MVC 4.0, Part 07 of 11: Security Concepts

page 1

Meet the expert: Don Kiely is a featured instructor on many of our SQL Server and Visual Studio courses. He is a nationally recognized author, instructor, and consultant specializing in Microsoft technologies. Don has many years of teaching experience, is the author or co-author of several programming books, and has spoken at many industry conferences and user groups. In addition, Don is a consultant for a variety of companies that develop distributed applications for public and private organizations.

Prerequisites: This course assumes that you are familiar and experienced with Microsoft's .NET Framework and ASP.NET development tools. You should be familiar with Web development and understand how HTTP and HTML work to produce Web pages for the user. You should have experience writing applications with ASP.NET 4.0 or later Web forms, and be familiar with how ASP.NET processes page requests, and have strong experience with .NET Framework 4.0 or later programming. You should have experience with Visual Studio 2012 for building Web application projects. Experience with building database applications using these tools will be helpful, although not strictly necessary.

Runtime: 02:33:25

Course description: In this course you'll explore a wide range of security threats and a variety of features in MVC that help you protect against them. We'll start with a discussion of critical security concepts, then look at some of the differences between Web Forms and MVC applications from a security perspective. Then you'll learn various techniques you can use to protect the integrity of application data, including how you can encrypt configuration file sections, use SSL for various security purposes, and hash passwords for storage. I'll finish up the course by looking at various serious threats that MVC applications face, and explore some of the options available for protecting against them.

Course outline:

MVC Security Concepts
- Introduction
- Critical Security Concepts
- Web Forms vs. MVC
- OWASP
- The OWASP Top 10 List
- Summary

Encrypting Configuration Files
- Introduction
- Encrypting Configuration
- Protected Configuration Providers
- Demo: machine.config
- Demo: Encrypt Connection Strings
- Demo: Encryption Code
- Demo: Encrypt External Files
- Summary

Secure Communication
- Introduction
- Secure Communication with SSL
- SSL in MVC
- Demo: Using SSL
- Demo: SSL Port
- Demo: Require SSL
- Demo: Require SSL Index
- Demo: Certicates
- Summary

Hashing Passwords
- Introduction
- Hashing Passwords for Storage
- Demo: Hashing Passwords
- Demo: Salted Hash
- Demo: Salted Hash Code
- Summary

Cross Site Scripting
- Introduction
- Cross-Site Scripting (XSS)
- Preventing XSS Attacks
- Anti-XSS Library
- Summary

SQL Injection
- Introduction
- SQL Injection
- Demo: SQL Injection
- Preventing SQL Injection
- Summary

Cross Site Request Forgeries
- Introduction
- Cross-Site Request Forgeries
- Demo: CSRF
- Demo: CSRF Example
- Demo: Transfer Headers
- Preventing CSRF Attacks
- Demo: Anti-Forgery Token
- Summary