

# Principles and Development of Secure Applications

## COURSE DESCRIPTION

This three-day course, a combination of our Application Security Principles course and our Secure Development Life Cycle course, provides you with the principles of application security, in addition to extensive opportunity to apply those principles to real development life cycle scenarios.

The Application Security Principles segment of the course provides lecture and labs on application security and its impact on application architecture and development. Principles and elements of secure architecture and coding are closely examined and tied directly to the vulnerabilities that they prevent or mitigate. The core training materials are independent of specific platforms and languages, which provide an excellent foundation in application security.

In the Secure Development Life Cycle portion of the course, you learn how to successfully integrate security into all phases of the software development lifecycle—from requirements and design through code review and security testing. Core class concepts include application risk profiling and the security review process at each stage of development. These concepts are taught with group exercises and case studies, which give students the real-world skills required to examine each stage of the software development lifecycle with a critical eye to security. Security test methodologies are discussed and hands-on labs are offered, using common security tools to perform security testing on sample applications. Symantec can also tailor the course content based on an organization's specific training needs.

Symantec instructors have in-depth security expertise drawn from years of experience and understanding of the complex issues involved in integrating security into fast-paced software development projects. Symantec instructors speak “the developers’ language” and their expertise enables them to make the course lessons relevant and immediately applicable.

### Delivery Method

Instructor-led

### Duration

3 days

### Course Objectives

By the end of this course, you should be able to

- Address security in the design of an application.
- Identify assets, threats, and countermeasures.
- Perform proper input validation.

- Avoid common coding mistakes that lead to application security vulnerabilities.
- Identify tools and techniques for secure implementation.
- Optimize the testing phase to identify vulnerabilities.
- Prevent application resource and information leaks.

### Who Should Attend

This course is for all members of the application development organization, including program managers, architects, developers, and testers. Familiarity with basic programming concepts enhances the understanding of content within the course.

### Prerequisites

You should have a working knowledge of one or more current structured programming languages, and familiarity with basic programming concepts. Some knowledge of the software development life cycle is helpful.

### Hands-On

This course includes practical exercises, demonstrations, and case studies that enable you to test your new skills and begin to transfer them into your working environment.

## COURSE OUTLINE

### *Application Security Principles (2 days)*

#### Lesson 1: Introduction to ASP

- Who Are Hackers?
- Types of Vulnerabilities
- The Vulnerability Lifetime
- Secure Software Development Life Cycle
- Recommended Resources

#### Lesson 2: Secure Design Goals and Faults

- Security Goals
- Hacker Goals

#### Lesson 3: Web Application Attacks

- Input Validation
- Regular Expressions
- Summary

#### Lesson 4: Other Faults

- Web Security Hazards
- Injection Attacks
- Directory Traversal

**Lesson 5: The Importance of Input Validation**

- Buffer Overflows
- Format String Attacks
- Integer Overflows
- Return Code Validation
- Cryptographic Deficiencies

**Secure Development Life Cycle (1 day)****Lesson 1: Security Requirements**

- Security Requirements
- Use and Abuse Cases
- Security Requirements Review

**Lesson 2: Secure Design**

- Design Review
- Sample Application

**Lesson 3: Threat Modeling and Risk Ranking**

- Threat Modeling
- Risk Ranking

**Lesson 4: Code Review Strategies**

- Code Review Methodologies
- Code Review Tools

**Lesson 5: Penetration Testing**

- Security and Penetration Tests
- Penetration Testing Tools

**Lesson 6: Secure Deployment**

- Secure Deployment
- Example: Blaster