



# 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

Developers and architects creating Web applications in Java.

### Prerequisites

Students should have an understanding of information security basics before taking this course; our Application Security Fundamentals course is the ideal prerequisite. This intermediate course requires knowledge of the Java language and familiarity with creating applications in Java.

### Length

Approximately 2 hours out-of-the-box.

### Delivery

This SCORM 1.2-compliant course can be integrated into a client's Learning Management System or it can be delivered as an on-demand service through Safelight's education portal.

### Modification

Clients can modify any course by removing standard content, modifying the sequence of course modules, changing the standard look and feel of the course template to reflect client design standards and/or replacing general security terms with client-specific terms.

### Customization

Clients can work with Safelight to customize any course by adding custom content, customizing existing content and/or creating new content to meet client-specific communication objectives and education goals.

# Course Overview

This intermediate course is designed for developers and architects creating Web applications in Java.

This highly interactive scenario-based course equips Java developers with deeper knowledge of Web application security, so that they can identify and mitigate common vulnerabilities, understand how these flaws are exploited and use coding best practices to proactively reduce application risk. Topics will include: security for Web applications; input validation and output sanitization; logging and exception handling; data access security basics; and privacy and secrets.

## Technical Specifications

### Courses

All of Safelight's courses are SCORM 1.2-complaint. Courses can be integrated into a client's Learning Management System or delivered as an on-demand service through Safelight's education portal.

## Minimum Requirements

### Computer that is less than 5 years old

- Screen resolution: 1280x 720
- Standard operating system:  
Mac OSX 10.x or above or  
Windows XP or above

### Web Browser

- Windows: Internet Explorer 6.0 SP3 and above
- Windows: Mozilla Firefox 3.0 and above
- Mac: Safari 4.0 and above

### Flash Player

- Adobe Flash Player: preferably version 10 or higher. Courses work with version 8 and 9, but not version 7

### Audio (highly recommended)

- If sound is unavailable, user can follow on-screen transcript

# Course Outline

## 1. Security for Web Applications

- 1.1 Web Browsers are Completely Open and Insecure
- 1.2 Input and Output Issues
- 1.3 Authentication and Authorization Issues
- 1.4 Session Management
- 1.5 Web-Specific Issues

## 2. Input Validation and Output Sanitization

- 2.1 Input Validation
- 2.2 Output Sanitization

## 3. Logging and Exception Handling

- 3.1 Logging
- 3.2 Exception Handling

## 4. Data Access Security Basics

- 4.1 Data Access Threats
- 4.2 Data Access Defenses
- 4.3 Data Access Methods
- 4.4 Data Access Logging

## 5. Privacy and Secrets

- 5.1 Privacy Overview
- 5.2 Privacy and Regulation
- 5.3 Code Privacy
- 5.4 Outbound Passwords
- 5.5 Random Numbers
- 5.6 Cryptography

# Security for Web Applications

# 1

## Overview

The unit begins by introducing students to the vulnerability of Web applications. The next two sections offer a deeper exploration of specific vulnerabilities, primarily input and output issues and authentication and authorization issues. In each instance, students are taught how to mitigate these common issues. In the next section students are given an overview of session management pitfalls and best practices. The unit concludes with an in-depth look at real-world scenarios and equips students to mitigate threats associated with data tampering, cross-site scripting, cross-site request forgery and HTTP response splitting.

## Learning Objectives

### 1.1

#### Web Browsers are Completely Open and Insecure

By the end of the scenario the student will be able to:

- Understand why Web applications are particularly vulnerable to certain security issues
- Recognize what common application vulnerabilities may look like in Web applications

### 1.2

#### Input and Output Issues

By the end of the scenario the student will be able to:

- Explain the impact of input and output issues such as cross-site scripting
- Express the importance of proper input validation and output sanitization

### 1.3

#### Authentication and Authorization Issues

By the end of the scenario the student will be able to:

- Understand the importance of authentication and authorization
- Distinguish between declarative and programmatic security

### 1.4

#### Session Management

By the end of the scenario the student will be able to:

- Explain the impact of the stateless nature of HTTP on Web applications
- Understand the qualities that make up a strong session management module

### 1.5

#### Web-Specific Issues

By the end of the scenario the student will be able to:

- Explain the mechanics of HTTP requests
- Discuss how to mitigate threats associated with data tampering, cross-site scripting, cross-site request forgery and HTTP response splitting

# Input Validation and Output Sanitization

# 2

## Overview

This unit begins by introducing students to the concepts of input validation and output sanitization. The next section takes an in-depth look at input, specifically identifying common approaches to validating input. The unit concludes by teaching students about output sanitization, illustrating the consequences of improperly sanitizing application output.

## Learning Objectives

### 2.1

#### Input Validation

By the end of the scenario the student will be able to:

- Identify common approaches to validating input
- List the data characteristics that need to be validated

### 2.2

#### Output Sanitization

By the end of the scenario the student will be able to:

- Appreciate the consequences of improperly sanitizing application output
- Describe the Java resources that help with output sanitization

# Logging and Exception Handling

## Overview

This unit focuses on logging and exception handling. The first section introduces the student to logging basics: it discusses what and when to log and provides a side-by-side look at two different logging frameworks, helping students understand when to use each. The next section explores exception handling, equipping students to recognize exception handling in Java and preparing them to handle exceptional situations they may encounter in their code.

## Learning Objectives

### 3.1

#### Logging

By the end of the scenario the student will be able to:

- Discuss logging basics including what and what not to log and when to log
- Compare two different logging frameworks, log4j and JDK logging, and describe how to implement logging using these frameworks in their applications

### 3.2

#### Exception Handling

By the end of the scenario the student will be able to:

- Recognize exception handling in Java
- Explore general considerations, uncaught exception handling, and other topics related to properly handling exceptional situations in their code

# Data Access Security Basics

# 4

## Overview

This unit teaches students the basics of data access security. The first section gives the student an overview of data access threats. The next section explores common defenses used to ward off data access threats. Next, the student is introduced to various data access methods and the levels of risk associated with their use. The unit concludes with a look at data access logging and proper log management.

## Learning Objectives

### 4.1

#### Data Access Threats

By the end of the scenario the student will be able to:

- Express the implication of common data access threats
- Describe examples of data access threats in real-world systems

### 4.2

#### Data Access Defenses

By the end of the scenario the student will be able to:

- Explain confidentiality, integrity and availability of data
- Discuss the principle of least privilege

### 4.3

#### Data Access Methods

By the end of the scenario the student will be able to:

- Recognize the level of risk associated with various data access methods
- List the steps necessary to convert from dynamic SQL to callable statements

### 4.4

#### Data Access Logging

By the end of the scenario the student will be able to:

- List the types of configurable logging solutions
- Appreciate the need for proper log management

## Overview

This unit places secure Java coding in context through a discussion of recent real-world data breaches that illustrate the impact of failing to create a clean production environment. The first section offers an overview of privacy concerns in software development and is followed by a section on the various laws and regulations that govern private data handling. The next section discusses the security implications surrounding outbound passwords. The unit concludes with sections on proper use of random numbers and cryptography to protect private data in Java code.

## Learning Objectives

### 5.1

#### Privacy Overview

By the end of the scenario the student will be able to:

- Understand how recent data breaches may impact development efforts
- Explain some of the potential consequences of failing to create a clean production environment

### 5.2

#### Privacy and Regulation

By the end of the scenario the student will be able to:

- List the major laws and regulations that govern how information is handled
- Discuss how these laws and regulations impact software development

### 5.3

#### Code Privacy

By the end of the scenario the student will be able to:

- Express the need to keep source code private
- List several activities that can help bolster the overall security of a solution

### 5.4

#### Outbound Passwords

By the end of the scenario the student will be able to:

- Discuss the risk posed to systems by improper handling of outbound passwords
- Recognize how to securely handle outbound password storage

### 5.5

#### Random Numbers

By the end of the scenario the student will be able to:

- Express why using the right type of random number generator is important and describe how to use it
- Recognize good random number use in Java source code

### 5.6

#### Cryptography

By the end of the scenario the student will be able to:

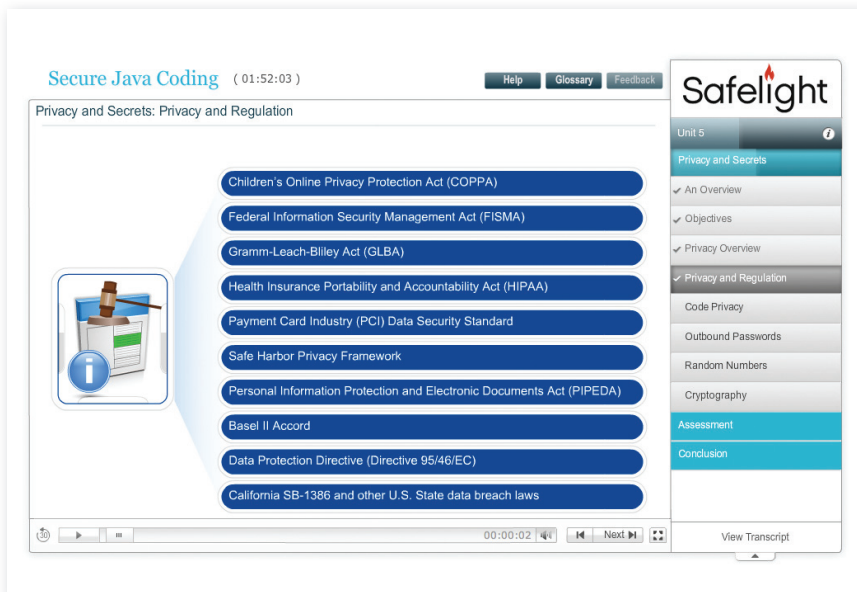
- Recognize why using pre-built cryptographic protocols and tools is important
- Understand why they should never build their own cryptography

# Interface & Interactivity



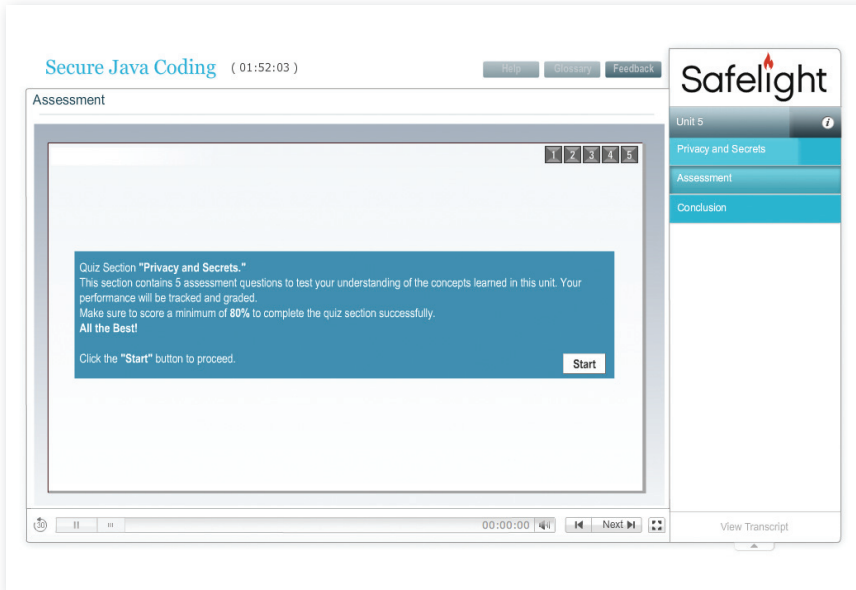
## Easy to Navigate Interface

All Safelight courses offer interfaces that are easy to navigate. Users are guided through the course content in a logical flow. From any screen, users can pause and fast forward the content, request to view a transcript, and navigate to a specific topic via the Menu option.



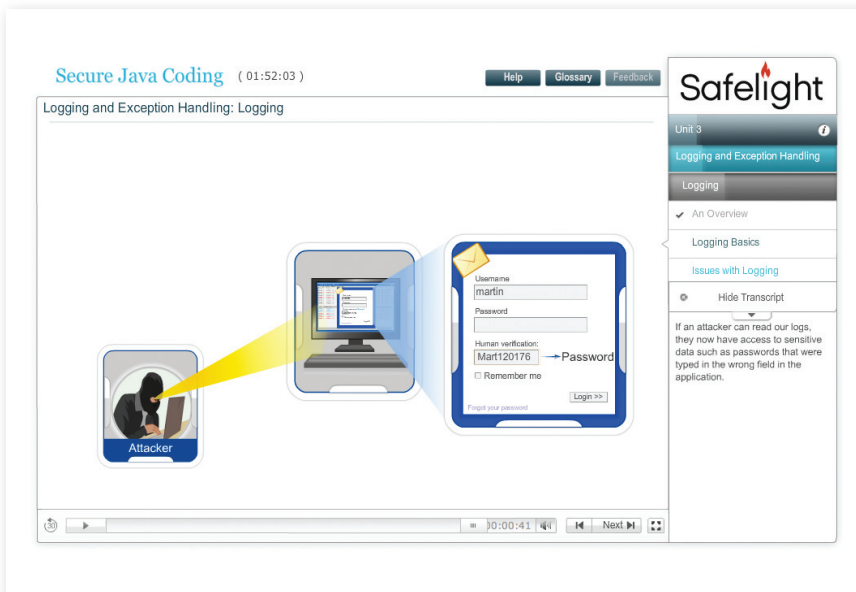
## Interactive Learning

The course has been designed with user interactions that keep students engaged and reinforce their learning; students are often asked to click on the screen to answer questions or make a selection.



## Integrated Assessment Quizzes

The course offers integrated assessments for each module. Each client can specify a pass/fail threshold for their students. All results from the assessments are written back to the host Learning Management System so that student participation can be tracked and audited.



## Auto-Scrolling Transcript

The course comes with an integrated transcript that auto-scrolls with the course audio. This feature can be expanded or collapsed depending on the student's preference. Transcript translation is helpful for students who speak English as a second language and is available as a course customization.

# Engaging Topics

The screenshot shows a video player interface for a course titled "Secure Java Coding". The video is at the 01:52:03 mark. The main content area displays a code snippet titled "Create a New Session Identifier on Login". The code is as follows:

```
public void doLogin(HttpServletRequest request) {  
    HttpSession oldSession = request.getSession(false);  
    if (oldSession != null) {  
        oldSession.invalidate();  
        // Create a new session if there was an old session  
        HttpSession newSession = request.getSession(true);  
        // transfer attributes from old to new  
        Enumeration enum = oldSession.getAttributeNames();  
        while (enum.hasMoreElements()) {  
            String name = (String) enum.nextElement();  
            Object value = oldSession.getAttribute(name);  
            newSession.setAttribute(name, value);  
        }  
    }  
    authenticate(request); // check user credentials  
}
```

The video player includes a progress bar at 00:00:02, navigation controls, and a "View Transcript" button. A sidebar on the right shows the course navigation menu with "Session Management" selected.

## Proper Session Management

This course presents patterns and techniques for correctly managing user sessions, the foundation for all authentication and authorization within Web applications.

The screenshot shows a video player interface for a course titled "Secure Java Coding". The video is at the 01:52:03 mark. The main content area displays a code snippet titled "Logging and Exception Handling: Exception Handling". The code is as follows:

```
try  
{  
    // do something  
}  
catch (SomeException e)  
{  
    // handle the exception  
}  
finally  
{  
    // clean up  
}
```

The video player includes a progress bar at 00:00:02, navigation controls, and a "View Transcript" button. A sidebar on the right shows the course navigation menu with "Exception Handling" selected.

## Proper Exception Handling

This course offers an in-depth look at proper exception handling, an area in which developers commonly make mistakes that introduce security vulnerabilities into applications.

Secure Java Coding (01:52:03) Help Glossary Feedback

## Data Access Security Basics: Data Access Defenses

Least Privilege

Stand Alone Security

Segmentation

00:00:42 Next View Transcript

**Safelight**

Unit 4

- Data Access Security Basics
  - An Overview
  - Objectives
  - Introduction
  - Data Access Threats
  - Data Access Defenses
    - An Overview
    - Principle of Least Privilege
    - Data Access Methods
    - Data Access Logging
  - Assessment
  - Conclusion

## Data Access Defenses

This course presents defenses that can be deployed for more secure data access, a critical element in an overall data protection scheme.

Secure Java Coding (01:52:03) Help Glossary Feedback

## Privacy and Secrets: Random Numbers

```

private static char[] characters = {
    'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j',
    'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't',
    'u', 'v', 'w', 'x', 'y', 'z', 'A', 'B', 'C', 'D',
    'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N',
    'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X',
    'Y', 'Z', '0', '1', '2', '3', '4', '5', '6', '7',
    '8', '9'
};

/** Creates a new instance of GenPassword*/
public String genPassword(int length)
{
    Random random = new Random(System.currentTimeMillis());
    StringBuilder sb = new StringBuilder(length);

    int r;
    for (int i=0; i<length; i++)
    {
        r = random.nextInt(62);
        sb.append(characters[r]);
    }
    return sb.toString();
}

```

00:01:21 Next View Transcript

**Safelight**

Unit 5

- Privacy and Secrets
  - An Overview
  - Objectives
  - Privacy Overview
    - Privacy and Regulation
    - Code Privacy
    - Outbound Passwords
    - Random Numbers
    - Cryptography
  - Assessment
  - Conclusion

## Proper Use of Random Numbers

This course presents proper use of random numbers in Java applications; these numbers are critical to many security mechanisms including session identifiers and cryptographic keys.

# Courses-at-a-Glance















GS

## General Staff

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

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.



# 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 10, 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](http://www.safelightsecurity.com)