Securing Java/ JEE Web Applications (TT8320-J)

Duration: 4 Days **Course Code: GK1123** **Delivery Method: Virtual and Classroom**

Overview:

Securing Java Web Applications is a lab-intensive, hands-on Java / JEE security training course, essential for experienced enterprise developers who need to produce secure JEE-based 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 JEE 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 JEE web applications in the most practical of terms.

Virtual and Classroom learning - V&C Select™

V&C Select™ is a simple concept and a flexible approach to delivery. You can 'select' a course from our public schedule and attend in person or as a virtual delegate. Virtual delegates do not travel to this course, we will send you all the information you need before the start of the course and you can test the logins.

Target Audience:

This is an intermediate -level JEE / web services 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.

Objectives:

- 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 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
- 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 as well as other components in your infrastructure

Prerequisites:

Students should have an understanding and a working

knowledge in the following topics, or attend these courses as a pre-requisite:

- TT2100 Mastering Java for OO Developers or TT2120 Java and OO Essentials for COBOL and Mainframe Developers or TT5140 Java Web Essentials for OO Developers
- TT5100 Mastering JEE Web Application Development

Content:

Introduction: Misconceptions

Security: The Complete Picture

- TJX: Anatomy of a Disaster?
- Causes of Data Breaches
- Heartland – Slipping Past PCI Compliance
- Target's Painful Christmas
- Meaning of Being Compliant
- Verizon's 2015 Data Breach Report and 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 ResourcesThreat 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

- 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 ControlUnprotected 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, CSRF, 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

Session: Best Practices

Lesson: Cryptography Overview

- Strong Encryption
- Message digests
- Keys and key managementCertificate management
- Encryption/Decryption

Lesson: Understanding What's Important

- Common Vulnerabilities and Exposures
- OWASP Top Ten for 2013
- CWE/SANS Top 25 Most Dangerous SW ErrorsMonster 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

Further Information:

For More information, or to book your course, please call us on 353-1-814 8200

info@globalknowledge.ie

www.globalknowledge.ie

Global Knowledge, 3rd Floor Jervis House, Millennium Walkway, Dublin 1