

Secure Coding in .NET - ASP.NET and C# Edition

Learn via: **Classroom**

Duration: **3 Day**

Overview

This comprehensive 3-day course is designed to educate professional programmers on the skills necessary to develop and deploy secure applications as a fundamental element of the entire application development process.

Prerequisites

There are no prerequisites for this course.

Who Should Attend

.NET Application Developers, C# Programmers, ASP.NET Developers; Managers, Architects and Technologists involved in deploying .NET applications

What You Will Learn

Upon Completing our Secure Coding in .NET will provide you with valuable knowledge and skills including the ability to:

- Understand common web application exposures and attacks
- Learn static analysis techniques for quickly finding web application flaws
- Understand the secure use of C#/VB.NET API
- Learn how to code defensively and perform proper input validation
- Learn threat modeling techniques to identify architectural issues as early as possible in the

Outline

1 - Introduction

- Web Application Environment and Components
- General Web Application Security Concepts
- .NET Framework Security Features

2 - Input Validation & Encoding

- Password Security
- Session Hijacking & Trapping
- Protecting User Sessions & Tokens
- Canonicalization Problems
- Parameter Manipulation

3 - Encryption, Confidentiality & Data Protection

- Cookie-Based Attacks
- Protecting Application Variables
- Cache Control Issues
- SSL Best Practices
- Protecting Usernames, Passwords and Personally Identifiable Information
- Common Cryptography Pitfalls

4 - Data Access

- Secure Database Programming
- Database Permissions Best Practices

- Parameterized Queries
- Common Stored Procedure Flaws

5 - Error Handling & Logging

- Attacking via Error Messages
- Secure Logging & Error Handling
- Input Driven Attacks
- Validation Best Practices
- Output Encoding

6 - Authentication, Authorization & Session Management

- Common Authentication Weaknesses
- Authorization Best Practices
- Controlling Application Access

7 - Server Configuration & Code Management

- Common Web & App Server Mis-Configurations
- Common Database Server Mis-Configurations
- Protecting Application Code

8 - XML Web Services

- Overview of WSDL, SOAP & AJAX
- Web Service Attacks
- AJAX Pitfalls
- Web Service Best Practices

9 - Application Threat Modeling

- Threat Modeling Concepts
- Application Context
- Identifying Attacks, Vulnerabilities & Countermeasures
- Threat Modeling Tools

10 - Practical Security Testing Techniques for Developers

- Useful Web Application Assessment Tools
- Determining the Severity of Vulnerabilities
- Dealing with Time Constraints