Certified Security Tester Course

Course Duration: 24 Hrs. **Course Code: CST**

Course Overview

The **Certified Security Tester** course is designed for software testing and quality assurance professionals who want to specialize in security testing. This course focuses on identifying, analyzing, and mitigating security risks in applications and systems through structured testing approaches. Participants will gain practical knowledge of security vulnerabilities, threat modeling, and security testing techniques aligned with industry standards, enabling them to ensure robust and secure software solutions.

What You'll Learn?

By completing this course, you will be able to:

- Understand core concepts of application and system security
- Identify common security vulnerabilities and threats
- Apply security testing techniques across different test levels
- Perform risk-based security testing
- Use tools to support vulnerability assessment and security testing
- Integrate security testing into agile and DevOps environments
- Improve overall software security and compliance

Target Audience

This course is ideal for:

- Software Testers and QA Engineers
- Security Testers and Ethical Testing Professionals

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

- Test Analysts and Technical Testers
- Developers involved in secure coding and testing
- Quality and Compliance professionals

Pre-Requisites

Participants should have:

- Basic understanding of software testing principles
- Familiarity with software development life cycles
- Knowledge of web and application technologies is beneficial
- Prior testing experience is preferred but not mandatory

Course Content

Module 1: Fundamentals of Security Testing

- Security concepts and terminology
- Threats, vulnerabilities, and risks
- Role of security testing in quality assurance

Module 2: Security Testing Principles and Approaches

- Risk-based security testing
- Static and dynamic security testing
- Security testing in different life cycles

Module 3: Common Vulnerabilities and Attacks

- OWASP Top 10 overview
- Authentication and authorization flaws
- Data protection and privacy issues

Module 4: Security Testing Techniques and Tools

- Vulnerability scanning and penetration testing basics
- Manual vs. automated security testing
- Overview of security testing tools

Module 5: Security Testing in Agile and DevOps

- Shift-left security and DevSecOps
- Integrating security testing into CI/CD pipelines
- Collaboration between teams

Module 6: Reporting, Compliance, and Improvement

- Security defect reporting and remediation
- Compliance and regulatory considerations
- Continuous improvement in security testing