Course Outline

Web Application Security Testing

Course Summary

Description

Custom built web applications are the security weak spot for most companies. Traditional IT security practices focus on firewalls, patching and hardening servers, virus scans, etc. While these are definitely important activities, hackers are often turning towards web applications as a means for attacking systems and stealing critical data. Securing these custom web applications is a challenging task.

This course covers all of the most common security weaknesses found in web applications. Students will learn how to look at their websites from a hacker's point of view, and will learn best practices for finding and resolving existing security vulnerabilities and building new web applications in a secure manner. The course contains unique and fun hands-on exercises to help students gain a fuller understanding of the concepts presented.

The focus of this course is on practical lessons that can be taken back and applied on the job. Students are given a methodology to use when conducting formal application security assessments, which covers how to do a thorough assessment, how to rate the risk of identified vulnerabilities, and how to compile the assessment results into an actionable report.

Topics

- HTTP 101
- Exploring Your Application
- Input Validation
- Session Management
- Authentication
- Securing the Logged-In Portion of Your Site
- Cryptography As It Applies to Web Applications

- Secure Website Configuration
- Google Hacking
- Web Application Security Products and Tools Overview
- Putting It All together – A Web Application Security Assessment Methodology
- Resources For Learning More

Audience

This course is designed for students looking for expert guidance on how to build an effective in-house application security assessment program and how to build security into your QA process

Prerequisites

The course contains coding examples in both Java and ASP.Net, but is not a programming course – web programming experience is helpful but not mandatory. Experience in working with websites, either as a QA analyst, security analyst, or developer is helpful for getting the most out of this course.

Duration

Two Days