95-748: Software and Security

Spring 2022

Instructor: Hasan Yasar
hyasar@cmu.edu, 412.268.9219

TA: Ashish Kaushik
ashishka@andrew.cmu.edu

Nicholas Bellante
nbellant@andrew.cmu.edu

Location and Time: HBH 1206, Mondays 6:20 PM - 9:10 PM

Course Description: This course exposes students with limited exposure to programming and software engineering development foundational concepts to enable further understanding of the challenges of insecure and vulnerable software. Students are exposed to basic programming constructs (such as variables, control structures, data structures, programming syntax) as well as the basic principles of object-oriented programming languages. The course also surveys the types of threats and vulnerabilities inherent in software and the origins of these deficiencies. A brief overview of secure coding concepts, principles and techniques are provided to students to provide exposure to how software can be made more secure and resilient and how security can be part of overall software development process.

Textbook: (Optional) Software Security - Building Security In, Author: Gary McGraw, ISBN: 0321356705

Assignments and Grading:

Final course grade:	10%	Participation
	20%	Quizzes
	30%	Assignments
	40%	Final Exam

Participation: Students are expected to participate in class activities and discussions.

Quizzes: Quizzes will be administered through canvas and will occur weekly. Students has to take quiz at the class

Homework: Homework assignments will be available via canvas. Homework is due on the date specified.

Course Policies:

Late Assignment: Assignment will be accepted up to 3 days late. The maximum grade for the assignment will decrease by 10% for each day late.

Collaboration: Students are encouraged to talk with each other, the TAs, and the instructor about the course and any assignments. Any assistance, though, must be limited to discussion of the problem and sketching general approaches to a solution. Each student must write out his or her own solutions to all problems, unless otherwise stated by the instructor. Consulting another student's or group's solution is prohibited, and submitted solutions may not be copied in any part from any source unless properly cited. These and any other form of unauthorized collaboration on assignments constitute cheating. If you have any questions about whether some activity would constitute cheating, please feel free to ask.

Academic Dishonesty: All instances of cheating or plagiarism will be dealt with according to the "CMU Policy on Cheating and Plagiarism," which can be found at: *http://www.cmu.edu/policies/documents/Cheating.html*. Policy violations will be dealt with on a case-by-case basis. Potential penalties include, but are not limited to, zero credit for the assignment and/or failure of the course.

Course Schedule:

Key Dates:
Jan 24th, Class Begins
Jan 31st - Project Announcement
March 2nd, Project Due
March 4th , Final Exam

Course Topics: The following is a brief list of potential course topics:

- Software Security Problems, Principles and Secure Risk Management Framework
- Set of Software Security Best practices
- Secure Software Design and Development
- Software Security in Enterprise Business

Learning Objectives;

- Investigate Software Security Problems and understand Principles and Secure Risk Management Framework
- Understand Set of Software Security Best practices
- Understand and practices Secure Software Design and Development practices
- Learn How to implement Software Security in Enterprise Business

Lectures Plan:

- *Jan 24th – Week -1*: Introduction, Software Security Problems
- *Jan 31st – Week -2*: Software Assurance Model: Risk Management Framework (Ch2), Security Best practices/ Known Security Flaws (Application – Low Level Vulnerabilities)
- *February 7th – Week -3*: Security Flaws – Application Low Level Vulnerabilities, Web applications, Cryptographic/Access controls, Networking
- *February 14th – Week-4*: Low level Vulnerabilities, Web applications, Cryptographic /Access controls, Networking and Web applications vulnerabilities,
- *Feb 21st – Week -5:* Secure Software Design and Development, Security Testing (Penn testing, Risk- Based Security Testing (Code Review, Architecture Risk Analysis – Ch3, 4,5,6,7)
- *Feb 28th – Week-6*: Security Testing (Abuse Cases- Operational testing – Ch8,9) Software Security in Enterprise Business/ Large Scale Software Development (Ch10), Review
- *March 4th :* Final Exam