VERSPRITE

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

www.VerSprite.com • Info@VerSprite.com

VERSPRITE

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.

VerSprite provides 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

www.VerSprite.com • info@VerSprite.com

HIGHLIGHTS:

- Richly animated entertaining stories make these educational modules 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

VerSprite's eLearning offerings fulfills your PCI compliance requirements for developers.

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.

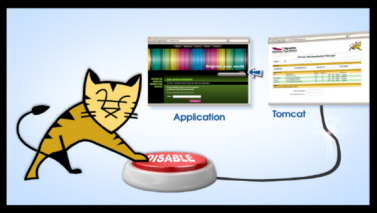
VERSPRITE

LEARN THE **OWASP TOP 10** WITH **VERSPRITE**

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.



A6 - SECURITY

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

A2 - BROKEN AUTHENTICATION

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

A7 - CROSS-SITE SCRIPTING (XSS)

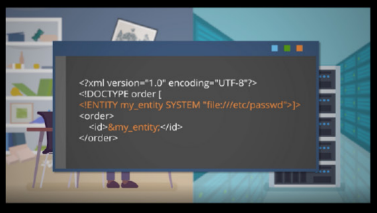
Learn about the most prevalent vulnerability facing developers today - Cross-Site Scripting.

A3 - SENSITIVE DATA MANAGEMENT

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

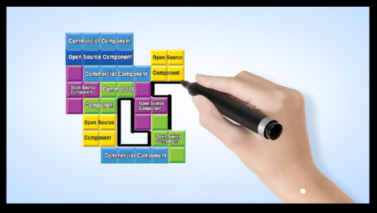
A8 - INSECURE DESERIALIZATION

Learn about the dangers of insecure deserialization. Review countermeasures to protect applications.



A4 - XML EXTERNAL WEAKNESS

Learn about inherent weakness in XML parsing and how a single type of default behavior can put your data and ultimately your users at risk.



A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES

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

A5 - BROKEN ACCESS

Learn about the risks of exposing privileged application functionality without the corresponding function level access control verifications.

A10 - INSUFFICIENT LOGGING & MONITORING

Learn about the dangers of insufficient logging and monitoring in your web applications.

www.VerSprite.com

info@VerSprite.com

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.

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 **VerSprite.**

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 VerSprite.

www.VerSprite.com • info@VerSprite.com

OWASP TOP TEN 2017 FOR DEVELOPERS

Duration: 3 hours to complete
Audience: Software Architects, Security Engineers, 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 2017 FOR MANAGERS

Duration: 45 minutes 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.

OWASP TOP TEN 2013-2017 DELTA FOR DEVELOPERS

Duration: 1 hour(s) to complete
Audience: Software Managers
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 2017 document; for students who have already completed the OWASP Top Ten 2013 for Developers module.

OWASP MOBILE TOP TEN 2017 FOR DEVELOPERS

Duration: 3 hours to complete
Audience: Software Architects, Security Engineers, and Software Testers
Overview: Participants of this course will gain a foundational understanding of mobile application security and secure programming practices based on the threats and vulnerabilities outlined in the Open Web Application Security Project's Mobile Top Ten document.

OWASP MOBILE TOP TEN 2017 FOR MANAGERS

Duration: 45 minutes to complete
Audience: Software Managers
Overview: Participants of this course will gain a foundational understanding of mobile application security based on the threats and vulnerabilities outlined in the Open Web Application Security Project's Mobile Top Ten document.

DEFENSIVE ENTERPRISE REMEDIATION

Duration: 1 hour(s) to complete
Audience: Software Architects, Security Engineers, 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(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(s) to complete
Audience: Software Architects and Security Engineers
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(s) to complete
Audience: Software Architects and Security Engineers
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(s) to complete
Audience: Software Architects and Security Engineers
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(s) to complete
Audience: Software Architects and Security Engineers
Overview: Participants of this course will gain a foundational understanding of writing secure software using JavaScript for both the client and the server.

BUILDING SECURE PYTHON APPLICATIONS

Duration: 1 hour(s) to complete
Audience: Software Architects and Security Engineers
Overview: Participants of this course will gain a foundational understanding of writing secure software on Python based platforms.

INTEGRATING SECURITY THROUGHOUT THE SDLC

Duration: 1 hour(s) to complete
Audience: Software Managers
Overview: Participants will understand the most important and essential security activities which can be conducted throughout the SDLC to reduce security issues.