Course Outline

CertNexus Cyber Secure Coder (CNX0032)

Course Summary

Description

The stakes for software security are very high, and yet many development teams deal with software security only after the code has been developed and the software is being prepared for delivery. As with any aspect of software quality, to ensure successful implementation, security and privacy issues should be managed throughout the entire software development lifecycle.

This course presents an approach for dealing with security and privacy throughout the entire software development lifecycle. You will learn about vulnerabilities that undermine security, and how to identify and remediate them in your own projects. You will learn general strategies for dealing with security defects and misconfiguration, how to design software to deal with the human element in security, and how to incorporate security into all phases of development.

Objectives

At the end of this course, students will be able to:

- Identify the need for security in your software projects.
- Eliminate vulnerabilities within software.
- Use a Security by Design approach to design a secure architecture for your software.
- Implement common protections to protect users and data.
- Apply various testing methods to find and correct security defects in your software.
- Maintain deployed software to ensure ongoing security.

Topics

- Identifying the Need for Security in Your Software Projects
- Handling Vulnerabilities
- Designing for Security
- Developing Secure Code
- Implementing Common Protections
- Testing Software Security

Audience

This course is designed for software developers, testers, and architects who design and develop software in various programming languages and platforms, including desktop, web, cloud, and mobile, and who want to improve their ability to deliver software that is of high quality, particularly regarding security and privacy.

This course is also designed for students who are seeking the Cyber Secure Coder (CSC) Exam CSC-210 certification.

Prerequisites

This course presents secure programming concepts that apply to many different types of software development projects. Although this course uses Python®, HTML, and JavaScript® to demonstrate various programming concepts, you do not need to have experience in these languages to benefit from this course. However, you should have some programming experience, whether it be developing desktop, mobile, web, or cloud applications. ProTech provides a variety of courses covering software development that you might use to prepare for this course, such as:

- Python Programming: Introduction
- Python Programming: Advanced
- HTML5: Content Authoring with New and Advanced Features
- SQL Querying: Fundamentals (Second Edition)~

Duration

Three days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Course Outline

CertNexus Cyber Secure Coder (CNX0032)

Course Outline

I. Identifying the Need for Security in Your Software Projects
- A. Identify Security Requirements and Expectations
- B. Identify Factors That Undermine Software Security
- C. Find Vulnerabilities in Your Software
- D. Gather Intelligence on Vulnerabilities and Exploits

II. Handling Vulnerabilities
- A. Handle Vulnerabilities Due to Software Defects and Misconfiguration
- B. Handle Vulnerabilities Due to Human Factors
- C. Handle Vulnerabilities Due to Process Shortcomings

III. Designing for Security
- A. Apply General Principles for Secure Design
- B. Design Software to Counter Specific Threats

IV. Developing Secure Code
- A. Follow Best Practices for Secure Coding
- B. Prevent Platform Vulnerabilities
- C. Prevent Privacy Vulnerabilities

V. Implementing Common Protections
- A. Limit Access Using Login and User Roles
- B. Protect Data in Transit and At Rest
- C. Implement Error Handling and Logging
- D. Protect Sensitive Data and Functions
- E. Protect Database Access

VI. Testing Software Security
- A. Perform Security Testing
- B. Analyze Code to find Security Problems
- C. Use Automated Testing Tools to Find Security Problems

VII. Maintaining Security in Deployed Software
- A. Monitor and Log Applications to Support Security
- B. Maintain Security after Deployment

VIII. Appendix A: Mapping Course Content to Cyber Secure Coder (Exam CSC-210)

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically