SecureCoding

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

Course Overview

Course Dates: Oct 21– Nov 1, 2024

Duration: 14 days

Instructional Hours: 15 contact hours

Delivery Format: Asynchronous online (courses)

Target Audience: Courses: IT and Cybersecurity practitioners or staff;
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
Dr. Hossain Shahriar	hshahriar@uwf.edu

Course Description

As cyberattacks are growing in numbers, many of the attacks are exploiting code level vulnerabilities. Further, the increased reliance on software outsourced from vendors and third parties are putting organizations and stakeholders more vulnerable to attacks. This course will cover the basics of secure application development principles. It will focus on OWASP top 10 bugs that can be found widely in open or closed source system, followed by some of the common tools that are available to detect them early. The course will provide examples and hands on practice opportunities.

Student Learning Outcomes: At the end of this course, students will be able to:
- Describe common secure programming principles
- Explain how attackers can exploit code level vulnerabilities
- Apply defense techniques to early detect vulnerabilities and best practices

The course addresses cybersecurity work roles as identified in NIST's Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

Cybersecurity Work Roles and Categories:
- Vulnerability Assessment Analyst (Protect and Defend, PR-VAM-001)
- Cyber Defense Infrastructure Support Specialist (Protect and Defend, PR-INF-001)
- Threat/Warning Analyst (Analyze, AN-EXP-001)
- Exploitation Analyst (Analyze, AN-TWA-001)
- Target Network Analyst (Analyze Targets, AN-TGT-002)
- Data administration (Operate and Maintain, OM-DTA-001)
- Data analyst (Operate and Maintain, OM-DTA-002)

Learning Outcomes mapped to the NICE Cybersecurity Workforce Framework Tasks:
Upon completion of the course, students will be able to:
- Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile (T0019)
- Develop content for cyber defense tools (T0020)
- Build, test, and modify product prototypes using working models or theoretical models (T0021)
- Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion (T0027)
- Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis (T0036)
- Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications (T0042)
- Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions (T0045)
- Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced. (T0046)
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation (T0047)
- Design and develop cybersecurity or cybersecurity-enabled products (T0053)
- Implement specific cybersecurity countermeasures for systems and/or applications (T00123)

Knowledge and Skills required to fulfill the above tasks mapped to the NICE Cybersecurity Workforce Framework:
- Knowledge of cyber threats and vulnerabilities (K0005)
- Knowledge of analytic tools and techniques for language, voice and/or graphic material(K0356)
- Knowledge of analytical standards and the purpose of intelligence confidence levels. (K0358)

- Knowledge of programming concepts (e.g., levels, structures, compiled vs. interpreted languages)(K0372)
- Knowledge of cyber intelligence/information collection capabilities and repositories (K0409)
- Knowledge of computer programming principles (K0016)
- Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions (K0046)
- Knowledge of current and emerging cyber technologies (K0335)
- Knowledge of access authentication methods (K0336)
- Explain various concepts of host hardening (K0205, S0121))
- Explain concepts and techniques of perimeter security (K0561, S0192)
- Knowledge of threat and/or target systems (K0604)
- Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities (K0106)
- Skill in identifying cyber threats which may jeopardize organization and/or partner interests (S0229)
- Skill in conducting trend analysis (S0169)

Course Information

Materials: All course materials will be provided by the instructor free of cost; the following are some online resources

- Cybersecurity: https://www.w3schools.com/cybersecurity/index.php
- IDE: https://colab.research.google.com/
- Python: https://www.w3schools.com/python/
- Matplotlib: https://www.w3schools.com/python/matplotlib_intro.asp
- Pandas: https://www.w3schools.com/python/pandas/default.asp

Machine learning: https://www.w3schools.com/python/python_ml_getting_started.asp

Technical Specifications:

Access to reliable internet and computer; the course will use Google Colab platform which will requires having Gmail account to create/reuse existing account of the learners; By enrolling for this course, I agree to abide by the Computing Resource Usage Agreement provided to me.

By enrolling for this course, I agree to abide by the Computing Resource 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
Assignment (5)	100%
Total:	**100%**

Course Overview / Schedule

Modules and Lessons	Assessment
Unit 1 - Course Overview: overview of secure app development;	Assignment 1
Unit 2 – OWASP top 10 common security problems for web app	Assignment 2
Unit 3 – Mitigation approaches for web app – static code analysis, dynamic analysis; Hands-on practice.	Assignment 3
Unit 4 – Secure coding practices for mobile app, DevOps, hands-on	Assignment 4
Unit 5 – Secure design, best practice guidelines	Assignment 5

uwf.edu/cybersecurity