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

Security Testing

Learn via: **Classroom**

Duration: **3 Day**

Overview

After getting familiar with the vulnerabilities and the attack methods, 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, dynamic web vulnerability testing 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. Many real life case studies support better understanding of various vulnerabilities.

Prerequisites

There are no prerequisites for this course.

Who Should Attend

Developers and testers.

What You Will Learn

- Understand basic concepts of security, IT security and secure coding
- Learn Web vulnerabilities beyond OWASP Top Ten and know how to avoid them
- Learn about XML security
- Learn client-side vulnerabilities and secure coding practices
- 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
- Web application security
- Client-side security
- Security testing
- Security testing techniques and tools
- Source code review
- Input validation
- Improper use of security features
- Testing the implementation
- Deployment environment
- Principles of security and secure coding
- Knowledge sources