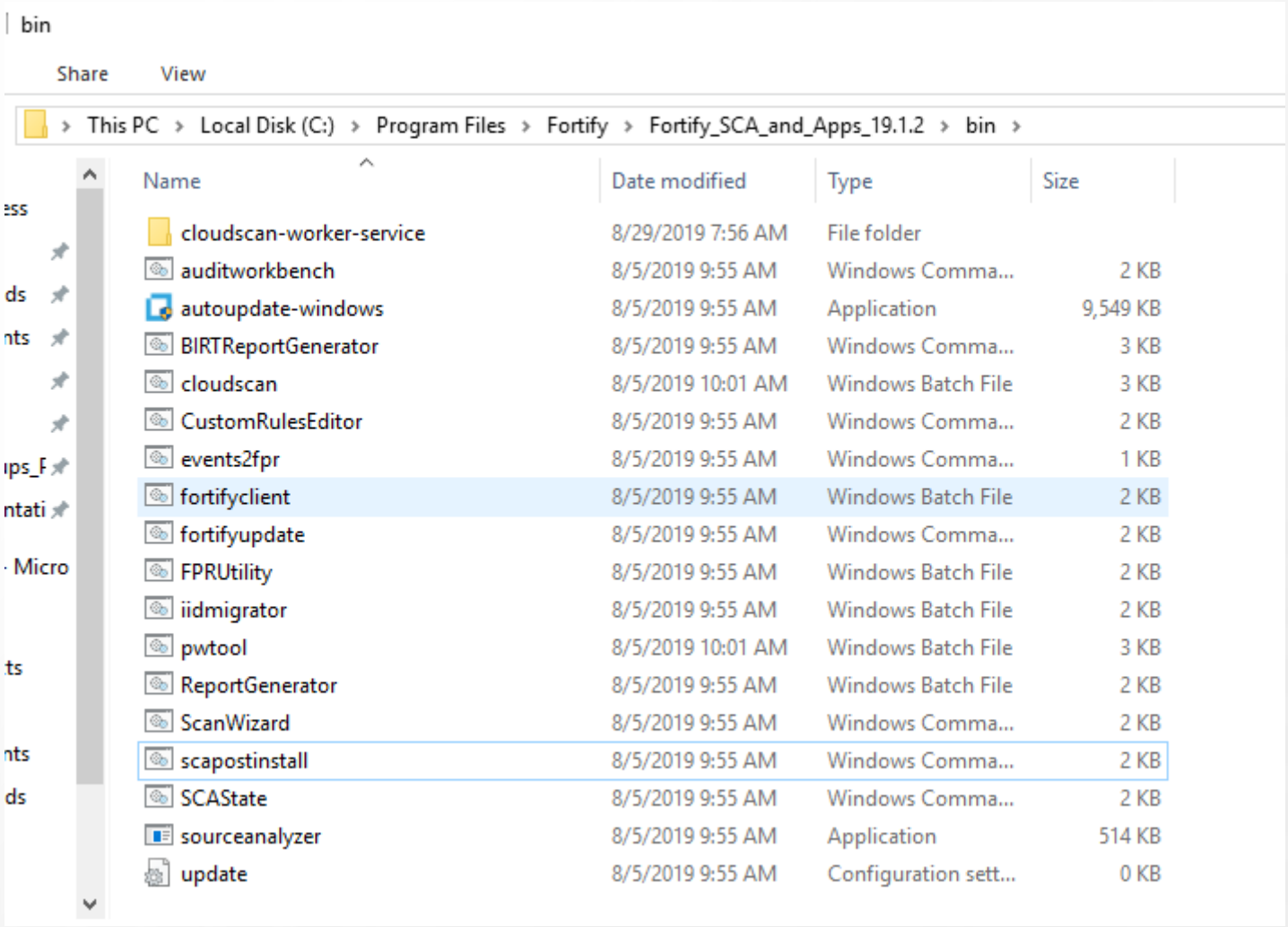
Fortify SCA Tools

Jonathan Couch
Fortify Security Support Engineer

Things you didn’t know you had

- Ships with all SCA installers
- Situationally useful



- Talk about 2 of these

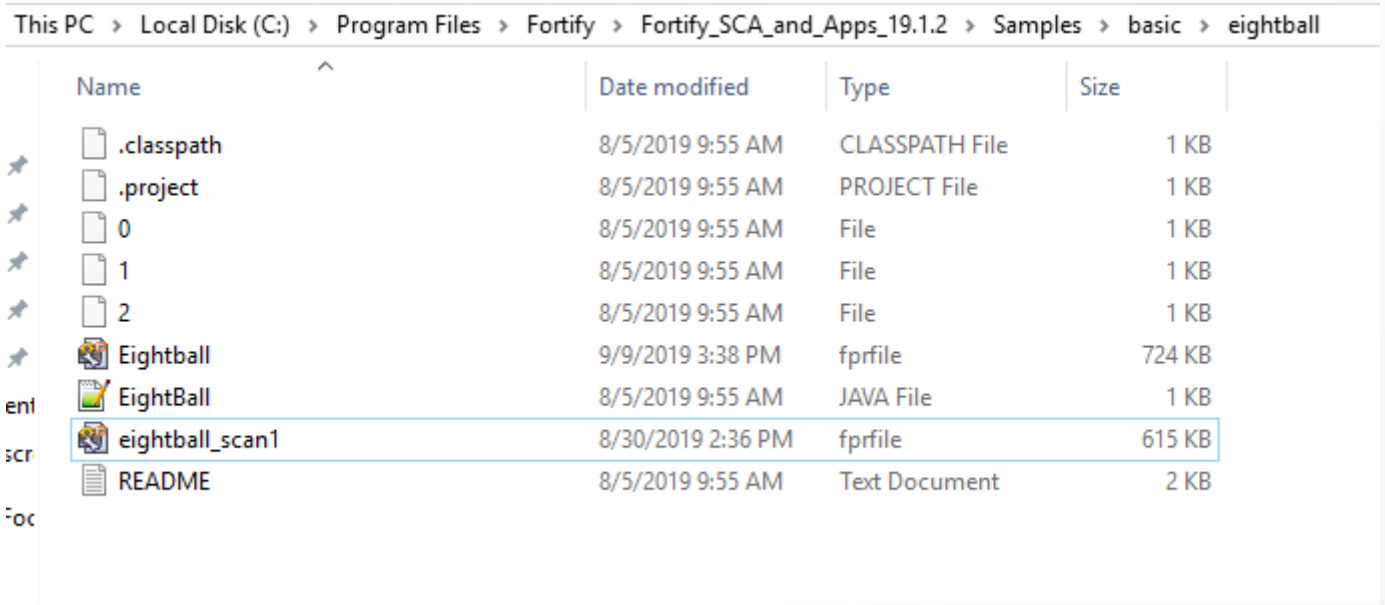
FPRUtility

- Allows you to interact with FPR’s
- Performs many of the same functions you expect from SSC.
- Merging

```
                    -f myProjectWithArchive.fpr

Merge Options:
    -merge                          Will perform a merge of the two passed projects

    -project                        The primary project used in the merge action. Conflicts
                                    will be resolved using the values found in this project.

    -source                         The secondary project to be used in the merge action.

    -f                              The file to be used as the output.  The primary project
                                    is the default output file.

    -forceMigration                 Force migration to run, even if the engine and rulepack
                                    versions of the two projects are the same.

    -useMigrationFile               Supply your own instance id mappings file.  This allows you
                                    to modify the mappings manually, instead of using the
                                    migration results.

    -iidmigratorOptions 'options'   List of options, surrounded by single quotes, that are
                                    passed on to the instance id migrator.

    -useSourceIssueTemplate       Force use of filter sets and folders from the issue template
                                    from the secondary project. The filter sets and folders from the
                                    primary project will be used by default.
```

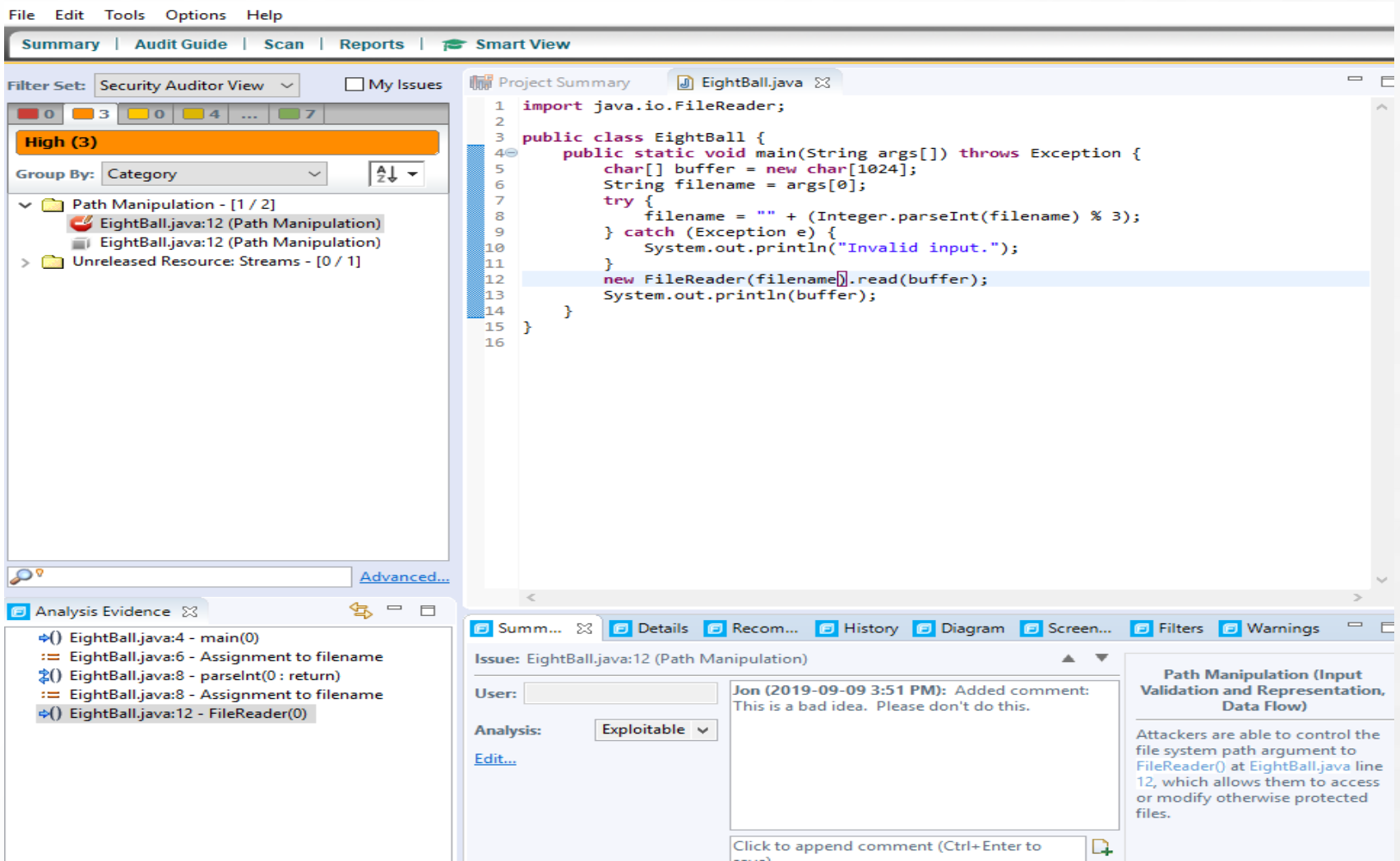
Merging FPRs

- >FPRUtility –merge -project <input>.fpr –source <existing>.fpr –f <result>.fpr



Merging FPRs

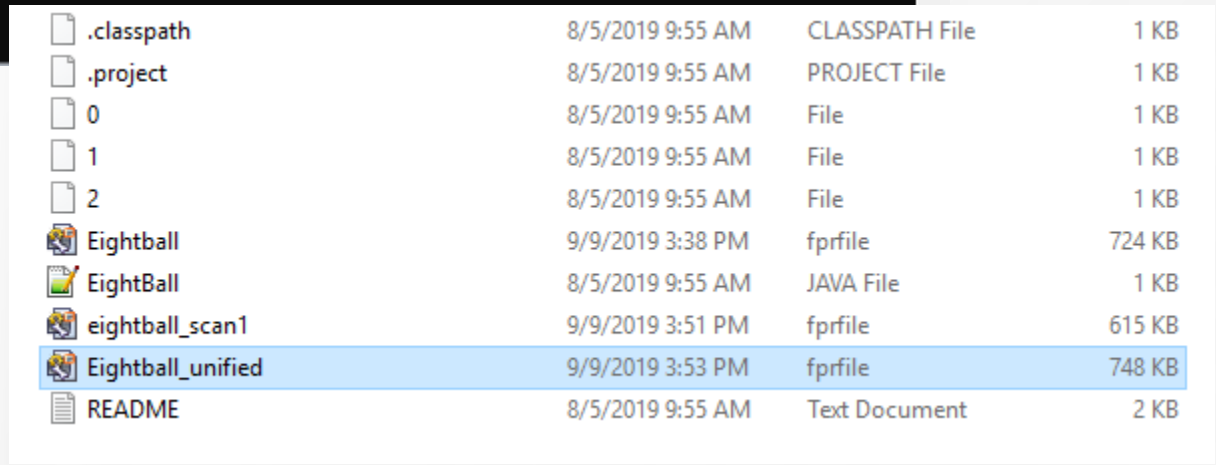
- We have Audit information that we want to preserve



The Merge

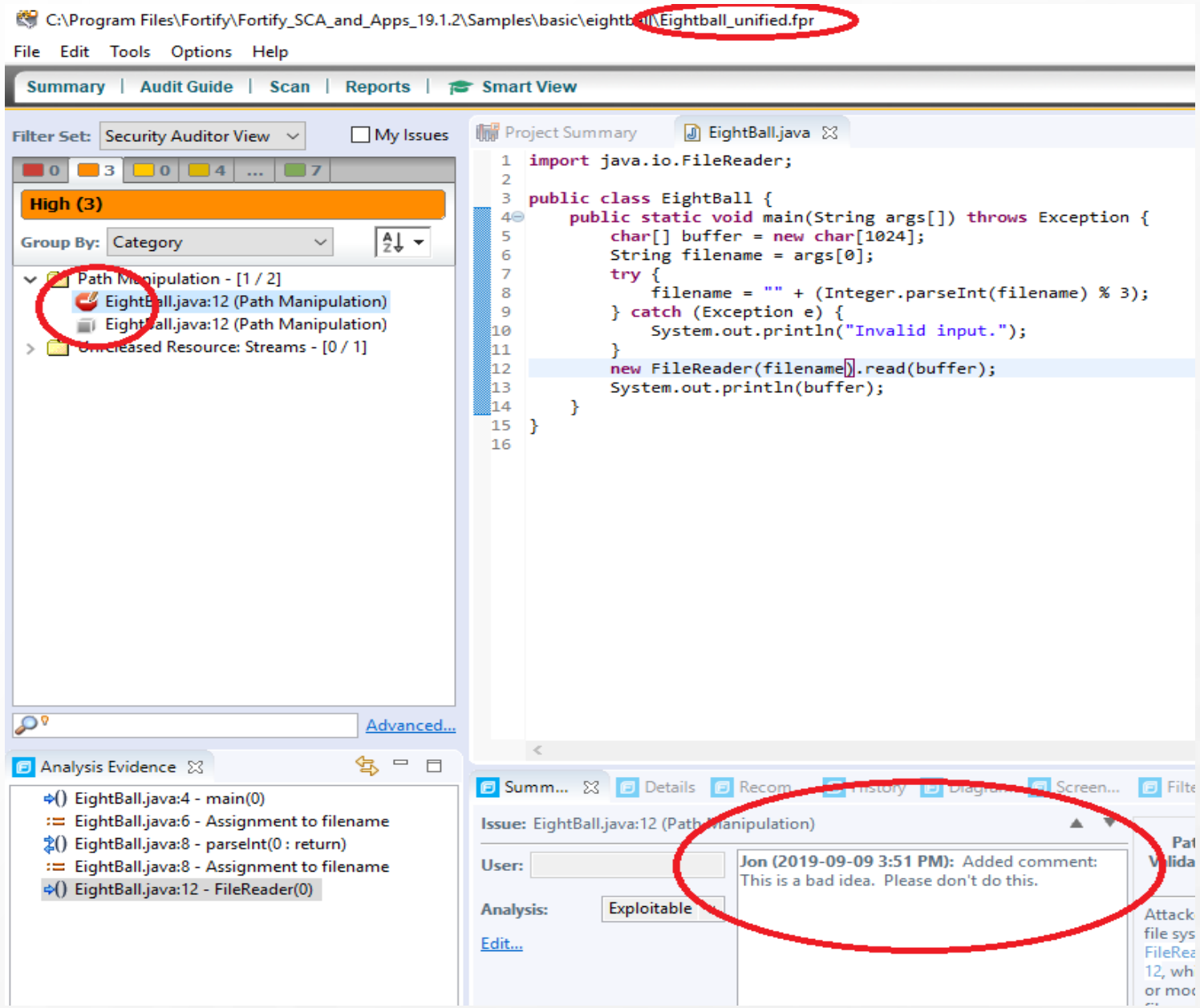
Pattern is <New> + <Old> = <Combined>

```
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>FPRUtility.bat -merge -project "C:\Program Files\Fortify\Fortif
y_SCA_and_Apps_19.1.2\Samples\basic\eightball\EightBall.fpr" -source "C:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1
.2\Samples\basic\eightball\eightball_scan1.fpr" -f "C:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\Samples\basic\e
ightball\Eightball_unified.fpr"

Found New Issue Template
========================
Would you like to keep the filter sets and folders from the existing template, or import the filter sets and folders fro
m the new issue template?
(1) New Template
(2) New Template (Remember my Response)
(3) Existing Template
(4) Existing Template (Remember my Response)
[Type the number of the answer and click Enter]
No answer, using default response: Existing Template

c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>_
```



Merged FPR

Audit information is preserved



Other useful functions

A host of information options

```
-information -signature -project myProject.fpr -f output.txt
-information -mappings -project myProject.fpr -f output.txt
-information -errors -project myProject.fpr -f output.txt
-information -functionsMeta -project myProject.fpr -f output.txt
-information -categoryIssueCounts -project myProject.fpr -f output.txt
-information -analyzerIssueCounts -project myProject.fpr -f output.txt
-information -search -project myProject.fpr -query "file:foo.java" -f output.txt
-information -search -project myProject.fpr -query "file:foo.java"
        -f output.txt -includeSuppressed -includeRemoved
-information -categoryIssueCounts -project myProject.fpr -search
        -query "file:foo.java" -f output.txt
-information -analyzerIssueCounts -project myProject.fpr -search
        -query "file:foo.java" -f output.txt
-information -categoryIssueCounts -project myProject.fpr -search
        -query "[Issue Age]:Removed" -includeRemoved -listIssues -f output.txt
-information -categoryIssueCounts -listIssues -project myProject.fpr -search
        -queryAll -f output.txt
-information -listIssues -project myProject.fpr -search
        -queryAll -f output.csv -outputFormat CSV
```

Information example

Issues in the project by Category

```
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>FPRUtility.bat -information -categoryIssueCounts -project "C:\P
rogram Files\Fortify\Fortify_SCA_and_Apps_19.1.2\Samples\basic\eightball\Eightball_unified.fpr"

Issue counts by category:

 "J2EE Bad Practices: Leftover Debug Code" => 1 Issues
 "Path Manipulation" => 2 Issues
 "Poor Logging Practice: Use of a System Output Stream" => 2 Issues
 "Unchecked Return Value" => 1 Issues
 "Unreleased Resource: Streams" => 1 Issues

Total for all categories => 7 Issues


c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>
```

Information example 2

Issues in the project by Analyzer

```
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>FPRUtility.bat -information -analyzerIssueCounts -project "C:\P
rogram Files\Fortify\Fortify_SCA_and_Apps_19.1.2\Samples\basic\eightball\Eightball_unified.fpr"

Issue counts by analyzer:

 "controlflow" => 1 Issues
 "dataflow" => 2 Issues
 "semantic" => 1 Issues
 "structural" => 3 Issues

Total for all analyzers => 7 Issues


c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>
```

Why?

- Allows you to interact with FPR’s
- Check FPR’s contents
- Merge FPR’s
- Extract or merge FPR-bundled Source

Why?

- Allows you to interact with FPR's
- Check FPR's contents
- Merge FPR's
- Extract or merge FPR-bundled Source

  programmatically

FortifyClient

Wrapper for API calls to SSC.

```
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>fortifyclient.bat

No command was specified

Commands:
          token - retrieve authentication token for scripted use of this utility
          listtokens - list generated authentication tokens
          invalidatetoken - invalidate previously generated authentication tokens
          listProjectVersions - list project versions available on server * Deprecated, use listApplicationVersions instead *
          listApplicationVersions - list application versions available on server
          listprojects - list project versions available on server * Obsolete *
          downloadFPR - download latest FPR for an application
          uploadFPR - upload an FPR to an application
          uploadSource - upload a Source Archive to an application
          import - import Fortify SRG Content Bundle into Micro Focus Fortify Software Security Center
          purgeProjectVersion - purge all artifacts in a project version scanned before a given date * Deprecated, use purgeApplicationVersion in
          purgeApplicationVersion - purge all artifacts in a application version scanned before a given date
          downloadAttachment - download audit attachment file
```

Use Case

Disaster has struck

FortifyClient to the rescue

- The first thing you will need is two Authentication Tokens

```
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>fortifyclient.bat token -gettoken AnalysisUploadToken -user adm
in -password [redacted]
Authorization Token: 98d2a95b-4395-4bce-baaf-1172d2bdeef2
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>
```

```
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>fortifyclient.bat token -gettoken AnalysisDownloadToken -u
ser admin -password [redacted]
Authorization Token: 6e49c6ac-2625-4528-8183-fed6238a9816
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>
```

- Copy these tokens somewhere, because you'll need them.

FortifyClient to the rescue

- Next, we need to retrieve a list of the Application Versions in the old system

```
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>fortifyclient.bat listApplicationVersions -url http://loca
lhost:8080/ssc -authtoken 98d2a95b-4395-4bce-baaf-1172d2bdeef2

ID      Name                    Version

2       UserGroupTest1                  1.0
3       UserGroupTest2                  New
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>
```

- And for each Application Name & Version, download the FPR

```
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>fortifyclient.bat downloadFPR -url http://localhost:8080/s
sc -authtoken 6e49c6ac-2625-4528-8183-fed6238a9816 -file "C:\DemoScripts\UserGroupTest1v1.0.fpr" -application UserG
roupTest1 -applicationVersion 1.0
Successfully downloaded file to C:\DemoScripts\UserGroupTest1v1.0.fpr
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>
```

FortifyClient to the rescue

- Once all the FPR's are downloaded from the old system, upload them to the new system

```
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>fortifyclient.bat uploadFPR -url http://localhost:8080/ssc
 -authtoken 98d2a95b-4395-4bce-baaf-1172d2bdeef2 -file "C:\DemoScripts\UserGroupTest1v1.0.fpr" -application UserGro
upTest1 -applicationVersion 1.0
Background submission succeeded.
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>fortifyclient.bat uploadFPR -url http://localhost:8080/ssc
 -authtoken 98d2a95b-4395-4bce-baaf-1172d2bdeef2 -file "C:\DemoScripts\UserGroupTest2vNew.fpr" -application UserGro
upTest2 -applicationVersion New
Background submission succeeded.
c:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin>
```

FortifyClient

- It’s not perfect, but it gets the current FPR’s with audit data moved.

FortifyClient

- It’s not perfect, but it gets the current FPR’s with audit data moved.

- Note that you will lose historical data

FortifyClient

- It’s not perfect, but it gets the current FPR’s with audit data moved.

- Note that you will lose historical data

- Issue trends over time
- Reporting

Why use FortifyClient?

- Accessible if you don't use API's
- Can be scripted

```
@echo off

set OLD_SERVER=http://localhost:8080/ssc

set UPLOAD_AUTH_TOKEN=98d2a95b-4395-4bce-baaf-1172d2bdeef2
set DOWNLOAD_AUTH_TOKEN=6e49c6ac-2625-4528-8183-fed6238a9816

call "C:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin\fortifyclient.bat" listApplicationVersions -url %OLD_SERVER% -authtoken %UPLOAD_AUTH_TOKEN% > C:\DemoScripts\ApplicationList.txt

SETLOCAL ENABLEDELAYEDEXPANSION
FOR /f "tokens=* delims=" %%i in (C:\DemoScripts\ApplicationList.txt) DO (
   set Line=%%i ^
   & FOR /f "tokens=1,2,3" %%a in ("!Line!") DO (
      IF NOT "%%a" == "ID" call "C:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin\fortifyclient.bat" downloadFPR -file "C:\DemoScripts\%%bv%%c.fpr" -application %%b -applicationVersion %%c -url %OLD_
    )
)
ENDLOCAL

rem cleanup
del c:\DemoScripts\ApplicationList.txt
cd c:\DemoScripts
@echo on
```

```
@echo off

set NEW_SERVER=http://localhost:8080/ssc

set UPLOAD_AUTH_TOKEN=98d2a95b-4395-4bce-baaf-1172d2bdeef2
set DOWNLOAD_AUTH_TOKEN=6e49c6ac-2625-4528-8183-fed6238a9816

call "C:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin\fortifyclient.bat" listApplicationVersions -url %OLD_SERVER% -authtoken %UPLOAD_AUTH_TOKEN% > C:\DemoScripts\ApplicationList.txt

SETLOCAL ENABLEDELAYEDEXPANSION
FOR /f "tokens=* delims=" %%i in (C:\DemoScripts\ApplicationList.txt) DO (
   set Line=%%i ^
   & FOR /f "tokens=1,2,3" %%a in ("!Line!") DO (
      IF NOT "%%a" == "ID" call "C:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin\fortifyclient.bat" uploadFPR -file "C:\DemoScripts\%%bv%%c.fpr" -application %%b -applicationVersion %%c -url %NEW_SE
    )
)
ENDLOCAL

rem cleanup
del c:\DemoScripts\ApplicationList.txt
cd c:\DemoScripts
@echo on
```

Questions

Thank you.

www.microfocus.com