Course Description

Writing Secure Code: Java

Foundstone® Services Training Course

Software insecurity has become one of the biggest security concerns facing organizations today. As hackers turn their attention to the software and applications that make up an organization's IT infrastructure, people are realizing that the best way to protect that infrastructure is to build secure software at the onset. Learn the practical techniques and technologies that are needed to design and build secure software. This course discusses a variety of software models with a special focus on web applications. Students will learn how to secure each stage of the software development lifecycle (SDLC) by understanding the foundational concepts for securing software.

Course Goals

- Process and techniques of building secure software.
- Secure user-management systems.
- Cryptography.
- Data-validation strategies.
- Error handling and exception management.
- Software security review techniques.

Agenda At A Glance

- Introduction
- Java Platform Security
- Cryptography
- Authentication
- Authorization
- Error Handling and Exception Management
- Data Validation
- Client-Side Security
- User Management
- Logging and Auditing
- Secure Code Review
- Advanced Java Security

Audience

- Software professionals who define, design, and architect solutions, as well as those who manage software development projects and teams, and those that audit the security of applications.

intel Security

Recommended Pre-Work

It is recommended that students have a working knowledge of Microsoft Windows administration, system administration concepts, a basic understanding of computer security concepts, and a general understanding of Internet services.

Course Outline

Module 1—Introduction

- Introduction/Purpose
- Software Security Overview

Module 2—Jave Platform Security

- Java Security Overview
- Java Runtime and Compile Time Security
- Java Security Manager
- Java Authentication and Authorization Service
- Servlet, JSP, and EJB Security

Module 3—Cryptography

- Definitions and Properties
- Common Mistakes
- Random Numbers
- Java Cryptography Extension
- Key Storage and Generation
- Java Secure Sockets Extension
- XML Encryption and Digital Signatures

Module 4—Authentication

- Authentication Protocols
- Common Mistakes
- Servlet Container Authentication
- Single Sign-On
- Code Signing

Module 5—Authorization

- Access Control Models
- Common Mistakes
- Least Privilege
- Discretionary Access Control
- Role-Based Access Controls
- Cross-Site Request Forgery
- Servlet Container Authorization
- Session Management
- EJB Authorization Controls
- Custom Authorization Implementations

Module 6—Error Handling and Exception Management

- Java Exception Fundamentals
- Exception Handling Patterns and Anti-Patterns
- Best Practices for Handling User Errors
- Servlet, JSP, EJB, and Struts Exceptions

Module 7—Data Validation

- Common Mistakes
- Trust Boundaries
- Data Validation Design
- Validation Strategies and Tactics
- Web Application Firewalls
- Character Encoding and Security
- Regular Expressions
- Common Data Validation Attacks
- Validating Non-Textual Data

Module 8—Client-Side Security

- Common Mistakes
- Reverse Engineering
- Code Obfuscation
- Anti-Tampering Measures

Course Description

Module 9—User Management

- Common Mistakes
- Secure Password Storage
- Password Reset Schemes
- Password Lockout Schemes
- Password Length and Complexity

Module 10—Logging and Auditing

- Common Mistakes
- What to Log
- Auditing
- What to do with Log Files
- Logging Frameworks

Module 11—Secure Code Review

- Secure Code Review Methodology
- Threat Modeling
- Automated Source Code Analysis
- Identifying Common Mistakes

Module 12—Advanced Java Security

- Access Protection
- Thread Safety
- Defensive Coding
- Serialization
- Java Native Interface

To order, or for further information, please call 1 888 847 8766 or email **SecurityEducation@intel.com**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com