Module 4. Software Security

Module Learning Objectives

This module allows students to explore various aspects of software security. Students will learn about major software vulnerabilities and how they can be exploited. By learning security best practices in each phase of software development life cycle, students will develop the build-security-in mentality. Furthermore, students will acquire knowledge and skills in defending, preventing, and mitigating software security threats.

Module Student Learning Outcomes

Upon completion of this module, students will be able to:

- Demonstrate in-depth understanding of various software vulnerabilities.
- Clearly describe different types of software security attacks.
- Illustrate techniques to strengthen software security at each phase of software development life cycle.
- Describe the characteristics of secure programming
- Implement the learned software security mentality/best practice in software development.
- Describe security issues associated with web-based systems.

Module design:

Submodule 1: System Security
• Operating System Security
• File System Security
Submodule 2: Low-level Attacks and Defense
• Lower-level attacks and exploits
• Defend low-level exploits
Submodule 3: Secure Programming
• Security requirements
• Defensive programming
• Secure programming practice
Submodule 4: Web-based System Security
• Web application technologies
• Web application vulnerabilities and attacks
• Secure web-based systems
• Web system attacks lab