Security Testing for Quality Professionals Training Course

Professional Development Training Course Outline

Category	Quality Assurance and ISO standards	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Security testing has become a crucial aspect of software quality assurance, driven by the increasing number of cyber threats and compliance requirements in today?ÇÖs digital landscape. Security Testing for Quality Professionals Training Course equips quality professionals with the essential skills to identify vulnerabilities, implement penetration testing strategies, and validate secure coding practices. Through hands-on learning, participants gain real-world expertise in applying trending tools, methodologies, and frameworks to ensure systems are resistant to attacks.

By focusing on practical techniques such as threat modeling, ethical hacking, and vulnerability scanning, this course empowers professionals to enhance system resilience and safeguard data integrity. Participants will be able to integrate security testing into the software development lifecycle (SDLC), ensuring higher quality, regulatory compliance, and improved trust in organizational digital assets.

Programme Curriculum

Security Testing for Quality Professionals Training Course

Introduction

Security testing has become a crucial aspect of software quality assurance, driven by the increasing number of cyber threats and compliance requirements in today?ÇÖs digital landscape. Security Testing for Quality Professionals Training Course equips quality professionals with the essential skills to identify vulnerabilities, implement penetration testing strategies, and validate secure coding practices. Through hands-on learning, participants gain real-world expertise in applying trending tools, methodologies, and frameworks to ensure systems are resistant to attacks.

By focusing on practical techniques such as threat modeling, ethical hacking, and vulnerability scanning, this course empowers professionals to enhance system resilience and safeguard data integrity. Participants will be able to integrate security testing into the software development lifecycle (SDLC), ensuring higher quality, regulatory compliance, and improved trust in organizational digital assets.

Course Objectives

1. Understand the fundamentals of security testing in software quality assurance
2. Apply penetration testing methodologies in real-world scenarios
3. Perform vulnerability assessments using industry-leading tools
4. Integrate security testing into DevSecOps pipelines
5. Conduct threat modeling for risk-based security testing
6. Implement secure coding review and verification practices
7. Analyze authentication and authorization mechanisms for flaws
8. Test APIs, web applications, and mobile apps for vulnerabilities
9. Execute network security testing techniques effectively
10. Ensure compliance with ISO 27001, GDPR, and OWASP standards
11. Utilize automation in security testing to improve efficiency
12. Report, document, and communicate security findings effectively
13. Build a proactive culture of security in QA and development teams

Organizational Benefits

1. Enhanced security resilience across applications and systems
2. Reduced risk of cyberattacks and data breaches
3. Improved compliance with global regulations and standards
4. Stronger collaboration between QA, development, and security teams
5. Higher customer trust through robust software security
6. Early detection and mitigation of security vulnerabilities
7. Streamlined integration of security testing into workflows
8. Increased ROI by minimizing remediation costs post-release
9. Improved incident response readiness within QA teams
10. Competitive advantage through secure and reliable products

Target Audiences

1. Quality Assurance Professionals
2. Software Test Engineers
3. IT Security Analysts
4. DevOps and DevSecOps Engineers
5. Application Developers
6. Compliance and Risk Officers
7. Project Managers in IT and Security domains
8. System Administrators

Course Duration: 5 days

Course Modules

Module 1: Introduction to Security Testing

- Overview of security testing in QA
- Importance of security in the SDLC
- Types of security threats and vulnerabilities
- Tools for introductory security testing
- Key standards (OWASP, ISO)
- Case Study: Role of security testing in a banking application

Module 2: Penetration Testing Fundamentals

- Concepts of penetration testing
- Steps in a penetration testing lifecycle
- Manual vs automated penetration testing
- Penetration testing tools and frameworks
- Legal and ethical considerations
- Case Study: Simulated attack on a retail e-commerce platform

Module 3: Vulnerability Assessment Techniques

- Difference between vulnerability assessment and penetration testing
- Automated vulnerability scanning tools
- Risk-based vulnerability prioritization
- Common vulnerability patterns
- Vulnerability remediation strategies
- Case Study: Handling vulnerabilities in a healthcare management system

Module 4: Secure Coding and Code Review

- Principles of secure coding
- Code review methodologies
- Static and dynamic analysis tools
- Common coding pitfalls leading to vulnerabilities
- Best practices for secure development
- Case Study: Secure coding audit in a mobile application

Module 5: Testing Authentication and Authorization

- Importance of access controls in applications
- Common flaws in authentication mechanisms
- Authorization testing techniques
- Multi-factor authentication testing
- Security misconfigurations in identity management
- Case Study: Breach simulation in a cloud-based HR system

Module 6: Web Application Security Testing

- Key vulnerabilities in web applications (OWASP Top 10)
- SQL injection and cross-site scripting testing
- Cross-site request forgery detection
- Tools for web application security testing
- Secure session management practices
- Case Study: Security assessment of a government portal

Module 7: API and Mobile Application Security

- API testing tools and techniques
- Mobile app-specific security vulnerabilities
- Security challenges in microservices
- Secure API design principles
- Testing API authentication mechanisms
- Case Study: API breach in a ride-sharing application

Module 8: Automation in Security Testing

- Role of automation in enhancing security testing
- CI/CD pipeline integration for security
- Popular automation frameworks and tools
- Benefits and limitations of automated testing
- Aligning automated testing with DevSecOps
- Case Study: Automated vulnerability scanning in a financial services firm

Training Methodology

- Interactive lectures with real-world examples
- Hands-on labs and practical tool usage
- Group discussions and problem-solving exercises
- Simulated attack and defense scenarios
- Case study analysis for applied learning
- Continuous assessments and feedback

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com