

Course title:

Hands on Web Application Testing: Assessing Web Apps the OWASP way.

Course Summary:

The goal of the training session is to teach students how to identify, test, and exploit web application vulnerabilities. The creator and project lead of the OWASP Live CD, now rebranded OWASP WTE, will be the instructor for this course and WTE will be a major component of the class. Through lecture, demonstrations, and hands on labs, the session will cover the critical areas of web application security testing using the OWASP Testing Guide v3 as the framework and a custom version of OWASP WTE as the platform. Students will be introduced to a number of open source web security testing tools and provided with hands on labs to sharpen their skills and reinforce what they've learned. Students will also receive a complementary DVD containing the custom WTE training lab, a copy of the OWASP Testing Guide, handouts and cheat-sheets to use while testing plus several additional OWASP references. Demonstrations and labs will cover both common and esoteric web vulnerabilities and includes topics such as Cross-Site Scripting (XSS), SQL injection, CSRF and Ajax vulnerabilities. Students are encouraged to continue to use and share the custom WTE lab after the class to further hone their testing skills.

Special Needs:

The training will include labs so laptops will be required by the attendees. A custom version of OWASP WTE will be provided to each student which will contain all the necessary tools and applications to test. Strictly speaking, Internet access and/or wireless won't be required since each laptop will be self-sufficient. However, Internet access may be useful for expounding on class discussion. The custom WTE lab environment will run on Windows, Mac OS X and Linux. A recent laptop with sufficient disk space and RAM to run a virtual machine will be required to run the labs. Both VMware and VirtualBox are supported.

Course Outline:

1. Day 1
  - a. Material
    1. Overview of the OWASP Testing Framework
    2. Information Gathering
    3. Configuration Management Testing
    4. Authentication Testing
  - b. 2 short breaks
  - c. 1 lunch break
  - d. Several demonstrations, mini-labs and one long lab
2. Day 2
  - a. Material
    1. Session Management Testing
    2. Authorization Testing
    3. Data Validation Testing
    4. Business Logic Testing
    5. Ajax Testing
  - b. 2 short breaks
  - c. 1 lunch break
  - d. Several demonstrations, mini-labs and one long lab