ProTech
protechtraining.com

"Charting the Course ... ... to Your Success!"

Developing Secure Web Applications

Course Summary

Description

This course provides students with the knowledge and skills that are needed to build Web applications by using secure coding techniques. Students will learn how to identify Web application security vulnerabilities and understand the trade-offs between functionality and performance when choosing the appropriate security mechanisms for their Web applications. Throughout this course, students will get hands-on experience in creating secure Web applications.

Objectives

At the end of this course, students will be able to:

- Define the basic principals of, and motivations for, Web security
- Perform a threat analysis of Web-accessible assets
- Use knowledge of authentication, Security Identifiers (SIDs), Access Control Lists (ACLs), impersonation, and the concept of running with least privilege to ensure access to only those system resources that are necessary to accomplish normal request processing
- Protect file system data by using the features in Microsoft Windows 2000
- Use the Microsoft SQL Server Security model and Microsoft ADO.NET to protect a Web application against SQL Server injection attacks
- Use one of the CryptoService classes of the System.Security.Cryptography namespace to transform a block of data into cyphertext
- Protect the portion of a Web application that requires private communications by using Secure Sockets Layer (SSL)
- Use general security coding best practices to ensure a secure Web application
- Use the Microsoft .NET Framework to build secure Web applications
- Employ a structured approach to testing for Web application security
- Use a systematic approach and knowledge of security best practices to secure an existing Web application

Topics

- Planning for Web Application Security
- Validating User Input
- Internet Information Services Authentication
- Securing Web Pages
- Securing File System Data
- Securing Microsoft SQL Server
- Helping to Project Communication Privacy and Data Integrity
- Encrypting, Hashing and Signing Data
- Testing Web Applications for Security

Audience

This course is intended for students who are responsible for the design and development of Web applications. These students typically have three to five years of experience in developing or designing distributed Web applications.

Prerequisites

Students should have familiarity with n-tier application architecture, experience in developing or designing distributed Web applications, experience with Microsoft C# and/or Microsoft Visual Basic .NET, experience in writing server-side and client-side scripts by using Active Server Pages (ASP) or Microsoft ASP.NET and familiarity with SQL Server 2000 and Microsoft Internet Information Services (IIS).

Duration

Three days

ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

Developing Secure Web Applications

Course Outline

I. Introduction to Web Security
- A. Why Build Secure Web Applications?
- B. Using the STRIDE Model to Determine Threats
- C. Implementing Security: An Overview

II. Planning for Web Application Security
- A. Lessons
- B. A Design Process for Building Secure Web Applications

III. Validating User Input
- A. User Input
- B. Types of User Input Attacks
- C. Performing Validation
- D. Revealing as Little Information as Possible to the User

IV. Internet Information Services Authentication
- A. Introduction to Web Client Authentication
- B. Configuring Access Permission for a Web Server
- C. Selecting a Secure Client Authentication Method
- D. Running Services As an Authenticated User

V. Securing Web Pages
- A. ASP Forms-Based Authentication
- B. .NET Code Access and Role-Based Security
- C. Overview of ASP.NET Authentication Methods
- D. Working with Windows-Based Authentication in ASP.NET security
- E. Working with ASP.NET Forms-Based Authentication
- F. Use security best practices and a complete understanding of the security model while implementing ASP.NET Web applications.

VI. Securing File System Data
- A. Overview of Securing Files
- B. Windows Access Control
- C. Creating ACLs Programmatically
- D. Protecting ASP.NET Web Application Files

VII. Securing Microsoft SQL Server
- A. SQL Server Connections and Security
- B. SQL Server Role-Based Security
- C. Securing SQL Server Communication
- D. Preventing SQL Injection Attacks

VIII. Helping to Project Communication Privacy and Data Integrity
- A. Introduction to Cryptography
- B. Working with Digital Certificates
- C. Management
- D. Using Secure Sockets Layer/Transport Layer Security Protocols
- E. Using Internet Protocol Security

IX. Encrypting, Hashing, and Signing Data
- A. Encryption and Digital Signing Libraries
- B. Using CAPICOM
- C. Using System.Security.Cryptography Namespace to Hash Data
- D. Using System.Security.Cryptography Namespace to Encrypt and Sign Data

X. Testing Web Applications for Security
- A. Testing Security in a Web Application
- B. Creating a Security Test Plan
- C. Performing Security Testing