Secure Coding

UWF Florida Cybersecurity Training Program
Offered by the University of West Florida Center for Cybersecurity

Course Overview

Course / Cyber Skills Exercise Dates: Oct 21– Nov 1, 2024

Duration: 14 days

Estimated Time Commitment: 14 hours per week

Instructional Hours: 15 Contact Hours

Delivery Format: Asynchronous online

Target Audience: Courses: IT and Cybersecurity practitioners

Required Prerequisites / Background: Students from any background is welcome, some prior knowledge of Cyber Security and coding useful but not essential

CEUs: 1.5, **CPEs:** 18

Course Instructor(s):

Instructor	Email
Stephen Hopkins, CISSP	shopkins@uwf.edu

Course Description

Desktop, web-based, and mobile device applications leverage the local device and the internet to create, modify, update, and delete data. Security flaws in the software development process provides vulnerabilities which attacks can leverage to cause confidentiality, integrity, and availability issues. This course covers secure software development including methodologies and resources to raise the level of software security. The course includes discussions on the OWASP top ten issues with internet integrated applications. This course uses a combination of lectures, discussions, and activities. The course will provide examples which provide the basis for firsthand practice opportunities.

NIST NICE Cybersecurity Workforce Framework Mapping

The course prepares for the following cybersecurity work roles as defined by the NICE Cybersecurity Workforce Framework. NIST's Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

Cybersecurity Work Roles and Categories:

Lifecycle Phase	Work Role
Design	SP-ARC-002 | Security Architect
Build	SP-DEV-001 | Software Developer
Deploy	OM-NET-001 | Network Operations Specialist
Operate	OM-STS-001 | Technical Support Specialist
Maintain	OM-DTA-001 | Database Administrator
Decommission	OV-LGA-001 | Cyber Legal Advisor

Course Information

Materials:

The uses the Canvas learning management system (LMS) for assignments, grading, and instructor-student communication.

This course uses a variety of materials. The instructor will provide all course materials through the Canvas LMS.

The instructor will identify some online resources during the lectures and exercises.

Technical Specifications:

Reliable high speed Internet connection | Computer with up-to-date browser.

Students should have a computer with microphone, speakers, camera (optional), capable of running Zoom sessions.

By enrolling for this course, I agree to abide by the Computing Resources Usage Agreement provided to me.

Grading:

Participants will be assigned a pass/fail grade. Participants must earn a total of 70% or higher on graded assessments to earn a passing grade.

Assessment	Percentage
Security Requirements Exercise	12.5

Risk Management Exercise	12.5
Security Threat Exercise	12.5
Use and Abuse Modeling Exercise	12.5
Threat Modeling Exercise	12.5
Operating System Hardening Exercise	12.5
Secure Software Exercise	12.5
Discussions	12.5
Total:	**100%**

Course Overview / Schedule

Modules and Lessons	Assessment
Module 1 Secure Software Introduction and Gathering Software Requirements	Security Requirements Exercise Discussions
Module 2 Risk Management	Risk Management Exercise Discussions
Module 3 Designing Secure Software Applications	Security Threat Exercise Discussions
Module 4 Testing Software Applications	Use and Abuse Modeling Exercise Discussions
Module 5 Implementing Secure Software Applications	Threat Modeling Exercise Discussions
Module 6 Programming Languages, Operating Systems, and Databases	Operating System Hardening Exercise Discussions
Module 7 OWASP Top 10	Secure Software Exercise Discussions