CertNexus Cyber Secure Coder Course

Course Duration: 8 Hrs. **Course Code: CSC-210**

Course Overview

The **CertNexus Cyber Secure Coder** course is designed for software developers and technical professionals who want to build security into applications from the ground up. This course focuses on secure coding principles, common software vulnerabilities, and best practices to prevent security breaches. Participants will learn how to identify, mitigate, and prevent security risks during the software development lifecycle while preparing for the CertNexus Cyber Secure Coder certification exam.

What You'll Learn?

By completing this course, you will be able to:

- Understand secure coding principles and best practices
- Identify common software vulnerabilities and threats
- Apply techniques to prevent OWASP Top 10 vulnerabilities
- Implement secure authentication and authorization
- Secure data handling and storage practices
- Integrate security into the SDLC and DevSecOps
- Prepare confidently for the CertNexus Cyber Secure Coder certification exam

Target Audience

This course is ideal for:

- Software Developers and Programmers

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

- Application Developers and Engineers
- DevOps and DevSecOps Professionals
- Technical Leads and Architects
- Professionals seeking secure coding certification

Pre-Requisites

Participants should have:

- Basic programming knowledge (any language)
- Understanding of web or application development concepts
- Familiarity with software development life cycles
- Interest in application security

Course Content

Module 1: Secure Coding Fundamentals

- Introduction to application security
- Secure coding principles
- Common attack vectors

Module 2: Common Vulnerabilities and Threats

- OWASP Top 10 overview
- Injection attacks and mitigation
- Cross-site scripting and request forgery

Module 3: Authentication, Authorization, and Session Management

- Secure authentication mechanisms
- Role-based access control

- Session handling best practices

Module 4: Secure Data Handling and Error Management

- Data validation and sanitization
- Encryption and secure storage
- Secure error and exception handling

Module 5: Secure Coding in the SDLC and DevSecOps

- Integrating security into development pipelines
- Secure code reviews and testing
- Automation and security tools

Module 6: Best Practices, Compliance, and Exam Preparation

- Secure coding standards and guidelines
- Regulatory and compliance considerations
- Certification exam overview and preparation tips