

Course Description: This course extends the Building and Testing Secure Web Applications course by adding a significant amount of Java specific content and exercises. Everything in the two-day version of the course is covered in this course. In addition, all language-specific content such as code examples, spot the bug exercises, and server specific recommendations have been translated to Java EE and its associated standard servers.

Three multistage hands-on Java programming labs have been added to this course. In these labs, the student not only finds flaws in a sample Java application, but then actually fixes the code using a Java IDE. They complete the lab stages by retesting to prove that they have fixed the target vulnerability for that stage.

Who Should Attend: This course is for JEE programmers and developers who want to provide secure coding for Java EE applications.

Prerequisites: Students should have experience with the design and implementation of Java EE applications. Familiarity with Eclipse is a plus but is not required.

Benefits of Attendance: Upon completion of this course, students will be able to:

- employ the security features involved with using HTTP (e.g., headers, cookies, SSL);
- apply application security design principles;
- identify and explain common web application security threats (e.g., cross-site scripting, SQL injection, denial of service attacks, "Man-in-the-middle" attacks, etc.) and implement mitigation techniques;
- handle credentials securely while providing the full range of authentication support functions, including login, change password, forgot password, remember password, logout, re-authentication, and timeouts;
- implement access control rules for the user interface, business logic, and data layers;
- recognize potential input validation issues, particularly injection and Cross-site Scripting (XSS) problems, and implement appropriate input validation mechanisms for user input and other sources of input;
- understand the dangers of command injection and techniques for avoiding the introduction of this type vulnerability;
- implement a consistent error (exception) handling and logging approach for an entire web application;

Course Outline:

Modules on XML and Web Services Security, including additional Web Services hands-on security testing labs

Numerous Spot the Bug Exercises are added where students are challenged to find real life security flaws in carefully constructed code samples

More in-depth discussion of topics from the 2-day course, including additional examples, code snippets, design patterns, and configuration recommendations