Course Outline

Secure Web Application Development

Course Summary

Description

Every major aspect of application security is covered, and each module includes both design and coding advice. Hands-on labs are provided to help students master the concepts in a highly interactive setting. The course focuses on application development strategies and tactics that secure software at the source.

Topics

- Security Principles Overview
- Information Disclosure
- Authentication
- Authorization and Access Control
- Session Management
- Secure Data Handling
- Cryptography
- Logging
- Web Service Security
- Secure Application Development
- Web Application Security Resources
- Web Application Security Tools

Audience

This course is designed to teach web application developers and architects how to build applications with world-class security. QA engineers, IT security analysts, and IT risk managers can also benefit from this course.

Prerequisites

The course is contains coding examples in both Java and ASP.Net, but can be customized for any development language. A working knowledge of HTML, JavaScript and any server-side programming language (ASP.Net, Java, PHP, ColdFusion, etc.) is recommended.

Duration

Two Days

Course Outline

Secure Web Application Development

Course Outline

I. ***Security Principles Overview***
- A. Importance of Security In the Software Development Lifecycle
- B. Regulations, Privacy and Compliance
- C. Impact of Security Defects
- D. Core Security Concepts
- E. Security Design Principles

II. ***Information Disclosure***
- A. Leakage in Web Technologies (HTML, HTTP, Files, Client-Side Objects, URLs, Web Services)
- B. Error Handling (Structured vs. Functional)
- C. Google Hacking

III. ***Authentication***
- A. Methods of Authentication
- B. 2-Factor Authentication
- C. Single Sign-On
- D. Common Authentication Attacks (Brute Force, Username Harvesting, etc.)
- E. Implementing Secure Authentication – Design and Coding

IV. ***Session Management***
- A. Overview of Sessions
- B. Threats to Sessions and Impact
- C. Common Implementation Mistakes and Exploits (Interception, Prediction, Brute Force, etc.)
- D. Implementing Secure Sessions – Design and Coding

V. ***Authorization and Access Control***
- A. Methods of Access Control
  1. Discretionary Access Control (DAC)
  2. Mandatory Access Control (MAC)
  3. Role-Based Access Control (RBAC)
  4. Rule-Based Access Control
- B. Common Authorization Attacks (Parameter Tampering, Privilege Escalation, Cross-Site Request Forgery, etc.)
- C. Implementing Secure Authentication – Design and Coding

VI. ***Secure Data Handling***
- A. Overview of Data Handling
  1. Integrity Validation
  2. Data Validation
  3. Business Rule Validation
- B. Common Exploits (SQL Injection, Cross-Site Scripting, HTTP Response Splitting, etc.)
- C. Implementing Secure Data Handling – Design and Coding

VII. ***Cryptography***
- A. Hashing
- B. Secure Password Storage
- C. Symmetric and Asymmetric Encryption
- D. Digital Signatures
- E. Certificates
- F. Key Distribution
- G. SSL and Digital Certificates
- H. Implementing Cryptography – Design and Coding

VIII. ***Logging***
- A. Logging Overview
- B. Threats and Considerations
- C. Implementing Logging – Design and Coding

IX. ***Web Service Security***
- A. Simple Object Access Protocol (SOAP)
- B. SOAP Related Protocols
- C. Security Assertion Markup Language (SAML)
- D. WS-Security
- E. REpresentational State Transfer (REST)
- F. REST Related Protocols
- G. JSON vs XML
- H. Implementing Secure Web Services – Design and Coding

Course Outline

Secure Web Application Development

Course Outline (cont.)

X. ***Secure Application Development***
- A. Software Development Life Cycle (SDLC)
- B. Threat Modeling
- C. Application Risk Levels
- D. Risk Assessment
  1. STRIDE and DREAD
  2. Severity Level Classifications

XI. ***Web Application Security Tools***

XII. ***Web Application Security Resources***

Lab Sessions

The in-person version of this course includes lab exercises that allow students to explore the security of their applications and to demonstrate attack techniques against a demo website. The exercises cover manual techniques to exploit the site and subvert application restrictions. The hands-on sessions include:

- Introduction To Interception Proxy Tools
- Information Gathering
- Session Token Identification
- Analyzing a Site's Session Handling Practices
- Exploiting Authorization Issues
- Harvesting Data with Burp Intruder
- Cross-Site Scripting
- SQL Injection
- Web Services