EC-Council Certified Application Security Engineer (CASE).NET

Course Overview

This is a 3-day class

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 trainings, CASE goes beyond just the guidelines on secure coding practices and includes secure requirement gathering, robust application design, and handling security issues in 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 who want to become application security engineers/analysts/testers Individuals involved in the role of developing, testing, managing, or protecting wide area of applications

Course Objectives

To ensure that application security is no longer an afterthought but a foremost one. To lay the foundation required by all application developers and development organizations, to produce secure applications with greater stability and fewer security risks to the consumer, therefore, making security a foremost thought. To ensure that the organizations mitigate the risk of losing millions due to security compromises that may arise with every step of application development process. To help individuals develop the habit of giving importance to security sacrosanct of their job role in the SDLC, therefore opening security as the main domain for testers, developers, network administrator etc.

EC-Council Certified Application Security Engineer (CASE).NET

Course Outline

1 IN-DEPTH UNDERSTANDING OF SECURE SDLC AND SECURE SDLC MODELS

2 KNOWLEDGE OF OWASP TOP 10, THREAT MODELLING, SAST AND DAST

3 CAPTURING SECURITY REQUIREMENTS OF AN APPLICATION IN DEVELOPMENT

4 DEFINING, MAINTAINING, AND ENFORCING APPLICATION SECURITY BEST PRACTICES

5 PERFORMING MANUAL AND AUTOMATED CODE REVIEW OF APPLICATION

6 CONDUCTING APPLICATION SECURITY TESTING FOR WEB APPLICATIONS TO ASSESS THE VULNERABILITIES

7 DRIVING DEVELOPMENT OF A HOLISTIC APPLICATION SECURITY PROGRAM

8 RATING THE SEVERITY OF DEFECTS AND PUBLISHING COMPREHENSIVE REPORTS DETAILING ASSOCIATED RISKS AND MITIGATIONS

9 WORKING IN TEAMS TO IMPROVE SECURITY POSTURE

10 APPLICATION SECURITY SCANNING TECHNOLOGIES SUCH AS APPSCAN, FORTIFY, WEBINSPECT, STATIC APPLICATION SECURITY TESTING (SAST), DYNAMIC APPLICATION SECURITY TESTING (DAST), SINGLE SIGN-ON, AND ENCRYPTION

11 FOLLOWING SECURE CODING STANDARDS THAT ARE BASED ON INDUSTRY-ACCEPTED BEST PRACTICES SUCH AS OWASP GUIDE, OR CERT SECURE CODING TO ADDRESS COMMON CODING VULNERABILITIES.

12 CREATING A SOFTWARE SOURCE CODE REVIEW PROCESS THAT IS A PART OF THE DEVELOPMENT CYCLES (SDLC, AGILE, CI/CD)