How to Find and Fix Software Vulnerabilities with Coverity Static Analysis

Bill Baloglu
Software Integrity Group, Synopsys, Inc.
San Francisco, California
Bill.Baloglu@synopsys.com

This hands-on workshop will combine minimal instruction with strong hands-on emphasis on practical lab exercises for attendees to practice the topics covered -- the expected duration will be 90 minutes:

- Introduction to Coverity static code analysis
- Integration of Analysis into Development Cycle
  - Clean after Check-in Approach
  - Clean before Check-in Approach
  - Continuous Clean Approach
- Category of Security Vulnerabilities
  - Quality Defects that can be exploits
  - Web Application Security flaws
- How to find and fix them with Coverity

The hands-on labs will give attendees the opportunity to run real-time Coverity analysis on a number of given codebases, to find vulnerabilities in both (a) and (b) categories (buffer overruns, cross-site scripting XSS, SQL Injections etc. with actionable advice on approaches and options to eliminate them.

The workshop attendees will be given access to their own dedicated virtual machines in our cloud-based lab platform. The VMs will be pre-configured with all the necessary software and sample codebases. Participant should bring their laptops with Wi-Fi network card, and a contemporary browser, such as Chrome, IE, FF, Safari or similar with HTML5 support, which they should run to validate compliance with our pre-check test: https://synopsys.instructorled.training/precheck.

At the session start, attendees will be provided with access codes to remotely connect to their virtual lab machines at https://synopsys.instructorled.training, using the Wi-Fi connectivity provided by the IEEE Sec Dev 2016 Conference.