

How to scan Flex code



This page has been made public for vendors

Question

How do I scan Flex code using Fortify?

Answer

The files extensions of Flex code that can be scanned with Fortify include the following:

- .as - ActionScript file containing script code for software targeting the Adobe Flash Player platform.
- .mxml - XML formatted files that can contain chunks of ActionScript code. They are dynamically compiled to SWF files. Fortify translates MXML files into ActionScript, and then runs them through the ActionScript parser. The ActionScript that is generated is intended to be simple to analyze; not rigorously correct like the Flex run-time model. As a consequence, you may get parse errors with MXML files. For instance, the XML parsing could fail, the translation to ActionScript could fail, and the parsing of the resulting ActionScript could also fail. If you see any errors that do not have a clear connection to the original source code, please notify HP Fortify Support.
- .swc - package of precompiled Flash symbols and ActionScript code, sometimes referred to as class libraries.
- .swf - (Small Web Format) Flash file format used for multimedia, vector graphics and ActionScript

Note that Fortify does not support .swz files

Flex code should normally be scanned with HP Fortify Static Code Analyzer using the command line interface, or with command line instructions included within a script. The basic command line syntax to scan ActionScript code is:

```
sourceanalyzer -b <build_id> -flex-libraries <listOfLibraries>
```

where `-flex-libraries <listOfLibraries>` is a semicolon-separated list (Windows) or a colon separated-list (non-Windows systems) of library names that you want to "link" to. In most cases, this list includes `flex.swc`, `framework.swc`, and `playerglobal.swc` (usually found in `frameworks/libs/` under your Flex SDK root).

Example 1:

To scan a simple application that contains only one MXML file (`FlexApp.mxml`) and a single SWF library (`MyLib.swf`), the command line would be:

```
sourceanalyzer -b MyFlexApp -flex-libraries lib/MyLib.swf -flex-sdk-root /home/myself/flex-sdk/ -flex-source-roots my/app/FlexApp.mxml
```

The command identifies the location of the libraries to include with `-flex-libraries (lib/MyLib.swf)`, and also identifies the Flex SDK with `-flex-sdk-root (/home/myself/flex-sdk/)` and the Flex source root locations with `-flex-source-roots (my/app/FlexApp.mxml)`.

`-flex-sdk-root` points to the root of a valid Flex SDK. In this example, the Flex SDK is located at `/home/myself/flex-sdk/`. This folder should contain a `frameworks` folder that contains a `flex-config.xml` file. It should also contain a `bin` folder that contains an `mxmclc` executable.

And

`-flex-source-roots` contains a `:` or `;` separated list of root directories in which MXML sources can be found. In this instance, the Flex source root is pointing at `my/app`, so `FlexApp.mxml` will get transformed into an object named `my.app.FlexApp`, (an object named `FlexApp` in the package `my/app`).

Note that `-flex-sdk-root` and `-flex-source-roots` are primarily for MXML translation, and are optional if you are scanning pure ActionScript. `-flex-libraries` is used for resolving all ActionScript

Example 2

The following example is for an application in which the source files are relative to the `src`

HPE Fortify Version	4.30 and later
Programming Language	<input type="checkbox"/> C/C++ <input type="checkbox"/> .NET <input type="checkbox"/> Java <input type="checkbox"/> Objective-C <input checked="" type="checkbox"/> Other
Fortify Audit Workbench	<input type="checkbox"/> Yes <input type="checkbox"/> No
Fortify IDE Plugin	<input type="checkbox"/> Yes <input type="checkbox"/> No
Other Fortify Component	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

Request code review tools, validations, and support [HERE](#).

directory. It uses a single SWF library, MyLib.swf, and the Flex and framework libraries from the Flex SDK.
sourceanalyzer -b MyFlexProject -flex-sdk-root /home/myself/flex-sdk/ -flex-source-roots src/ -flex-libraries lib/MyLib.swf src/**/*.mxml src/**/*.as

In this example, the Flex SDK is located at /home/myself/flex-sdk/. It is not necessary to explicitly specify the .SWC files found under the -flex-sdk-root. SCA will automatically locate all .SWC files under the specified Flex SDK root, and it assumes that these are libraries intended for use in translating the ActionScript or mxml files.
src/**/*.mxml src/**/*.as at the end of the command indicates that all .mxml files and all .as files in all subdirectories of each of the src directories will be scanned.

Example 3

In this example, the Flex SDK root and Flex libraries are specified in the SCA properties file since typing in the data is time consuming and it tends to be constant. The application may be divided into two sections and stored in folders: a main section folder and a modules folder. Each folder contains an src folder where the paths should be begun. Wildcards are used in file specifiers to pick up all the .mxml and .as files in both of the src folders. An MXML file in main/src/com/foo/util/Foo.mxml will be translated as an ActionScript class named Foo in the package com.foo.util, for example, with the source roots specified here:

```
sourceanalyzer -b MyFlexProject -flex-source-roots main/src:modules/src  
./main/src/**/*.mxml ./main/src/**/*.as ./modules/src/**/*.mxml ./modules/src/**/*.as
```

About Handling Resolution Warnings

To see all warnings that were generated during your build, enter the following command before you start the scan phase:

```
sourceanalyzer -b <build_id> -show-build-warnings
```

About ActionScript Warnings

You may receive a message similar to:

The ActionScript front end was unable to resolve the following imports: a.b at y.as:2.
foo.bar at somewhere.as:5. a.b at foo.mxml:8.

This error occurs when SCA cannot find all of the libraries it needs. You may need to specify additional SWC or SWF Flex libraries (-flex-libraries option, or com.fortify.sca.FlexLibraries property) so that SCA can complete the analysis.

References

- HPE Fortify Static Code Analyzer User Guide, Chapter 9: Translating Flex and ActionScript