Building Secure Web Applications in Java/Java EE: 
Break ‘em and Build ‘em Biathlon

Course Summary

Description
This rapid immersion class is for experienced web application software developers who want to take a quick but deep dive into the biggest web application security issues. The class is built extensively around a series of hands-on lab exercises in which the students first learn first-hand the details of today’s biggest web application security defects and how to exploit them. This is immediately followed by a set of labs in which the students learn to remediate those same defects by implementing appropriate fixes in a JavaEE-based web application. This rapid fire approach to breaking and then fixing the security on an actual web application enables students to deeply understand and internalize the biggest security problems faced by today’s web application developers.

Topics
- Class introduction and setup
- Breaking web application security
- Coding labs – fixing web application security
- Design Reviews Using Threat Modeling
- Conducting Effective Code Reviews
- Security Testing
- Contest – The Challenge!
- Questions and Answers
- Class Close

Audience
Web application Developers, Designers and Architects

Prerequisites
Experience with developing web applications in Java

Duration
Three days
“Charting the Course ... 
... to Your Success!”

Building Secure Web Applications in Java/Java EE: 
Break ‘em and Build ‘em Biathlon

Course Outline

I. Class introduction and setup
   A. Brief introduction to the class, exercises, and expected outcomes
   B. Students install and configure software tools to be used in the upcoming exercises
   C. The instructor demonstrates the tools and runs through a sample exercise to ensure all students can use the tools correctly

II. Breaking web application security
   A. Walk through numerous web app security defects, including OWASP Top-10 (2013)
      1. Injection flaws (including SQLi)
   B. Walk through numerous web app security defects, including OWASP Top-10 (2013)
      1. Broken authentication and session management
      2. Cross-site scripting (XSS)
   C. Walk through numerous web app security defects, including OWASP Top-10 (2013)
      1. Cross-site request forgery (CSRF)
      2. Broken access control
   D. Walk through numerous web app security defects, including OWASP Top-10 (2013)
      1. Server misconfiguration
      2. Reliance on weak components
      3. Client side code reliance
      4. Code quality resulting in security issues
   E. Questions and answers

III. Coding labs – fixing web application security
   A. First, an architectural and source code overview of the app used in the labs
   B. How to build and deploy
   C. Hands-on labs in which numerous vulnerabilities are discovered and fixed
      1. XSS
      2. SQLi
      3. Access control
      4. Others
   D. Walk-through and discussion of all source code used in remediating the vulnerabilities
   E. Hands-on labs in which numerous vulnerabilities are discovered and fixed
      1. SQLi
   F. Hands-on labs in which numerous vulnerabilities are discovered and fixed
      1. Access control
   G. Hands-on labs in which numerous vulnerabilities are discovered and fixed
      1. Others
   H. Questions and Answers

IV. Design Reviews Using Threat Modeling
   A. Reviewing designs using threat modeling
   B. Finding the weaknesses in an application architecture
   C. Documenting how the weaknesses can be exploited
   D. Deciding what and how to mitigate the weaknesses
   E. Group exercise, threat modeling a real world system

V. Conducting Effective Code Reviews
   A. Overview of manual vs. automated code review methods
   B. Integrating code review tools into the code development process

VI. Security Testing
   A. Overview of effective security testing techniques
      1. Fuzzing
      2. Dynamic validation analysis
      3. Penetration testing
      4. Risk based testing
   B. Case study

VII. Contest – The Challenge!
   A. Students are put to the test to see who can finish the contest first
   B. The lessons taught in this class are used to solve a puzzle that is highly representative of attacking/testing a modern web application

VIII. Questions and Answers

IX. Class Close