



Implementing Security for Applications

M2840

5 day

Overview :

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.

Target Audience :

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

At the end of the course, delegates 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.

Course Content :

Overview of Application Security

- The Importance of Application Security
- Application Security Best Practices

Implementing Platform Security Best Practices

- 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

Implementing Coding Security Best Practices

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

Using .NET Framework Security Features

- Implementing CLR Security Mechanism
- Implementing Security Using Application Domains

Implementing Role-based Security

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

Implementing Code-Access Security

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

Implementing Cryptography in .NET

- Implementing Symmetric Cryptography
- Implementing Asymmetric Cryptography

Securing ASP.NET Applications

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

Securing Remote .NET Applications

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

Configuring .NET Security

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

Implementing Security Testing

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

Deploying Applications with Security

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

Course Prerequisites :

Delegates are required to meet the following prerequisites:

- 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#.

Testing and Certification :

Recommended as preparation for exam(s):

- Exam 70-330: Implementing Security for Applications with Microsoft Visual Basic .NET
- Exam 70-340: Implementing Security for Applications with Microsoft Visual C# .NET

Follow on Courses :

Further Information :

M2840/

For more information, or to book your course, please call Global Knowledge Danmark
Address: Kirkebjerg Alle 88, 2605 Brøndby
Telephone: +45 44 88 18 00
Email: training@globalknowledge.dk
Web: www.globalknowledge.dk