



Application Security for Managers

Application Security Training Datasheet

1 Day
Training

Managers,
Leaders,
CTO/CIOs

Instructor led

Application Security for Managers

COURSE OVERVIEW

Developers and security analysts are increasingly becoming involved in application security initiatives. Managers need to understand both the technical nature of their teams' involvement with security initiatives as well as the business case for performing activities.

This class arms managers with the knowledge necessary to make effective, risk-based decisions about application projects that balance business needs with security requirements. Security Compass brings extensive enterprise security assessment and prioritization experience to its highly successful training platform in this class

LEARNING OBJECTIVES

- Articulate the Return on Investment and make perform tradeoff analysis on various application security review findings by risk)
- Understand attacks that hackers use to break into applications
- Understand common activities used by organizations to secure their applications

COURSE DETAILS

Audience

Information security managers,
software development managers,
project managers

Instructor Led Delivery

1 Day on-site training

Prerequisite knowledge

Basic technical background, such as prior programming or network infrastructure experience

Prior information security experience useful but not mandatory

Outline, at a glance

Introduction

- Application security vs. traditional security

1. Authentication

- Factors of Authentication
- User Enumeration
- Password Reset
- Brute Force
- Password Sniffing

2. Session Management

- Session hijacking
- Content caching

3. Data Validation

- Input validation overview
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- SQL injection
- Data encoding issues
- Parameter manipulation
- XML attacks

4. Secure Software Development

- Secure SDLC
- Security requirements
- Application security standards and guidelines
- Secure design & architecture
- Threat modeling
- Secure development
- Source code review, manual vs. static analysis
- Secure testing
- Secure quality assurance
- Secure deployment
- Web application firewalls
- Enterprise activities
- Training and awareness
- Remediation tracking

5. Building a Business Case

- Costs of application security activities
- Prioritizing multiple applications

Introduction

About

Managers will learn about how application security is different from traditional security in the technology space. Students will learn about the importance of application security how it must be treated differently.

Topics & Learning Objectives

1

Application Security vs. Traditional Security

Students will be able to:

- Express the difference between traditional security and application security
- Describe why application security is important and how developers are key to securing applications

Authentication

About

Managers will discover how attackers can use weak authentication to take advantage of client facing web applications. Students will learn about the common attacks taken against login screens and how to defend against such attacks.

Topics & Learning Objectives

1.1

Factors of Authentication

Students will be able to:

- Express the three factors of knowledge, possession and physical authentication
- Understand the benefits and weaknesses to each mechanism

1.2

Authentication Weaknesses

Students will be able to:

- Describe what kinds of weaknesses plague authentication mechanisms
- Recognize authentication weaknesses and describe how they can be exploited. Explain the most effective means to defend against such attacks for:
 - user enumeration,
 - password reset attacks
 - brute forcing
 - password sniffing attacks

Session Management

About

Managers will be able to understand how attackers take advantage of bad session management to exploit privileges within web applications. Students should be able to describe the ways in which a session may be hijacked.

Topics & Learning Objectives

2.1

Hijacking Sessions

Students will be able to:

- See how attackers exploit session management weaknesses and the results of these attacks

2.2

Content Caching

Students will be able to:

- Explain how cached content can be exploited by attackers to take advantage of sessions

Data Validation

About

Collection and use of data is one of the most important aspects to web applications. This makes it a high target for attack. Managers will learn the most common data validation issues when it comes to modern web applications and learn best practices to defending against these coding defects.

Topics & Learning Objectives

3.1

Methods of Validation

Students will be able to:

- Explain blacklist and whitelist validation techniques

3.2

Cross-site Scripting (XSS) and Defense

Students will be able to:

- Explain what XSS is and how it affects your applications
- Understand output encoding techniques to defend against XSS

3.3

Cross-site Request Forgery and Defense

Students will be able to:

- Describe how CSRF is, and how it can be used in combination with XSS by attackers to gain information from your applications

3.4

SQL Injection and Defense

Students will be able to:

- Understand how SQL injection happens and why
- Describe concepts that developers should be aware of to prevent SQLi

3.5

Parameter Manipulation

Students will be able to:

- Identify parameter manipulation issues in URL and form fields
- Understand how to defensively program against these vulnerabilities

3.6

XML Attacks

Students will be able to:

- Describe how attackers can use web services against your organization

Secure Software Development

About

Managers will learn about the importance to a secure development lifecycle. Students will learn about creating application security guidelines, threat modeling, developing secure code and reviewing code. We will also discuss the importance of testing code, training, and how to track remediation issues.

Topics & Learning Objectives

4.1

Security Requirements

Students will be able to:

- Describe how application security standards and guidelines can help reduce the number of defects in applications
- Describe secure designs and architecture and fixing issues early in the SDLC
- Express why Threat modeling is an important design stage activity

4.2

Secure Development

Students will be able to:

- Understand the importance to developing secure code and instilling this methodology on your developers
- Differentiate between manual and automated source code analysis and the pros/cons of each

4.3

Secure Testing and Deployment

Students will be able to:

- Describe how software security testing is different from user acceptance testing
- Understand that code must also consider the environment to which it will be deployed, including firewalls and enterprise activities
- Express the importance to tracking of remediation along the SDLC

4.4

Training and Awareness

Students will be able to:

- Understand the importance of developer training in security

Building a Business Case

About

It is important that managers learn how to successfully build a business case for security. This module will help them understand how to accomplish this important task.

Topics & Learning Objectives

5.1

Costs of Application Security Activities

Students will be able to:

- Learn how to determine the cost of application security activities
- Understand how to demonstrate to upper management the need for security and the ways to obtain funding.

5.2

Prioritizing Multiple Applications

Students will be able to:

- Learn about categorizing applications by risk and what information held within an application makes it more higher risk

What can we do for you?

We understand application security. We breathe it. We strive to provide you with the best training experience for your staff.

Our experience helping our clients research and manage real world security risks allows us to drive our training material with the latest threats and vulnerabilities seen in every day engagements.

What does that mean? It means that your staff is ready to respond to with forward thinking concepts to securing your business' most sensitive applications.

Here to help.

Reach out to Security Compass' advisors who can help.

Oliver Ng

Director of Training
oliver@securitycompass.com
1-888-777-2211 ext. 125

Sahba Kazerooni

Director of Professional Services
sahba@securitycompass.com
1-888-777-2211 ext. 103

