Secure Web Application Lifecycle Development (5 Days)

The ***Secure Web Application Lifecycle Development*** is a lab intensive, hands-on web application security training course, essential for experienced web developers who need to produce secure web applications. In addition to teaching basic programming skills, this course digs deep into sound processes and practices that apply to the entire software development lifecycle.

In this course, students thoroughly examine best practices for defensively coding web applications, including XML processing and web services. Students will repeatedly attack and then defend various assets associated with a fully-functional web application. This hands-on approach drives home the mechanics of how to secure web applications in the most practical of terms.

Security experts agree that the least effective approach to security is "penetrate and patch". It is far more effective to "bake" security into an application throughout its lifecycle. After spending significant time trying to defend a poorly designed (from a security perspective) web application, developers are ready to learn how to build secure web applications starting at project inception. The final portion of this course builds on the previously learned mechanics for building defenses by exploring how design and analysis can be used to build stronger applications from the beginning of the software lifecycle.

Although this edition of the course is language-agnostic, it may also be presented using Java or Microsoft .NET programming languages.

Course Objectives: What You'll Learn

Students who attend **Secure Web Application Development** will leave the course armed with the skills required to recognize actual and potential software vulnerabilities, implement defenses for those vulnerabilities, and test those defenses for sufficiency. This course quickly introduces developers to the most common security vulnerabilities faced by web applications today. Each vulnerability is examined from a coding perspective through a process of describing the threat and attack mechanisms, recognizing associated vulnerabilities, and, finally, designing, implementing, and testing effective defenses. In many cases, there are labs that reinforce these concepts with real vulnerabilities and attacks. Students are then challenged to design and implement the layered defenses they will need in defending their own applications.

Working in an interactive learning environment, guided by our application security expert, attendees will learn to:

- Understand potential sources for untrusted data
- Understand the consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections
- Be able to test web applications with various attack techniques to determine the existence of and effectiveness of layered defenses
- Prevent and defend the many potential vulnerabilities associated with untrusted data
- Understand the vulnerabilities of associated with authentication and authorization
- Be able to detect, attack, and implement defenses for authentication and authorization functionality and services
- Understand the dangers and mechanisms behind Cross-Site Scripting (XSS) and Injection attacks
- Be able to detect, attack, and implement defenses against XSS and Injection attacks
- Understand the concepts and terminology behind defensive, secure, coding
- Understand the use of Threat Modeling as a tool in identifying software vulnerabilities based on realistic threats against meaningful assets
- Perform both static code reviews and dynamic application testing to uncover vulnerabilities in web applications
- Design and develop strong, robust authentication and authorization implementations
- Understand the fundamentals of XML Digital Signature and XML Encryption as well as how they are used within the web services arena
- Be able to detect, attack, and implement defenses for XML-based services and functionality
- Understand techniques and measures that can used to harden web and application servers
- Understand and implement the processes and measures associated with the Secure Software Development (SSD)
- Understand the basics of security testing and planning
- Work through a comprehensive testing plan for recognized vulnerabilities and weaknesses

This class is “technology-centric”, designed to train attendees in essential secure coding and development skills, coupling the most current, effective techniques with the soundest industry practices.
The course provides a solid foundation in basic terminology and concepts, extended and built upon throughout the engagement. Students will examine various recognized attacks against web applications. Processes and best practices are discussed and illustrated through both discussions and group activities.

The second portion of the course steps through a series of vulnerabilities illustrating in very real terms the right way to implement secure web services. The last portion of the course examines several design patterns that can be used to facilitate better application architecture, design, implementation, and deployment.

Audience & Pre-requisites: Who Should Attend

This is an **intermediate-level** course designed for application project stakeholders who wish to get up and running on developing well defended web applications. Familiarity with a programming language (such as Java, .Net or C++) is required, and real world programming experience is highly recommended.

Workshop Topics Covered

Introduction: Misconceptions
- Security: The Complete Picture
- Seven Deadly Assumptions
- Anthem, Sony, Target, Heartland, and TJX Debriefs
- Causes of Data Breaches
- Meaning of Being Compliant
- Verizon’s 2015 Data Breach Report
- 2015 PCI Compliance Report

Session: Foundation

Lesson: Security Concepts
- Motivations: Costs and Standards
- Open Web Application Security Project
- Web Application Security Consortium
- CERT Secure Coding Standards
- Assets are the Targets
- Security Activities Cost Resources
- Threat Modeling
- System/Trust Boundaries

Lesson: Principles of Information Security
- Security Is a Lifecycle Issue
- Minimize Attack Surface Area
- Layers of Defense: Tenacious D
- Compartmentalize
- Consider All Application States
- Do NOT Trust the Untrusted

Session: Vulnerabilities

Lesson: Unvalidated Input
- Buffer Overflows
- Integer Arithmetic Vulnerabilities
- Unvalidated Input: From the Web
- Defending Trust Boundaries
- Whitelisting vs Blacklisting

Lesson: Overview of Regular Expressions
- Regular Expressions
- Working With Regexes in Java
- Applying Regular Expressions

Lesson: Broken Access Control
- Access Control Issues
- Excessive Privileges
- Insufficient Flow Control
- Unprotected URL/Resource Access
- Examples of Shabby Access Control
- Session and Session Management

Lesson: Broken Authentication
- Broken Quality/DoS
- Authentication Data
- Username/Password Protection
- Exploits Magnify Importance
- Handling Passwords on Server Side
- Single Sign-on (SSO)

Lesson: Cross Site Scripting (XSS)
- Persistent XSS
- Reflective XSS
- Best Practices for Untrusted Data

Lesson: Injection
- Injection Flaws
- SQL Injection Attacks Evolve
- Drill Down on Stored Procedures
- Other Forms of Injection
- Minimizing Injection Flaws

Lesson: Error Handling and Information Leakage
- Fingerprinting a Web Site
- Error-Handling Issues
- Logging In Support of Forensics
- Solving DLP Challenges

Lesson: Insecure Data Handling
- Protecting Data Can Mitigate Impact
- In-Memory Data Handling
- Secure Pipes
- Failures in the SSL Framework Are Appearing

Lesson: Insecure Configuration Management
- System Hardening: IA Mitigation
- Application Whitelisting
- Least Privileges
- Anti-Exploitation
- Secure Baseline

Lesson: Direct Object Access
- Dynamic Loading
- Direct Object References

Lesson: Spoofing and Redirects
- Name Resolution Vulnerabilities
- Fake Certs and Mobile Apps
- Targeted Spoofing Attacks
- Cross Site Request Forgeries (CSRF)
- CSRF Defenses are Entirely Server-Side
- Safe Redirects and Forwards

Lesson: Understanding What's Important

- Common Vulnerabilities and Exposures
- OWASP Top Ten for 2013
- CWE/SANS Top 25 Most Dangerous SW Errors
- Monster Mitigations
- Strength Training: Project Teams/Developers
- Strength Training: IT Organizations

Session: Defending XML, Services, and Rich Interfaces

Lesson: Defending XML

- XML Signature
- XML Encryption
- XML Attacks: Structure
- XML Attacks: Injection
- Safe XML Processing

Lesson: Defending Web Services

- Web Service Security Exposures
- When Transport-Level Alone is NOT Enough
- Message-Level Security
- WS-Security Roadmap
- XWSS Provides Many Functions
- Web Service Attacks
- Web Service Appliance/Gateways

Lesson: Defending Rich Interfaces and REST

- How Attackers See Rich Interfaces
- Attack Surface Changes When Moving to Rich Interfaces
- Bridging and its Potential Problems
- Three Basic Tenets for Safe Rich Interfaces
- OWASP REST Security Recommendations

Session: Secure Development Lifecycle (SDL)

Lesson: SDL Process Overview

- Software Security Axioms
- Security Lifecycle – Phases

Lesson: Applying Processes and Practices

- Awareness
- Application Assessments
- Security Requirements
- Secure Development Practices
- Security Architecture/Design Review
- Security Code Review
- Configuration Management and Deployment
- Vulnerability Remediation Procedures

Lesson: Risk Analysis

- Threat Modeling Process
- 1. Identify Security Objectives
- 2. Describe the System
- 3. List Assets
- 4. Define System/Trust Boundaries
- 5. List and Rank Threats
- 6. List Defenses and Countermeasures

Session: Security Testing

Lesson: Testing Tools and Processes

- Security Testing Principles
- Black Box Analyzers
- Static Code Analyzers
- Criteria for Selecting Static Analyzers

Lesson: Testing Practices

- OWASP Web App Penetration Testing
- Authentication Testing
- Session Management Testing
- Data Validation Testing
- Denial of Service Testing
- Web Services Testing
- Ajax Testing