



SECURE JAVA CODING

COURSE OVERVIEW

Safelight

All software development teams have a critical role to play in protecting sensitive information.

By identifying and resolving vulnerabilities early in the software development lifecycle, your team can substantially—and cost-effectively—reduce information risk.

Only recently have companies begun to meaningfully integrate security into the software development lifecycle. Secure coding has been greatly advanced by the adoption of formal software security assurance methodologies such as Microsoft SDL, OWASP's SAAM and BSIMM. Central to the successful implementation of these methodologies is role-specific training for all development staff—whether they are architects, developers, QA testers or managers.

Our courses for development teams begin with an overview of fundamental secure coding principles. Students learn the many ways in which vulnerabilities in software code may be exploited by attackers and are shown the value of secure development. Building on this understanding of the risks inherent in software development, students learn solid architecture, design, testing and implementation principles. From there, they explore ways to root out security issues within existing systems and how to effectively respond to evolving security threats.



COURSE DETAILS

Target Learners

This course is designed for technical team members associated with application development efforts coded in Java. Roles include Java developers of various languages, architects, technical QA staff and database administrators.

Prerequisites

Students should have an understanding of information security basics before taking this course; Safelight's Application Security Fundamentals course is the ideal prerequisite.

Length

This course can be configured to be 1 or 2 days in length with or without lab exercises. The client can customize the course by selecting from a menu of topics.

Delivery

Instructor-led and on-demand options available.

Course Overview

This role-specific intermediate course is designed for experienced Java developers and architects who work with Java development teams. This focused course equips students with a clear understanding of the built-in security features of Java as well as best practices for coding securely. Topics will include: Web applications; input validation and output sanitization; logging and exception handling; data access security basics; and privacy and secrets. Students should have an understanding of information security basics before taking this course; our Application Security Fundamentals course is the ideal prerequisite.

Learning Objectives

After completing this course, students will be able to:

- Understand the issues involved in building secure Web applications in Java.
- Explain the security issues with XML and Web services.
- Discuss the need for maintaining confidentiality of private data and explain specific strategies.
- Explain specific techniques that can be used to successfully validate input, including the appropriate use of regular expressions.
- Understand the importance of using a logging framework and explain techniques for making optimal use of audit logs.
- Explain the proper ways to handle exceptions within an application.
- Discuss strategies for avoiding information disclosure within a Java Web application.
- Understand the basic mechanisms of cryptography.
- Understand and discuss various threats to data security, including insecure communications, insecure data storage and over-privileging.
- Explain a variety of ways to protect data from inappropriate access, including applying the principle of least privilege, making appropriate database calls from the application and encrypting backups.
- Understand and discuss the primary approaches to testing an application for security, including architecture review, code review and penetration testing.
- Understand and explain how to find and fix SQL injection, cross-site scripting and cross-site request forgery issues after participating in a series of hands-on labs.

Our Instructors

Rob Cheyne

Rob Cheyne, co-founder of Safelight Security, spends his time perfecting the fine art of instructor-led training by applying the latest best practices in adult learning to the information security field. He is a Boston-based information security expert who has taught training classes to over 12,000 students, including developers, architects, and managers for industry-leading organizations. He has over 20 years of experience in the information technology field and has been working in information security since 1998. Over the years, he has played the role of software developer, systems integrator, security consultant and trainer. Rob regularly speaks at security conferences, and frequently presents to the Boston OWASP chapter on a variety of security topics. His specialties are application security architecture and information security training. He was an early employee of @stake, a highly regarded pioneer in information security consulting. In this role, he led and conducted secure architecture and design reviews, secure code reviews, application penetration tests, and security assessments for numerous Fortune 500 companies. Rob worked on @stake's SmartRisk Analyzer team, building software that automatically scans applications for vulnerabilities. He was the author of LC4, a version of the award-winning LOphtCrack password auditing tool. @stake was acquired by Symantec Corporation in October 2004. Rob earned a B.S. in Computer Information Systems from Bentley University.

John Carmichael

John Carmichael, Director of Product Management, creates computer-based training courses at Safelight Security as an integral part of the product team. He has applied his software security expertise to the creation and delivery of security training for some of the world's largest organizations. His experience is rooted in a background of software development with deep expertise in a myriad of languages and environments. He has developed enterprise-class software for large organizations such as Massachusetts Executive Office of Health and Human Services and Computer Science Corporation. Previously, John was a security trainer and consultant at Security Innovation and Cigital. John earned a B.S. degree in Computer Science and Business Administration from the University of Vermont and a M.S. degree in Computer Information System Security from Boston University.

Kevin Poniatowski

Kevin Poniatowski travels the world in his role as a Senior Trainer for Safelight Security, teaching employees at an array of organizations about information security. He has delivered application security presentations to technical and non-technical staff in numerous civic organizations. He has also published an article in the Microsoft Developers Network on the topic of Testing for Cross-Site Request Forgery. Kevin entered the information security field with Security Innovation, where he split time between course development and delivering instructor-led courses. He began his career working for more than a decade as an application developer in the defense industry, where he focused on flight safety for pilots and navigators within the armed forces. Kevin earned a B.A. degree in Economics from the University of Michigan and a B.S. degree in Computer Science from Florida State University.

Paul Hinkle

Paul Hinkle, co-founder and CTO with Safelight Security, works on security research, course design and course development. Paul has partnered with leading clients in the financial industry and in government and has delivered training in information security to more than 6,000 IT professionals. He has 14 years of experience in application development and information security. He brings a passion and talent for communicating his security expertise to employees across all levels of an organization. Prior to Safelight, Paul joined Symantec as part of the @stake acquisition. In the role of principal security instructor, he helped build education offerings in secure application development and management of the secure development lifecycle and infrastructure security. Prior to @stake, Paul developed training skills at Web-Methods, a leading Web services infrastructure company. He also worked as a consultant for Inventa and as a software systems designer for NetResponse, where he gained significant expertise in all phases of the software development lifecycle. Paul earned a B.A. degree in Biology from Johns Hopkins University.

Course Topics: Day One

Unit	Hours	Description
Course Introduction	45 minutes	Student/instructor introductions and course introduction. Highlights real-world attacks on Web applications.
Building Secure Web Applications in Java	30 minutes	Introduces students to the issues surrounding the construction of Web applications such as input/output, authentication/authorization, and session management.
BREAK	15 minutes	
Building Secure Web Applications in Java	60 minutes	Continued.
XML and Web Services	30 minutes	An introduction into XML and Web service security issues.
LUNCH	60 minutes	
Privacy and Secrets	45 minutes	Discuss the need for maintaining confidentiality and how regulations dictate this process. Also includes discussion about outbound passwords and random numbers.
Input Validation and Output Sanitization in Java	45 minutes	Discuss the need for validating input from all sources and performing output sanitization to protect the users of the application. Includes exercises concerning the validation of input and sanitization of output.
BREAK	15 minutes	
Logging and Exception Handling in Java	30 minutes	Discuss the process of logging securely and how proper exception handling creates a more secure Web application.
Introduction to Cryptography	45 minutes	High-level overview of cryptography basics. Covers symmetric and asymmetric key encryption, along with secure hashing.
Data Access Security	45 minutes	Introduces the importance of understanding data access threats and defenses.
Course Wrap-up	15 minutes	Summary and course review.
TOTAL	8 HOURS	

Course Details: Day One

Building Secure Web Applications

Objectives

Introduction

Web Browsers are Completely Open and Insecure

Input and Output Issues

- › Preventing cross-site scripting attacks
- › Preventing HTTP response splitting
- › Control redirects
- › Control email forms

Authentication and Authorization Issues

- › Use standard frameworks
- › Protect all resources and data
- › Declarative vs. programmatic security
- › Don't allow client-side control of critical state data

Session Management

- › Use strong session identifiers
- › Create a new session identifier on login
- › Enforce session timeouts
 - › Inactivity timeout
 - › Hard limit timeout
- › Terminate session upon logout

Web Specific Issues

- › Use POST, not GET
- › Maintain control over request ordering
- › Preventing cross-site request forgery

XML and Web Services

Brief Overview

Parsing and Validating XML

- › Validating parsers and their limitations
- › Don't trust external resources
- › XML injection and output sanitization
- › Encoding considerations
- › XPATH query injection

Authorize and Audit Sensitive Requests

JavaScript Hijacking

JavaScript, JSON and Preventing Direct Execution

Privacy and Secrets

Objectives

Introduction

Privacy and Regulation

- › What is private information?
- › Handling private information

What is Private Information?

Handling Private Information

Code Privacy, Enforce a Clean Production Environment

- › Remove sample code
- › Delete backups
- › Delete debug code
- › Eliminate backdoors
- › Prohibit Easter eggs

Outbound Passwords

- › Use keys when possible
- › Keep passwords out of source code
- › Don't store clear text passwords
- › Limit access

Random Numbers

Cryptography

- › Data in motion, use standard protocols
- › Data at rest, use proven tools
- › Don't roll your own

Course Details: Day One

Input Validation and Output Sanitization in Java

Brief Overview

Input Validation

- › Review of input validation process
- › Java regular expressions
- › Regular expression exercise
 - › Date
 - › Credit card number
 - › Email address

Output Sanitization

- › Information disclosure vulnerability
- › Real world examples of information disclosure
- › Information disclosure exercise
- › HTML encoding in Java

Logging and Exception Handling in Java

Logging

- › Why logging has to be secure
- › Use a single logging API
- › Log exceptions
- › Keep informational and warning messages configurable
- › Log important actions
- › The importance of timestamps
- › Protect your logs
 - › Log forgery and other output sanitization problems
 - › Authorization issues: reading and writing logs

Exception Handling

- › Checking return codes
- › Exception handling best practices
- › Checked vs. unchecked exceptions
- › Catch everything at the top level
- › Preventing resource leaks

Introduction to Cryptography

Cryptography Basics

- › Symmetric encryption
- › Asymmetric encryption
- › Secure Hashes
- › Random number generation

Cryptography Risks Overview

Cryptography primitives in Java

- › Java cryptographic architecture
- › Java cryptographic extensions

Data Access Security

Data Access Security Basics

Understanding Data Access Threats

- › An overview
- › Example: FTP
- › Example: database authorization

Data Access Defenses

- › An overview
- › Principle of least privilege

Database Query Methods

- › An overview
- › SQL callable statements and stored procedures
- › SQL prepared statements
- › Converting dynamic SQL to prepared statements

Course Topics: Day Two

Unit	Hours	Description
Day One Review	15 minutes	Review of the material learned in day one.
Security Testing Approaches	60 minutes	Discusses various ways to test applications for security issues. Includes a discussion of architecture reviews, code reviews and penetration testing.
Architecture Review Lab	30 minutes	Students examine several common architectures for security flaws.
BREAK	15 minutes	
Penetration Test Lab	90 minutes	Students find flaws in a live Java application.
LUNCH	60 minutes	
Java Secure Code Review	30 minutes	Students will review Java code looking for security vulnerabilities.
SQL Injection Lab	45 minutes	Students will test for SQL injection vulnerabilities, find the bug in the code, and fix the code.
BREAK	15 minutes	
Cross-Site Scripting (XSS) Lab	45 minutes	Students will test for XSS vulnerabilities, find the bug in the code, and fix the code.
Cross-Site Request Forgery (CSRF) Lab	60 minutes	Students learn to find and address a common issue called cross-site request forgery in live code.
Course Wrap-up	15 minutes	Summary and course review.
TOTAL	8 HOURS	

Course Details: Day Two

Security Testing Approaches

Architecture Review

Code Review

Penetration Testing

Architecture Review Lab

Find Issues in Three Different Architectures

- › Web
- › Client/Server
- › Mainframe

Discuss Issues as a Group

Penetration Test Lab

Information Leakage

Identify Authentication Issues

Identify & Attack Password Reset Mechanism

Bypass Client-Side Controls

SQL Injection

Cross-Site Scripting

Parameter Tampering

Java Secure Code Review Lab

Identify Common Coding Issues

- › SQL injection
- › Cross-site scripting
- › Information leakage
- › Poor error handling
- › Poor auditing & logging
- › Client-side security controls

Discuss issues as a group

SQL Injection Lab

Find SQL Injection Vulnerability in Application

Find and Fix SQL Injection Vulnerability in the Java Code

Test SQL Injection Vulnerability to Show Fix Worked

Review Solution As Group

Cross-Site Scripting (XSS) Lab

Find XSS Vulnerability in Application

Find and Fix XSS Vulnerability in the Java Code

Test XSS Vulnerability to Show Fix Worked

Review Solution As Group

Cross-Site Request Forgery (CSRF) Lab

Test for CSRF Vulnerability in Application

Find and Fix CSRF Vulnerability in the Java Code

Test CSRF Vulnerability to Show Fix Worked

Review Solution As Group

Courses-at-a-Glance















GS

General Staff

- Information Security Awareness 
- Information Privacy Awareness 
- Security Awareness for Management 
- Compliance  

DS

Development Staff

- Introduction to the Secure Software Development Lifecycle (S-SDLC) 
- Application Security Fundamentals  
- Secure Java Coding  
- Secure .NET Coding  
- Secure Web Coding  
- Secure C/C++ Coding  
- Architecting Secure Systems 
- QA Testing for Secure Applications 
- Language-Neutral Secure Coding 

IT

IT Operations Staff




- Security 101 for Systems Administrators 
- Database Security Fundamentals 
- Infrastructure Security Fundamentals  

The Safelight Difference

We bring an uncommon set of perspectives to our work as security educators—we understand how developers build technology, how organizations use it and how attackers break it.

- The depth and breadth of our security knowledge and experience is unmatched among training companies. Security is not one-size-fits-all and we are uniquely positioned to understand what security means for your organization.
- We are solely focused on education. Unlike security consulting firms that add a day or two of training to their engagements, we are fully dedicated to developing and delivering educational content—whether instructor-led or on-demand.
- We speak the language—a few in fact! Development, IT, security, lines of business—they all speak a different language and come to security with different perspectives, biases and (sometimes) misconceptions. We are fluent in the language—and the culture—of each of these groups, making us ideal translators in organization-wide conversations about security.
- We are adaptive, flexible and client-focused. Our modular curriculum offers flexibility and we know how to get education programs up and running quickly.




COURSES

-  On-Demand Course
-  Instructor-Led Course
-  Coming Soon

GS

General Staff

COURSES

-  On-Demand Course
-  Instructor-Led Course
-  Coming Soon

Security is every employee's responsibility. There is not a person in your organization who could not do something—however unwittingly—to expose sensitive information. General staff across marketing, human resources, sales, operations, legal, finance and customer service handle personally identifiable information, payment information, protected health information, intellectual property, confidential company plans and financials. Many of these people carry this sensitive information into the world outside the office on laptops, mobile phones, USB drives and paper—just in the course of doing their work every day.

Security rests in all of these employees' hands in different ways. A misstep by any of one of them could create an opportunity for a motivated attacker. A shift in the way employees think about and protect sensitive information can be a company's best protection. Safelight's on-demand and instructor-led courses for general staff are designed to reduce your organization's information risk by increasing security awareness among your business staff.

Information Security Awareness

This introductory course is designed for all general staff in roles such as human resources, legal, marketing, finance, sales, operations and customer service. This course equips employees to recognize the value of different types of information, to understand the scope, nature and origin of the diverse risks to such information, and to behave proactively to protect this information in their everyday work. Topics include computer crime, social engineering, physical security, technology threats, and information security self-defense.



Information Privacy Awareness

This introductory course is designed for general staff in roles such as human resources, legal, finance, marketing, sales, operations and customer service who handle personally identifiable information (PII), regulated financial information, protected health

information (PHI) and organizational intellectual property as part of their jobs. This course equips employees to recognize different types of private information, to identify the diverse risks to such information, to understand their organizational, regulatory and legal responsibilities in handling private information, and to take the necessary steps to protect it. This course is specifically designed to help companies comply with State Privacy Laws such as MA 201 CMR 17. The course may be customized to meet the specific compliance requirements of the laws and industry regulations under which your organization operates. Topics include identifying personal information, the electronic transmission and storage of personal data, physical data handling, maintaining data security, overseeing service providers and identifying other types of sensitive data.



Security Awareness for Management

This course is designed for executives and senior management across your organization. This brief, focused workshop equips your organization's leadership team to identify the information risk inherent in your operations and to evaluate strategies for mitigating this risk across the organization. Topics include security myths and misconceptions that disable your organization, real-world threats, the impact of security and regulatory compliance, high-level security principles and strategies, and current information security best practices.



Compliance




This course is being designed. Please contact us for more information.



DS

Development Staff

COURSES

-  On-Demand Course
-  Instructor-Led Course
-  Coming Soon

Introduction to the Secure Software Development Lifecycle (S-SDLC)

The most successful security education programs are role-specific and customized for each organization's internal policies and development methodologies. Safelight starts Introduction to S-SDLC by interviewing internal security team and development staff to understand development team policies, controls, and methodologies. One to two weeks of customization will result in customized role-specific courses designed for application developers, project managers, architects, quality assurance testers, and systems and database administrators. This course equips the entire development team to reduce information risk by deeply integrating security into the development life cycle. Topics include internal policies and controls, application security fundamentals, secure coding, architecting secure systems, and testing for security.



By identifying and resolving vulnerabilities early in the software development lifecycle, your team can substantially—and cost-effectively—reduce information risk. Only recently have companies begun to meaningfully integrate security into the software development lifecycle. Secure coding has been greatly advanced by the adoption of formal software security assurance methodologies. Essential to the successful implementation of these methodologies is role-specific training for all development staff—whether they are architects, developers, QA testers or managers.

Our courses for development teams begin with an overview of fundamental secure coding principles. Students learn the many ways in which vulnerabilities in software code may be exploited by attackers and are shown the value of secure development. Building on this understanding of the risks inherent in software development, students learn solid architecture, design, testing and implementation principles. From there, they explore ways to root out security issues within existing systems and how to effectively respond to evolving security threats.

Application Security Fundamentals

This foundational course is designed for all staff who participate in application development projects—developers, architects, testers and project managers. This introduction to application security equips students with a common vocabulary, an understanding of common attacks against software and a set of tools and techniques for building more secure applications. Topics include the OWASP Top Ten, key security principles, setting information security goals and controls, validating and sanitizing input and output, and managing risk and security in the SDLC.



Secure Java Coding

This role-specific intermediate course is designed for experienced Java developers and architects who work with Java development teams. This focused course equips students with a clear understanding of the built-in

security features of Java as well as best practices for coding securely. Topics include Web applications, input validation and output sanitization, logging and exception handling, data access security basics, and privacy and secrets. Students should have an understanding of information security basics before taking this course; our Application Security Fundamentals course is the ideal prerequisite.



Secure .NET Coding

This role-specific intermediate course is designed for experienced developers and architects working in a .NET environment. This focused course equips students with a clear understanding of the built-in security features of .NET as well as best practices for coding securely. Topics will include: authentication; authorization; auditing and logging; exception handling; input validation; an introduction to cryptography;

and application testing approaches. Students should have an understanding of information security basics before taking this course; our Application Security Fundamentals course is the ideal prerequisite.



Secure Web Coding

This role-specific intermediate course is designed for developers, architects and technical QA staff who code Web-facing applications. This focused course equips students with a clear understanding of common attacks against Web-facing applications and best practices for coding securely. Topics include building secure Web applications, XML and Web services, input/output validation, top Web vulnerabilities, application security tools, and privacy and secrets. Students should have an understanding of information security basics before taking this course; our Application Security Fundamentals course is the ideal prerequisite.



Secure C/C++/C# Coding

This role-specific intermediate course is designed for developers, architects and database administrators working on development efforts coded in C/C++/C#. This focused course equips development teams with a deeper understanding of application security, a clear understanding of the most common attacks against software coded in C/C++/C#, and best practices for coding securely. Topics include memory corruption bugs, design bugs, privacy and secrets, secure coding, static analysis and fuzzing. The instructor-led format of this course also offers students

a series of hands-on labs focused on architecture review, penetration tests, secure code review, client tampering, network sniffing and server-side attack defense. Students should have an understanding of information security basics before taking this course; our Application Security Fundamentals course is the ideal prerequisite.



Architecting Secure Systems

This course is designed for experienced developers and architects. This two-day course equips students with a comprehensive understanding of secure system design. This course uses the students' own architectures as examples, so results are directly applicable right after class. The course includes a live architecture review of actual architectures to demonstrate how to conduct a full-fledged architecture review. Topics will include: methods of attack; security goals and controls; security principles; network security; host security; application security; an introduction to cryptography; identifying and managing risk; security policies and security assessments.



QA Testing for Secure Applications

This introductory course is designed for quality assurance professionals who need to understand how to test their systems for security. The course offers students a comprehensive introduction to common application vulnerabilities and their exploitation and equips them to test for these vulnerabilities before applications go into production. Through lab-based learning, students identify vulnerabilities in a sample application and learn

to take these lessons back to their own applications. Topics will include: the attacker mindset; security testing tools and techniques; the basics of netcap and nmap; mapping the application; error handling and information leakage; common authentication flaws; authorizations flaws; exploitation of logic errors; advanced SQL injection attacks; cross-site scripting attacks; cross-site request forgery; Web services forgery; buffer overflows; and rootkit technology.



Language-neutral Secure Coding




This role-specific intermediate course is designed for experienced developers, architects and QA professionals working on application development teams that code in mixed technologies. This course uses language-neutral examples to equip students with an intermediate-level understanding of common application vulnerabilities and best practices for coding securely. Many concepts are illustrated through secure Web and Java coding examples. Topics include handling input and output, an introduction to cryptography, planning for secure deployment and operations, security testing, architecture review, and penetration testing techniques. Students should have an understanding of information security basics before taking this course; our Application Security Fundamentals course is the ideal prerequisite.



IT

IT Operations Staff

COURSES

-  On-Demand Course
-  Instructor-Led Course
-  Coming Soon

Employees who are on the front lines of deploying, managing and securing information technology must be well-equipped to protect sensitive information. We provide role-specific, on-demand and instructor-led security training programs to help your entire information technology team—from system architects to database administrators—deploy, maintain and protect the enterprise infrastructure.

Security 101 for Systems Administrators

This introductory course is designed for network administrators, systems administrators, data center teams and other IT staff. This course equips students to better understand and protect network, data center and systems operations. Topics will include: operating systems access control; network access control; application access controls; user access management; monitoring system access and use; operational procedures and responsibilities; and audit controls and tools.



Database Security Fundamentals

This role-specific course is designed for DBAs, IT staff and technical QA staff who build and/or test SQL databases. The course equips these staff with a clear understanding of best practices for deploying secure systems using databases. Topics will include: database hardening; audit controls; client-to-database and database-to-database authentication & access controls; implementing and enforcing the principle of least privilege; proper use of Web services when accessing databases; and common database attacks (including advanced SQL injection). Also covered is a detailed introduction to the benefits and pitfalls of database encryption.



Infrastructure Security Fundamentals

This course is being designed. Please contact us for more information.



About Safelight

Safelight is a leader in security education—our integration of deep security expertise and innovative approaches to interactive learning sets us apart. We help organizations build comprehensive education programs that go beyond training to measurably shift the way employees think about the value of information and their role in protecting it. We offer a full range of instructor-led and on-demand courses for development, IT and general staff; each role-specific course is part of a larger program designed to cultivate a culture of security across the organization.



220 West Exchange Street, Providence, RI 02903 P 800.616.4969 F 401.632.4001

www.safelightsecurity.com