EC-Council Certified Application Security Engineer (CASE) . Net + Voucher d'examen

Durée: 3 Jours Réf de cours: CASE-NET Version: 1.0 Méthodes d'apprentissage: Classe à distance

Résumé:

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.

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

Individuals involved in the role of developing, testing, managing, or protecting a wide area of applications or individuals hoping to become application security engineers/analysts/testers

Objectifs pédagogiques:

- **After completing this course you should be able to:**
- Understand secure SDLC and secure SDLC models in-depth
- Apply the knowledge of OWASP Top 10, threat modelling, SAST and DAST
- Capture security requirements of an application in development
- Define, maintain and enforce application security best practices
- Perform manual and automated code review of application
- Conduct application security testing for web applications to assess the vulnerabilities
- Drive the development of a holistic application security program
- Rate the severity of defects and publishing comprehensive reports detailing associated risks and mitigations
- Work in teams to improve security posture
- Use Application security scanning technologies such as AppScan, Fortify, WebInspect, static application security testing (SAST), dynamic application security testing (DAST), single sign-on, and encryption
- Follow secure coding standards that are based on industry-accepted best practices such as OWASP Guide, or CERT Secure Coding to address common coding vulnerabilities.
- Create a software source code review process that is a part of the development cycles (SDLC, Agile, CI/CD)

Pré-requis:

To be eligible to apply to sit for the CASE exam the candidate must either:

Test et certification

Recommended as preparation for the following exams:

- EC-Council Certified Application Security Engineer Exam -

- Attend the official EC-Council CASE training through an accredited EC-Council Partner (Accredited Training Centre/ iWeek/ iLearn) (All candidates are required to pay the USD100 application fee unless your training fee already includes this) or
- Be an ECSP (.NET/ Java) member in good standing or
- Have a minimum of 2 years working experience in InfoSec/ Software domain or
- Have any other industry equivalent certifications such as GSSP .NET/Java

Candidates for this exam must have attended CASE training through an accredited EC-Council Partner and meet the other EC-Council Eligilibity Criteria.

Contenu:

Understanding Application Security, Threats and Attacks

- What is a Secure Application
- Need for Application Security
- Most Common Application Level Attacks
- Why Applications become Vulnerable to Attacks
- What Consistutes Comprehensive Application Security ?
- Insecure Application: A Software Development Problem
- Software Security Standards, Models and Frameworks

Security Requirements Gathering

- Importance of Gathering Security Requirements
- Security Requirement Engineering (SRE)
- Abuse Case and Security Use Case Modeling
- Abuser amd Security Stories
- Security Quality Requirements Engneering (SQUARE)
- Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

Secure Application Design and Architecture

- Relative Cost of Fixing Vulnerabilities at Different Phases of SDLC
- Secure Application Design and Architecture
- Goal of Secure Design Process
- Secure Design Actions
- Secure Design Principles
- Threat Modeling
- Decompose Application
- Secure Application Architecture

Secure Coding Practices for Input Validation

- Input Validation
- Why Input Validation ?
- Input Validation Specification
- Input Validation Approaches
- Input Filtering
- Secure Coding Practices for Input Validation: Web Forms
- Secure Coding Practices for Input Validation: ASP.NET Core
- Secure Coding Practices for Input Validation: MVC

Secure Coding Practices for Authentication and Authorization

- Authentication and Authorization
- Common Threats on User Authentication and Authorization
- Authentication and Authorization: Web Forms
- Authentication and Authorization: ASP .NET Core
- Authentication and Authorization: MVC
- Authentication and Authorization Defensive Techniques : Web Forms
- Authentication and Authorization Defensive Techniques : ASP .NET Core
- Authentication and Authorization Defensive Techniques : MVC

Secure Coding Practices for Cryptography

- Cryptographic
- Ciphers
- Block Ciphers Modes
- Symmetric Encryption Keys
- Asymmetric Encryption Keys
- Functions of Cryptography
- Use of Cryptography to Mitigate Common Application Security Threats
- Cryptographic Attacks
- Techniques Attackers Use to Steal Cryptographic Keys
- What should you do to Secure .Net Applications for Cryptographic Attacks
- .NET Cryptographic Name Spaces
- .NET Cryptographic Class Hierarchy
- Symmetric Encryption
- Symmetric Encryption: Defensive Coding Techniques
- Asymmetric Encryption
- Asymmetric Encryption: Defensive Coding Techniques
- Hashing
- Digital Signatures
- Digital Certificates
- XML SIgnatures
- ASP.NET Core Specific Secure Cryptography Practices

Secure Coding Practices for Session Management

- What are Exceptions/Runtime Errors ?
- Need for Secure Error/Exception Handling
- Consequences of Detailed Error Message
- Exposing Detailed Error Messages
- Considerations: Designing Secure Error Messages
- Secure Exception Handling
- Handling Exceptions in an Application
- Defensve Coding practices against Information Disclosure
- Defensive Coding practices against Improper Error Handling
- ASP .NET Core: Secure Error Handling Practices
- Secure Auditing and Logging
- Tracing .NET
- Auditing and Logging Security Checklists

Static and Dynamic Application Security Testing (SAST and DAST)

- Static Application Security Testing
- Manual Secure Code Review for Most Common Vulnerabilities
- Code Review: Check List Approach
- SAST Finding
- SAST Report
- Dynamic Application Security Testing
- Automated Application Vulnerability Scanning Tools
- Proxy-based Security Testing Tools
- Choosing between SAST and DAST

Secure Deployment and Maintenance

- Secure Deployment
- Prior Deployment Activity
- Deployment Activities: Ensuring Security at Various Levels
- Ensuring Security at Host Level
- Ensuring Security at Network Level
- Ensuring Security at Application Level
- Web Application Firewall (WAF)
- Ensuring Security at IIS Level
- Sites and Virtual Directories
- ISAPI Filters
- Ensuring Security at .NET Level
- Ensuring Security at SQL Server Level
- Security Maintenance and Monitoring

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement