



Course Content

Course Description:

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.

At Course Completion:

After completing this course, student 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.

Target Student:

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.

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.



Cyber Secure Coder

Course ID #: 7000-117-ZZ-Z

Hours: 21

Topics:

Lesson 1: Identifying the Need for Security in Your Software Projects

- Topic A: Identify Security Requirements and Expectations
- Topic B: Identify Factors That Undermine Software Security
- Topic C: Find Vulnerabilities in Your Software
- Topic D: Gather Intelligence on Vulnerabilities and Exploits

Lesson 2: Handling Vulnerabilities

- Topic A: Handle Vulnerabilities Due to Software Defects and Misconfiguration
- Topic B: Handle Vulnerabilities Due to Human Factors
- Topic C: Handle Vulnerabilities Due to Process Shortcomings

Lesson 3: Designing for Security

- Topic A: Apply General Principles for Secure Design
- Topic B: Design Software to Counter Specific Threats

Lesson 4: Developing Secure Code

- Topic A: Follow Best Practices for Secure Coding
- Topic B: Prevent Platform Vulnerabilities
- Topic C: Prevent Privacy Vulnerabilities

Lesson 5: Implementing Common Protections

- Topic A: Limit Access Using Login and User Roles
- Topic B: Protect Data in Transit and At Rest
- Topic C: Implement Error Handling and Logging
- Topic D: Protect Sensitive Data and Functions
- Topic E: Protect Database Access

Lesson 6: Testing Software Security

- Topic A: Perform Security Testing
- Topic B: Analyze Code to find Security Problems
- Topic C: Use Automated Testing Tools to Find Security Problems

Lesson 7: Maintaining Security in Deployed Software

- Topic A: Monitor and Log Applications to Support Security
- Topic B: Maintain Security after Deployment