.findbugs.annotations.DefaultAnnotationForFields

Indicates that all members of the class or package should be annotated with the default value of the supplied annotation class.

### **2.20.7 edu.umd.cs.findbugs.annotations.DefaultAnnotationForMethods**

Indicates that all members of the class or package should be annotated with the default value of the supplied annotation class.

### **2.20.8 edu.umd.cs.findbugs.annotations.DefaultAnnotationForParameters**

Indicates that all members of the class or package should be annotated with the default value of the supplied annotation class.

### **2.20.9 edu.umd.cs.findbugs.annotations.DesireNoWarning (Deprecated)**

The annotation based approach is useless for lambdas.

### **2.20.10 edu.umd.cs.findbugs.annotations.DesireWarning (Deprecated)**

The annotation based approach is useless for lambdas.

### **2.20.11 edu.umd.cs.findbugs.annotations.DischargesObligation**

Mark a method as cleaning up a resource.

### **2.20.12 edu.umd.cs.findbugs.annotations.ExpectWarning (Deprecated)**

The annotation based approach is useless for lambdas.

### **2.20.13 edu.umd.cs.findbugs.annotations.NonNull**

The annotated element must not be null.

### **2.20.14 edu.umd.cs.findbugs.annotations.NoWarning (Deprecated)**

The annotation based approach is useless for lambdas.

### **2.20.15 edu.umd.cs.findbugs.annotations.Nullable**

The annotated element could be null under some circumstances. This is treated the same way as not being annotated.

### 2.20.16 edu.umd.cs.findbugs.annotations.OverrideMustInvoke

Used to annotate a method that, if overridden, must (or should) be invoked by an invocation on super in the overriding method.

### 2.20.17 edu.umd.cs.findbugs.annotations.PossiblyNull (Deprecated)

Use *CheckForNull* instead. The name of which more clearly indicates that not only could the value be null, but that good coding practice requires that the value be checked for null.

### 2.20.18 edu.umd.cs.findbugs.annotations.ReturnValuesAreNonnullByDefault

This annotation can be applied to a package, class or method to indicate that the methods in that element have nonnull return values by default unless there is: An explicit nullness annotation The method overrides a method in a superclass (in which case the annotation of the corresponding parameter in the superclass applies) there is a default annotation applied to a more tightly nested element.

### 2.20.19 edu.umd.cs.findbugs.annotations.SuppressFBWarnings

Used to suppress SpotBugs warnings.

### 2.20.20 edu.umd.cs.findbugs.annotations.SuppressWarnings (Deprecated)

Use *SuppressFBWarnings* instead.

### 2.20.21 edu.umd.cs.findbugs.annotations.UnknownNullness

Used to indicate that the nullness of element is unknown, or may vary in unknown ways in subclasses.

### 2.20.22 edu.umd.cs.findbugs.annotations.CleanupObligation (Deprecated)

Mark a class or interface as a resource type requiring cleanup.

### 2.20.23 edu.umd.cs.findbugs.annotations.CreatesObligation (Deprecated)

Mark a constructor or method as creating a resource which requires cleanup. The marked method must be a member of a class marked with the CleanupObligation annotation.

## 2.20.24 edu.umd.cs.findbugs.annotations.DischargesObligation (Deprecated)

Mark a method as cleaning up a resource. The marked method must be a member of a class marked with the CleanupObligation annotation.