



Certified Application Security Engineer (CASE) Java



Course Description

The **CASE Java** program is designed to be a hands-on, comprehensive application security training course that will help software professionals create secure applications. It trains software developers on 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 required in today's insecure operating environment.



Course Outline

- Understanding Application Security, Threats, and Attacks
- Security Requirements Gathering
- Secure Application Design and Architecture
- Secure Coding Practices for Input Validation
- Secure Coding Practices for Authentication and Authorization
- Secure Coding Practices for Cryptography
- Secure Coding Practices for Session Management
- Secure Coding Practices for Error Handling
- Static and Dynamic Application Security Testing (SAST & DAST)
- Secure Deployment and Maintenance



Key Outcomes

- Security Beyond Secure Coding - Challenging the traditional mindset where secure application means secure coding
- Testing and credentialing secure application development across all phases of the SDLC
- CASE Program maps to many Specialty Areas under "Securely Provision category" in the NICE 2.0 Framework
- Covers techniques such as Input Validation techniques, Defense Coding Practices, Authentications and Authorizations, Cryptographic Attacks, Error Handling techniques, and Session Management techniques, among many others



Exam Information

- Exam Title: Certified Application Security Engineer (Java)
- Exam Code: 312-96
- Number of Questions: 50
- Duration: 2 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%