CASP, Part 9 of 9: Assessments

Meet the expert: David Bigger is the lead trainer at Bigger IT Solutions. He has been information technology for a little over 20 years and has been training all over the US. He has worked with companies like US Military, Lockheed Martin, General Dynamics, Dominos Pizza, University of Utah and Expedia

Prerequisites: This course assumes that the student has familiarity with information technology and basic networking. The student should also be familiar with basic security concepts, whether through the CompTIA Advanced Security Practitioner Parts 1-6 or outside study. No scripting or “hacking” experience is required.

Runtime: 55:50

Course description: You made a new application last week, but is it secure? This course takes a look at Application security, specifically the things that might go wrong including Cross Side Scripting, SQL Injection attacks, and buffer overflows. But it won’t be all doom and gloom – this course will also take a look at some security frameworks and controls that can be put in place to better help protect applications from compromise. This course is part of a series covering the CompTIA Advanced Security Practitioner (CASP).

Course outline:

Vulnerability Scans
- Introduction
- Assessments
- Vulnerability Scans
- Scans
- When to Scan
- Requirements
- Summary

Penetration Tests
- Introduction
- Penetration Test
- Footprinting and Recon
- Scanning
- Enumeration
- Hacking
- Summary

Assessment Tools
- Introduction
- Methods and Tools for Assessment
- Port Scanners
- NMap
- Vulnerability Scanners
- Password Crackers
- Fuzzers
- PsTools
- Metasploit
- Summary