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

CASE - Certified Application Security Engineer Certification Training (CASE JAVA)

Course Description

SecureNinja's Certified Application Security Engineer (CASE) – Java certification is designed to equip software developers, security professionals, and application testers with the knowledge and skills to secure Java applications throughout the Software Development Lifecycle (SDLC). This hands-on course focuses on integrating secure coding principles into development processes, mitigating security vulnerabilities, and ensuring compliance with industry standards.

Why Choose CASE Java?

•Industry-Recognized Certification: Validate your expertise in secure Java application development.

•Hands-On Learning: Gain practical experience through real-world case studies, secure coding labs, and attack simulations.

•SDLC Integration: Learn to embed security measures at every stage of software development.

•Updated Curriculum: Stay ahead with the latest application security best practices and OWASP Top 10 threats.

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

Topics Covered

•Secure coding principles and best practices for Java applications

•Secure software development lifecycle (SDLC) and threat modeling

•OWASP Top 10 vulnerabilities and how to prevent them

•Input validation, authentication, and authorization security measures

•Secure session management and cryptography implementation

•Secure database access and handling injection attacks

•Application logging and error handling for security

•Web services and API security

•Security testing methodologies and tools

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

•Secure deployment practices and post-deployment monitoring

Who is it for?

•Software Developers and Programmers

•Application Security Engineers

•Software Architects

•Security Analysts

•Penetration Testers and Ethical Hackers

•Web Application Testers

•Professionals involved in SDLC security

Who Would Benefit?

•Developers looking to integrate security into Java applications

•IT professionals responsible for securing enterprise applications

•Organizations wanting to build robust and secure Java applications

•Security professionals seeking to enhance their secure coding knowledge

Prerequisites

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/Java

Course Outline

Module 1: Secure Software Development Lifecycle (SDLC)

Module 2: Threat Modeling and Risk Management

Module 3: Secure Coding Principles in Java

Module 4: OWASP Top 10 Vulnerabilities and Mitigation

Module 5: Secure Input Validation and Data Handling

Module 6: Authentication, Authorization, and Session Security

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

Module 7: Secure Cryptographic Implementations

Module 8: Database Security and Injection Prevention

Module 9: Logging, Monitoring, and Error Handling

Module 10: Web Services and API Security

Module 11: Security Testing and Compliance Strategies

Module 12: Secure Deployment and Post-Development Security

Course Length

- 3 Days
- 24 Hours

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 build and secure Java applications while ensuring compliance with security best practices and industry standards.