

Course 1 - Overview & Security Best Practices

Industry Audience: Managers, Developers, QA, and doc writers.

Duration: 2.5 full days or 5 half days

Topics:

Overview of training & motivation for it

Trust & Risk

Security principles & requirements

System configuration & environment

Resource exhaustion

Trust management (technical; social engineering)

Course 2 - Input Validation and File System Security

Industry Audience: Developers, highly skilled QA (e.g. ones who write code)

Duration: 2.5 full days or 5 half days

Topics:

buffer overflows

format string vulnerabilities

code injection

input validation

randomness

file system security

Course 3 - Network Security

Industry Audience: Developers and Architects for firewalls, network IDS, penetration testing, VPN, and any other program that deals heavily in networking. People must have a sound background in network protocols to make use of this course.

Duration: 2.5 full days or 5 half days

Topics:

Network vulnerabilities at the physical layer, the link layer, network layer, and the transport layer. Covers spoofing, denial-of-service, man-in-the-middle, amplification, redirects, wireless, etc.