

SC DEV 203: SECURE CODING IN .NET

After taking this advanced class students will be able to develop secure Microsoft .NET applications. Students will learn to define and identify secure code, differentiate between secure coding methods, employ secure code in practice and design and judge effectiveness of secure coding practice.

The class focuses on learning by doing. Concepts are presented in short lecture-demonstration sessions, and then students are challenged in hands-on labs to make reasoned choices and implement secure code. Each heading in the detailed outline includes Hands-On labs with applications that must be modified in some way to make them secure. Students are required to execute various real world solutions including fixing broken applications, adding security functionality, replacing poorly written code, finding vulnerabilities and doing runtime testing.

All labs are executed in a real world, preconfigured development environment. Days 1 and 2 focus on web applications and day 3 focuses on core .NET security. Students secure coding abilities will be materially sharpened after this class.

DURATION & INTENDED AUDIENCE

- Duration: 3 days
- Intended Audience:
 - .NET Developers and Architects
 - Senior software QA

PRE-REQUISITE KNOWLEDGE

- Knowledge of common application security vulnerabilities (e.g. OWASP Top 10) recommended
- Experience developing ASP.NET applications in C# or VB.NET.
- Experience with Microsoft Visual Studio 2005/2008 recommended.
- Some experience or understanding of Internet Information Services is an asset.

LEARNING OBJECTIVES

- Understand what various defensive technologies do and how they work
- Evaluate alternatives for application security solutions
- Gain hands-on experience in writing code to add security controls into vulnerable apps
- Understand less publicized areas of application security (e.g. concurrency)

LEARNING ENVIRONMENT & TAKEAWAYS

- Course book containing printouts of each slide along with detailed notes in paragraph form
- Hard and soft copy of a secure coding checklist featuring class topics

CONTACT INFO

- Phone: 1-888-777-2211 x 1
- Email: training@securitycompass.com

DETAILED OUTLINE

DAY 1: INPUT VALIDATION

Web Application Attacks

- Cross Site Scripting
- Cross Site Request Forgery
- SQL Injection
- HTTP Response Splitting
- Parameter Manipulation
- Proxies (using Fiddler)

Validation Concerns

- Character Encoding
- Input Validation
- Output Encoding
- Blacklisting/Whitelisting

Validation Techniques

- Validation Controls
- Server vs. Client-side validation
- Regular Expressions
- HTML Encoding
- CAPTCHA
- ADO.NET
- Stored Procedures
- LINQ

DAY 2: ACCESS CONTROL

Authentication

- IIS / ASP.NET pluggable authentication architecture
- ASP.NET Handlers, Modules and the HTTP Pipeline
- Basic & Digest Authentication
- .NET Form Based Authentication Framework
- Windows Authentication
- Authorization, OS security, and Impersonation
- SSL Client Certificates
- Authentication Policies

Protecting Sessions

- Secure Session ID generation
- Session data, and persistence
- Session policies, expiry, etc.
- Session Hijacking
- Session Fixation

Protecting Sessions

- Brute Force Attacks
- Weak Password Storage
- Password Reset
- Secret Questions

DAY 3: SECURE .NET

Architecture

- Defense in depth
- Least Privilege
- Thread Safety
- Structured Exception Handling
- Application Logging and Auditing
- Secure Coding Principals

.NET Encryption Services

- Encryption Principals
- Securing communications
- Protecting data at rest

Assorted Topics

- Code Access Security overview
- Strongly Named Assemblies and Code Signing
- WS-Security (WCF) in .NET
- Tools of the trade (FxCop, NUnit, MbUnit, CCNet, VSTS, TestDriven.NET, etc.)