

Application Security Principles

COURSE DESCRIPTION

The Application Security Principles course provides lecture and demonstrations 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. Demonstrations present common application exploits and testing techniques. The core training materials are independent of specific platforms and languages, which provide an excellent foundation in application security.

Symantec can also tailor courses to address specific platforms or coding languages, based on an organization's training needs. Symantec instructors have in-depth security expertise drawn from years of experience and understanding of the complex issues involved in security strategy, design, implementation, and operations.

Delivery Method

Instructor-led

Duration

One day

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.

COURSE OUTLINE

Application Security Principles

OWASP Top 10 Security Issues

- Common Coding Errors

- Technical Demonstrations / Labs

Security Principles

- Security As a Process
- Principle of Least Privilege
- Input Validation and Output Sanitation

Elements of a Secure Design

- Authentication and Authorization
- Data Confidentiality and Integrity
- Nonrepudiation, Auditing, and Availability

Handling Input and Output Securely

- Stopping Attackers Through Input Validation
- Limiting Attackers Through Output Sanitation

Introduction to Threat Modeling

- Security During the Design Phase
- Privileges and Trust Boundaries
- Prioritizing and Focusing Security Resources Appropriately

Risk Management

- Security Risk Process
- Risk Identification and Rating

More Information

Contact a Custom Learning Services specialist

customlearning@symantec.com

About Symantec

Symantec is the global leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure. Symantec's Norton brand of products is the worldwide leader in consumer security and problem-solving solutions. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
1 408 517 8000
1 800 721 3934
www.symantec.com