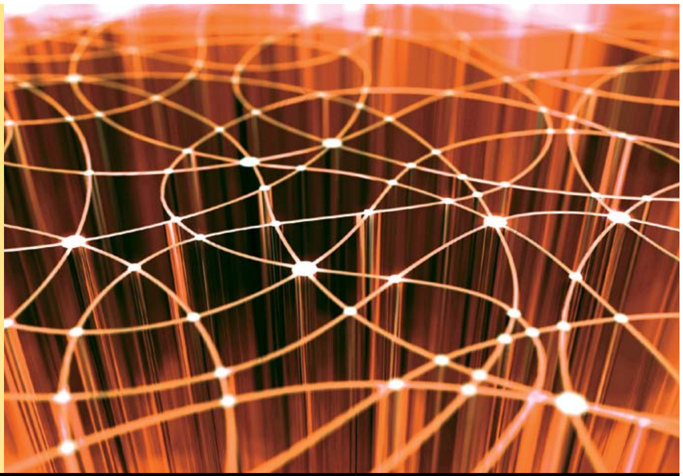
DEV544: Secure Coding in .NET: Developing Defensible Applications

Course Length: Four Days • 24 CPE Credits
Laptop Required

Have you ever wondered if ASP.NET Request Validation is effective? Have you been concerned that XML Web services might be introducing unexamined security issues into your application? Should you feel un-easy relying solely only on the security controls built into the ASP.NET framework? Secure Coding in ASP.NET will answer these questions and far more.



The emphasis of the class is a hands-on examination of the practical aspects of securing .NET applications during development.

During this four-day course we will analyze the defensive strategies and technical underpinnings of the ASP.NET framework and learn where, as a developer, you can leverage defensive technologies in the framework, and where you need to build security in by hand. We'll also examine strategies for building applications that will be secure both today and in the future.

Rather than focusing on traditional Web attacks from the attacker's perspective, this class will show developers first how to think like an attacker, and will then focus on the latest defensive techniques specific to the ASP.NET environment.

What You Will Learn

- Web Application Attacks
  - Cross Site Scripting
  - Cross Site Request Forgery (CSRF)
  - SQL Injection
  - HTTP Response Splitting
  - Parameter Manipulation
- Web Application Proxies
- Using Fiddler
- Code Access Security
- Assemblies
- Global Assembly Cache
- Execution Model
- Authentication
  - IIS / ASP.NET pluggable authentication architecture
  - Basic & Digest Authentication
  - .NET Form Based Authentication Framework
  - Windows Authentication
  - Authorization, OS security, and Impersonation
  - SSL Client Certificates
  - Authentication Policies
- NET Encryption Services
  - Encryption Principals
  - Securing communications
  - Protecting data at rest
- Strong and Weak Named Assemblies
- The Common Language Runtime
- Security Zones
- Evidence
- Code Groups
- Permissions
- Hacking .NET Security

Who Should Attend

This class is focused specifically on software development but is accessible enough for anyone who's comfortable working with code and has an interest in understanding the developer's perspective:

- Software developers and architects
- Senior software QA specialists
- System and security administrators
- Penetration Testers

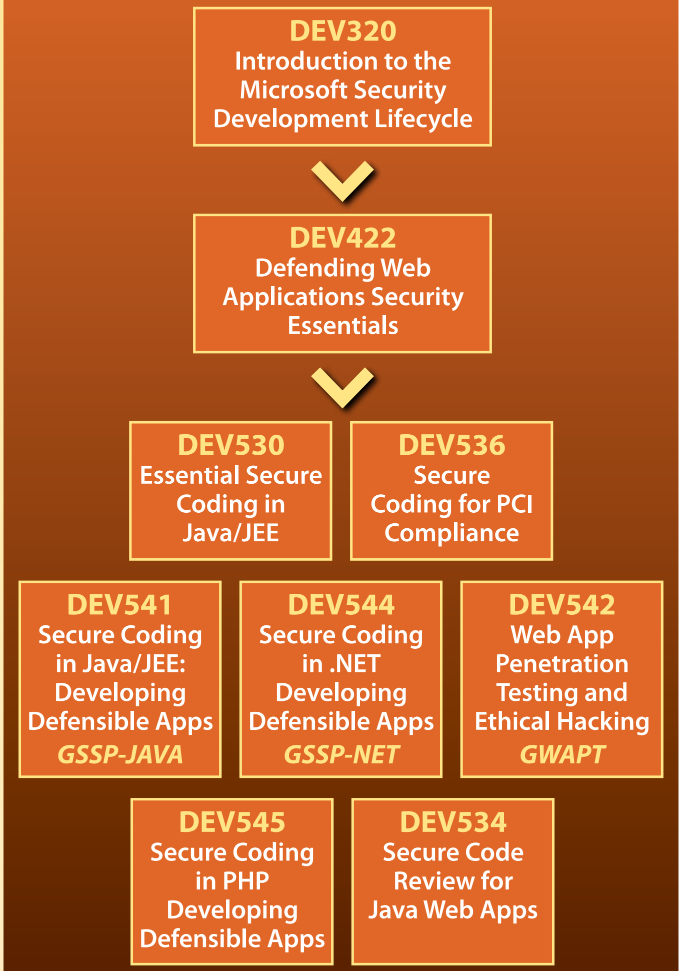
Prerequisites

- Experience with programming in ASP.NET using either Visual Basic or C#. All class work will be performed in C#.
- While this class briefly reviews basic web attacks, some prior understanding of issues such as XSS and SQL injection is recommended.

Looking for a great software development resource?

SANS Software Security Institute Web site (www.sans-ssi.org) is a community-focused site offering AppSec professionals a one-stop resource to learn, discuss, and share current developments in the field. It also provides information regarding SANS AppSec training, GIAC certification, and upcoming events. New content is added regularly, so please visit often. And don't forget to share this information with your fellow application security, developer, and IT security professionals.

DEVELOPER CURRICULUM



DEV320
Introduction to the Microsoft Security Development Lifecycle

DEV422
Defending Web Applications Security Essentials

DEV530
Essential Secure Coding in Java/JEE

DEV536
Secure Coding for PCI Compliance

DEV541
Secure Coding in Java/JEE: Developing Defensible Apps
GSSP-JAVA

DEV544
Secure Coding in .NET Developing Defensible Apps
GSSP-NET

DEV542
Web App Penetration Testing and Ethical Hacking
GWAPT

DEV545
Secure Coding in PHP Developing Defensible Apps

DEV534
Secure Code Review for Java Web Apps

Get GSSP-.NET Certified

GIAC SECURE SOFTWARE PROGRAMMER - .NET
GSSP-.NET

Reinforce what you learned in training and prove your skills and knowledge with a GSSP-NET certification.
www.giac.org

SANS www.sans.org

For more information, visit www.sans-ssi.org
When registering, use this promo code ***DEV544***