Web Application Penetration Testing - 2 Days

Description

This hands-on course will teach attendees a basic methodology (based on the OWASP ASVS 4.0 standard) for web application penetration testing and an introduction to the processes used. Students will walk through phases of a web application penetration test, including:

- Information Gathering
- Configuration Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Error Handling
- Automation Handling
- Injection Testing
- Logical Flaws Testing
- Weak Cryptography Testing
- Client Side Testing
- various tools and tactics used in each phase

The course is heavily focused on hands-on labs so that attendees have the opportunity to actually use common tools and techniques. By the end of the 2-day training, students will understand the structure of a web application penetration test and have the experience necessary to begin practicing the demonstrated toolsets.

Pre-requisites

Students are expected to have some prior knowledge of web applications (i.e. be familiar with URLs, web servers, proxies, etc), and some general IT experience. Familiarity with web programming languages and a basic understanding of security concepts is also useful. This is not an advanced security class, however students with little IT experience may struggle to keep up.

Student Equipment and Software Requirements

All students attending the training will need a laptop with a recent version of Burp Suite Community installed. OWASP ZAP can also be used, but the course examples will be provided using Burp Suite Community edition. Administrative rights are not required. No other commercial software is necessary.