Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

CASE - Certified Application Security Engineer Certification Training (CASE.NET)

Course Description

SecureNinja's Certified Application Security Engineer (CASE) – .NET certification training is designed to provide software developers, security professionals, and application testers with the expertise needed to build and secure .NET applications. This hands-on program integrates security into the Software Development Lifecycle (SDLC), addressing common vulnerabilities and ensuring compliance with industry standards and best practices. Participants will gain in-depth knowledge of secure coding principles, attack prevention techniques, and security implementation strategies for .NET applications.

Why Choose CASE .NET?

•Industry-Recognized Certification: Enhance credibility with a globally respected application security credential.

•Hands-On Learning: Work with real-world case studies, security-focused coding labs, and attack simulations.

•Comprehensive Security Integration: Learn to embed security measures at every stage of the SDLC.

•Up-to-Date Curriculum: Covers the latest OWASP Top 10 vulnerabilities, secure coding best practices, and compliance requirements.

•Career Growth: Ideal for professionals looking to specialize in secure .NET application development.

Topics Covered

•Secure coding principles and best practices for .NET applications

•Secure Software Development Lifecycle (SDLC) and threat modeling

•OWASP Top 10 vulnerabilities and mitigation strategies

•Secure authentication, authorization, and session management in .NET

•Input validation and secure data handling techniques

•Secure cryptography implementation for .NET applications

•Protection against SQL Injection, Cross-Site Scripting (XSS), and CSRF attacks

•Secure API and web services development

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

•Security testing methodologies and secure deployment strategies

•Secure logging, monitoring, and error handling

Who is it for?

•.NET Developers and Programmers

•Application Security Engineers

•Software Architects

•Security Analysts and Penetration Testers

•Web Application Testers

•IT Professionals involved in SDLC security

Who Would Benefit?

•Developers looking to enhance the security of .NET applications

•IT professionals responsible for securing enterprise software

•Organizations aiming to build secure .NET applications

•Security professionals seeking expertise in secure application development

Prerequisites

Completion of official EC-Council CASE .NET training through an accredited provider

ECSP (.NET/Java) membership in good standing

Minimum of two years of work experience in InfoSec or software development

Equivalent certifications such as GSSP .NET

Course Outline

Module 1: Secure Software Development Lifecycle (SDLC)

Module 2: Threat Modeling and Risk Management for .NET Applications

Module 3: Secure Coding Practices in .NET

Module 4: OWASP Top 10 Vulnerabilities and Prevention Strategies

Module 5: Secure Input Validation and Data Handling in .NET

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Module 6: Authentication, Authorization, and Session Security

Module 7: Cryptographic Security in .NET Applications

Module 8: Database Security and Injection Prevention Techniques

Module 9: Logging, Monitoring, and Secure Error Handling

Module 10: Web Services and API Security in .NET

Module 11: Security Testing Methodologies for .NET Applications

Module 12: Secure Deployment and Post-Development Security Strategies

Exam Details

Number of Questions: 50

Exam Duration: 2 hours

Passing Score: 70%

Exam Format: Multiple-choice

Exam Availability: Online via EC-Council exam portal

This course is ideal for professionals looking to secure .NET applications by integrating robust security practices throughout the software development process while ensuring compliance with industry best practices and regulatory requirements.