Document Generated: 11/13/2024

Learning Style: Virtual Classroom

Provider: Java

Difficulty: Intermediate

Course Duration: 5 Days

Developing Secure Java Web Applications - Lifecycle (SDLC) (TT8325-J)

About this course:

Secure Java Web Application Development Lifecycle (SDL) is a lab-intensive, hands-on Java / JEE security training course, essential for experienced enterprise developers who need to engineer, maintain, and support secure JEE-based web applications. In addition to teaching basic secure 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, rich interfaces, and both RESTful and SOAP-based web services. Students will repeatedly attack and then defend various assets associated with fully-functional web applications and web services. This hands-on approach drives home the mechanics of how to secure JEE 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.

A key component to our ***Best Defense IT Security Training Series***, this workshop is a companion course with several developer-oriented courses and seminars. Although this edition of the course is Java-specific, it may also be presented using .Net or other programming languages.

The average salary of a Java Developer is **$69,722** per year.

Course Objective:

- 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
- 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
- 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
- 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 Java-based web applications
- Design and develop strong, robust authentication and authorization implementations within the context of JEE
- Understand the fundamentals of XML Digital Signature and XML Encryption as well as how they are used within the web services arena
- To detect, attack, and implement defenses for both RESTful and SOAP-based web services and functionality
- Understand techniques and measures that can used to harden web and application servers as well as other components in your infrastructure
- Understand and implement the processes and measures associated with the Secure Software Development (SSD)
- Acquire the skills, tools, and best practices for design and code reviews as well as testing initiatives
- Understand the basics of security testing and planning
- Work through a comprehensive testing plan for recognized vulnerabilities and weaknesses

Audience:

- This is an **intermediate -level** JEE programming course, designed for developers who wish to get up and running on developing well defended software applications. This course may be customized to suit your team's unique objectives.

Prerequisite:

- Familiarity with Java and JEE is required and real world programming experience is highly recommended. Ideally students should have approximately 6 months to a year of Java and JEE working knowledge.

Course Outline:

Module 1: Foundation

Lesson: Who is Safe?

- Assumptions We Make
- Security: The Complete Picture
- Anthem, Sony, Target, Heartland, and TJX Debriefs
- Verizon's 2017 Data Breach Report

- Attack Patterns and Recommendations
- Tutorial: Working with Eclipse (JEE Version) and Tomcat
- Tutorial: Working with the HSQL Database
- Exercise: Case Study Setup and Review

Lesson: Security Concepts

- Motivations: Costs and Standards
- Open Web Application Security Project
- Web Application Security Consortium
- CERT Secure Coding Standards
- Microsoft SDL
- Assets and Trust Boundaries
- Threat Modeling
- Exercise: Case Study Asset Analysis

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

Module 2: Vulnerabilities (Part 1)

Lesson: Unvalidated Input

- Buffer Overflows
- Integer Arithmetic Vulnerabilities
- Unvalidated Input: From the Web
- Defending Trust Boundaries
- Whitelisting vs Blacklisting
- Exercise: Defending Trust Boundaries
- Exercise: Defending Trust Boundaries With Regular Expressions

Lesson: Broken Access Control

- Access Control Issues
- Excessive Privileges
- Insufficient Flow Control
- Unprotected URL/Resource Access
- Examples of Shabby Access Control
- Sessions 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)
- Exercise: Defending Authentication

Lesson: Cross Site Scripting (XSS)

- XSS Patterns
- Persistent XSS
- Reflective XSS
- Best Practices for Untrusted Data
- Exercise: Defending Against XSS

Lesson: Injection

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

Module 3: Vulnerabilities (Part 2)

Lesson: Error Handling and Information Leakage

- Fingerprinting a Web Site
- Error-Handling Issues
- Logging In Support of Forensics
- Solving DLP Challenges
- Exercise: Error Handling

Lesson: Insecure Data Handling

- Protecting Data Can Mitigate Impact
- In-Memory Data Handling
- Secure Pipes
- Failures in TLS/SSL Framework
- Exercise: Defending Sensitive Data

Lesson: Insecure Configuration Management

- System Hardening: IA Mitigation
- Application Whitelisting
- Least Privileges
- Anti-Exploitation
- Secure Baseline

Lesson: Direct Object Access

- Remote File Inclusion
- Redirects and Forwards
- Direct Object References
- Exercise: Unsafe Direct Object References

Lesson: Spoofing, CSRF, and Redirects

- Name Resolution Vulnerabilities
- Fake Certs and Mobile Apps
- Targeted Spoofing Attacks
- Cross Site Request Forgeries (CSRF)
- CSRF Defenses
- Exercise: Cross-Site Request Forgeries

Module 4: Best Practices

Lesson: Cryptography Overview

- Strong Encryption
- Message Digests
- Encryption/Decryption
- Keys and Key Management
- NIST Recommendations

Lesson: Understanding What's Important

- Common Vulnerabilities and Exposures
- OWASP 2017 Top Ten
- CWE/SANS Top 25 Most Dangerous SW Errors
- Monster Mitigations
- Strength Training: Project Teams/Developers
- Strength Training: IT Organizations
- Exercise: Recent Incidents

Module 5: Defending XML, Services, and Rich Interfaces

Lesson: Defending XML

- XML Signature
- XML Encryption
- XML Attacks: Structure
- XML Attacks: Injection
- Safe XML Processing
- Exercise: Safe XML Processing
- Exercise: Dynamic Loading Using XSLT

Lesson: Defending Web Services

- Web Service Security Exposures
- When Transport-Level Alone is NOT Enough
- Message-Level Security
- WS-Security Roadmap
- Java's XWSS API
- Web Service Attacks
- Web Service Appliance/Gateways
- Exercise: Web Service Attacks

Lesson: Defending Rich Interfaces and REST

- How Attackers See Rich Interfaces
- Attack Surface Changes When Moving to Rich Interfaces and REST
- Bridging and its Potential Problems
- Three Basic Tenets for Safe Rich Interfaces
- OWASP REST Security Recommendations
- OAuth 2.0 and OpenID
- Exercise: Working with OAuth

Module 6: Secure Development Lifecycle (SDL)

Lesson: SDL Process Overview

- Types of Security Controls
- Phases of Typical Data-Oriented Attack
- Phases: Offensive Actions and Defensive Controls
- Security Lifecycle Activities

Lesson: Applying Processes and Practices

- Threat Modeling Process
- Modeling Assets and Trust Boundaries
- Modeling Data Flows
- Exercise: Threat Modeling

Lesson: Risk Analysis

- Identifying Threats
- Relating Threats to Model
- Mitigating Threats
- Reviewing the Application
- Exercise: Security Review

Module 7: Security Testing

Lesson: Testing Tools and Processes

- Security Testing Principles

- Dynamic 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

Credly Badge:

Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges