APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Secure Coding Fundamentals Training

Applied Technology Academy

Secure Coding Fundamentals is a hands-on, two-day foundational course that teaches developers to write defensible code. Students learn secure-coding concepts and terminology, how exploits work, and how to detect, attack and defend against the most dangerous software errors — from injection and cross-site scripting to broken authentication, XML External Entities and broken access control — mapped to the CWE/SANS Top 25.

LEVEL	DURATION	DELIVERY	LABS	PREREQUISITE
Basic / Foundational	**2 days**	**Instructor-led · live online or classroom**	**Hands-on labs & demos**	**Programming in one language**

Course Outline

- **Module 1: Bug Hunting Foundation**
  - Why hunt bugs, the language of cybersecurity, the changing threat landscape, an AppSec dissection of SolarWinds, the human perimeter, and interpreting the Verizon Data Breach Investigations Report. Labs & demos: a case study in failure.
- **Module 2: Moving Forward from Hunting Bugs**
  - Removing bugs using the CWE/SANS Top 25, the Web Application Security Consortium (WASC), CERT Secure Coding Standards, the Microsoft Security Response Center, and software-specific threat intelligence.
- **Module 3: Foundation for Securing Web Applications**
  - Principles of information security, security as a lifecycle issue, minimizing attack surface, layered defense, compartmentalization, considering all application states, and never trusting untrusted data.
- **Module 4: Bug Stomping 101**
  - Unvalidated data and buffer overflows; injection and SQL injection; broken authentication and session management; sensitive data exposure; XML External Entities (XXE); and broken access control — with hands-on defense labs.
- **Module 5: Bug Stomping 102**
  - Cross-Site Scripting (persistent, reflective and DOM-based); deserialization and vulnerable components; insufficient logging and monitoring; and spoofing and Cross-Site Request Forgery (CSRF) — with hands-on defense labs.

Prerequisites

Programming experience in at least one common programming language.

Learning Objectives

- Understand the concepts and terminology behind defensive, secure coding, including the phases and goals of a typical exploit
- Perform bug hunting and vulnerability testing safely and appropriately, and use organizational defect-reporting mechanisms
- Recognize common software exploits and the value of a multi-layered defense-in-depth approach
- Identify examples from the CWE Top 25 Most Dangerous Software Errors and their security consequences
- Identify untrusted data sources and the consequences of mishandling them (denial of service, XSS, injection)
- Detect, attack and defend authentication, authorization, XSS, injection, XXE, file-upload and access-control weaknesses
- Use code scanners, dynamic scanners and web application firewalls (WAFs) effectively, and implement robust testing strategies
- Harden web and application servers and identify resources for ongoing threat intelligence

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.