

Implementing Security for Applications

GWE28400—Five days—Instructor-led



Introduction

This five-day instructor-led class provides students with a thorough grounding in Microsoft .NET security implementation and general development security best practices. This course will prepare a student to take the Implementing Security for Applications exam.

Audience

This course is intended for experienced, professional application developers, including those employed by software companies or working on corporate development teams.

At Course Completion

After completing this course, students will be able to:

- Explain the basic concept of application security.
- Implement platform security best practices.
- Implement coding security best practices.
- Implement security using CLR and application domains.
- Implement role-based security by using the Microsoft .NET Framework.
- Implement CAS to secure applications.
- Implement cryptography in .NET.
- Improve the Security of remote applications built on the .NET Framework.
- Improve the Security of ASP.NET applications.
- Manage and configure security policies using Framework tools.
- Test application security.
- Deploy applications in a manner that minimizes security risks.

Prerequisites

Before attending this course, students:

- Should have a minimum of 1 year of experience using Microsoft Visual Studio .NET 2003 (.NET Framework 1.1) and 2–3 years of additional development experience.
- Should be experienced in either Visual Basic .NET or Visual C#.

Microsoft Certification exams

This course will help the student prepare for the following Microsoft Certification exams:

- Implementing Security for Applications with Microsoft Visual Basic .NET
- Implementing Security for Applications with Microsoft Visual C# .NET

Course Materials

The student kit includes a comprehensive workbook and other necessary materials for this class.

Course Outline

Module 1: Overview of Application Security

This module introduces students to the concept of application security. It explains the importance of security and the various application security loopholes. The module discusses the essential components of a successful Secure Development Process, such as threat modeling and threat mitigation. In addition, the module explains the security best practices.

Lessons

- The Importance of Application Security
- Application Security Best Practices

Lab: Threat Modeling and Threat Mitigation

After completing this module, students will be able to:

- Explain the basic concept of application security

Module 2: Implementing Platform Security Best Practices

This module focuses on implementing platform security best practices. It discusses the concept of ACLs and DACLs and enables students to use various built-in functions for implementing platform security using ACLs and DACLs. The module also explains how to create custom accounts with least privilege for running Microsoft ASP.NET applications and how to view audit trails. In addition, the module explains how to implement security defaults in an application. Finally, the module discusses the use of digital certificates and signatures and how to implement platform cryptography.

Lessons

- Security Best Practices for COM+, IIS, and SQL Server 2000
- Using ACLs and DACLs
- Using Windows Least-Privilege Accounts
- Using Audit Trails
- Implementing Platform Cryptography
- Implementing Data Protection

Lab: Using ACLs and DPAPI

After completing this module, students will be able to:

- Implement platform security best practices

Module 3: Implementing Coding Security Best Practices

This module focuses on implementing coding security best practices. It enables students to validate application input for securing applications. The module also discusses how to secure local and third-party components and evaluate canonicalization issues. In addition, the module enables students to implement error-handling guidelines to defend against security exceptions.

Lessons

- Validating Application Input
- Evaluating Canonicalization Issues
- Using Security Exceptions

Lab: Verifying User Input

After completing this module, students will be able to:

- Implement coding security best practices

Module 4: Using .NET Framework Security Features

This module focuses on .NET Framework security features. It explains how to use stack walks to defend against lurking attacks. In addition, the module enables students to implement security using application domains.

Lessons

- Implementing CLR Security Mechanism
- Implementing Security Using Application Domains

Lab: Invoking a Third-Party Assembly in Application Domain

After completing this module, students will be able to:

- Implement security using CLR and application domains

Module 5: Implementing Role-based Security

This module discusses programming techniques for implementing role-based security by using the Microsoft .NET Framework.

Lessons

- Basics of Role-Based Security
- Role-Based Security with Principal and Identity Objects
- Role-Based Security with Permission Objects

Lab: Implementing Role-based Security

After completing this module, students will be able to:

- Implement role-based security by using the Microsoft .NET Framework

Module 6: Implementing Code-Access Security

This module focuses on implementing CAS. It explains how to work with code access permissions and apply CAS checks. In addition, the module discusses the default membership conditions and the four CAS policy levels.

Lessons

- Overview of Code-Access Security
- Performing Basic Security Operations
- Performing Imperative Security Operations
- Performing Declarative Security Operations
- Adding Permission Requests

Lab: Implementing Code-Access Security

After completing this module, students will be able to:

- Implement CAS to secure applications

Module 7: Implementing Cryptography in .NET

This module focuses on implementing symmetric and asymmetric cryptography to secure .NET applications.

Lessons

- Implementing Symmetric Cryptography
- Implementing Asymmetric Cryptography

Lab: Implementing Symmetric and Asymmetric Cryptography

After completing this module, students will be able to:

- Implement cryptography in .NET

Module 8: Securing ASP.NET Applications

This module focuses on securing ASP.NET applications. It discusses the various ASP.NET security features, such as authentication, authorization and impersonation, and how to implement each of these security features. In addition, the module explains how to secure Web files and folders.

Lessons

- Implementing Authentication in ASP.NET Applications
- Implementing Authorization in ASP.NET Applications
- Implementing Impersonation in ASP.NET Applications
- Securing Web Files and Folders

Lab: Securing ASP.NET Applications Using Form Authentication and SQL Server

After completing this module, students will be able to:

- Secure ASP.NET applications

Module 9: Securing Remote .NET Applications

This module focuses on securing remote .NET applications. The module enables students to implement Web Service Enhancements. It also explains how to configure remoting for security.

Lessons

- Introducing .NET Application Security
- Implementing Authentication and Authorization in .NET Remoting Applications
- Introducing Web Service Security
- Implementing WS Security

Lab: Securing Remote .NET Applications

After completing this module, students will be able to:

- Secure remote .NET applications

Module 10: Configuring .NET Security

This module focuses on configuring security using .NET tools. It explains how to manage security policies using Mscorcfg.msc and Caspol.exe.

Lessons

- Managing Security Policies Using Mscorcfg.msc
- Managing Security Policy Levels Using Mscorcfg.msc

Lab: Configuring .NET Security

After completing this module, students will be able to:

- Manage and configure security policies using .NET Framework tools

Module 11: Implementing Security Testing

This module focuses on testing application security. It explains the need for security testing and discusses the best practices to be followed for security testing. The module also explains how to assess application security by using techniques such as footprint analysis and penetration testing. In addition, the module enables students to test application security by using various security testing tools.

Lessons

- Overview of Security Testing
- Creating a Security Test Plan
- Performing Security Testing

Lab: Testing Application Security

After completing this module, students will be able to:

- Test application security

Module 12: Deploying Applications with Security

This module focuses on deploying secure applications. It enables students to sign assemblies. In addition, the module discusses strong-named assemblies and how to configure security settings with Mscorcfg.exe and Caspol.exe.

Lessons

- Deploying .NET Applications with Security Settings
- Deploying .NET Applications with Publisher Identity and Code Integrity

Lab: Deploying Applications with Security

After completing this module, students will be able to:

- Deploy applications in a manner that minimizes security risks.