CYBER SECURITY DIVISION

2014 R&D SHOWCASE AND TECHNICAL WORKSHOP

SWAMP: Removing the Barriers to Adopting and Improving Software Assurance Capabilities

Morgridge Institute for Research

Miron Livny

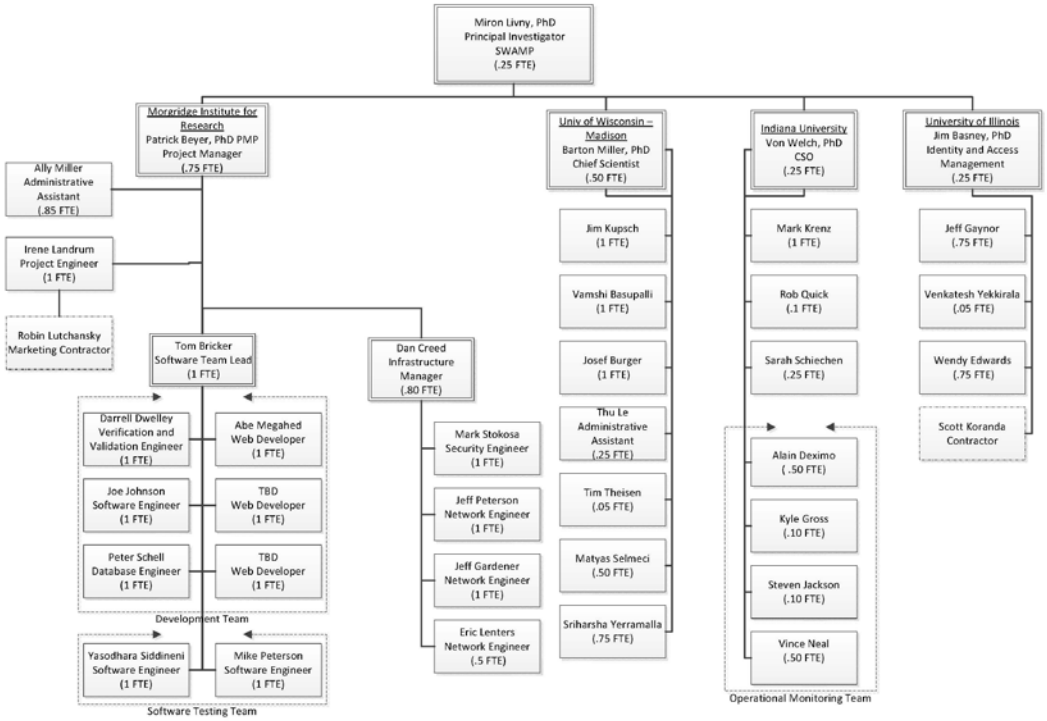
12/18/2014

Homeland Security

Science and Technology

Software Assurance Marketplace (SWAMP) Team

Designing, building, and operating the **SWAMP** is a joint effort of four research institutions: Morgridge Institute for Research (lead), Indiana University, University of Illinois Urbana-Champaign, and University of Wisconsin-Madison.



Miron Livny, MIR

Jim Basney, UIUC

Bart Miller, UW

Von Welch, IU

Consumer Need

- Developers of software assurance tools need effective means to continuously evaluate their technologies.
- Software developers need effective continuous software assurance capabilities that they can integrate into their development workflows without impacting their time to market.
- Consumers of software components need services that enable them to evaluate the quality of the components they deploy or integrate into their software stack.
- Educators need to expose their students to a diverse collection of state-of-the-art software assurance technologies.
- The community as a whole needs an open and powerful facility that supports the managed sharing of tools and software packages and viewing combined results of multiple tools.

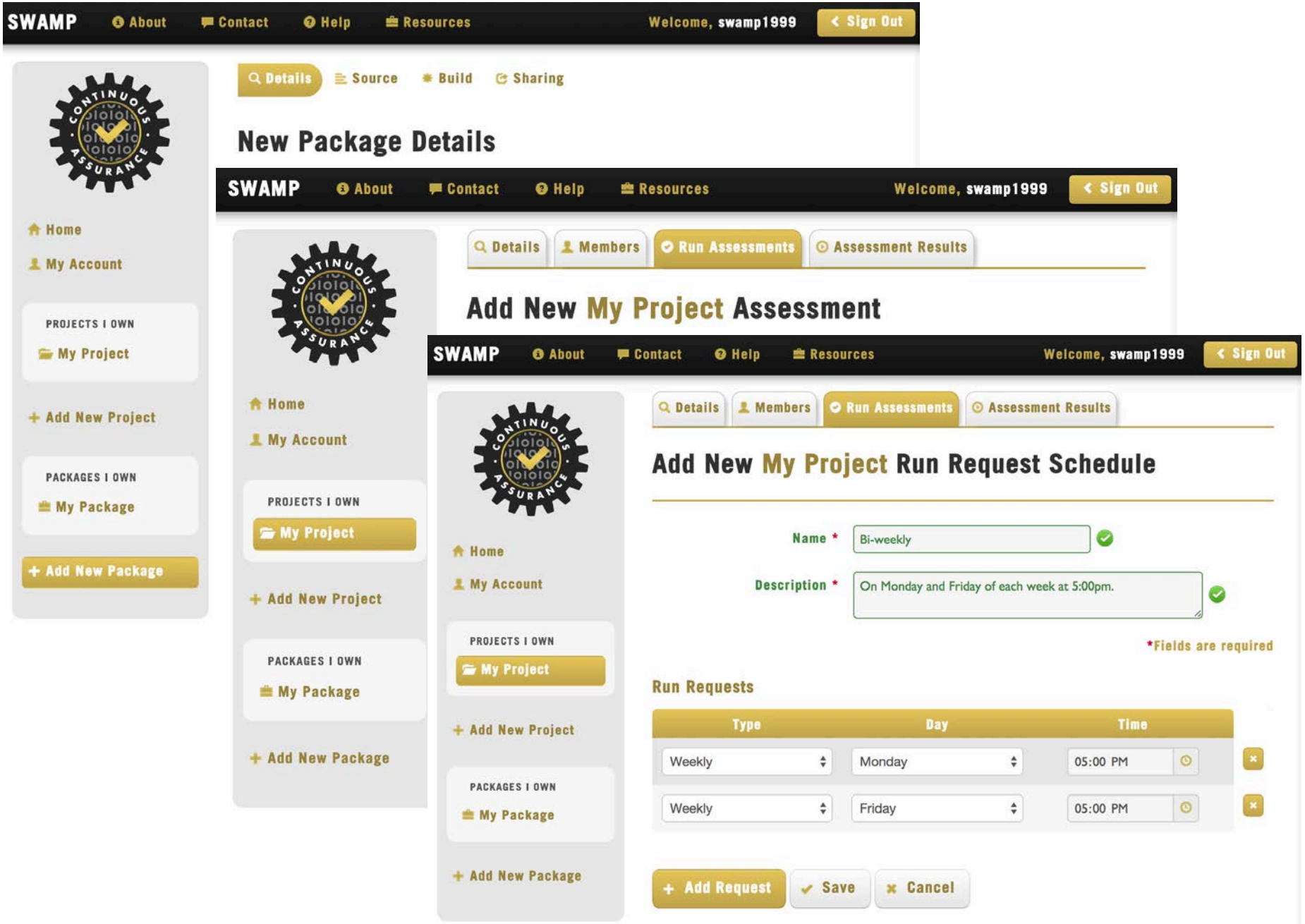
Lower the barriers and increase the value!

Approach

- Offer a unified interface to a diverse set of software assurance tools
  - Develop software capabilities for invoking tools and collecting assessment results
  - Facilitate the unique needs (technical and legal) of commercial tools
- Provide a rich suite of software packages for tool evaluation
- Design, build, and operate an open facility that meets the diverse and changing needs of the community
  - Flexible data model that treats packages, tools, and assessment results as first-class objects
  - Secure operation that supports privacy and enables managed sharing
  - Powerful and extensible processing and storage capacity
  - Active interaction with the community to identify trends, promote adoption, and collect feedback

Approach (Cont.)

- Allow for easy integration of SWAMP capabilities with existing software development workflows via application programming interfaces (APIs)
  - Minimize the barriers to registration, uploading software packages, running assessments, and viewing the results from multiple tools
  - Integration with commonly used IDEs
  - Integration with commonly used software repositories
- Allow the deployment of private SWAMPs for sensitive software (a network of SWAMPs)
  - All software is developed under Apache license
  - Managed as an open-source project


SWAMP
About
Contact
Help
Resources
Welcome, swamp1999
Sign Out
Details
Source
Build
Sharing
New Package Details
Home
My Account
PROJECTS I OWN
My Project
Add New Project
PACKAGES I OWN
My Package
Add New Package
Members
Run Assessments
Assessment Results
Add New My Project Assessment
Add New My Project Run Request Schedule
Name *
Bi-weekly
Description *
On Monday and Friday of each week at 5:00pm.
*Fields are required
Run Requests
Type
Day
Time
Weekly
Monday
05:00 PM
Weekly
Friday
05:00 PM
Add Request
Save
Cancel

SWAMP | About | Contact | Help | Resources | Policies | Welcome, pbeyeradmin | Sign Out

Details | Members | Run Assessments | Assessment Results

TEst Assessment Results

Filters

snappy-c > Analysis Run 5 | Code Dx

https://swa-csaweb-pd-01.mir-swamp.org/proxy-3A696410-7BFE-11E4-9C62-E091AF31F99C/run/5/

Projects | Help | Logged in as pbeyeradmin | version 1.5.1-SW-1 - 9/29/2014 | CodeDx

snappy-c » Analysis Run 5

Created on 12/4/2014 | Uploaded on 12/4/2014 | 188 total weaknesses | View

Weakness Flow

Filters

Weakness count 188 / 188

Tool
- Clang (2.1%)
- Cppcheck (1.1%)
- GCC (96.8%)

Severity
- Unspecified (10.6%)
- Low (85.1%)
- Medium (3.2%)
- High (1.1%)

Codebase Location

Tool Overlaps

CWE

Status
- New (100%)

Displaying all weaknesses

Bulk Operations for the 188 matching weaknesses | Change status... | Generate report

Weaknesses

Id	Tool	Rule	CWE	Severity	Codebase Location	Status
318	Clang	Undefined allocation of 0 bytes (CERT MEM04-C; CWE-1...	131	High	sgverify.c:116	New
317	Clang	Undefined allocation of 0 bytes (CERT MEM04-C; CWE-1...	131	High	sgverify.c:40	New
484	GCC	GNU C returns a bogus size for function types and void	440	Medium	sgverify.c:44	New
380	GCC	GNU C returns a bogus size for function types and void	440	Medium	snappy.c:294	New
376	GCC	GNU C returns a bogus size for function types and void	440	Medium	snappy.c:273	New
372	GCC	GNU C returns a bogus size for function types and void	440	Medium	snappy.c:244	New
323	Cppcheck	invalidPrintfArgType_sint	-	Medium	sgverify.c:180	New
319	Clang	Result of operation is garbage or undefined	457	Medium	snappy.c:284	New
501	GCC	Unused function parameter	398	Low	sgverify.c:72	New
500	GCC	Suspicious conversion	704	Low	sgverify.c:182	New
499	GCC	Mixed declarations and Code	398	Low	sgverify.c:173	New
498	GCC	Suspicious conversion	704	Low	sgverify.c:167	New
497	GCC	Mixed declarations and Code	398	Low	sgverify.c:161	New
496	GCC	Mixed declarations and Code	398	Low	sgverify.c:151	New
495	GCC	Mixed declarations and Code	398	Low	sgverify.c:145	New
494	GCC	signed to unsigned conversion	195	Low	sgverify.c:130	New
493	GCC	Mixed declarations and Code	398	Low	sgverify.c:126	New
492	GCC	Suspicious conversion	704	Low	sgverify.c:122	New
491	GCC	Mixed declarations and Code	398	Low	sgverify.c:120	New

Benefits

Broader adoption of higher quality software assurance technologies that results in more secure deployed software

- Easy access to an integrated view of assessment results from multiple tools
- “Do it early, and do it often.” (continuous) approach to software assurance
- Managed sharing of tools, test suites, and results
- Classroom integration of powerful software assurance capabilities
- A testing and evaluation ground for new and mature software assurance tools and technologies
- Private SWAMP installations enable building private/local continuous software assurance facilities.

Competition

- Software assessment services for open-source software offered by commercial tool vendors (e.g. Coverity Scan)
- Providers of continuous integration services (e.g. Travis CI)

Current Status

- SWAMP has been operational since 02/14.
- 10 software assurance tools are available for public usage.
  - C/C++ (Clang Static Analyzer, CppCheck, GCC warnings, Parasoft C/C++test)
  - Java (FindBugs with Find Security Bugs, PMD, Checkstyle, error-prone, Parasoft Jtest)
  - Python (Pylint)
- Agreement with four commercial tool vendors on adding their tools to the SWAMP (Parasoft, GrammaTech, Veracode, Red Lizard)
- 400+ software packages are available for public usage.
  - Including the NIST Juliet and SATE test suites for C/C++ and Java
- Fully integrated viewing of multiple assessment results with Code Dx
- Support for GitHub identities and uploading software packages from git repositories
- ~400 user registrations
- >750 weekly assessment runs

Coming Soon (First Quarter of 2015)

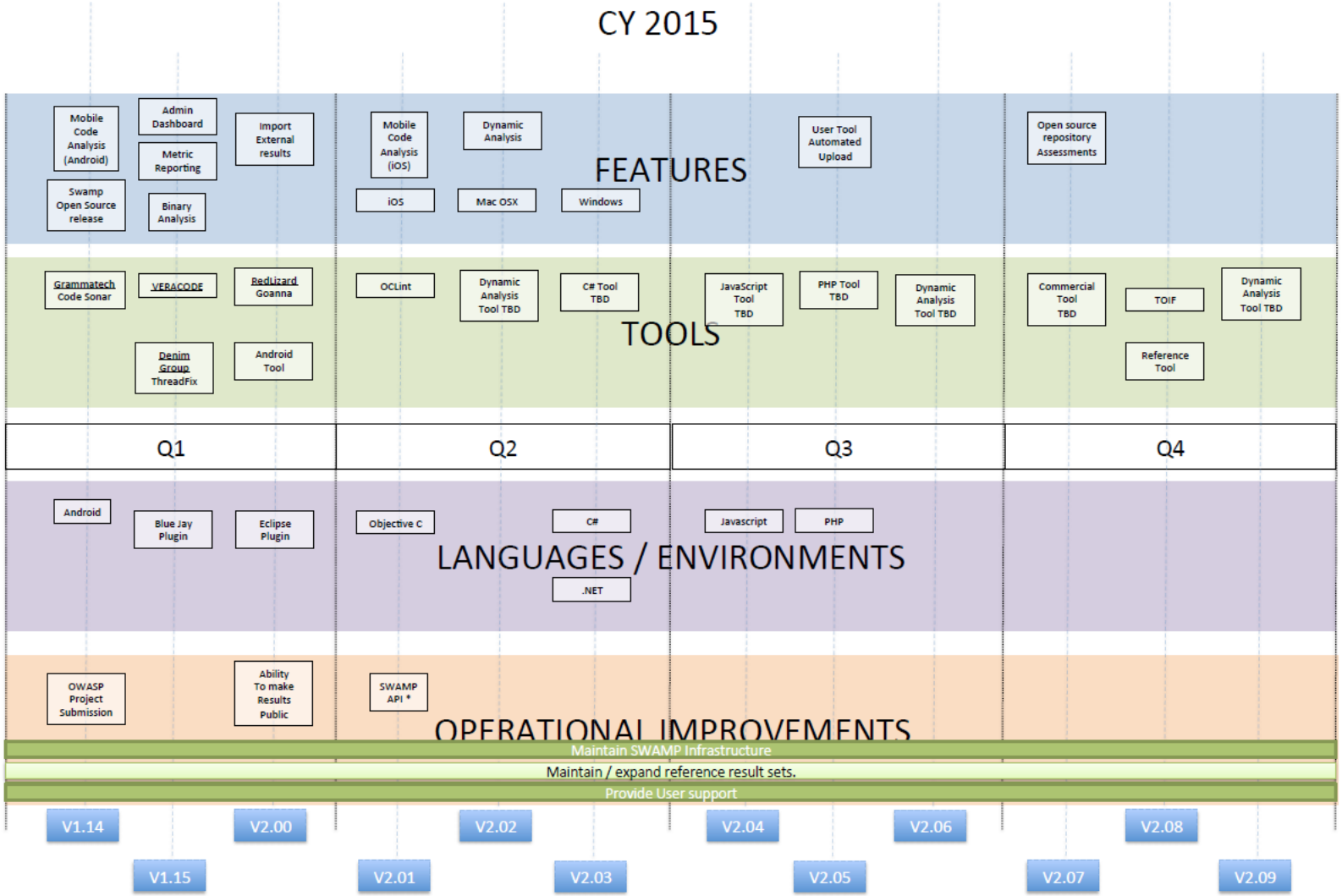
- Plug-ins for IDEs: Eclipse, IntelliJ IDEA, and BlueJ
- Support for the Android platform
- Host CodeSonar (GrammaTech), Goanna (Red Lizard), and SAST (Veracode)
- Offer the ThreadFix Vulnerability Management Tool (Denim Group)
- Establish the SWAMP as an OWASP Project

Contacts

Join the SWAMP
as a provider or a consumer at
https://continuousassurance.org

• PI and Director	Miron Livny	mlivny@morgridgeinstitute.org
• Chief Scientist	Bart Miller	bmiller@cs.wisc.edu
• Project Manager	Pat Beyer	pbeyer@continuousassurance.org
• SWAMP Support		support@continuousassurance.org

SWAMP
SOFTWARE ASSURANCE MARKETPLACE



20 November 2014

nitial functionality will occur by the added date, but increases in functionality will occur over many releases. Multi-step process and is spread out over many releases.

Welcome to the SWAMP

The Software Assurance Marketplace (SWAMP) is a service that provides continuous software assurance capabilities to developers and researchers.

This no-cost code analysis service is open to the public. Let the SWAMP help you to build better, safer, and more secure code today!

Sign Up! | Sign Up with GitHub!

GitHub | Search GitHub | Explore | Features | Enterprise | Blog

Sign in

Username or Email

Password (forgot password)

Sign in

SWAMP | About | Contact | Help | Resources | Policies

User Registration Form

SWAMP promotional code

First name *

Last name *

Email address *

Confirm email address *

SWAMP username *

SWAMP password *

Confirm SWAMP password *

Submit | Cancel