Maslak Mahallesi, Maslak Meydan Sk. No:5. Spring Giz Plaza. Maslak/İstanbul
+90 212 282 7700 - info@bilginc.com

Security Testing Native Code

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **3 Day**

Overview

In this course, after getting familiar with the common weaknesses and their consequences that can allow hackers to attack your system, participants learn about the general approach and the methodology for security testing, and the techniques that can be applied to reveal specific vulnerabilities. Security testing should start with information gathering about the system (ToC, i.e. Target of Evaluation), then a thorough threat modeling should reveal and rate all threats, arriving to the most appropriate risk analysis-driven test plan.

Security evaluations can happen at various steps of the SDLC, and so we discuss design review, code review, reconnaissance and information gathering about the system, testing the implementation and the testing and hardening the environment for secure deployment. Many different security testing techniques are introduced in details, like taint analysis and heuristics-based code review, static code analysis or fuzzing. Various types of tools are introduced that can be applied in order to automate security evaluation of software products, which is also supported by a number of exercises, where we execute these tools to analyze the already discussed vulnerable code.

This course prepares testers and QA staff to adequately plan and precisely execute security tests for applications written in C or C++, select and use the most appropriate tools and techniques to find even hidden security flaws, and thus gives essential practical skillls..

Prerequisites

There are no prerequisites for this course.

Who Should Attend

C and C++ developers, testers

What You Will Learn

- Understand basic concepts of security, IT security and secure coding
- Realize the severe consequences of unsecure buffer handling
- Understand the architectural protection techniques and their weaknesses
- Learn about typical coding mistakes and how to avoid them
- Be informed about recent vulnerabilities in various platforms, frameworks and libraries
- Learn about denial of service attacks and protections
- Understand security testing approaches and methodologies
- Get practical knowledge in using security testing techniques and tools
- Learn how to set up and operate the deployment environment securely
- Get sources and further readings on secure coding practices

Outline

- IT security and secure coding
- x86 machine code, memory layout and stack operations
- Buffer overflow
- Common coding errors and vulnerabilities
- Denial of service
- Security testing
- Security testing techniques and tools
- Deployment environment
- Principles of security and secure coding

- Knowledge sources