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

Advanced Software Security - Beyond Ethical Hacking

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

Duration: **5 Days**

Overview

Despite all of your efforts, the code you have been writing your entire career is full of weaknesses you never knew existed. During this training, you will be learnt with all of the attackers' tricks and how to mitigate them.

Prerequisites

There are no prerequisites for this course.

Who Should Attend

Software engineers.

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
- Have a practical understanding of cryptography
- Understand some recent attacks against cryptosystems
- Realize the severe consequences of unsecure buffer handling in native code
- Understand the architectural protection techniques and their weaknesses
- Realize the severe consequences of unsecure buffer handling
- Learn about denial of service attacks and protections
- 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
- Practical cryptography
- Cryptographic vulnerabilities
- x86 machine code, memory layout and stack operations
- Buffer overflow and its exploitation
- Some additional native code-related vulnerabilities
- XML security
- Denial of service
- Input validation
- Error and exception handling
- Improper use of security features

- Code quality problems
- Security testing techniques and tools
- Deployment environment
- Principles of security and secure coding
- Knowledge sources