Global Knowledge™

Attacking and Securing Java / JEE Web Applications (TT8320-J)

Duration: 4 Days **Course Code: GK1123**

Overview:

Attacking and Securing Java Web Applications is a lab-intensive, hands-on Java / JEE security training course that provides a unique coverage of Java application security. In this course, students begin with penetration testing, hunting for bugs in Java web applications. They then thoroughly examine best practices for defensively coding web applications, covering all the OWASP Top Ten as well as several additional prominent vulnerabilities (such as file uploads, CSRF and direct object references). Students will repeatedly attack and then defend various assets associated with fully functional web applications and services. This hands-on approach drives home the mechanics of how to secure JEE web applications in the most practical of terms.

A key component to our *Best Defense IT Security Training Series*, this workshop is a companion course with several developer-oriented courses and seminars. Our bug hunting class introduces penetration testing, illustrating how hackers can probe and exploit our applications. Our developing secure software class introduces various security measures that can be applied through the software lifecycle. The combination of ethical hacking, secure coding, and secure lifecycle training provides student with the complete experience in application security. Although this edition of the course is Java specific, it may also be presented using .Net, NodeJS or other programming languages.

This "skills-centric" course is about 50% hands-on lab and 50% lecture, designed to train attendees in secure web application development, coding and design, coupling the most current, effective techniques with the soundest industry practices. Our engaging instructors and mentors are highly experienced practitioners who bring years of current "on-the-job" experience into every classroom.

Target Audience:

This is an intermediate -level programming course, designed for experienced Java developers who wish to get up and running on developing well defended software applications. 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.

Objectives:

- Working in a hands-on learning environment, guided by our expert team, attendees will learn:
- Ensure that any hacking and bug hunting is performed in a safe and appropriate manner
- Identify defect/bug reporting mechanisms within their organizations
- Setup and use various tools and techniques to determine a web application's operational environment
- Setup and use various tools and techniques to enumerate all aspects of a web application
- Setup and use various tools and techniques to scan a web application for vulnerabilities
- Work with specific tools for targeted vulnerabilities
- Avoid common mistakes that are made in bug hunting and vulnerability testing
- Understand the concepts and terminology behind defensive, secure coding including the phases and goals of a typical exploit
- 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
- 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
- Detect, attack, and implement defenses against XSS and Injection attacks
- Understand the risks associated with XML processing, file uploads, and server-side interpreters and how to best eliminate or mitigate those risks
- Learn the strengths, limitations, and use for tools such as code

- Develop an appreciation for the need and value of a multilayered defense in depth
- Understand potential sources for untrusted data
- scanners, dynamic scanners, and web application firewalls (WAFs)
- 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:

- TT5102 JEE Web Application Development Essentials

Follow-on-Courses:

Our Java tracks include a wide variety of follow-on courses and learning paths for leveraging Java for next-level development, testing, security and more. Please see our Java Developer Training Suite & Learning Paths list of courses, or inquire for recommendations based on your specific role and goals.

Content:

Session: Bug Hunting Foundation

Lesson: Why Hunt Bugs?

- Security and Insecurity
- Dangerous Assumptions
- Attack Vectors
- Lab: Case Studies in Failure

Lesson: Safe and Appropriate Bug Hunting/Hacking

- Working Ethically
- Respecting Privacy
- Bug/Defect Notification
- Bug Bounty Programs

Session: Scanning Web Applications

Lesson: Scanning Applications Overview

- Scanning Beyond the Applications
- Fingerprinting
- Vulnerability Scanning: Hunting for Bugs
- Reconnaissance Goals
- Data Collection Techniques
- Fingerprinting the Environment
- Enumerating the Web Application

Session: Moving Forward from Hunting Bugs

Lesson: Removing Bugs

- Open Web Application Security Project (OWASP)
- OWASP Top Ten Overview
- Web Application Security Consortium
- CERT Secure Coding Standards
- Bug Hunting Mistakes to Avoid
- Tools and Resource

Session: Foundation for Securing Applications

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
- Tutorial: Working with Eclipse and TomEE
- Tutorial: Working with the HSQL Database
- Lab: Case Study Setup and Review

Session: Bug Stomping 101

Lesson: Unvalidated Data

- Buffer Overflows
- Integer Arithmetic Vulnerabilities
- Unvalidated Data: Crossing Trust Boundaries
- Defending Trust Boundaries
- Whitelisting vs Blacklisting
- Lab: Defending Trust Boundaries

Lesson: A1: Injection

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

Lesson: A2: Broken Authentication

- Quality and Protection of Authentication Data
- Handling Passwords on Server Side
- SessionID Risk Reduction
- HttpOnly and Security Headers
- Lab: Defending Authentication

Lesson: A3: Sensitive Data Exposure

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

Lesson: A4: XML External Entities (XXE)

- XML Parser Coercion
- XML Attacks: Structure
- XML Attacks: Injection
- Safe XML Processing
- Lab: Safe XML Processing
- Lab: Dynamic Loading Using XSLT (Optional)

Lesson: A5: Broken Access Control

- Access Control Issues
- Excessive Privileges
- Insufficient Flow Control
- Unprotected URL/Resource Access
- Examples of Shabby Access Control
- Sessions and Session Management
- Lab: Unsafe Direct Object References
- Lab: Spotlight on Verizon Exploit

Session: Bug Stomping 102

Lesson: A7: Cross Site Scripting (XSS)

- XSS Patterns
- Persistent XSS
- Reflective XSS
- DOM-based XSS
- Best Practices for Untrusted Data
- Lab: Defending Against XSS

Lesson: A8/9: Deserialization/Vulnerable Components

- Deserialization Issues
- Identifying Serialization and Deserializations
- Vulnerable Components
- Software Inventory
- Managing Updates
- Lab: Spotlight on Equifax Exploit

Lesson: A10: Insufficient Logging and Monitoring

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

Lesson: Spoofing, CSRF, and Redirects

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

Session: Moving Forward with Application Security

Lesson: Applications: What Next?

- Common Vulnerabilities and Exposures
- CWE/SANS Top 25 Most Dangerous SW Errors
- Strength Training: Project Teams/Developers
- Strength Training: IT Organizations
- Leveraging Common AppSec Practices and Controls
- Lab : Reprtig incidents
- Lab: Spotlight on Capitol One Exploit

Lesson: Making Application Security Real

- Cost of Continually Reinventing
- Paralysis by Analysis
- Actional Application Security

Additional Tools for the Toolbox

Lesson: A6: Security Misconfiguration

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

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK