

- Learn how testing professionals can effectively security test software
- Discover how applications are developed and tested with security in mind
- Learn how to use security requirements to plan your testing efforts
- Explore key aspects of security testing—web security, threat modeling, risk assessment
- Examine technical and team skills you need for success
- Learn to use common security testing tools for a variety of testing purposes

Course Description

Your organization is doing well with functional, usability, and performance testing. However, you know that software security is a key part of your assurance and compliance strategy for protecting applications and critical data. Left undiscovered, security-related defects can wreak havoc in a system when malicious invaders attack. If you don't know where to start with security testing and don't know what you are looking for, this course is for you. It describes how to get started with security testing, introducing foundational security testing concepts and showing you how to apply those security testing concepts with free and commercial tools and resources. Offering a practical risk-based approach, the instructor discusses why security testing is important, how to use security risk information to improve your test strategy, and how to add security testing into your software development lifecycle.

Practice of Security Testing

Explore security testing in an informal and interactive workshop setting. Examples are studied through a series of small group exercises and discussions.

Who Should Attend

This course is appropriate for software development and testing professionals who want to begin doing security testing as part of their assurance activities. Test and development managers will benefit from this course as well. A background in software testing is necessary for this course.

This class will have several hands-on exercises done in small groups. Laptops are suggested but not required. All exercises are cloud-based so there are no requirements to download programs to your laptop.

Course Outline

Introduction to Security Testing

Information Security Background
CIAA++

Understanding Software Application Risk

The Software Security Problem
Understanding Risk
Threat Modeling
Architecture Risk Analysis
Risk Assessment Exercise
Prioritizing Security Assurance

Application Security Testing Approaches

Types of App Security Testing
Discovery & Reconnaissance Analysis
Vulnerability Scanning

Security Testing to Thwart Attacks

Security Testing Authentication

Attacks Against Authentication
Session IDs and Cookies
Authentication Testing
Race Conditions
Session Management
Replay Attacks
Cross Site Request Forgery (CSRF)
Testing Authentication Exercise

Security Testing Authorization / Access Control

Testing Access Control
Security Testing Authorization Exercise

Security Assessments

Red Teaming

Security & Compliance Audit

How They Are Similar

How They Are Different

Reconnaissance and Scanning Demos

Security Requirements

Functional Security Requirements

Non-Functional Security Requirements

Addressing Conflicts

Identifying Security Requirements

Security Requirements Exercise

Use and Abuse Cases

Security Testing Input Fields

Input Validation

Data Validation

Common Attacks

Security Testing Input Fields Exercise

Database Testing for Security

Security Testing for Data Storage

Security Testing Databases Exercise

Security Testing Code and Resources

Integrating Security into Your Testing Process

Security in an Agile World

Security in a Waterfall World

Developing a Security Test Plan

Tools to Support Security Testing

Security Tools in a DevOps Process

Exploiting Vulnerabilities Exercise

Wrap Up