

Certified Application Security Engineer (CASE) .Net

Duration : 3 Days

Course Content

The Certified Application Security Engineer (CASE) credential is developed in partnership with large application and software development experts globally.

The CASE credential tests the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices in today's insecure operating environment.

The CASE certified training program is developed concurrently to prepare software professionals with the necessary capabilities that are expected by employers and academia globally. It is designed to be a hands-on, comprehensive application security course that will help software professionals create secure applications. The training program encompasses security activities involved in all phases of the Software Development Lifecycle (SDLC): planning, creating, testing, and deploying an application.

Unlike other application security training, CASE goes beyond just the guidelines on secure coding practices and includes secure requirement gathering, robust application design, and handling security issues in the post-development phases of application development.

This makes CASE one of the most comprehensive certifications on the market today. It is desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

Who Should Attend

Individuals involved in the role of developing, testing, managing, or protecting wide area of applications

Prerequisites

.NET Developers with a minimum of 2 years of experience and individuals who want to become application security engineers/analysts/testers

Inixindo bandung

Jl. Cipaganti no.95 bandung – TLP/FAX : 022.2032831 | www.inixindobdg.co.id

Course Outline

Module 1: Understanding Application Security, Threats, and Attacks

Module 2: Security Requirements Gathering

Module 3: Secure Application Design and Architecture

Module 4: Secure Coding Practices for Input Validation

Module 5: Secure Coding Practices for Authentication and Authorization

Module 6: Secure Coding Practices for Cryptography

Module 7: Secure Coding Practices for Session Management

Module 8: Secure Coding Practices for Error Handling

Module 9: Static and Dynamic Application Security Testing (SAST & DAST)

Module 10: Secure Deployment and Maintenance

Inixindo bandung

Jl. Cipaganti no.95 bandung – TLP/FAX : 022.2032831 | www.inixindobdg.co.id