Application Security Training Program

Table of Contents

Introduction

Knowledge about application security, threats, and best practices makes the difference between replicating the same problem across multiple sites and building secure applications by design.

WhiteHat Security offers a formal Application Security Training Program targeting all technical stakeholders within the Software Development Lifecycle. Such technical stakeholders include but are not limited to:

DEVELOPERS

Individuals whose primary responsibility is the software design and execution of project specifications.

SOFTWARE ENGINEERS

Individuals whose primary responsibility is defining and influencing high level project architectures and corresponding specifications.

SECURITY MANAGERS

Individuals whose primary responsibility is overseeing and guiding execution of software development processes.

eLearning Paths

eLearning Paths are tracks within the portal allowing you to allocate classes and paths as appropriate for job roles, to track progress, and award completion. Each eLearning track will award a certificate of completion for each individual class as it is completed, as well as an Award of Completion certificate upon for the entire Program. eLearning Paths include:

- Developer eLearning Track – ~7 Hours
- IT Security/Management eLearning Track – ~2 Hours
- Java Developer Track – ~7 Hours
- General Security Awareness Track – ~1 Hour

Classes included in each eLearning Track:

Developer eLearning Track

- OWASP Top Ten for Developers
- Defensive Enterprise Remediation
- Foundational Exam

IT Security / Management eLearning Track

- OWASP Top Ten for Managers
- Integrating Security Throughout the SDLC
- Threat Modeling

Java Developer Track

- OWASP Top 10 for Developers
- Building Secure Java EE Applications

General Security Awareness track

- General Security Awareness

Course Catalog

The Program provides a wide variety of training courses specifically designed to suit the needs of the organization's technical stakeholders. This course catalog is organized in a way that is inline with the roles and responsibilities of applicable technical stakeholders. Furthermore, this catalog should allow for growth overtime to accommodate structural and technical changes within the organization.

DEFENSIVE ENTERPRISE REMEDIATION

DURATION: 1 hour of content, approximately 1.5 hour(s) to complete

AUDIENCE: Software Engineers, Software Architects and Software Testers

OVERVIEW: Participants of this course will gain a foundational understanding of mitigating specific classes of vulnerability with emphasis on the Java and C# programming languages.

OWASP TOP TEN FOR DEVELOPERS

DURATION: 5 hour(s) of content, approximately 8 hour(s) to complete

AUDIENCE: Software Engineers, Software Architects and Software Testers

OVERVIEW: Participants of this course will gain a foundational understanding of application security and secure programming practices based on the threats and vulnerabilities outlined in the Open Web Application Security Project's Top Ten document.

OWASP TOP TEN FOR MANAGERS

DURATION: 1 hour of content, approximately 1.5 hour(s) to complete

AUDIENCE: Software Managers

OVERVIEW: Participants of this course will gain a foundational understanding of Application security based on the threats and vulnerabilities outlined in the Open Web Application Security Project's Top Ten document.

THREAT MODELING

DURATION: 1 hour of content, approximately 1.5 hour(s) to complete

AUDIENCE: Software Architects and Security Engineers

OVERVIEW: Participants of this course will gain an understanding of the threat modeling process and how it is used to identify and prioritize threats.

BUILDING SECURE ASP.NET APPLICATIONS

DURATION: 1 hour of content, approximately 1.5 hour(s) to complete

AUDIENCE: Software Engineers and Software Architects

OVERVIEW: Participants of this course will gain a foundational understanding of writing secure software on ASP.NET based platforms.

BUILDING SECURE MOBILE APPLICATIONS

DURATION: 1 hour of content, approximately 1.5 hour(s) to complete

AUDIENCE: Software Engineers and Software Architects

OVERVIEW: Participants of this course will gain a foundational understanding of of building secure mobile applications with high level coverage of android and iOS platforms.

BUILDING SECURE JAVA EE APPLICATIONS

DURATION: 1 hour of content, approximately 1.5 hour(s) to complete

AUDIENCE: Software Engineers and Software Architects

OVERVIEW: Participants of this course will gain a foundational understanding of writing secure software on Java Enterprise Edition based platforms.

BUILDING SECURE JAVASCRIPT APPLICATIONS

DURATION: 1 hour of content, approximately 1.5 hour(s) to complete

AUDIENCE: Software Engineers and Software Architects

OVERVIEW: Participants of this course will gain a foundational understanding of writing secure software using JavaScript for both the client and the server.

INTEGRATING SECURITY THROUGHOUT THE SDLC

DURATION: 1 hour of content, approximately 1.5 hour(s) to complete

AUDIENCE: Software Engineers, Software Managers, Security Personnel

OVERVIEW: Participants will understand the most important and essential application security activities to conduct through the SDLC to reduce security issues.

GENERAL SECURITY AWARENESS

DURATION: 1 hour of content, approximately 1.5 hour(s) to complete

AUDIENCE: Any Employee

OVERVIEW: Participants of this course will gain a foundational understanding of corporate security from physical access to logical controls and online safety.

FOUNDATIONAL EXAM

DURATION: 1 hour of content, approximately 1.5 hour(s) to complete

AUDIENCE: Software Engineers and Software Architects

OVERVIEW: Participants of this course will gain a foundational understanding of writing secure software using JavaScript for both the client and the server.

About WhiteHat Security

WhiteHat Security has been in the business of securing web applications for 17 years. Combining advanced technology with the expertise of its global Threat Research Center (TRC) team, WhiteHat delivers application security solutions that reduce risk, reduce cost and accelerate the deployment of secure applications and web sites. The company's flagship product, WhiteHat Sentinel, is a software-as-a-service platform providing dynamic application security testing (DAST), static application security testing (SAST), and mobile application security assessments. The company is headquartered in San Jose, Calif., with regional offices across the U.S. and Europe. For more information on WhiteHat Security, please visit www.whitehatsec.com

WhiteHat SECURITY®

WHITEHAT SECURITY, INC. 1741 Technology Dr. #300, San Jose, CA 95110 • 1.408.343.8300 • www.whitehatsec.com