coveros

Security Testing for Test Professionals

Integrating security into your testing process

Description

Today's software applications are often security-critical, making security testing an essential part of a software quality program. This 2-day course provides software testers with the knowledge necessary to integrate security testing into their everyday testing activities. Learn how to:

- define sound security requirements (functional and non-functional)
- effectively test security features,
- identify security risks and validate their absence,
- test web applications for common web security vulnerabilities,
- test API's and other subsystems for security

Practice testing a variety of security features that are common on today's software applications Take home valuable tools and techniques for effectively testing your applications for security going forward.

Security Testing for Test Professionals includes exercises to practice identifying actual software vulnerabilities within applications. Tools and techniques for effectively security testing applications will be demonstrated.

Attendees will leave *Security Testing for Test Professionals* with an in-depth understanding of how to integrate security testing into your existing software testing process.

Who Should Attend?

The audience includes software testers and software engineers in test as well as test managers and software developers who need to understand security testing.

2 Day Course Outline

1. Introduction to Security Testing
   a. History of information security
   b. The software security problem
   c. Understanding software risk
   d. Security testing approaches

2. Security requirements
   a. Functional security requirements
   b. Non-functional security requirements
   c. Integrating security requirements into test plans

3. Testing Authentication and Session Management
   a. Common approaches to authentication
   b. Testing password functionality
   c. Testing credentials

4. Testing Access Control
   a. Access control policies
   b. Testing access control across application layers

5. Input Validation
   a. Common input mistakes
   b. Validating web input
   c. Cross site scripting

6. Database Testing for Security
   a. Introduction to database security
   b. Testing database access
   c. Testing for SQL injection vulnerabilities

7. Testing Data Privacy
   a. Introduction to privacy methods and concerns
   b. Testing cryptographic libraries
   c. Avoiding replay attacks

8. Integrating Security Testing into Your Testing Process
   a. Security requirements
   b. Security test planning
   c. Tools to support security testing

Contact Us for More Information:

Coveros, Inc.
4000 Legato Road, Suite 1100
Fairfax, VA 22033
703-349-6109
www.coveros.com