



APPLICATION SECURITY FUNDAMENTALS

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 introductory course is designed for all team members associated with application development efforts. Roles include developers, architects, business analysts, project managers, quality assurance professionals, system administrators and database administrators.

Prerequisites

No background in information security is necessary.

Length

1 day

Delivery

Instructor-led and on-demand options are available.

Course Overview

This foundational course is designed for all staff who participate in application development projects—developers, architects, testers, business analysts 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 will 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.

Learning Objectives

After completing this course, students will be able to:

- Discuss real-world security incidents that have recently occurred and explain the various motivations behind them.
- Explain the attacker mindset and why it is critical to think like an attacker in order to build secure systems.
- Discuss the four main drivers behind security, including business drivers, regulatory requirements, technology and threats.
- Understand common security misconceptions and explain why they are not true. For many people, this is the most valuable section of the course.
- Understand the security issues that are most likely to cause problems in their own applications, and explain how to fix them. Addresses all the issues from the OWASP Top 10 including SQL injection, cross-site scripting and cross-site request forgery.
- Explain the three primary drivers behind security—confidentiality, integrity and availability—and discuss how these apply to their own systems.
- Understand the three primary security controls—authentication, authorization and auditing—and discuss how they apply to their own systems.
- Understand the 12 security principles that, if applied correctly, can significantly improve the security of any application, and discuss ways that these principles can be implemented in their own systems.
- Discuss a variety of ways in which security can be applied throughout the software development lifecycle (SDLC).
- Explain why security applies no matter what lifecycle methodology is in place (Waterfall, Agile, etc).

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

Unit	Hours	Description
Course Introduction	45 minutes	Student/instructor introductions and course introduction. Highlights real-world incidents, the attacker mindset, and security misconceptions.
OWASP Top 10 Security Issues	60 minutes	Introduction to the security issues that are most likely to cause problems in students' environments. Includes live instructor demonstrations of key issues.
BREAK	15 minutes	
OWASP Top 10 Security Issues	60 minutes	Continued.
LUNCH	60 minutes	
Security Goals and Controls	60 minutes	Discussion of confidentiality, integrity, and availability along with authentication, authorization, and auditing and logging.
Security Principles	75 minutes	Teaching development teams how to think about security. Builds a strong foundation for developing secure applications.
BREAK	15 minutes	
Handling Input and Output Securely	45 minutes	Discussion of two of the most critical security issues and how to deal with them.
Security in the SDLC	30 minutes	Discussion of ways to incorporate security into every phase of the development lifecycle.
Course Wrap-up	15 minutes	Summary and course review.
TOTAL	8 HOURS	

Course Details

Introduction

What You Are Up Against

- › Real-world Incidents
- › What's at stake?
- › The attacker mindset
- › Changing attack vectors

Clearing Up Security Misconceptions

- › Firewalls do not guarantee security
- › SSL does not make you secure
- › Client-side security does not exist
- › Unvalidated input and unsanitized output
- › Beware of integration points
- › Internal is not safer than external
- › Quality assurance is not security testing
- › The application is not the network
- › Security functionality does not imply quality
- › Tools are not solutions
- › Patches do not guarantee security
- › All software has bugs, even yours
- › Don't reinvent the wheel

OWASP Top 10 Security Issues

Injection Flaws (Demo)

Cross-site Scripting (Demo)

Security Misconfiguration

Broken Authentication and Session Management

Insecure Direct Object Reference

Failure to Restrict URL Access

Cross-site Request Forgery (Demo)

Insufficient Transport Layer Protection

Insecure Cryptographic Storage

Unvalidated Redirects and Forwards

Security Goals and Controls

Confidentiality

Integrity

Availability

Authentication

Authorization

Auditing and Logging

Security Principles

Security is a Process

Keep Security Simple

Question All Assumptions

Layered Security

Structural Security

Segmentation

Stand-alone Security

Principle of Least Privilege

Validate Input

Sanitize Output

Fail Closed

Test Everything!

Handling Input and Output

Why Validate Input

When to Validate Input

How to Validate Input

Why Sanitize Output

When to Sanitize Output

How to Sanitize Output

Security in the SDLC

Identifying Risk

Application Feasibility

Requirements

Design

Development

Testing

Deployment


Operations

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

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.



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.

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