

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

Name	Date modified	Type	Size
cloudscan-worker-service	8/29/2019 7:56 AM	File folder	
auditworkbench	8/5/2019 9:55 AM	Windows Comma...	2 KB
autoupdate-windows	8/5/2019 9:55 AM	Application	9,549 KB
BIRTRReportGenerator	8/5/2019 9:55 AM	Windows Comma...	3 KB
cloudscan	8/5/2019 10:01 AM	Windows Batch File	3 KB
CustomRulesEditor	8/5/2019 9:55 AM	Windows Comma...	2 KB
events2fpr	8/5/2019 9:55 AM	Windows Comma...	1 KB
fortifyclient	8/5/2019 9:55 AM	Windows Batch File	2 KB
fortifyupdate	8/5/2019 9:55 AM	Windows Comma...	2 KB
FPRUtility	8/5/2019 9:55 AM	Windows Batch File	2 KB
iidmigrator	8/5/2019 9:55 AM	Windows Batch File	2 KB
pwtool	8/5/2019 10:01 AM	Windows Batch File	3 KB
ReportGenerator	8/5/2019 9:55 AM	Windows Batch File	2 KB
ScanWizard	8/5/2019 9:55 AM	Windows Comma...	2 KB
scapostinstall	8/5/2019 9:55 AM	Windows Comma...	2 KB
SCAState	8/5/2019 9:55 AM	Windows Comma...	2 KB
sourceanalyzer	8/5/2019 9:55 AM	Application	514 KB
update	8/5/2019 9:55 AM	Configuration sett...	0 KB

FPRUtility

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

```
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`

This PC > Local Disk (C:) > Program Files > Fortify > Fortify_SCA_and_Apps_19.1.2 > Samples > basic > eightball

Name	Date modified	Type	Size
.classpath	8/5/2019 9:55 AM	CLASSPATH File	1 KB
.project	8/5/2019 9:55 AM	PROJECT File	1 KB
0	8/5/2019 9:55 AM	File	1 KB
1	8/5/2019 9:55 AM	File	1 KB
2	8/5/2019 9:55 AM	File	1 KB
Eightball	9/9/2019 3:38 PM	fprfile	724 KB
EightBall	8/5/2019 9:55 AM	JAVA File	1 KB
eightball_scan1	8/30/2019 2:36 PM	fprfile	615 KB
README	8/5/2019 9:55 AM	Text Document	2 KB

Merging FPRs

- We have Audit information that we want to preserve

The screenshot displays a security tool interface with the following components:

- Menu Bar:** File, Edit, Tools, Options, Help.
- Navigation:** Summary | Audit Guide | Scan | Reports | Smart View.
- Filter Set:** Security Auditor View. My Issues checkbox is present.
- Issue Summary:** High (3) issues. Group By: Category. Issues include Path Manipulation (2) and Unreleased Resource: Streams (1).
- Code Editor:** Shows the source code for `EightBall.java`. Line 12 is highlighted, corresponding to the selected issue: `new FileReader(filename).read(buffer);`.
- Analysis Evidence:** Lists the execution flow: `EightBall.java:4 - main(0)`, `EightBall.java:6 - Assignment to filename`, `EightBall.java:8 - parseInt(0 : return)`, `EightBall.java:8 - Assignment to filename`, and `EightBall.java:12 - FileReader(0)`.
- Issue Details:** Issue: `EightBall.java:12 (Path Manipulation)`. User: Jon (2019-09-09 3:51 PM). Analysis: Exploitable. Comment: "Added comment: This is a bad idea. Please don't do this."
- Path Manipulation (Input Validation and Representation, Data Flow):** Description: "Attackers are able to control the file system path argument to `FileReader()` at `EightBall.java` line 12, which allows them to access or modify otherwise protected files."











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\Fortify_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\eightball\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 from 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>
```

 .classpath	8/5/2019 9:55 AM	CLASSPATH File	1 KB
 .project	8/5/2019 9:55 AM	PROJECT File	1 KB
 0	8/5/2019 9:55 AM	File	1 KB
 1	8/5/2019 9:55 AM	File	1 KB
 2	8/5/2019 9:55 AM	File	1 KB
 Eightball	9/9/2019 3:38 PM	fprfile	724 KB
 EightBall	8/5/2019 9:55 AM	JAVA File	1 KB
 eightball_scan1	9/9/2019 3:51 PM	fprfile	615 KB
 Eightball_unified	9/9/2019 3:53 PM	fprfile	748 KB
 README	8/5/2019 9:55 AM	Text Document	2 KB

Merged FPR

Audit information is preserved

The screenshot displays the Fortify SCA interface for a merged FPR. The file path is `C:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\Samples\basic\eightball\Eightball_unified.fpr`. The interface shows a summary of issues, with a 'High (3)' category selected. The issue list shows two instances of 'Path Manipulation' in `EightBall.java:12`, one of which is circled in red. The code editor shows the following Java code:

```
1 import java.io.FileReader;
2
3 public class EightBall {
4     public static void main(String args[] throws Exception {
5         char[] buffer = new char[1024];
6         String filename = args[0];
7         try {
8             filename = "" + (Integer.parseInt(filename) % 3);
9         } catch (Exception e) {
10            System.out.println("Invalid input.");
11        }
12        new FileReader(filename).read(buffer);
13        System.out.println(buffer);
14    }
15 }
16
```

The 'Analysis Evidence' pane shows the following stack trace:

- EightBall.java:4 - main(0)
- EightBall.java:6 - Assignment to filename
- EightBall.java:8 - parseInt(0 : return)
- EightBall.java:8 - Assignment to filename
- EightBall.java:12 - FileReader(0)

The 'Analysis Evidence' pane also shows a comment from Jon (2019-09-09 3:51 PM): "Added comment: This is a bad idea. Please don't do this." The analysis is marked as 'Exploitable'.

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:\Program 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:\Program 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 instead *
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 admin -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 -user 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://localhost: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/ssc -authtoken 6e49c6ac-2625-4528-8183-fed6238a9816 -file "C:\DemoScripts\UserGroupTest1v1.0.fpr" -application UserGroupTest1 -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

```
1 @echo off
2
3 set OLD_SERVER=http://localhost:8080/ssc
4
5 set UPLOAD_AUTH_TOKEN=98d2a95b-4395-4bce-baaf-1172d2bdeef2
6 set DOWNLOAD_AUTH_TOKEN=6e49c6ac-2625-4528-8183-fed6238a9816
7
8 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
9
10 SETLOCAL ENABLEDELAYEDEXPANSION
11 FOR /f "tokens=* delims=" %i in (C:\DemoScripts\ApplicationList.txt) DO (
12     set Line=%i ^
13     & FOR /f "tokens=1,2,3" %a in ("!Line!") DO (
14         | IF NOT "%a" == "ID" call "C:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin\fortifyclient.bat" downloadFPR -file "C:\DemoScripts\%bv%.fpr" -application %b -applicationVersion %c -url %OLD_!
15     )
16 )
17 ENDLOCAL
18
19 rem cleanup
20 del c:\DemoScripts\ApplicationList.txt
21 cd c:\DemoScripts
22 @echo on
```

```
1 @echo off
2
3 set NEW_SERVER=http://localhost:8080/ssc
4
5 set UPLOAD_AUTH_TOKEN=98d2a95b-4395-4bce-baaf-1172d2bdeef2
6 set DOWNLOAD_AUTH_TOKEN=6e49c6ac-2625-4528-8183-fed6238a9816
7
8 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
9
10 SETLOCAL ENABLEDELAYEDEXPANSION
11 FOR /f "tokens=* delims=" %i in (C:\DemoScripts\ApplicationList.txt) DO (
12     set Line=%i ^
13     & FOR /f "tokens=1,2,3" %a in ("!Line!") DO (
14         | IF NOT "%a" == "ID" call "C:\Program Files\Fortify\Fortify_SCA_and_Apps_19.1.2\bin\fortifyclient.bat" uploadFPR -file "C:\DemoScripts\%bv%.fpr" -application %b -applicationVersion %c -url %NEW_SEI
15     )
16 )
17 ENDLOCAL
18
19 rem cleanup
20 del c:\DemoScripts\ApplicationList.txt
21 cd c:\DemoScripts
22 @echo on
```



Questions

Thank you.

www.microfocus.com

