Java EE Secure Coding Camp | Attacking and Securing Java EE Web Applications

Code: TT8320-J
Length: 4 days
URL: View Online

Attacking and Securing Java EE Web Applications is a lab-intensive, hands-on Java EE 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.

Students will leave the course armed with the skills required to recognize actual and potential software vulnerabilities and implement defenses for those vulnerabilities. This course begins by developing the skills required to fingerprint a web application and then scan it for vulnerabilities and bugs. Practical labs using current tools and techniques provide students with the experience needed to begin testing their own applications. Students also gain a deeper understanding of how attackers probe applications to understand the runtime environment as well as find potential weaknesses. This course the introduces developers to the most common security vulnerabilities faced by web applications today. Each vulnerability is examined from a Java/JEE perspective through a process of describing the threat and attack mechanisms, recognizing associated vulnerabilities, and, finally, designing, implementing, and testing effective defenses.

Although this edition of the course is Java-specific, it may also be presented using .Net or other programming languages.

Skills Gained

- Ensure that any bug hunting is performed in a safe and appropriate manner
- Identify defect/bug reporting mechanisms within their organizations
- 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
- Develop an appreciation for the need and value of a multilayered defense in depth
- 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

- 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
- Understand techniques and measures that can used to harden web and application servers as well as other components in your infrastructure

Who Can Benefit

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

Prerequisites

Familiarity with Java and Java EE 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.

Students should have basic development skills and a working knowledge in the following topics, or attend these courses as a pre-requisite:

- TT5102 Java EE Web Application Development Essentials

Course Details

Session: Bug Hunting Foundation

- Lesson: Why Hunt Bugs?
- Lesson: Safe and Appropriate Bug Hunting/Hacking

Session: Moving Forward From Hunting Bugs

- Lesson: Removing Bugs

Session: Foundation for Securing Web Applications

- Lesson: Principles of Information Security

Session: Bug Stomping 101

- Lesson: Unvalidated Data
- Lesson: A1: Injection
- Lesson: A2: Broken Authentication
- Lesson: A3: Sensitive Data Exposure
- Lesson: A4: XML External Entities (XXE)
- Lesson: A5: Broken Access Control

Session: Bug Stomping 102

- Lesson: A6: Security Misconfiguration
- Lesson: A7: Cross Site Scripting (XSS)
- Lesson: A8/9: Deserialization/Vulnerable Components
- Lesson: A10: Insufficient Logging and Monitoring
- Lesson: Spoofing, CSRF, and Redirects

Session: Secure Development Lifecycle (SDL)

- Lesson: SDL Overview

Session: Moving Forward with Application Security

- Lesson: Applications: What Next?
- Lesson: Making Application Security Real

Schedule (as of 4)

Date	Location	
May 20, 2024 – May 23, 2024	Virtual	**Enroll**
Jul 15, 2024 – Jul 18, 2024	Virtual	**Enroll**
Sep 9, 2024 – Sep 12, 2024	Virtual	**Enroll**
Oct 21, 2024 – Oct 24, 2024	Virtual	**Enroll**
Dec 9, 2024 – Dec 12, 2024	Virtual	**Enroll**
