

From Continuous Integration to Continuous Assurance



**James A. Kupsch,
Barton P. Miller, Vamshi Basupalli, Josef Burger**

Computer Sciences Department, University of Wisconsin
Software Assurance Marketplace (SWAMP)



IEEE Software Technology Conference
September 26, 2017



Software Development

Goal is to **create correctly functioning software systems**

Software systems vary from simple to complex:

Simple	Measure	Complex
1	Lines of Code	1,000,000's
1	Programs	many
minutes	Effort	years
none	External Dependencies	many
1 person	Team size	many
1 location	Geography	many

Software Development Methodologies help manage complexity



Software Development Methodologies

Developed to deal with complexity, so software is produced in a more consistent manner to improve:

- **Quality** (correctness, reliability, security, ...)
- Completion time

Many methodologies have been developed; one of the earliest documented from 1970 is the *Waterfall Model*:



Other methodologies such as prototyping, Incremental Spiral, XP, RAD, Agile, Test Driven Development, CI, and Dev Ops vary in steps, order and cycles

Common to all methodologies is **Implementation** and **Testing**



Implementation Practices



Implementation is the practice of writing the source code

Common practices

- Source code created using a:
 - Text editor (such as vim or emacs)
 - IDE (such **Eclipse**, IntelliJ, Visual Studio or Xcode) incorporates text editor and other development functions in a single user interface
- Use a build automation system (such as make, ant, maven or gradle)
 - automates common tasks such as building and packaging
 - Provides consistency
- Use a Source Code Management System (SCMS) (such as **git**, **svn**, cvs or mercurial):
 - Manages revisions of the source code
 - Easily merges changes from team members allowing concurrent development
- Continuous Integration (CI) System (such as **Jenkins**)
 - Automates building and testing, and scheduling
 - Allows dashboards views of results and trends



Testing Practices

Testing or Software Assurance (SwA) is the practice of **verifying software**:

- operates as intended (**correctness**)
- Has no unintended functionality (**lacks security weaknesses**)

Common practices:

Static Analysis (focus of the SWAMP)

- Testing without running the code (inspect source code or binary)
- Tools include compilers, simple lexical tools and those that do deep analysis on whole programs

Dynamic Analysis

- Testing by validating behavior of code driven by a testing framework
- Includes units test, test suites, penetration testing, and monitoring API usage

Use multiple tools and types of analysis to increase SwA

- Different tools find different weaknesses
- Different types of analysis catch different types of weaknesses



Software Assurance Marketplace (SWAMP)



Facilitates SwA allowing easy use of multiple SCA tools

- No need to install tools
- Declare how to build once, and all applicable tools work
- No modification to source code
- No modification to build system
- Supports different operation systems

Web-based facility

- Web User Interface
- Web API

Developed by four institutions:

- Morgridge Institute for Research (MIR)
- University of Wisconsin–Madison
- University of Illinois Urbana-Champaign
- Indiana University



Using SWAMP

MIR-swamp

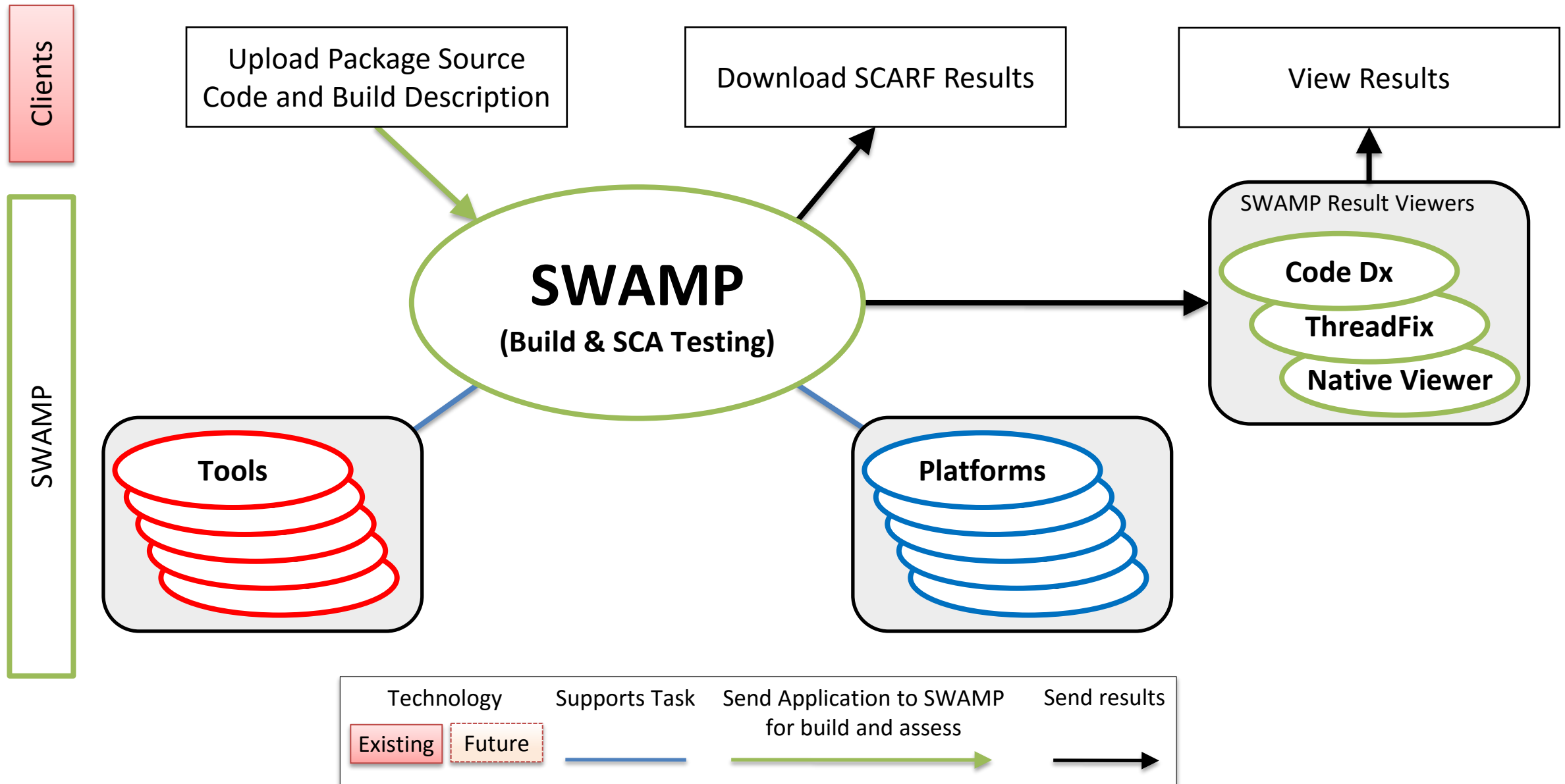
- Hosted and operated by MIR
- No cost to use
- Capable of performing 100's of concurrent assessments
- Commercial tools are available to educational and open source users
- <https://www.mir-swamp.org>

SWAMP-in-a-Box (SiB)

- On-premise SWAMP for those that do not want to (or cannot) use MIR-swamp
- Same functionality as MIR-swamp except commercial tools
- Commercial tools are BYoL (bring your own license)
- Download from <https://continuousassurance.org/swamp-in-a-box>



Core SWAMP Functionality

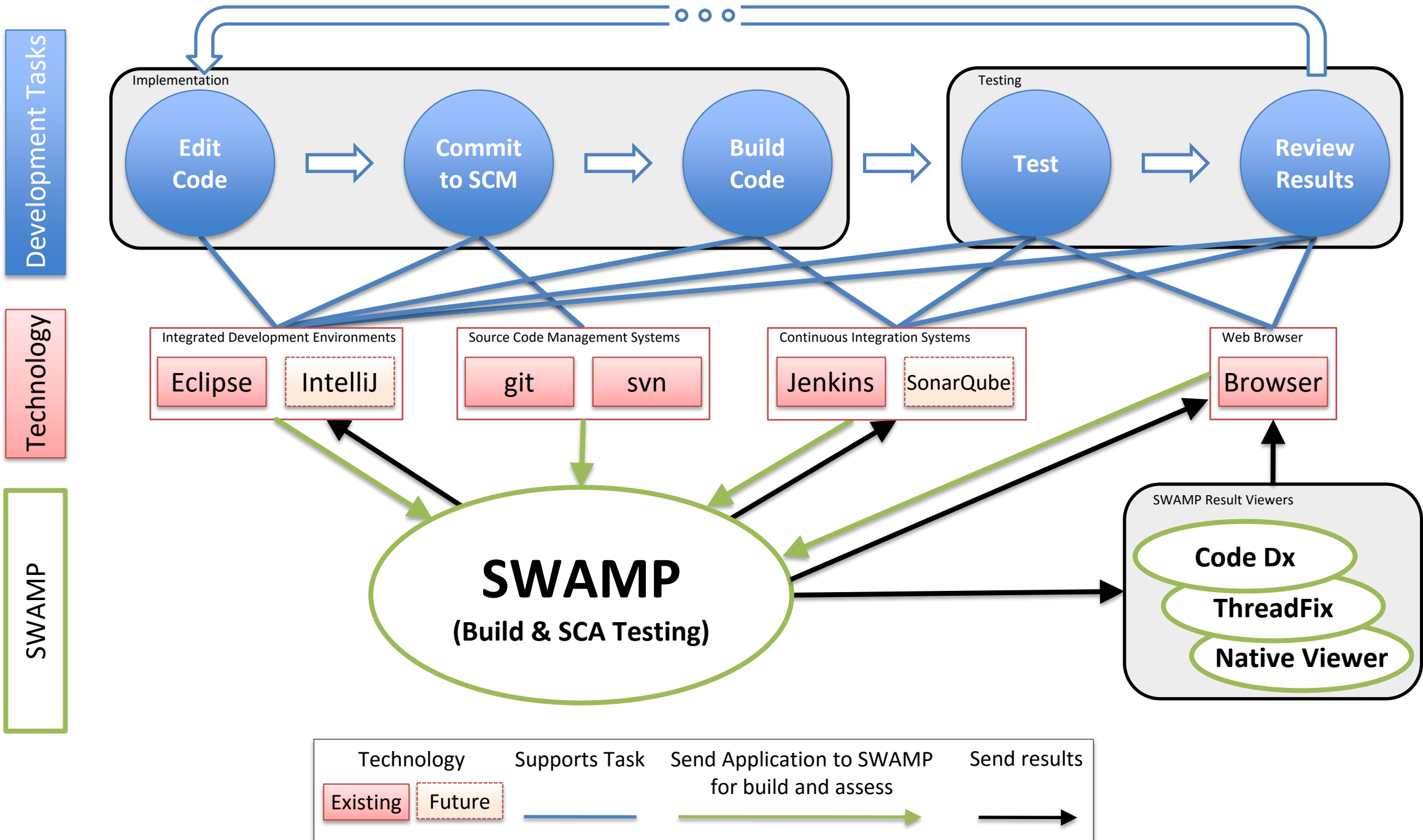




SWAMP Tools and Platforms

	Tools		Platforms
C/C++	Python	JavaScript	Debian
Cppcheck	Bandit	ESLint	Ubuntu
Clang Static Analyzer	Flake8	Flow	CentOS
Gcc Warnings	Pylint	JSHint	Scientific Linux
Parasoft C/C++Test *	Ruby	Retire.js	Fedora
GrammarTech CodeSonar *	Brakeman	HTML	
Synopsys Coverity *	Dawncanner	HTML Tidy	
Java	Reek	CSS	
FindBugs with	Rubocop	CSS Lint	
FindSecurityBugs and	Ruby-lint	XML	
fb-contrib plug-ins	PHP	XML Lint	
Error Prone	PHPMD	Code Metrics (all)	
PMD	PHP_Codesniffer	Cloc	
Checkstyle		Lizard	
OWASP Dependency-Check			
Parasoft Jtest *			
Android			
Android Lint			
RevealDroid			

* Commercial Tool (requires license for SiB)





SWAMP Web Interface



Packages

- Add new packages and versions
- Upload source code or pull from github
- Configure build

Assessments

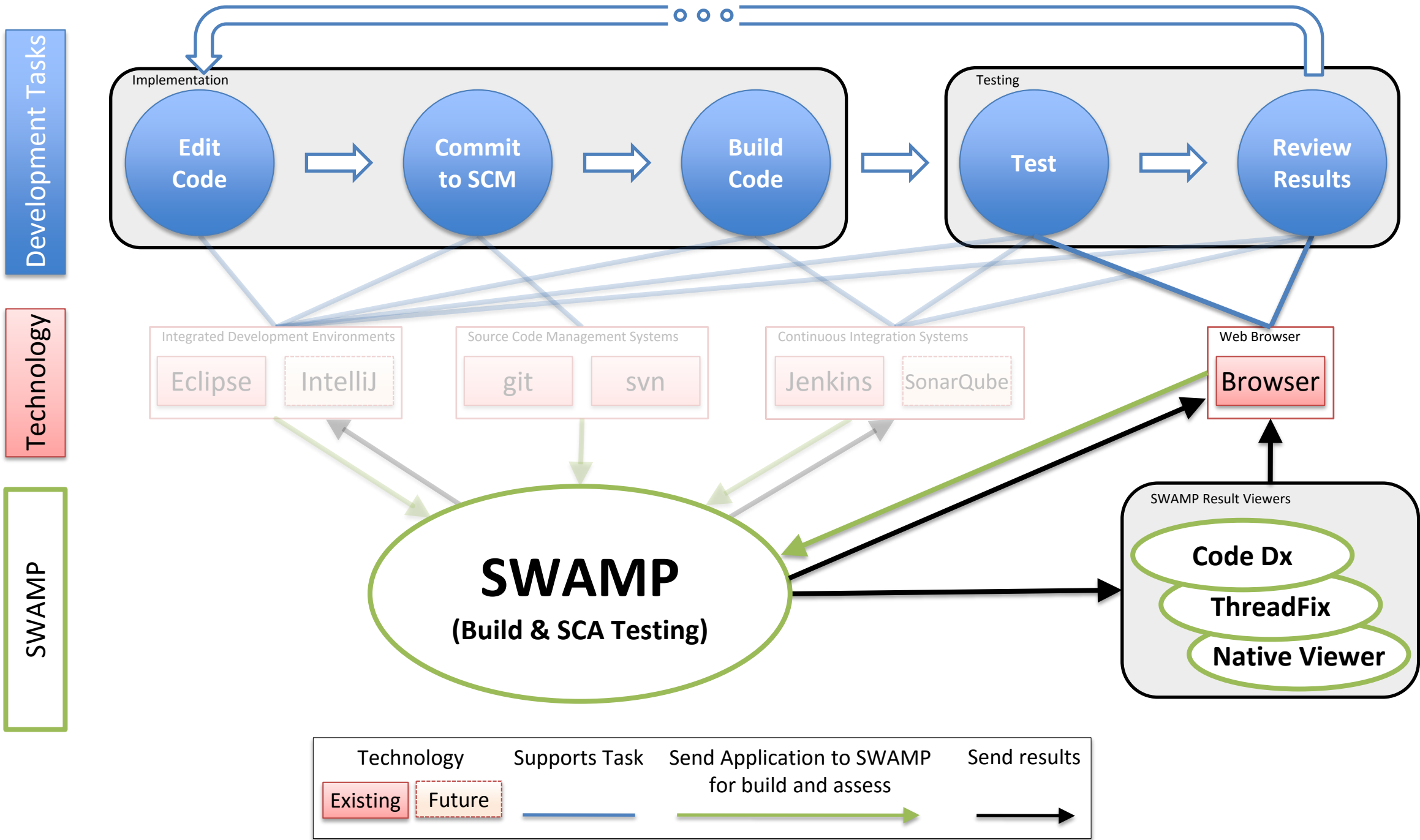
- Select package
- Select tools
- Select platform (operating system)

Results

- View results directly in web interface using one of three viewers
 - Code Dx, Secure Decisions
 - SWAMP Native Viewer
 - ThreadFix, Denim Group
- Download results in SCARF (SWAMP Common Assessment Result Format)

Web-based UI is not right for some developers

- Outside normal developer workflow
- Doesn't fit their toolset



You last signed in on
08/24/2017



SWAMP

SOFTWARE ASSURANCE MARKETPLACE

Do It Early. Do It Often.



Packages

Upload your code and manage your software packages.

0



Assessments

Perform assessments on packages using code analysis tools.

0



Results

View the status and results of completed assessments.

0



Runs

View assessments scheduled to run at regular intervals.

0



Projects

Create projects to share results with other users.

0



Events

View events associated with your projects & account.

5





Add New Package

[Home](#) / [Packages](#) / [Add New Package](#)

Details

Source

Build

Name *

scarf-io

Description

File source

Local file system

The package source code is located on your local hard drive.

Remote Git repository

The package source code is located on a remote Git server.

File *

Choose File scarf-io3.zip

formats supported

Version *

1.0

Version notes

① Name Package

② Package source via archive upload or git

③ Package source archive

*Fields are required

Next

Cancel



Add New Package

[Home](#) / [Packages](#) / [+ Add New Package](#)

[Details](#) **</> Source** [Build](#)

Package path * [Select](#)

Language *

[Show File Types](#)

Java type

Java source
The package contains uncompiled Java code in its original source code format (.java files).

Java bytecode
The package contains Java code which has been compiled (.class, .jar, or .apk files).

Android
The package contains uncompiled Java code for the Android platform.

Java version

[Next](#) [Prev](#) [Cancel](#)

④ Top-level directory (defaulted)

⑤ Language of the package: Java 8 Source Code (defaulted)

Build system * Ant

JAVA SOURCE BUILD INFO

Advanced settings

[Configure](#) [Build](#)

Build settings

Build path	<input type="text"/>	?	Select
Build file	<input type="text"/>	?	Select
Build options	<input type="text"/>	?	
Build target	<input type="text" value="clean build"/>	?	

⑥ Package build (and configuration) settings. All values default to reasonable values. *Build target* is overridden.

*Fields are required

Package dependencies

*Fields are required

Build script

The following is the Unix shell script that will be executed to build this package version. If you have a machine running your target platform, you can execute this script on your local machine to validate it, if you wish.

```
unzip scarf-io3.zip
cd scarf-io3/
ant clean build
```


Build system * Ant

JAVA SOURCE BUILD INFO

Advanced settings

[Configure](#) [Build](#)

Build settings

Build path [Select](#)

Build file [Select](#)

Build options

Build target

Build Script

```
unzip scarf-io3.zip  
cd scarf-io3/  
ant clean build
```

*Fields are required

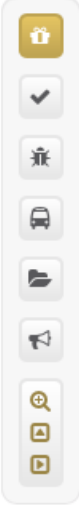
Package dependencies

*Fields are required

Build script

The following is the Unix shell script that will be executed to build this package version. If you have a machine running your target platform, you can execute this script on your local machine to validate it, if you wish.

```
unzip scarf-io3.zip  
cd scarf-io3/  
ant clean build
```



scarf-io Package

[Home](#) / [Packages](#) / [scarf-io](#)

[Assessments](#) **0** [Results](#) **0** [Runs](#) **0**

Name	scarf-io	Edit
Language	Java 8 Source Code	
Creation date	08/24/2017	
Last modified date	08/24/2017	
External URL	none	
Description	none	

Versions

[+ Add New Version](#)

The following versions of this software package are available:

Version	Notes	Date Added
1.0		08/24/2017 15:38

[▶ Run New Assessment](#) [🗑 Delete Package](#)



Run New Assessment of scarf-io

[Home](#) / [Assessments](#) / [+ Run New Assessment](#)

To create a new assessment, please specify the following information:

Package

Select a version:

1.0

① Assess version 1.0 of the package

Tool

Select a tool to use:

All

Select a version:

Latest

② Assess with all tools

[▶ Save and Run](#)

[Save](#)

[Cancel](#)



Filters

no project

scarf-io version 1.0

any tool

any platform

any date

50 items



Viewer

 Code Dx Threadfix Native**Notice:** No results have been selected - viewing results will display previously viewed results. Auto refresh[View Assessment Results](#)

<input type="checkbox"/>	Package	Tool	Platform	Date	Status	Results
<input type="checkbox"/>	scarf-io 1.0	checkstyle 7.4	Ubuntu Linux 16.04 LTS 64-bit Xenial Xerus	08/24/2017 15:41	performing assessment	
		error-prone 2.0.15			performing assessment	
		Findbugs 3.0.1			performing assessment	
		OWASP Dependency Check 1.4.4			performing assessment	
		PMD 5.5.2			performing assessment	

 Show numbering Show grouping[Delete Assessment Results](#)

Filters

no project

scarf-io version 1.0

any tool

any platform

any date

50 items

x

Viewer

 Code Dx Threadfix Native

Results status table with in-progress assessments

Package	Tool	Platform	Date	Status	Results
scarf-io 1.0	checkstyle 7.4	Ubuntu Linux 16.04 LTS 64-bit Xenial Xerus	08/24/2017 15:41	performing assessment	
	error-prone 2.0.15			performing assessment	
	Findbugs 3.0.1			performing assessment	
	OWASP Dependency Check 1.4.4			performing assessment	
	PMD 5.5.2			performing assessment	

[Delete Assessment Results](#)



Filters no project scarf-io version 1.0 any tool any platform any date 50 items X

Viewer Code Dx Threadfix Native

Notice: No results have been selected - viewing results will display previously viewed results. X

Auto refresh

[View Assessment Results](#)

<input type="checkbox"/>	Package	Tool	Platform	Date	Status	Results
<input type="checkbox"/>	scarf-io 1.0	checkstyle 7.4	Ubuntu Linux 16.04 LTS 64-bit Xenial Xerus	08/24/2017 15:41	finished	225
<input type="checkbox"/>		error-prone 2.0.15			finished	6
<input type="checkbox"/>		Findbugs 3.0.1			finished	12
<input type="checkbox"/>		OWASP Dependency Check 1.4.4			finished	0
<input type="checkbox"/>		PMD 5.5.2			finished	44

Show numbering Show grouping

[Delete Assessment Results](#)

Filters no project scarf-io version 1.0 any tool any platform any date 50 items

Results status table with assessments complete and weakness counts

Auto refresh

Select assessments and click "View Assessment Results" to view

[View Assessment Results](#)

<input type="checkbox"/>	Package	Tool	Platform	Date	Status	Results
<input type="checkbox"/>	scarf-io 1.0	checkstyle 7.4	Ubuntu Linux 16.04 LTS 64-bit Xenial Xerus	08/24/2017 15:41	finished	225
<input type="checkbox"/>		error-prone 2.0.15			finished	6
<input type="checkbox"/>		Findbugs 3.0.1			finished	12
<input type="checkbox"/>		OWASP Dependency Check 1.4.4			finished	0
<input type="checkbox"/>		PMD 5.5.2			finished	44

Filters

Weakness count 48 / 48

Tool

- Checkstyle (2.1%)
- FindBugs (25%)
- PMD (72.9%)

Severity

- Unspecified (2.1%)
- Low (29.2%)
- Medium (64.6%)
- High (4.2%)

Codebase Location

Tool Overlaps

CWE

Status

- New (100%)

Displaying all weaknesses

Bulk Operations for the 48 matching weaknesses



Change status... ▾

Generate report ▾

Weaknesses

Id	Tool	Rule	CWE	Codebase Location	Status
10	FindBugs	ISB_TOSTRING_APPENDING	-	BugTrace.java:36	New ▾
5	FindBugs	ISB_TOSTRING_APPENDING	-	BugInstance.java:166	New ▾
48	PMD	Each class should declare at least one constructor	398	MetricSummary.java:3-90	New ▾
47	PMD	Bean members should serialize	398	InitialInfo.java:6	New ▾
46	PMD	Each class should declare at least one constructor	398	BugTrace.java:3-40	New ▾
45	PMD	Each class should declare at least one constructor	398	InstanceLocation.java:3-39	New ▾
44	PMD	Bean members should serialize	398	BugInstance.java:11	New ▾
43	PMD	Bean members should serialize	398	BugInstance.java:8	New ▾
42	PMD	Bean members should serialize	398	Location.java:4	New ▾
41	PMD	Each class should declare at least one constructor	398	Constants.java:3-79	New ▾
39	PMD	StdCyclomaticComplexity	-	ScarfXmlReader.java:467-510	New ▾
38	PMD	Method cyclomatic complexity	398	ScarfXmlReader.java:467-510	New ▾
37	PMD	StdCyclomaticComplexity	-	ScarfXmlReader.java:416-465	New ▾
36	PMD	Method cyclomatic complexity	398	ScarfXmlReader.java:416-465	New ▾
35	PMD	StdCyclomaticComplexity	-	ScarfXmlReader.java:289-334	New ▾
34	PMD	ModifiedCyclomaticComplexity	-	ScarfXmlReader.java:289-334	New ▾
33	PMD	Method cyclomatic complexity	398	ScarfXmlReader.java:289-334	New ▾
32	FindBugs	XXE_XMLSTREAMREADER	-	ScarfXmlReader.java:520	New ▾
31	PMD	StdCyclomaticComplexity	-	ScarfXmlReader.java:194-254	New ▾
30	PMD	Method cyclomatic complexity	398	ScarfXmlReader.java:194-254	New ▾
29	FindBugs	Potential path traversal (read file)	22	ScarfXmlReader.java:539	New ▾
28	PMD	StdCyclomaticComplexity	-	ScarfXmlReader.java:140-192	New ▾
27	PMD	Method cyclomatic complexity	398	ScarfXmlReader.java:140-192	New ▾
23	PMD	Bean members should serialize	398	ScarfXmlReader.java:32	New ▾
20	PMD	Bean members should serialize	398	ScarfXmlReader.java:31	New ▾

Showing 25 of 48 weaknesses. Displaying 1 to 25 of 48 Weaknesses

Filters

Weakness count 48 / 48

Tool

- Checkstyle (2.1%)
- FindBugs (25%)
- PMD (72.9%)

Severity

- Unspecified (2.1%)
- Low (29.2%)
- Medium (64.6%)
- High (4.2%)

Codebase Location

Tool Overlaps

CWE

Sta

Displaying all weaknesses

Bulk Operations for the 48 matching weaknesses Change status... Generate report

Weaknesses

Id	Tool	Rule	CWE	Codebase Location	Status
10	FindBugs	ISB_TOSTRING_APPENDING	-	BugTrace.java:36	New
5	FindBugs	ISB_TOSTRING_APPENDING	-	BugInstance.java:166	New
48	PMD	Each class should declare at least one constructor	398	MetricSummary.java:3-90	New
47	PMD	Bean members should serialize	398	InitialInfo.java:6	New
46	PMD	Each class should declare at least one constructor	398	BugTrace.java:3-40	New
45	PMD	Each class should declare at least one constructor	398	InstanceLocation.java:3-39	New
44	PMD	Bean members should serialize	398	BugInstance.java:11	New
43	PMD	Bean members should serialize	398	BugInstance.java:8	New
42	PMD	Bean members should serialize	398	Location.java:4	New

Sortable Weaknesses showing Tool, Rule (type), CWE, file and line (click for details)

Id	Tool	Rule	CWE	Codebase Location
10	FindBugs	ISB_TOSTRING_APPENDING	-	BugTrace.java:36
5	FindBugs	ISB_TOSTRING_APPENDING	-	BugInstance.java:166
48	PMD	Each class should declare at least one constructor	398	MetricSummary.java:3-90
47	PMD	Bean members should serialize	398	InitialInfo.java:6
46	PMD	Each class should declare at least one constructor	398	BugTrace.java:3-40
45	PMD	Each class should declare at least one constructor	398	InstanceLocation.java:3-39
44	PMD	Bean members should serialize	398	BugInstance.java:11

Weakness Flow

Filters

Weakness count 48 / 48

Tool

- Checkstyle (2.1%)
- FindBugs (25%)
- PMD (72.9%)

Severity

- Unspecified (2.1%)
- Low (29.2%)
- Medium (64.6%)
- High (4.2%)

Codebase Location

Tool Overlaps

CWE

Status

- New (100%)

Filters and Summary Data

Filters

Weakness count 48 / 48

Tool

- Checkstyle (2.1%)
- FindBugs (25%)
- PMD (72.9%)

Severity

- Unspecified (2.1%)
- Low (29.2%)
- Medium (64.6%)
- High (4.2%)

Codebase Location

Tool Overlaps

CWE

Status

- New (100%)

Displaying all weaknesses

Bulk Operations

Weaknesses

Id	Tool	Severity	Status
10			
5			
48			
47			
46			
45			
44			
43			
42			
41			
39			
38			
37			
36			
35			
34			
33			
32			
31			
30			
29			
28			
27			
23			
20	PMD	Bean members should serialize	398

Codebase Location	Status
BugTrace.java:36	New
BugInstance.java:166	New
MetricSummary.java:3-90	New
InitialInfo.java:6	New
BugTrace.java:3-40	New
InstanceLocation.java:3-39	New
BugInstance.java:11	New
BugInstance.java:8	New
Location.java:4	New
Constants.java:3-79	New
ScarfXmlReader.java:467-510	New
ScarfXmlReader.java:467-510	New
ScarfXmlReader.java:416-465	New
ScarfXmlReader.java:416-465	New
ScarfXmlReader.java:289-334	New
ScarfXmlReader.java:289-334	New
ScarfXmlReader.java:289-334	New
ScarfXmlReader.java:520	New
ScarfXmlReader.java:194-254	New
ScarfXmlReader.java:194-254	New
ScarfXmlReader.java:539	New
ScarfXmlReader.java:140-192	New
ScarfXmlReader.java:140-192	New
ScarfXmlReader.java:32	New
ScarfXmlReader.java:31	New

Projects

scarf-io » Analysis Run 1 Created on 7/19/2017 Uploaded on 7/19/2017 48 total weaknesses

View

Weakness Flow

Filters

Weakness count 48 / 48

Tool

- Checkstyle (2.1%)
- FindBugs (25%)
- PMD (72.9%)

Severity

- Unspecified (2.1%)
- Low (29.2%)
- Medium (64.6%)
- High (4.2%)

Codebase Location

Tool Overlaps

CWE

Status

- New (100%)

Displaying all weaknesses

Bulk Operations for the 48 matching weaknesses

Change status...

Weaknesses

Id	Tool	Rule	Severity	Status
10	FindBugs	ISB_TOSTRING_APPENDING	-	New
5	FindBugs	ISB_TOSTRING_APPENDING	-	New
48	PMD	Each class should declare at least one constructor	3	New
47	PMD	Bean members should serialize	3	New
46	PMD	Each class should declare at least one constructor	3	New
45	PMD	Each class should declare at least one constructor	3	New
44	PMD	Bean members should serialize	3	New
43	PMD	Bean members should serialize	3	New
42	PMD	Bean members should serialize	3	New
41	PMD	Each class should declare at least one constructor	3	New
39	PMD	StdCyclomaticComplexity	-	New
38	PMD	Method cyclomatic complexity	3	New
37	PMD	StdCyclomaticComplexity	-	New
36	PMD	Method cyclomatic complexity	3	New
35	PMD	StdCyclomaticComplexity	-	New
34	PMD	ModifiedCyclomaticComplexity	-	New
33	PMD	Method cyclomatic complexity	3	New
32	FindBugs	XXE_XMLSTREAMREADER	-	New
31	PMD	StdCyclomaticComplexity	-	New
30	PMD	Method cyclomatic complexity	3	New
29	FindBugs	Potential path traversal (read file)	2	New
28	PMD	StdCyclomaticComplexity	-	New
27	PMD	Method cyclomatic complexity	3	New
23	PMD	Bean members should serialize	398	New
20	PMD	Bean members should serialize	398	New

Triage Settings

scarf-io > Analysis Run 5 > Weakness 88 **Potential path traversal (read file)** detected by **FindBugs** [PATH_TRAVERSAL_IN]
 First seen on **9/1/2017** 29 weaknesses in this file 1 similar weakness in this analysis run **Medium** severity
CWE 22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') [[CWEVis](#) | [MITRE](#)]

jump to top ^

jump to weakness v

The weakness occurs in [scarf-io-build7-date2017-08-24-143804.zip/src/parser/ScarfXmlReader.java](#) on line **524**

```
499     } catch (XMLStreamException e) {
500         // TODO Auto-generated catch block
501         // printStackTrace();
```

Weakness type, tool and description.

scarf-io > Analysis Run 5 > Weakness 88 **Potential path traversal (read file)** detected by **FindBugs** [PATH_TRAVERSAL_IN]
 First seen on **9/1/2017** 29 weaknesses in this file 1 similar weakness in this analysis run **Medium** severity
CWE 22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') [[CWEVis](#) | [MITRE](#)]

Weakness location.

The weakness occurs in [scarf-io-build7-date2017-08-24-143804.zip/src/parser/ScarfXmlReader.java](#) on line **524**

```
519     }
520     parse();
521 }
522
523 public void parseFromFilepath(String filepath) {
524     File f = new File(filepath);
525     if (!f.exists()) {
526         System.err.println("Error: Invalid filepath");
527     }
528     else {
529         parseFromFile(f);
530     }
531 }
532
533 /*
534 public static void main(String[] args) {
535     System.out.println("1st arg: " + args[0]);
536     ScarfXmlReader r = new ScarfXmlReader();
537     r.parseFromFilepath(args[0]);
538 }
539 */
540
541 }
```

- admin**
7 minutes ago
Status set to **Gone** during Analysis Run 8 by **admin**
about an hour ago
- Status set to **Unresolved** during Analysis Run 7 by **admin**
about an hour ago
- Status set to **Gone** during Analysis Run 6 by **admin**
about an hour ago
- Status set to **Unresolved** during Analysis Run 3 by **admin**
4 days ago
- Status set to **New** during Analysis Run 2 by **admin**
7 days ago

Triage entry and viewing.

Status

Unresolved

Activity Stream

Post

Clear

Write comments with Markdown

Status set to **Unresolved** during Analysis Run 9 by **admin**

7 minutes ago

Status set to **Gone** during Analysis Run 8 by **admin**

about an hour ago

Status set to **Unresolved** during Analysis Run 7 by **admin**

about an hour ago

Status set to **Gone** during Analysis Run 6 by **admin**

about an hour ago

Status set to **Unresolved** during Analysis Run 3 by **admin**

4 days ago

Status set to **New** during Analysis Run 2 by **admin**

7 days ago

The weakness occurs in **scarf-io**

```
499     } catch (XMLStreamException e) {
500         // TODO Auto-generated catch block
501         //e.printStackTrace();
502         logger.error(e.getMessage());
503     }
504     return metric;
505 }
506 private boolean isEnabled() {
507     return (reader != null);
508 }
509
510 public void parseFromStream(InputStream in) throws IOException {
511     try {
512         XMLInputFactory xif = XMLInputFactory.newInstance();
513         XMLStreamReader reader = xif.createXMLStreamReader(in);
514     } catch (FileNotFoundException e) {
515         System.err.println(e.getMessage());
516     } catch (XMLStreamException e) {
517         System.err.println(e.getMessage());
518     }
519 }
520
521
522
523 public void parseFromFile(String filename) throws IOException {
524     File f = new File(filename);
525     if (!f.exists()) {
526         System.err.println("File not found: " + filename);
527     }
528     else {
529         parseFromStream(new FileInputStream(f));
530     }
531 }
532
533
534
535 public static void main(String[] args) {
536     ScarfXMLReader r = new ScarfXMLReader();
537     r.parseFromFile("test.xml");
538 }
539
540
541 }
```

Status

Unresolved

Activity Stream

Post

Clear

Write comments with Markdown

Status set to **Unresolved** during Analysis Run 9 by **admin**

7 minutes ago

Status set to **Gone** during Analysis Run 8 by **admin**

about an hour ago

Status set to **Unresolved** during Analysis Run 7 by **admin**

about an hour ago

Status set to **Gone** during Analysis Run 6 by **admin**

about an hour ago

Status set to **Unresolved** during Analysis Run 3 by **admin**

4 days ago

Status set to **New** during Analysis Run 2 by **admin**

7 days ago

Weakness 88 Details | Code Dx

jump to top

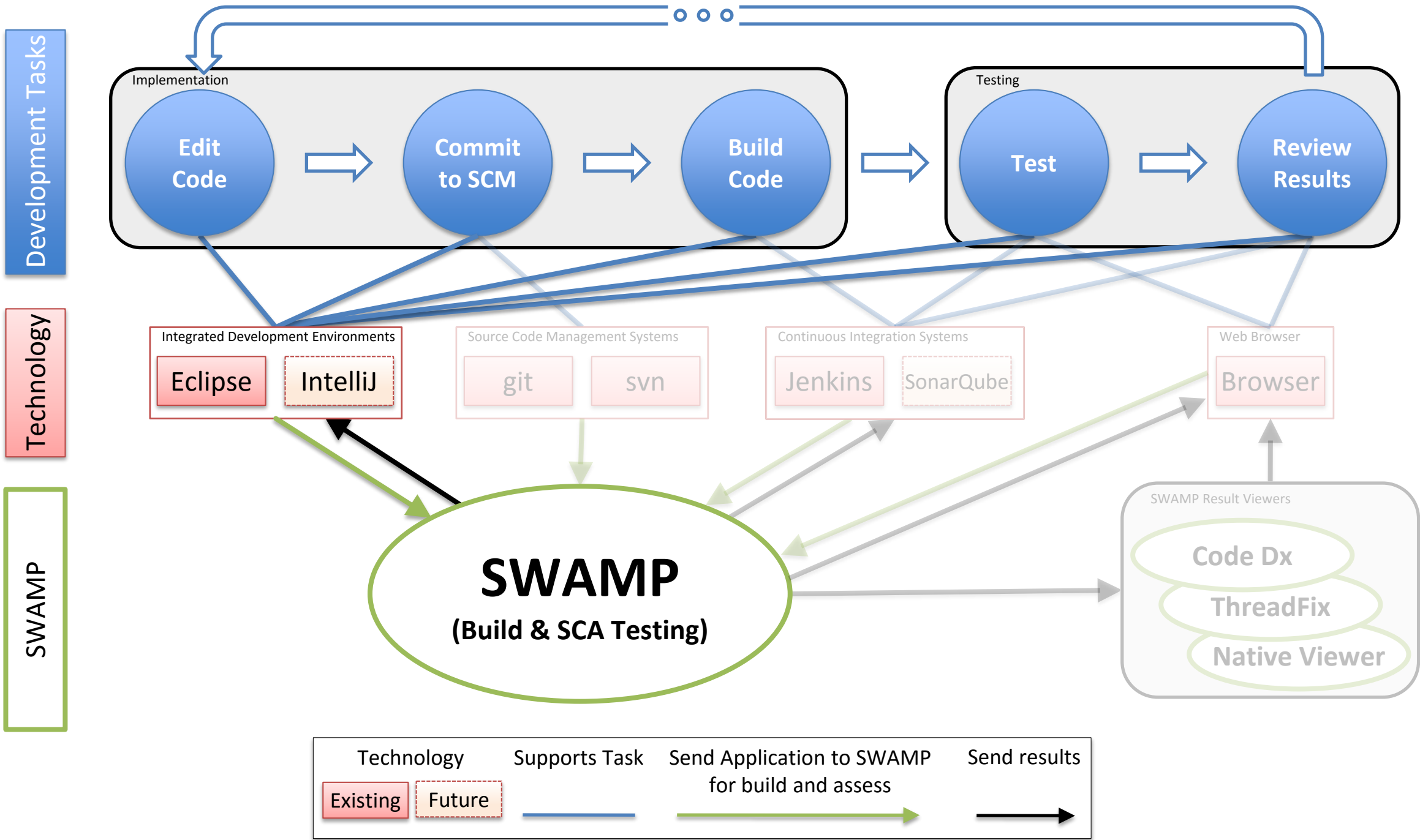
jump to weakness

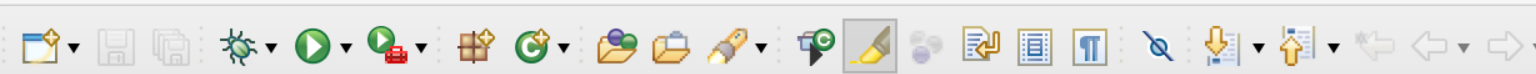
Line markers show current and other weaknesses



SWAMP Eclipse Plug-in

- Supports Java, C and C++
- Allows use of all the Java, C and C++ tools with no additional tool configuration or installation
- Requires minimal configuration
- Build information is extracted directly from Eclipse
- Source files, build script, and dependencies packaged and sent to SWAMP
- View results directly in Eclipse
- After configuration, one-click on the SWAMP button reassesses
- Available from the Eclipse marketplace (search for swamp)





Package Explorer

- scarf-io3 [scarf-io3 master]
 - src
 - (default package)
 - Constants.java
 - ScarfInterface.java
 - ScarfXmlReader.java**
 - datastructures
 - Referenced Libraries
 - JRE System Library [Java SE 8 [1.8.0]]
 - Assessment_Output
 - lib
 - build.xml
 - LICENSE
 - package.conf
 - README.md
 - scarf-io3.iml

```

ScarfXmlReader.java
513
514 public void parseFromFile(File f) {
515     InputStream stream = null;
516     try {
517         XMLInputFactory factory = XMLInputFactory.newIns
518             stream = new FileInputStream(f);
519         reader = factory.createXMLStreamReader(stream);
520     } catch (FileNotFoundException e) {
521         System.err.println("Error: Unable to open XML st
522     } catch (XMLStreamException e) {
523         System.err.println("Error: Unable to open XML st
524     } finally {
525         if (stream != null){
526             try {
527                 stream.close();
528             } catch (IOException e) {
529                 // TODO Auto-generated catch block
530                 logger.error(errMsg, e);
531             }
532         }
533     }
534     parse();
535 }
    
```

Outline

- ScarfXmlReader
 - reader : XMLStreamReader
 - scarfCallbacks : ScarfInterface
 - logger : Logger
 - errMsg : String
 - ScarfXmlReader(ScarfInterface)
 - parse() : void
 - handleElement(String) : void
 - handleAnalyzerReport() : InitialInfo
 - getChars(String) : String
 - handleMetricSummaries() : List<Metric
 - handleMetricSummary() : MetricSumma
 - handleBugInstance() : BugInstance
 - handleBugTrace() : BugTrace
 - handleInstanceLocation() : InstanceLoca
 - handleBugSummary() : BugSummary
 - handleBugCategory() : BugCategory
 - handleMethods() : List<Method>

Problems @ Javadoc Declaration


0 items

Description	Resource	Path	Location	Type

Eclipse Marketplace

Select solutions to install. Press Install Now to proceed with installation.
Press the "more info" link to learn more about a solution.



Search Recent Popular Favorites Installed  Eclipse Newsletter (July)

Find:

SWAMP Eclipse Plug-in



The SWAMP Eclipse Plug-in allows users to easily run static analysis tools available on the Software Assurance Marketplace (<https://www.continuousassurance.org/>)... [more info](#)

by [Software Assurance Marketplace](#), Apache 2.0
[software assurance static analysis SWAMP Source Code Analyzer](#)



Installs: **43** (3 last month)

Marketplaces



< Back

Install Now >

Cancel

Finish

Install the SWAMP Eclipse
plug-in from within Eclipse
(search for "SWAMP")

SWAMP Eclipse plug-in is now installed. Showing

- 1 SWAMP menu and
- 2 SWAMP perspective button

```
514 public void parseFromFile(File f) {  
522     }catch (XMLStreamException e) {  
523         System.err.println("Error: Unable to open XML st  
524     }finally {  
525         if (stream != null){  
526             try {  
527                 stream.close();  
528             } catch (IOException e) {  
529                 // TODO Auto-generated catch block  
530                 logger.error(errMsg, e);  
531             }  
532         }  
533     }  
534     parse();  
535 }
```

Package Explorer

- scarf-io3 [scarf-io3 master]
 - src
 - Referenced Libraries
 - JRE System Library [Java SE 8 [1.8.
 - Assessment_Output
 - lib
 - build.xml
 - LICENSE
 - package.conf
 - README.md
 - scarf-io3.iml

ScarfXmlReader

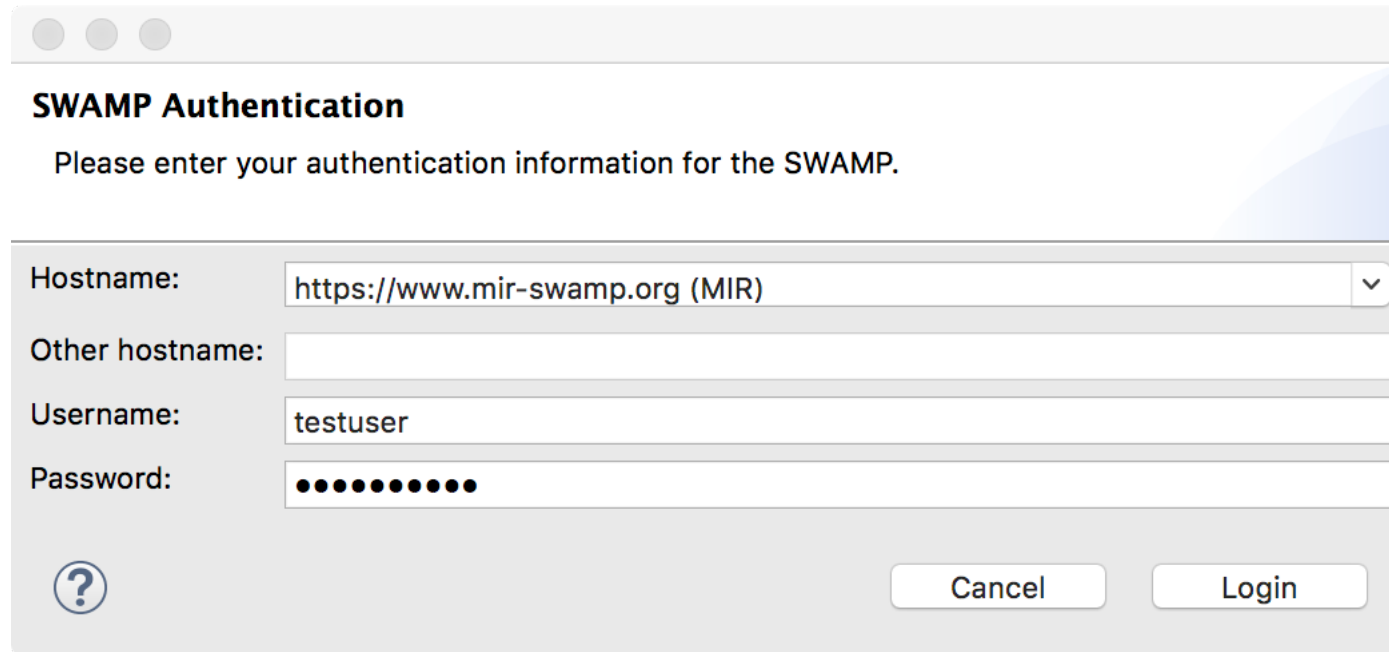
- reader : XMLStreamReader
- scarfCallbacks : ScarfInterface
- logger : Logger
- errMsg : String
- ScarfXmlReader(ScarfInterface)
- parse() : void
- handleElement(String) : void
- handleAnalyzerReport() : InitialInfo
- getChars(String) : String
- handleMetricSummaries() : List<MetricS
- handleMetricSummary() : MetricSumma
- handleBugInstance() : BugInstance
- handleBugTrace() : BugTrace
- handleInstanceLocation() : InstanceLoca
- handleBugSummary() : BugSummary
- handleBugCategory() : BugCategory
- handleMethods() : List<Method>

Problems

0 items

Description	Resource	Path	Location	Type

One time configuration of SWAMP hostname and user's SWAMP credentials



SWAMP Authentication


Please enter your authentication information for the SWAMP.

Hostname:

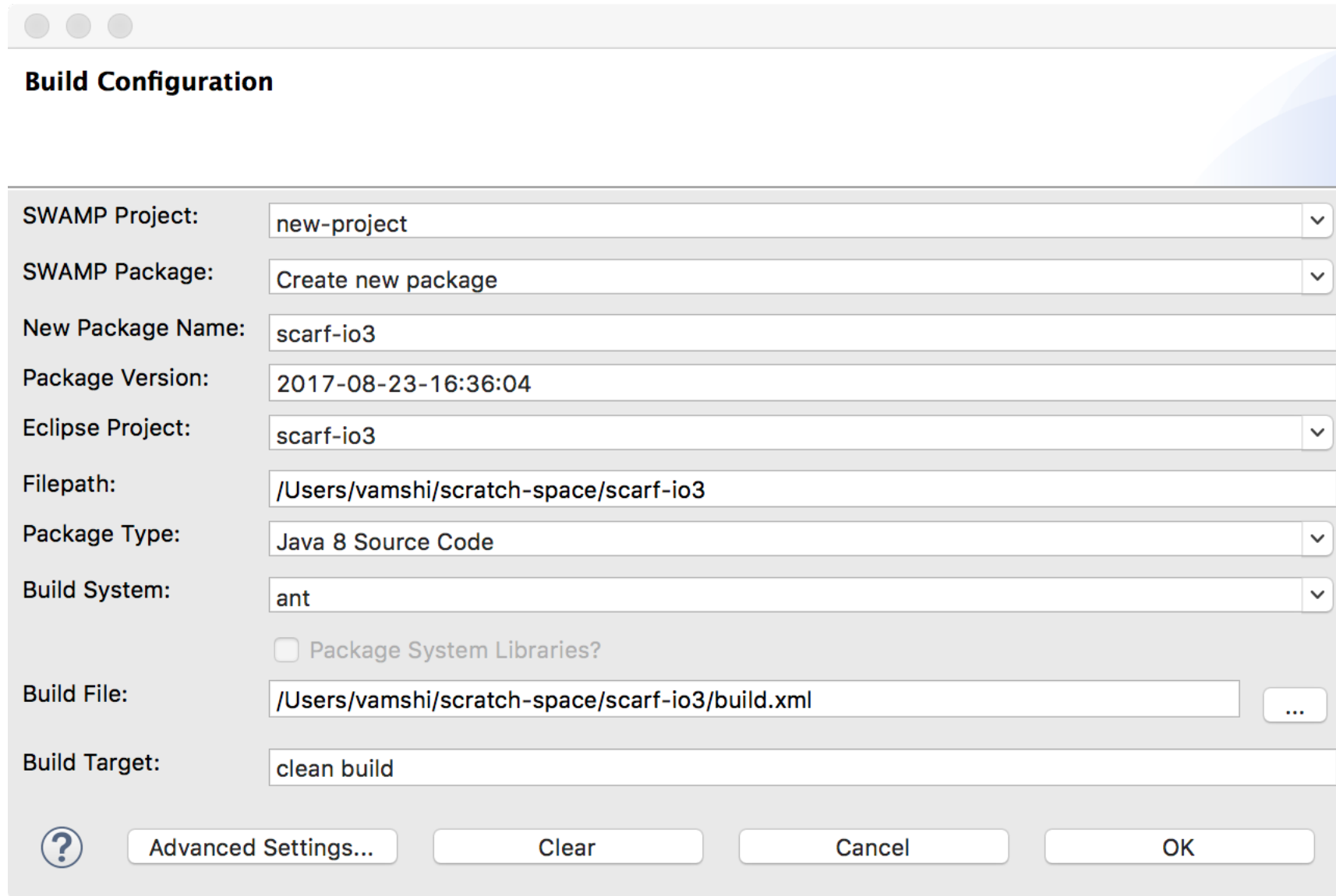
Other hostname:

Username:

Password:



Package configuration (default values should work without modification)

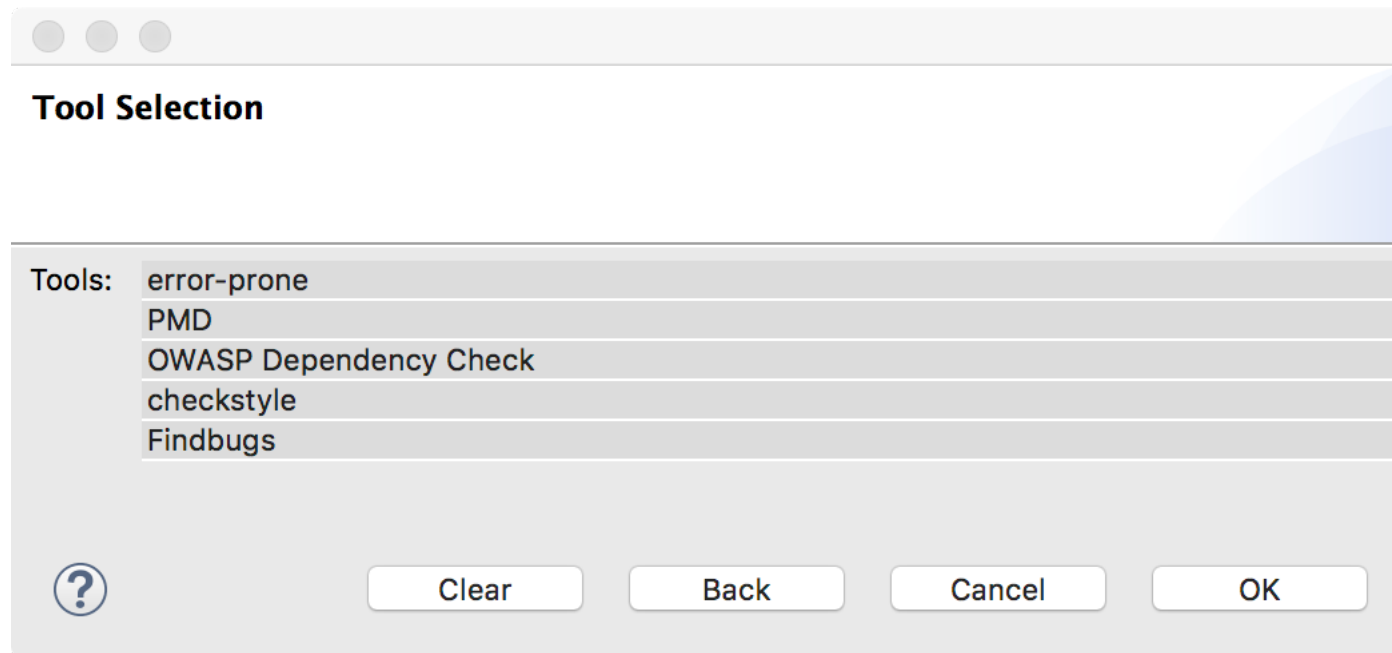


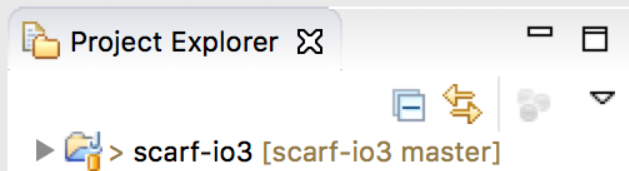
The image shows a 'Build Configuration' dialog box with the following fields and values:

- SWAMP Project: new-project
- SWAMP Package: Create new package
- New Package Name: scarf-io3
- Package Version: 2017-08-23-16:36:04
- Eclipse Project: scarf-io3
- Filepath: /Users/vamshi/scratch-space/scarf-io3
- Package Type: Java 8 Source Code
- Build System: ant
- Package System Libraries?
- Build File: /Users/vamshi/scratch-space/scarf-io3/build.xml
- Build Target: clean build

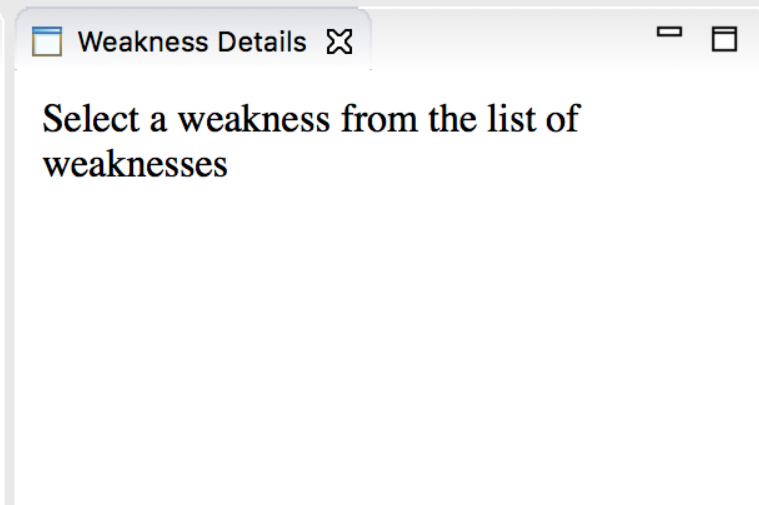
Buttons at the bottom: ? (Help), Advanced Settings..., Clear, Cancel, OK.

Tool selection (default is all tools)





```
ScarfXmlReader.java
525         if (stream != null){
526             try {
527                 stream.close();
528             } catch (IOException e) {
529                 // TODO Auto-generated catch block
530                 logger.error(errMsg, e);
531             }
532         }
533     }
534     parse();
535 }
536
537 public void
538 File f
539 if (f.e
540     pa
541 } else
542     Sys
543 }
544 }
545 }
```



SWAMP Assessment Status Dashboard after clicking SWAMP menu to start an assessment, showing 5 in-progress assessments

SWAMP Package ^	Version	Tool	Submission Time	Status	Count
scarf-io3	2017-08-23-16:50:42	error-prone	2017-08-23-16:51:05	Performing assessment	
scarf-io3	2017-08-23-16:50:42	PMD	2017-08-23-16:51:06	Performing assessment	
scarf-io3	2017-08-23-16:50:42	OWASP Dependency Check	2017-08-23-16:51:06	Starting assessment r...	
scarf-io3	2017-08-23-16:50:42	checkstyle	2017-08-23-16:51:07	Performing assessment	
scarf-io3	2017-08-23-16:50:42	Findbugs	2017-08-23-16:51:07	Performing assessment	



Quick Access



Project Explorer

scarf-io3 [scarf-io3 master]

```
ScarfXmlReader.java
525         if (stream != null){
526             try {
527                 stream.close();
528             } catch (IOException e) {
529                 // TODO Auto-generated catch block
530                 logger.error(errMsg, e);
531             }
532         }
533     }
534     parse();
535 }
536
537 public void parseFromFilepath(String filepath) {
538     F
539     i
540
541 }
542
543 }
544
545 }
```

Weakness Details

Select a weakness from the list of weaknesses

**SWAMP Assessment Status Dashboard
after assessments finish, showing weakness counts**

Weaknesses Assessment Status Dashboard Console

SWAMP Package ^	Version	Tool	Submission Time	Status	Count
scarf-io3	2017-08-23-16:50:42	error-prone	2017-08-23-16:51:05	Finished	6
scarf-io3	2017-08-23-16:50:42	PMD	2017-08-23-16:51:06	Finished	44
scarf-io3	2017-08-23-16:50:42	checkstyle	2017-08-23-16:51:07	Finished	225
scarf-io3	2017-08-23-16:50:42	Findbugs	2017-08-23-16:51:07	Finished	12
scarf-io3	2017-08-23-16:50:42	OWASP Dependency Check	2017-08-23-16:51:06	Finished	0

- ① SWAMP Weakness panel showing the table of weaknesses with the weakness on line 538 selected
- ② markers indicating a weakness on the line
- ③ weakness details

```

532     }
533     }
534     parse();
535     }
536
537     public void parseFromFilePath(String filepath) {
538         File f = new File(filepath);
539         if (f.exists()) {
540             parseFromFile(f);
541         } else {
542             System.err.println("Error: Invalid filepath");
543         }
544     }
545

```

Weakness Details

Message: File(...) reads a file whose location might be specified by user input
Bug Path:

Resolution:

Line number: 538

File name: scarf-io3/src/ScarfXmlReader.java

Weakness group: SECURITY

Weakness code: PATH_TRAVERSAL_IN

Tool: findbugs 3.0.1

Weaknesses Assessment Status Dashboard

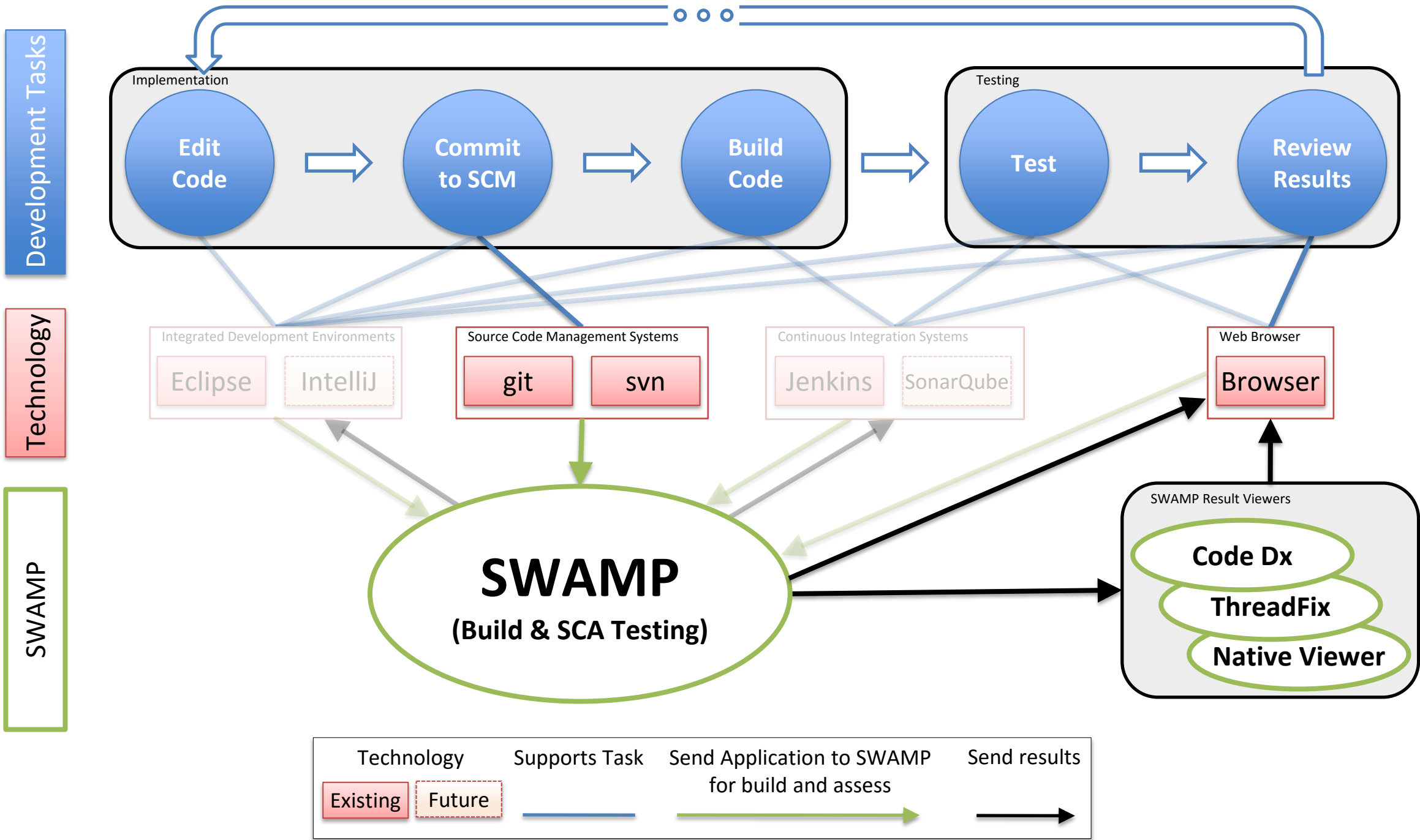
Show All/Show File

File	Start Line	End Line	Group
scarf-io3/src/datastructures/InstanceLocation.java	34	34	PERFORMANCE
scarf-io3/src/ScarfXmlReader.java	194	194	STYLE
scarf-io3/src/ScarfXmlReader.java	140	140	STYLE
scarf-io3/src/ScarfXmlReader.java	538	538	SECURITY
scarf-io3/src/ScarfXmlReader.java	519	519	SECURITY
scarf-io3/src/datastructures/BugSummary.java	7	7	JavaBeans



SWAMP SCMS plug-ins

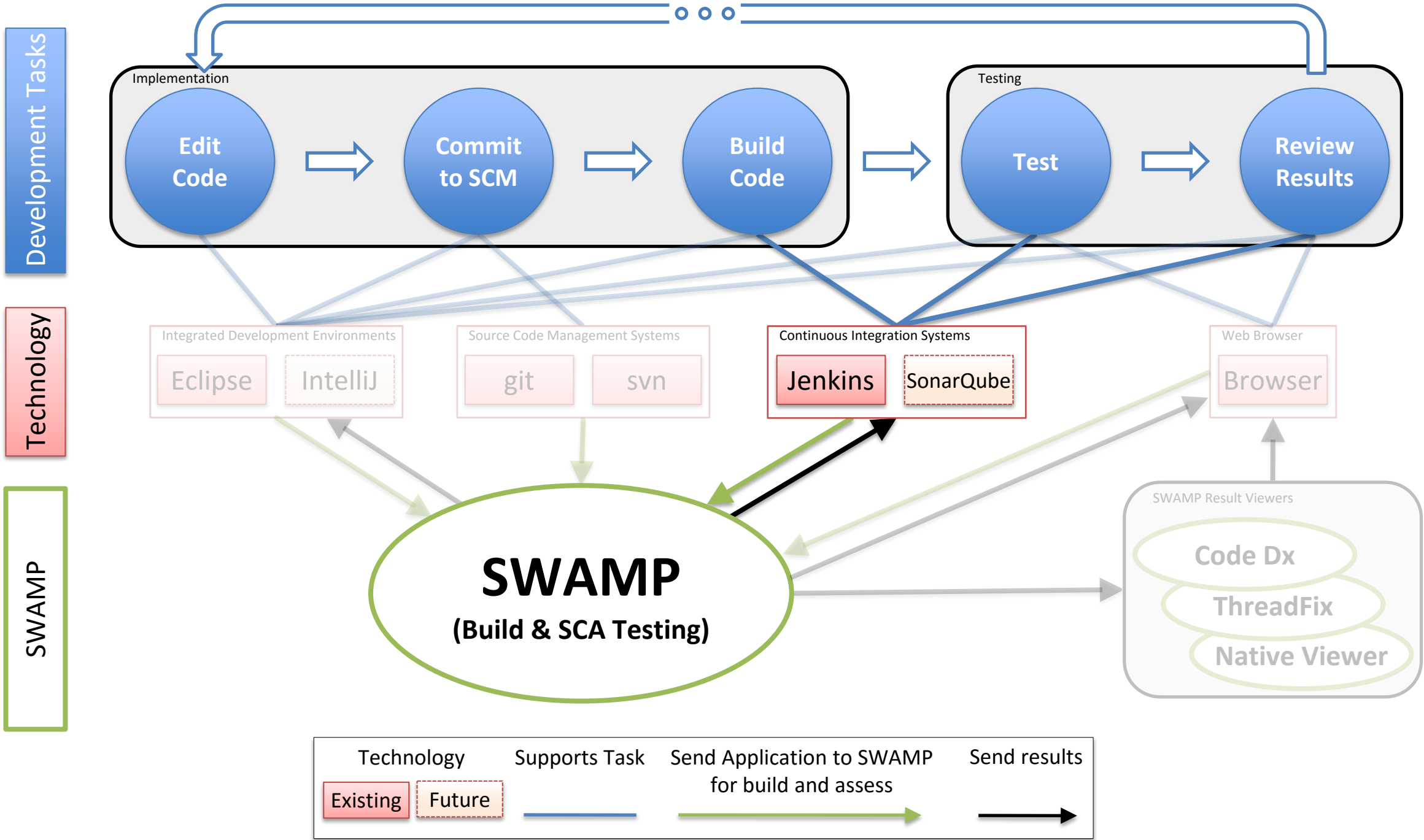
- Supports all SWAMP languages and tools
- Requires one-time configuration of how to build the software
- No inherent UI
 - Configuration is done with text files
 - Results must be download or viewed using the SWAMP web UI
- Can trigger assessment based on
 - Commits or merges
 - Specific branches
- Available from github at <https://github.com/mirswamp/swamp-scms-plugin>





SWAMP Jenkins Plug-in

- Supports all SWAMP languages and tools
- Requires one-time configuration of how to build the software
- View results and trend data directly in Jenkins
- After configuration, the configured SWAMP tools are run each time the packages is built and tested using Jenkins' mechanisms
 - Scheduled
 - Events such as SCMS check-in
 - On-demand
- Available from the Jenkins marketplace (search for swamp)





Jenkins

[ENABLE AUTO REFRESH](#)

[New Item](#)

[People](#)

[Build History](#)

[Manage Jenkins](#)

[My Views](#)

[Credentials](#)

[add description](#)

All +

S	W	Name ↓	Last Success	Last Failure	Last Duration
		scarf-io3	17 min - #2	N/A	8 min 4 sec

Icon: [S](#) [M](#) [L](#)

[Legend](#) [RSS for all](#) [RSS for failures](#) [RSS for just latest builds](#)

Build Queue —

No builds in the queue.

Build Executor Status —

1 Idle
2 Idle

Back to Dashboard

Manage Jenkins

Filter: swa

Updates Available Installed Advanced

Install ↓	Name	Version
<input type="checkbox"/>	Self-Organizing Swarm Plug-in Modules	3.4
<input checked="" type="checkbox"/>	SWAMP Plugin This plugin submits and assesses your package on the SWAMP and gives back the results of the test.	1.0.3
<input type="checkbox"/>	jenkins-testswarm-plugin	1.2
<input type="checkbox"/>	Wall Display Master Project	0.6.34

Install without restart

Download now and install after restart

Update information obtained: 56 n

Install the SWAMP Jenkins plug-in from Plugin Manager page (search for "SWAMP")

One time configuration of SWAMP hostname and user's SWAMP credentials

- Environment variables
- Tool Locations

SWAMP

Swamp Username ?

Swamp Password ?

SWAMP URL ?

Success

Default Project ?

Verbose Mode ?

Usage Statistics

- Help make Jenkins better by sending anonymous usage statistics and crash reports to the Jenkins project. ?

Timestamper

System clock time format ?



SWAMP Assessment

Package Settings

Package Directory	<input type="text"/>	?
Package Name	scarf-io3	?
Package Version	build:\$build-date:\$date	?
Package Language	Java	?
Package Language Version	<input type="text"/>	?

Save Apply

Build Settings

Configure package name and type

Build Settings

Build System	<input type="text" value="ant"/>	?
Build Directory	<input type="text"/>	?
Build File	<input type="text"/>	?
Build Target	<input type="text" value="clean build"/>	?
Build Command	<input type="text"/>	?
Build Options	<input type="text"/>	?
Configuration Command	<input type="text"/>	?
Configuration Options	<input type="text"/>	?
Configuration Directory	<input type="text"/>	?

Save

Apply

Assessment Settings

Project Name

Configure
build
settings

General

Source Code Management

Build Triggers

Build Environment

Build

Post-build Actions

Assessment Settings

Project Name

new-project

Assessments

Tool

Findbugs

Platform

Ubuntu Linux

Tool

PMD

Platform

Ubuntu Linux

Tool

error-prone

Platform

Ubuntu Linux

Save

Apply

Select tools

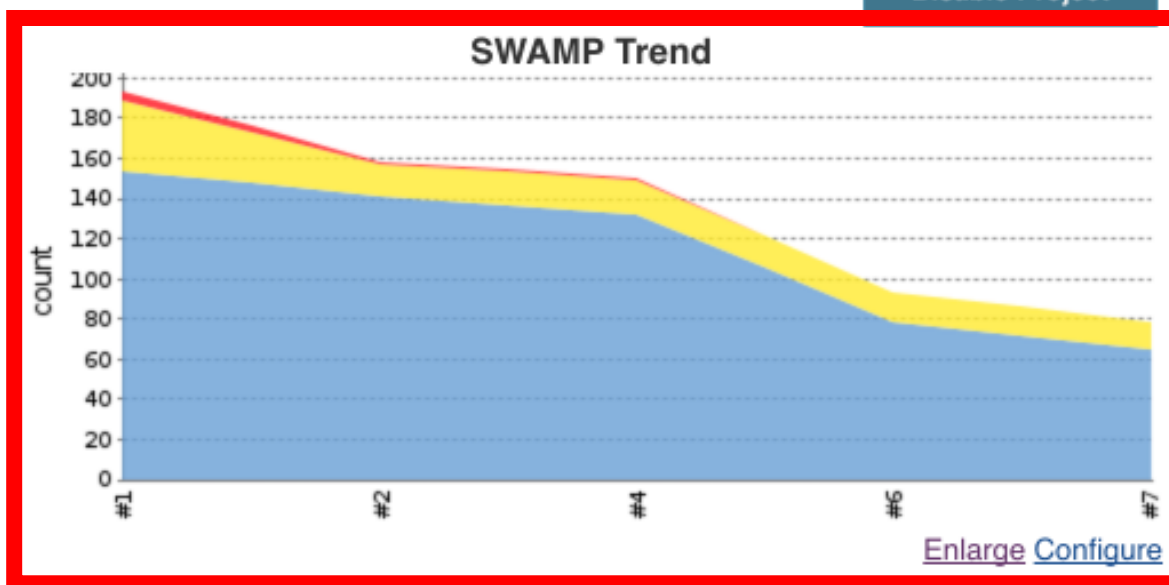
- Back to Dashboard
- Status
- Changes
- Workspace
- Build Now
- Delete Project
- Configure
- SWAMP Warnings

Project scarf-io

[add description](#)

Disable Project

- [Workspace](#)
- [Recent Changes](#)



Permalinks








- [Last build \(#7\), 6 min 56 sec ago](#)
- [Last stable build \(#7\), 6 min 56 sec ago](#)
- [Last successful build \(#7\), 6 min 56 sec ago](#)
- [Last completed build \(#7\), 6 min 56 sec ago](#)

Build History trend

find x

#7	Aug 24, 2017 2:38 PM
#6	Aug 24, 2017 2:28 PM
#4	Aug 24, 2017 2:21 PM
#2	Aug 24, 2017 1:56 PM
#1	Aug 24, 2017 12:02 PM

Main Jenkins dashboard displays a trend graph of SWAMP weaknesses with colors indicating severity

-  [Back to Project](#)
-  [Status](#)
-  [Changes](#)
-  [Console Output](#)
-  [Edit Build Information](#)
-  [Delete Build](#)
-  **SWAMP Assessment**

① Warnings Trend

All Warnings	New Warnings	Fixed Warnings
193	193	0

② Summary

Total	High Priority	Normal Priority	Low Priority
193	5	35	153

Details

③

Folders	Files	Categories	Types	Warnings	Origin	Details	New	High	Normal
Low									

④

Source Folder	Total	Distribution
src	105	
src/datastructures	88	
Total	193	

View SWAMP Results

- ① Trend Summary
- ② Priority Summary
- ③ Select grouping category
- ④ Sortable summary table grouped by *Folders*

Details

- Folders
- Files**
- Categories
- Types
- Warnings
- Origin
- Details
- New
- High
- Normal

Low

File	Total	Distribution
BugCategory.java	12	
BugInstance.java	21	
BugSummary.java	5	
BugTrace.java	5	
Constants.java	2	
InitialInfo.java	9	
InstanceLocation.java	10	
Location.java	4	
Method.java	7	
Metric.java	6	
MetricSummary.java	9	
ScarfInterface.java	13	
ScarfXmlReader.java	90	
Total	193	

Weakness data grouped by *Files*

Folders	Files	Categories	Types	Warnings	Origin	Details	New	High	Normal
Low	①	②	③	④	⑤				
File	Source Folder	Priority ↓	Type	Category					
ScarfXmlReader.java:110	src	High	findbugs:STYLE	LSC_LITERAL_STRING_COM					
ScarfXmlReader.java:309	src	High	findbugs:STYLE	LSC_LITERAL_STRING_COM					
ScarfXmlReader.java:339	src	High	findbugs:STYLE	LSC_LITERAL_STRING_COM					
ScarfXmlReader.java:365	src	High	findbugs:STYLE	LSC_LITERAL_STRING_COM					
BugSummary.java:22	src/datastructures	High	findbugs:CORRECTNESS	LSYC_LOCAL_SYNCHRONIZI					
Constants.java:2	src	Low	pmd:Controversial	AtLeastOneConstructor					
ScarfXmlReader.java:463	src	Low	pmd:Java Logging	AvoidPrintStackTrace					
MetricSummary.java:81	src/datastructures	Low	pmd:Optimization	UseStringBufferForStringApper					
MetricSummary.java:80	src/datastructures	Low	pmd:Optimization	UseStringBufferForStringApper					
MetricSummary.java:3	src/datastructures	Low	pmd:Controversial	AtLeastOneConstructor					
ScarfXmlReader.java:96	src	Low	pmd:Controversial	OnlyOneReturn					
Metric.java:55	src/datastructures	Low	pmd:Optimization	UseStringBufferForStringApper					
Metric.java:54	src/datastructures	Low	pmd:Optimization	UseStringBufferForStringApper					
Metric.java:53	src/datastructures	Low	pmd:Optimization	UseStringBufferForStringApper					
Metric.java:52	src/datastructures	Low	pmd:Optimization	UseStringBufferForStringApper					
Metric.java:3	src/datastructures	Low	pmd:Controversial	AtLeastOneConstructor					
Method.java:6	src/datastructures	Low	pmd:Design	ImmutableField					
Method.java:6	src/datastructures	Low	pmd:JavaBeans	BeanMembersShouldSerialize					

Sortable Warnings Table

- ① File and line number
- ② Containing folder
- ③ Priority
- ④ Tool type and major warning category
- ⑤ Minor warning category

Folders | Files | Categories | Types | Warnings | Origin | **Details** | New | High | Normal

Low

Constants.java:2 , pmd:Naming, Priority: Low
All classes and interfaces must belong to a named package
Constants.java:2 , pmd:Controversial, Priority: Low
Each class should declare at least one constructor
ScarfInterface.java:8 , pmd:Naming, Priority: Low
All classes and interfaces must belong to a named package
ScarfInterface.java:10 , error-prone, Priority: Low
[StaticOrDefaultInterfaceMethod] Static and default methods in interfaces are not allowed in android builds.
ScarfInterface.java:10 , pmd:Unused Code, Priority: Low
Avoid modifiers which are implied by the context
ScarfInterface.java:14 , error-prone, Priority: Low

Warnings Details includes a description of the weakness

Jenkins x

localhost:8080/job/scarf-io/7/swampResult/source.-7392930067175371306/#514

Jenkins > scarf-io > #7 > SWAMP Assessment > ScarfXmlReader.java

View source code of
weakness location

```
516     System.err.println("Error: Unable to open XML stream in specified file");
517 } catch (XMLStreamException e) {
518     System.err.println("Error: Unable to open XML stream in specified file");
519 }
520 parse();
521 }
522
523 public void parseFromFilepath(String filepath) {
524     File f = new File(filepath);
525     if (!f.exists()) {
526         System.err.println("Error: Invalid filepath");
527     }
528     else {
529         parseFromFile(f);
530     }
531 }
532
533 /*
534 public static void main(String[] args) {
535     System.out.println("1st arg: " + args[0]);
536     ScarfXmlReader r = new ScarfXmlReader();
537     r.parseFromFilepath(args[0]);
538 }
539 */
540
541 }
```




SWAMP Java API and Command Line Interface



- Integrate new tools and workflows with the SWAMP
- Allows Java programs or scripts to
 - Create new packages
 - Upload new versions
 - Get list of packages, package versions, tools, platforms, create assessments, check status of assessments, and download results
- Requires one-time configuration of how to build the software
- Results can be downloaded or viewed using the SWAMP web UI
- Available from github at <https://github.com/mirswamp/java-cli>



Software Products

SWAMP is all open source

Separate Products include

- SWAMP-in-a-Box
- SWAMP Eclipse plug-in
- SWAMP Jenkins plug-in
- Git and subversion plug-ins
- Java API and CLI library
- Build monitoring frameworks
- SCARF input/output library
- SCARF DB loads SCARF into a database

<https://continuousassurance.org/open-source-software/>

Questions?

<https://continuousassurance.org>
swamp@continuousassurance.org



SWAMP
SOFTWARE **ASSURANCE** MARKETPLACE