scademy
secure coding academy

The secure coding landscape

CL-OSC | Classroom | 2 days

Variants: Java, C#, PHP, Node.js, technology agnostic

Audience: Product and line managers, software developers
Preparedness: General software design and development
Exercises: Demonstrated

The course introduces some common security concepts, gives an overview about the nature of the vulnerabilities regardless of the used programming languages and platforms, and explains how to handle the risks that apply regarding software security in the various phases of the software development lifecycle. Without going deeply into technical details, it highlights some of the most interesting and most aching vulnerabilities in various software development technologies, and presents the challenges of security testing, along with some techniques and tools that one can apply to find any existing problems in their code.

Outline:

- Agenda
- IT security and secure coding
- Security challenges of various platforms – highlights –
- Challenges of security testing
- Principles of security and secure coding
- Knowledge sources

Participants attending this course will:

- Understand basic concepts of security, IT security and secure coding
- Understand Web vulnerabilities both on server and client side
- Realize the severe consequences of unsecure buffer handling
- Be informated about some recent vulnerabilities in development environments and frameworks
- Learn about typical coding mistakes and how to avoid them
- Understand security testing approaches and methodologies
- Get sources and further readings on secure coding practices

scademy
secure coding academy

Related courses:

- CL-CMI - C and C++ security master course (x86) (Classroom, 5 days)
- CL-CMA - C and C++ security master course (ARM) (Classroom, 5 days)
- CL-WSM - Web application security master course (Classroom, 5 days)
- CL-JSM - Java and Web application security master course (Classroom, 5 days)
- CL-NSM - C# and Web application security master course (Classroom, 5 days)
- CL-WTS - Web application security testing (Classroom, 3 days)
- CL-STS - Security testing (Classroom, 3 days)

Note: Our classroom trainings come with a number of easy-to-understand exercises providing live hacking fun. By accomplishing these exercises with the lead of the trainer, participants can analyze vulnerable code snippets and commit attacks against them in order to fully understand the root causes of certain security problems. All exercises are prepared in a plug-and-play manner by using a pre-set desktop virtual machine, which provides a uniform development environment.

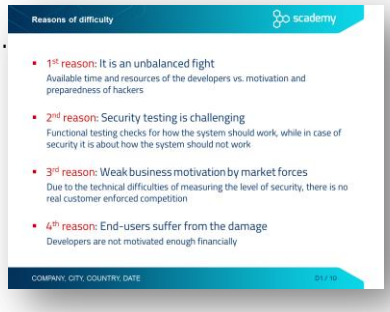
scademy
secure coding academy

Detailed table of contents

Agenda

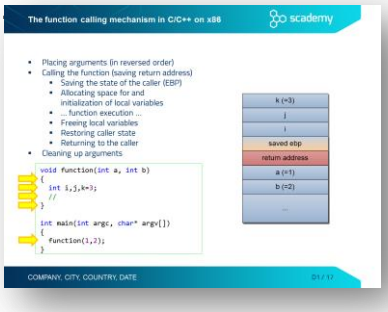
IT security and secure coding

- Nature of security
- What is risk?
- Different aspects of IT security
- IT security vs. secure coding
- From vulnerabilities to botnets and cybercrime
    - Nature of security flaws
    - Reasons of difficulty.....
    - From an infected computer to targeted attacks
    - Cybercrime – an organized network of criminals



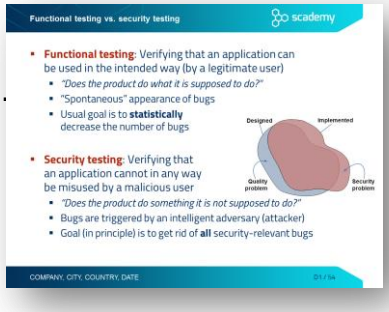
Security challenges of various platforms – highlights –

- Secure coding topics
- C/C++ (native code) secure coding
    - The function calling mechanism in C/C++ on x86 .....
    - Buffer overflow on the stack
    - Overwriting the return address
    - Exploiting stack overflow – jumping to arbitrary address
    - Exploiting stack overflow – injecting malicious code
    - Architecture level mitigation techniques (C/C++)
- Web application security
    - Exercise – SQL injection
    - Typical SQL Injection attack methods
    - Blind and time-based SQL injection
    - Insecure direct object reference (IDOR)
    - Persistent XSS
    - Reflected XSS
    - Exercise – Cross Site Scripting



- Clickjacking
  - Protection against Clickjacking
  - Anti frame-busting – dismissing protection scripts
  - Protection against busting frame busting
  - Form tampering
  - Exercise – Form tampering
- Java platform security
  - Secure coding issues in Java
  - The Seven Pernicious Kingdoms
  - Case study – Java Calendar vulnerability
    - The most exploited flaw in Java at the time
    - The actual mistake in java.util.Calendar – spot the bug!
  - Case study – The double bug in Java
    - A generic Denial of Service attack against the Java environment
    - The "2.2250738585072012e-308 bug"
    - Exercise Double Bug

Challenges of security testing



- Functional testing vs. security testing
- Security vulnerabilities
- Prioritization – risk analysis

Principles of security and secure coding

- Matt Bishop's principles of robust programming
- The security principles of Saltzer and Schroeder

Knowledge sources

- Secure coding sources – a starter kit
- Vulnerability databases
- Java secure coding sources
- .NET secure coding guidelines at MSDN
- .NET secure coding cheat sheets
- Recommended books – C/C++
- Recommended books – Java
- Recommended books – .NET and ASP.NET