Third party analyzers

This guide will show you how to use Kiuwan in combination with third-party analyzers.

Contents:

Introduction to analyzing with third-party analyzers

Kiuwan provides some mechanisms to complement Kiuwan analyses with third-party analyzers.

This could be very useful if you are new to Kiuwan and you were already using other 3rd-party analyzers. You can use Kiuwan's own analyzers, keep using your existing analyzers, and integrate all the results into the Kiuwan dashboard.

> There are two possible approaches:
>
> - Let Kiuwan **execute 3rd-party rules**
> - Execute 3rd-party analyzers from your custom mechanism and let Kiuwan **import 3rd-party results**

Executing an analysis with 3rd-party rules

Kiuwan Local Analyzer can execute 3rd-party rules if your application is configured to use a model that contains third-party rules.

This applies to **PMD**, **FindBugs,** and **Checkstyle**.

Executing an analysis with PMD or Checkstyle rules

To execute an analysis with PMD or Checkstyle rules, just create a custom model that contains those rules for your application.

To import those rules into your custom model, select **Import Rulesets** from the **Rules** tab of your custom model.

Please visit Models Manager User Guide for further information on Kiuwan models.

Executing an analysis with Findbugs rules

To execute an analysis with Findbugs rules, you should specify the folders to analyze in an standard order so Findbugs can find all the needed information when called:

1. A folder with .class files (Findbugs analyzes bytecode, so the first folder should point to your compiled code).
2. A folder with the corresponding source files (so kiuwan knows where to show the defects found).
3. A folder that will be used as auxiliary classpath entry, if your findbugs rules need one.

Note that you must specify the first and second folders to make Findbugs work as expected.

Once the folders are specified in the correct order, just launch the analysis.

Importing results from 3rd-party analyzers

Kiuwan can **import** results from other analyzers. You can analyze with **MS FxCop** or **HP Fortify** and view all results in Kiuwan dashboards.

Run your analyzer by your own and then convert the results to a XML file with this format:

```
<?xml version='1.0' encoding='UTF-8'?>
<kiuwan>
 <defects>
 <violation>
 <file line="600" name="src/com/optimyth/jkqa/cqm/CQMConfidenceEvaluator.
java"><![CDATA[public class CQMConfidenceEvaluator extends
BaseConfidenceEvaluator implements]]></file>
 <rule code="OPT.JAVA.CDCI.PJDCC"/>
 </violation>
 <violation>
 <file line="650" name="src/com/optimyth/jkqa/cqm/CQMConfidenceEvaluator.
java" hashed="true">1c54de24397760c0fb37b8a1d4949f1050008d3a</file>
 <rule code="OPT.JAVA.CDCI.PJDCC"/>
 </violation>
 <violation>
 <file name="src/com/optimyth/jkqa/cqm/CQMConfidenceEvaluator.java"/>
 <rule code="OPT.JAVA.STR.ECOM"/>
 </violation>
 </defects>
</kiuwan>
```

Important note

The name of the file with the violations converted to the above Kiuwan format, has to start with the "**kiuwan_**" prefix.

For example: ***kiuwan_my3rpartytool_report.xml***.

You can find a tool that converts the output of Ms FxCop and HP Fortify on this Github repository. Rule codes specified in XML must be active in your quality model, so you have to import in Quality Model Management all rule definitions managed by your analyzer. Each rule definition is a XML that contains the rule documentation. You can use Kiuwan Rule Developer to build these files using a graphic interface.

Then, upload the Kiuwan format defects file to Kiuwan using Kiuwan Local Analyzer:

```
agent.cmd -s "c:\src" -n myapp -x "c:\myreports" ignore=rules
```

You can merge your defects with Kiuwan's or you can ignore Kiuwan analyzer results using the *ignore* parameter.