Foundstone Writing Secure Code - ASP.NET (C#)

Duration: 4 Days   Course Code: GK9823

Overview:

In this course, you will gain an understanding of the key security features of the .NET platform, the common web security pitfalls developers make, and how to build secure and reliable web applications using ASP.NET. You will work through hands-on code examples that highlight issues and prescribe solutions. You will also cover both the current version of the .NET framework and relevant security features in the .NET updates.

Target Audience:

This course is for professional software developers or software security auditors who have been working with the .NET framework and developing ASP.NET web application using C# code for at least one year.

Objectives:

- The process and techniques of writing secure code
- Effective authentication and authorization techniques
- The most frequent web application vulnerabilities and how to avoid them
- Secure user management systems
- Data validation strategies
- Effective error handling and exceptions management
- Software security testing techniques

Prerequisites:

- A comprehensive knowledge of the .NET framework, the C# language, and web technology is required.

Follow-on-Courses:

- There are no follow-ons for this course.

Content:

1. Introduction

- Course Content and Format
- Secure Design Principles
- Hacme Bank

2. .NET Platform Security

- .NET Language Security Features
- Strong Name Signing
- .NET Common Language Runtime (CLR) Security Mechanisms
- Code Access Security (CAS)

3. Advanced .NET Security

- Concepts
- Partial Trust ASP.NET
- Code Access Security
- Microsoft Windows CardSpace

4. Cryptography

- .NET System Cryptography Namespace
- Common Cryptographic Mistakes
- Other Cryptographic Features in .NET
- .NET Algorithm Recommendations

5. Authentication

- ASP.NET Authentication
- Forms Authentication
- Windows Authentication/Kerberos
- Code Signing (Authenticate)
- Impersonation and Delegation

6. User Management

- Password Storage and Quality
- Account Lockout Schemes
- Strategies for Password Reset
- Membership API

7. Authorization

- Access Control Models
- Session Management
- Common Authorization Flaws
- Role Manager
- ASP.NET/IIS Authorization

8. Data Validation

- Input and Output Validation
- Regular Expressions
- SQL Injection, Cross-Site Scripting (XSS), and Other Attacks
- Data Validation Controls and Libraries
- Preventing Validation Attacks
- Canonicalization Issues

9. Client-Side Security

- Client-Side Security Mistakes
- Licensing Schemes
- Security Objectives for Thick Clients
- Secure Code Protection
- Reverse Engineering
- Code Access Security on the Client
- Byte Code Manipulation
- Secure Design Patterns

10. Security Testing

- White Box Techniques
- Black Box Techniques
- Unit Testing

11. Web Services

- Web Services Risks
- Web Service Attacks
- Web Service Defense Techniques
- Survey of Security Technologies
- Windows Communication Foundation
- Web Services Security Patterns

12. Error Handling and Exception Management

- Exception Handling Patterns and Anti-Patterns
- ASP.NET Exception Frameworks
- Best Practices for Handling User Errors

13. Logging and Auditing

- Common Mistakes with Logging
- Logging Best Practices

14. Secure Code Review

- Threat Modeling
- Secure Code Review Methodology
- Manual Code Review
- Automated Code Scanning Tools
- Practical Strategies for Conducting Code Reviews

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.co.uk

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK