CASP, Part 6 of 9: Application Security

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 Part 1 course or outside study. No scripting or "hacking" experience is required.

Runtime: 01:32:01

Course description: Take a look at application security and put your development skills under a microscope. Specifically, explore all the things that might go wrong in your application development including cross-site scripting, SQL Injection attacks, and buffer overflows. But don't worry, it won't be all doom and gloom in this course. You'll also delve into some security frameworks and controls that can be put in place to help to better protect your applications from being compromised. This course is part of a series covering the CompTIA Advanced Security Practitioner (CASP).

Course outline:

Cross Site Scripting
• Introduction
• Application Security
• Terms
• Vulnerabilities
• XSS - Cross Site Scripting
• XSS
• XSS - What Can Happen?
• XSS - How?
• Defending Against XSS
• Summary

SQL Injection
• Introduction
• SQL Injection
• What Can Happen?
• What to Look for
• Defending SQL Injections
• Buffer Overflows
• Summary

Session ID
• Introduction
• Session IDs
• How to Get Session IDs
• Stop Taking My ID
• Summary

Controls
• Introduction
• Controls for Application Security
• Secure Coding Practices
• What Kind of Practices?

• WAF
• What Can a WAF Do
• Where a WAF Goes
• Code Reviews
• Summary

Security Frameworks
• Introduction
• Security Frameworks
• Standard Libraries
• OWASP
• ISO/IEC 27000
• WASC
• WS-Security
• Summary