

Secure Coding and Web App Pen Testing

Description

This two-day course is designed to introduce web application developers to the world of web application vulnerabilities through a combination of practical and thought exercises. The course leverages the Samurai WTF environment as a test lab, and primarily focuses on the execution and defensive measures for the OWASP Top 10 vulnerabilities.

Agenda

Day One:

- Introduction
- Standards & Guidelines
 - PCI
 - HIPAA
 - OWASP
 - Other
- Testing Methodology Overview
- Test Lab & Class Targets
- Vulnerabilities, Tools & Defenses
 - Injection
 - Cross-site Scripting
 - Broken Authentication

Day Two

- Vulnerabilities, Tools & Defenses (cont...)
 - Insecure Direct Object References
 - Sensitive Data Exposure
 - Missing Function Level Access Control
 - Cross-Site Request Forgery
 - Known Vulnerabilities
 - Redirects and Forwards
- Automated Scanners
- Testing Web Services
- Student Scavenger Hunt Challenge (with dojo-scavenger)