Software Assurance Tools at Indiana University:

A Return to the SWAMP

Rob Quick
Research Technologies Manager High Throughput Computing
Operations Officer - OSG
Operations Officer - SWAMP

Do It Early. Do It Often.
Top 10 Common Weakness Enumerations

❖ CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
❖ CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
❖ CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
❖ CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
❖ CWE-306 Missing Authentication for Critical Function
❖ CWE-862 Missing Authorization
❖ CWE-798 Use of Hard-coded Credentials
❖ CWE-311 Missing Encryption of Sensitive Data
❖ CWE-434 Unrestricted Upload of File with Dangerous Type
❖ CWE-807 Reliance on Untrusted Inputs in a Security Decision

Software Assurance Motivation

- The world we live in today is **software-centric**, introducing **significant risks** to confidential data and physical resources.
- Applications are leaving the protected enterprise network environment and moving onto the web.
- Anything with an outward face to the Internet is an entry point for an attack.
- Few developers are trained and equipped to build secure code.
- Even those well equipped often utilize code developed by others.

V. Welch
The Tools

❖ Key assets in this battle are the software assessment tools that can scan the program for defects (weaknesses). However, using these tools comes with challenges:

❖ Each tool is good at finding some particular problem; no tool is good at everything (or even most things).

❖ Configuring, maintaining, and using these tools can be cumbersome, time consuming and tricky.

V. Welch
A Framework

- No single Software Assurance (SwA) tool is going to bridge the gap between software and assured software.
- A software assurance (SwA) framework allows construction and automation of SwA workflows.
- Our framework provides code analysis, result normalization and labeling, result merging and integration, visualization, result evaluation and annotation, and risk assessment.
- Aggregates, orchestrates and automates use of SwA tools rather than being a tool itself.
- Should support use cases of software developers, SwA Tool developers, SwA researchers, software users, and educators.

V. Welch
Welcome to the SWAMP

❖ A continuous assurance platform that enables significant improvements in the quality of SwA tools while broadening adoption of SwA methodologies

❖ Consists of:

❖ 30(and growing) static analysis assessment tools
❖ State-of-the-art assessment results viewer
❖ “Plumbing” that simplifies access to SwA tools
❖ Provides a hub for software assurance projects
❖ Supports managed access to tools, packages and results
❖ Maintains confidentiality of software and results at the discretion of the user

V. Welch
Vision of Continuous Assurance

- **Continuous integration (CI)** is the practice, in software engineering, of merging all developer working copies with a shared mainline several times a day.

- **Continuous Assurance (CoA)** takes the software engineering practice of Continuous Integration to a new level. CoA incorporates SwA tools into the frequent process of building and testing the software throughout its life cycle.

V. Welch
What is 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!
## Languages Supported

<table>
<thead>
<tr>
<th>SWAMP</th>
<th>SiB</th>
</tr>
</thead>
<tbody>
<tr>
<td>C/C++</td>
<td>C/C++</td>
</tr>
<tr>
<td>Java source</td>
<td>Java source</td>
</tr>
<tr>
<td>Java bytecode</td>
<td>Java bytecode</td>
</tr>
<tr>
<td>Python</td>
<td>Python</td>
</tr>
<tr>
<td>Ruby</td>
<td>Ruby</td>
</tr>
<tr>
<td>PHP</td>
<td>PHP</td>
</tr>
<tr>
<td>Javascript</td>
<td>Coming Soon:</td>
</tr>
<tr>
<td>HTML</td>
<td>PHP</td>
</tr>
<tr>
<td>CSS</td>
<td>Javascript</td>
</tr>
<tr>
<td>XML</td>
<td></td>
</tr>
</tbody>
</table>
Tools Supported

SWAMP

- Open tools
  - Android lint
  - Bandit
  - Brakeman
  - checkstyle
  - Clang Static Analyzer
  - cppcheck
  - CSS Lint
  - Dawn
  - error-prone
  - ESLint
  - Findbugs
  - Flake8
  - Flow
  - GCC
  - HTML Tidy
  - JSHint
  - OWASP Dependency Check
  - PHPMD
  - PHP_CodeSniffer
  - PMD
  - Pylint
  - Reek

- Commercial tools
  - Ruby-lint
  - Retire.js
  - RevealDroid
  - RuboCop
  - ruby-lint
  - XML Lint

SiB

- Bandit
- Brakeman
- checkstyle
- Clang Static Analyzer
- cppcheck
- Dawn
- error-prone
- Findbugs
- Flake8
- GCC
- HTML Tidy
- JSHint
- OWASP Dependency Check
- PHPMD
- PHP_CodeSniffer
- PMD
- Pylint
- Reek
- Ruby-lint
- Retire.js
- RevealDroid
- RuboCop
- ruby-lint
- XML Lint
Platforms Supported

**SWAMP**
- Android
- CentOS Linux 5 32-bit and 64-bit
- CentOS Linux 6 32-bit and 64-bit
- Debian Linux
- Fedora Linux
- Red Hat Enterprise Linux 6 32-bit and 64-bit
- Scientific Linux 5 32-bit and 64-bit
- Scientific Linux 6 32-bit and 64-bit
- Ubuntu Linux

**SiB**
- Ubuntu Linux

**Upcoming:**
- Mac OS X
- Microsoft Windows
http://mir-swamp.org/

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!

Get results in just three steps:
Rather than spending time installing, licensing and configuring software assessment tools on your own machine, let the SWAMP do the work for you.

1) Upload your package
First, upload your code. Rest assured that it will remain private and secure.

2) Run your assessment
Next, create and run an assessment by choosing a package, tool, and platform.

3) View your results
Last, view your results using a native viewer or Code Dx™ for full featured analysis.
The rest of this session...

- Get a SWAMP Account
- Identify and Acquire Interesting Packages
- Move the Package to the SWAMP
- Run an Assessment
- View Results

https://tinyurl.com/swampdemo
• SWAMP Website: https://continuousassurance.org/
• SiB Info: https://continuousassurance.org/swamp-in-a-box/
• Bart’s and Elisa’s full slide set: https://static1.squarespace.com/static/5047a5a6e4b0dcecada15549/t/54071f4ce4b00e19c7ef11c9/1409752908265/Miller-Heymann-NSF-2014.pdf
• SWAMP-in-a-Box git repo https://github.com/mirswamp/deployment