FAR MORE THAN SIMPLY FULFILLING YOUR **SECURITY TRAINING REQUIREMENT**

KMI LEARNING

INFRARED SECURITY

INTRODUCTION

ADVANCED APPLICATION SECURITY TRAINING FOR YOUR **MANAGERS**, **DEVELOPERS** AND **ARCHITECTS**

BUILD A SOLID AND SCALABLE EDUCATIONAL PROGRAM FOR YOUR **ENTIRE DEVELOPMENT TEAM**

Education is the cornerstone of any modern application security program. Developers, managers, architects and testers must be fully aware of a large variety of attacks and, more importantly, how to defend your organization's web and mobile applications. With that in mind, Infrared Security has built the most effective, educational and entertaining application security e-learning platform on the market: Infrared Spectrum. Infrared Spectrum distills innumerable live classes into highly effective and engaging e-learning material that will instill core security knowledge into your staff and management team.

Infrared Spectrum is a full application security educational platform, featuring security learning tracks for "technical" and "less-technical" participants. Technical modules feature code-level guidance across many programming languages. Participants of our offerings will be able to more readily identify, mitigate, and prevent common security vulnerabilities within their applications and their software development life-cycles (SDLC).

- Participants gain a deep understanding of major risks inherent to web and mobile applications
- Defenses for each security issue covered in depth across multiple languages and platforms
- Courses cover a wide range of topics with role-specific learning paths
- SCORM compliant library can be hosted in your internal LMS or accessed within our 24/7 cloud-based hosting environment

HIGHLIGHTS:

- Richly animated entertaining stories make these educational modules extremely enjoyable to watch
- Full access to our library of security eLearning courses
- Role based training perfect for managers, developers, architects and testers
- SCORM compliant, perfect for Self-Hosting or in Infrared's included Cloud-Hosting service.

Fulfills PCI DSSv3 6.5 Compliance Requirement

Infrared Security's eLearning offerings fulfills your PCI compliance requirements for developers. But beyond that, developers love to learn from Infrared Security's eLearning series.

Throughout the various modules, we highlight the risks associated with the processing of credit card information throughout the various application layers. Information gleaned from this series can be used to produce secure coding guidelines needed to enforce consistent secure programming practices throughout your organization. Learn how achieving PCI compliance spans people, process, and technology today!

MOST **POPULAR** COURSE

02

INFRARED SECURITY

LEARN THE **OWASP TOP 10** WITH **INFRARED SECURITY**

This series of eLearning modules focuses on the most common security vulnerabilities and attack vectors facing application developers today as defined by the OWASP Top Ten. Participants of these modules will explore the OWASP Top Ten through detailed analysis of real-world examples, rich visualizations of attacks, as well as detailed discussions of mitigation strategies with supporting code examples. After completing these modules, participants will be able to more readily identify, mitigate, and prevent common security vulnerabilities within their own applications.

A1 - INJECTION

Learn how to identify and secure the use of interpreters with a focus on SQL Injection.

A2 - BROKEN AUTHENTICATION AND SESSION MANAGEMENT

Learn about the most common attacks used against identity verification and management controls.

A3 - CROSS-SITE SCRIPTING (XSS)

Learn about the most prevalent vulnerability facing developers today - Cross-Site Scripting.

A4 - INSECURE DIRECT OBJECT REFERENCES

Learn about the risks of exposing sensitive resource identifiers without proper authorization verification.

A5 - SECURITY MISCONFIGURATION

Learn about the core principles needed to properly secure environmental configuration files.

A6 - SENSITIVE DATA EXPOSURE

Learn about data classification and sensitive data management throughout the application layers.

A7 - MISSING FUNCTION LEVEL ACCESS CONTROL

Learn how to design, implement, and integration function level access control API.

A8 - CROSS-SITE REQUEST FORGERY (CSRF)

Learn how the synchronizer token pattern can thwart the sleeping giant that is Cross-Site Request Forgery.

A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES

Learn about the need for visibility into the security of 3rd party components used by applications.

A10 - UNVALIDATED REDIRECTS AND FORWARDS

Learn how validation and indirection can be used to verify redirect and forward destinations.

KMI LEARNING

HOST ANY WAY YOU WANT

CLOUD HOSTING

Step 1:
Start by browsing to the Cloud LMS Provider and log in using your provisioned credentials.

Step 2:
View the courses currently accessible within your account. Simply select the desired course name to begin.

Step 3:
See the completed modules within the series. Select any module link to begin viewing lesson details.

Step 4:
Start your lesson with access to additional resources including PDF versions of the scripts and external reading materials.

SELF HOSTING

Step 1:
Download the SCORM compliant eLearning files provided directly by Infrared Security, LLC.

Step 2:
Create a course within your internal LMS and upload the corresponding SCORM compliant files.

Step 3:
Provision access to the security training course to users from within your LMS.

Step 4:
Periodically refresh your course content using updates provided quarterly by Infrared Security, LLC.

INFRARED SECURITY

Infrared Security is an application security company focused on providing developers the guidance, resources, automation, and services to produce more secure code.

With our diverse and mature set of experiences, Infrared Security is capable of working closely with developers to identify, design, implement, and integrate required application security controls mitigating the most significant risks to the business.

Our staff is composed of a rare breed of application security experts with real world development experience. This unique combination of experience enables us to help your developers identify and eliminate security vulnerabilities in a way that actually makes sense! Start eliminating security vulnerabilities at the source.

Infrared Security, LLC.
http://www.infraredsecurity.com

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.

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.

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 how to build secure mobile applications targeting the iOS and Android 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.