SAND2018-7725D

RISE

Attracting and Developing Top Level IT and R&D CS/CE/Cyber Professionals

Developing Secure Software

SWAMP-in-a-Box for Continuous Software Analysis

Oliver Reed, Brigham Young University

Project Mentors: Gary Huang, Org. 9371 and John McCloud, Org. 9366

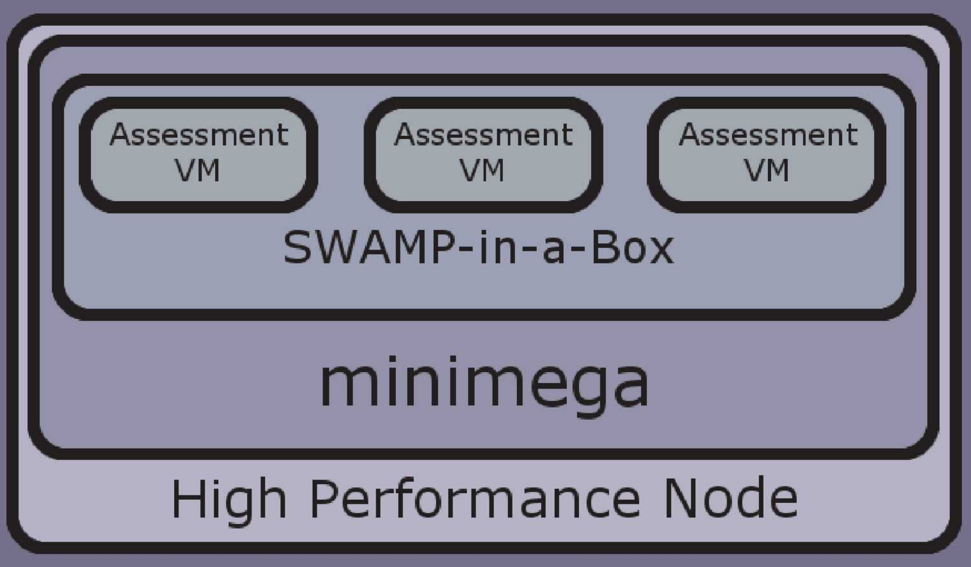
When developing software, programmers are often encouraged to finish the product with a focus on speed of development. In many cases, this focus leads to security being ignored or forgotten. After creating a solution to a problem the developer may have a couple of weeks to go through and fix security issues, but often this is not enough time to analyze and resolve possible security issues.

One solution is to integrate security practices into the continuous integration/continuous deployment (CI/CD) processes. If every time a developer adds code to a project he or she has to verify that a minimum security standard is met, certain vulnerabilities can be spotted and corrected with relative ease.

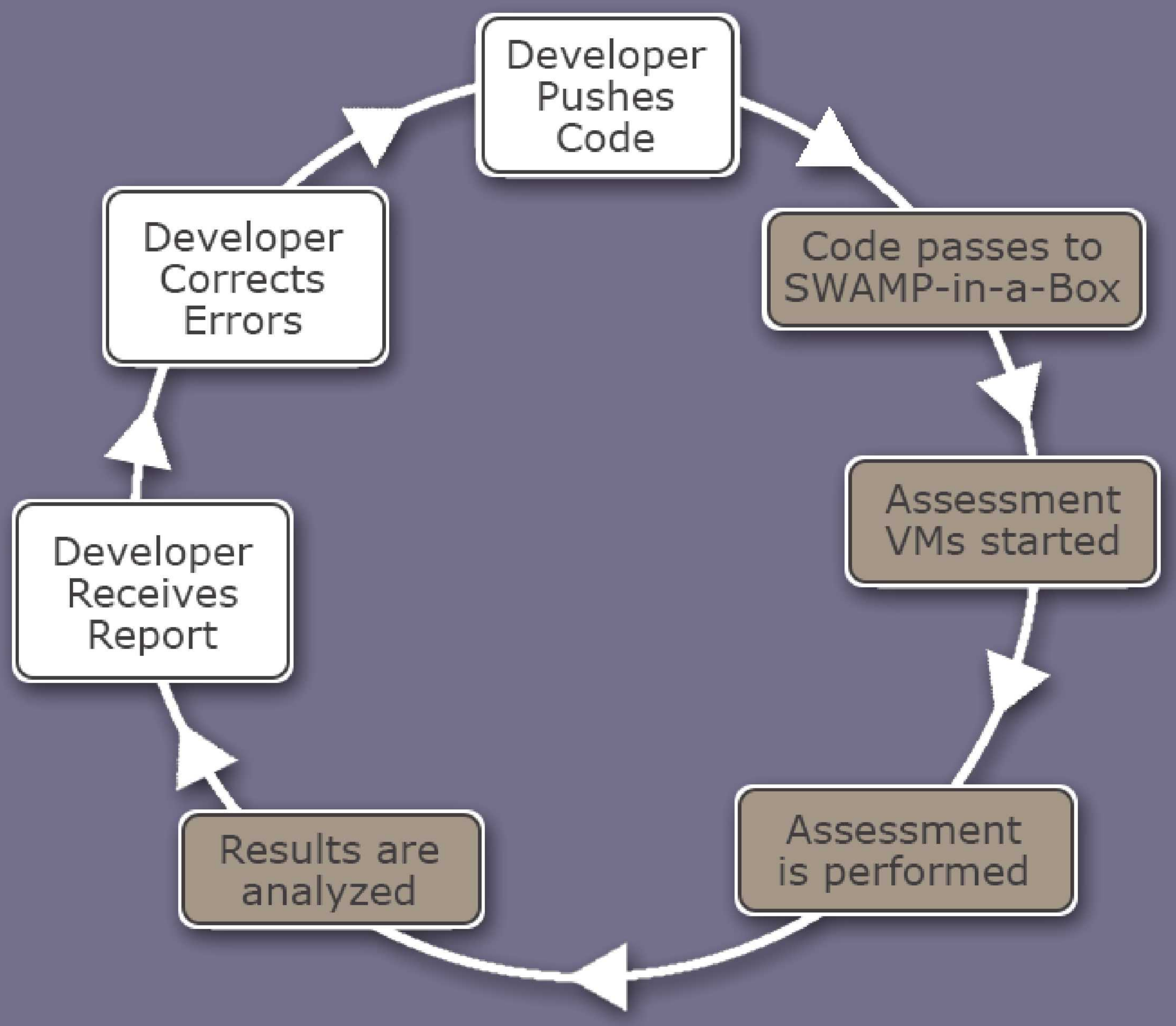
SWAMP-in-a-Box is an application to implement the Software Assurance Marketplace's (SWAMP) chosen tools for some of the most commonly used programming languages. In comparison with *MIR-SWAMP*, *SWAMP-in-a-Box* is self-hosted and customizable. It comes pre-built with many static application security testing (SAST) programs and can be configured to work with more.

Language	Number of Tools
C/C++	3
Java	5
Python	3
JavaScript	5
CSS	2
HTML	1
PHP	2
Ruby	3
Ruby on Rails	5

By utilizing one of the high performance computing clusters and a free and open source software developed at Sandia called *minimega* we can quickly create virtual machines to test and use *SWAMP-in-a-Box.*



With SWAMP-in-a-Box developers are able to incorporate secure coding practices with little extra effort. The graph below shows a simplified example development cycle. Everything the developer does is in white while everything *SWAMP-in-a-Box* would do is in brown.



Some problems that *SWAMP-in-a-Box* will catch are:

- Buffer overflow
- Incompatible type comparisons
- Integer overflows
- Null pointer dereferences
- Uninitialized Variables
- Memory leaks
- Insecure modules
- Hardcoded passwords

The earlier bugs and security issues are identified and fixed the less money and time will be wasted in repairing them in the future.

There is still much to do with *SWAMP-in-a-Box*. Future work will include the configuration of the SAST applications to reduce the number of false positives and combining their output to increase the quality and usefulness of the results.

CONTINUOUS ASSURANCE

SWAMP
SOFTWARE ASSURANCE MARKETPLACE

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2018-XXXXC.

U.S. DEPARTMENT OF ENERGY NNSA National Nuclear Security Administration