

Current Class Offering: December 8 - 9, 2008 – Call for Details and Reservations.

Securing Java Web Applications - OWASP Top 10

This course guides the participant through the top ten security vulnerabilities of Java websites. Using the OWASP project top ten list, this course explains the vulnerability, provides samples of the flaw, provides solutions to protect the application, and provides tests to check site security.

This course involves hands-on demonstrations of each potential vulnerability.

This course satisfies PCI Data Security Standard Requirements for custom software developer training.

Prerequisites: Students should be experienced Java developers.

Length: 2 days

Outline:

- Overview of the OWASP Project
- Top Ten
 - Cross Site Scripting
 - Injection Flaws
 - Malicious File Execution
 - Insecure Direct Object Reference
 - Cross Site Request Forgery
 - Information Leakage and Improper Error Handling
 - Broken Authentication and Session Management
 - Insecure Cryptographic Storage
 - Insecure Communications
 - Failure to Restrict URL Access
- Conclusion