Information Systems Department
University of Maryland Baltimore County
Baltimore Maryland 21250
Departmental Office: room ITE 404 ph. 410-455-3206

IS 472-01 Software Security Fall 2017

Important Information:

Meets:	Tuesdays and Thursdays, 11:30am-1pm, in ITE 469
Professor:	Dr. Carolyn Seaman
Office:	ITE 404B
Phone:	410-455-3937
Email:	cseaman@umbc.edu
Office hours:	Wednesdays 10-11:30 and Fridays 12-3, and by appointment
Required text:	Secure Software Development by Jason Grembi, Cengage Learning
	(other required readings will be provided by the instructor)

Course Description

Many cybersecurity attacks are facilitated by software vulnerabilities, i.e. characteristics of software source code that unintentionally allow unauthorized access to computer memory. Future cybersecurity professionals require an understanding of various techniques that can be applied throughout the software development lifecycle to prevent, detect, and remove such vulnerabilities. Through this course, students will: 1) Develop an understanding of common vulnerabilities and emerging attacks; 2) Learn how to apply secure coding standards and techniques to ensure that their source code is as free from vulnerabilities as possible; 3) Be provided hands-on experience in identifying and preventing software vulnerabilities.

Prerequisite: IS 247

Learning Objectives:

After successfully completing this course, students should:

- Understand how each phase of the Software Development Life Cycle (SDLC) contributes to developing secure software
- Understand how software vulnerabilities are exploited in cyber attacks
- Be able to apply secure coding principles
- Be able to apply techniques in design, coding, quality assurance, and maintenance, for producing secure software
- Understand the published standards in place for secure software development

Instructional Methods:

Typically, class sessions are of two types: lecture/discussion and in-class exercises. In addition, there will be several guest lectures throughout the semester, given by outside experts in particular topics. Lecture/discussion classes will consist of a lecture delivered by the instructor, with multiple opportunities for participation and discussion from all students in the class. Active participation in discussions is expected. In-class exercises will involve hands-on work practicing techniques and skills. Exercises are explained in more detail below.

Blackboard site

A Blackboard site will be maintained for the course throughout the semester. The site will contain all **announcements** pertinent to the course, as well as all class materials, handouts, and assignments. You will also use the Blackboard site to submit most assignments. **Each student is responsible for checking the site regularly, and for being aware of any information posted there.** In particular, it is advised that you check the Blackboard site on the day before each class in order to download any handouts you will need during class, and any information about preparing for class.

Office Hours

Every student is strongly encouraged to make use of office hours. I am willing to go over anything you are having problems with, or to discuss any issues having to do with the course or the program. My official office hours are listed above, but I am also available by appointment, which means that you should call or email me before stopping by my office to make sure that I will be in if it's outside of the stated office hours. Please feel free to discuss things with me via email and phone as well. I check both numerous times each day and will respond promptly. I cannot guarantee that I will check my messages on the weekend, but I often do.

Class Preparation and Student Success

All of the reading assignments should be completed before the class in which the material is to be discussed. Students should expect that for every 3 credit hour course they are devoting at least 9 additional hours preparing and studying course materials which are required or suggested. Quizzes at the beginning of class are meant to motivate you to come to class prepared. Above all, do not fall behind on the exercises, as most of them build on previous exercises. Students should come see me if they need additional guidance or advice about how to succeed in this course.

Grading

The University's Undergraduate Catalogue states that, "A, indicates superior achievement; B, good performance; C, adequate performance; D, minimal performance; F, failure". There is specifically no mention of any numerical scores associated with these letter grades. Consequently, there are no pre-defined numerical boundaries that determine final letter grades. These boundaries can only be defined at the end of the semester after all scores have been earned. At that point, numerical boundaries for final letter grades can be defined (usually using a "curve"). This means that it is not appropriate to assume that a given numerical score corresponds to a particular letter grade. It is also important to understand that final letter grades reflect academic achievement and not effort.

While I am more than happy to correct mistakes in the computation of grades and grade recording errors, in all other situations final letter grades are not negotiable.

Your final course grade will be based on scores received on three exams, reading quizzes, and in-class exercises, as follows:

- Exams (3) – 15% each
  There will be three exams occurring throughout the semester (see the Schedule, below). All will be take-home, open-book, essay question exams. See Policies, below, for my rules about missing exams.

- Quizzes – 10%
  There will be a minimum of 5 quizzes during the course of the semester (probably more). The quizzes will be in-class, closed-book, and unannounced. Each quiz will be given at the beginning of the class

session, and the topic of the quiz will be limited to what was covered in the assigned reading for that day. The objective of the quizzes is to motivate students to attend class, arrive on time, be prepared for class, and keep up with the assigned reading. I will drop each student's lowest quiz grade in calculating the final grade for the semester. See Policies, below, for my rules about missing quizzes.

- In-class exercises – 45%
  There will be several in-class exercises over the course of the semester (see the Schedule on Blackboard). Each exercise will involve the application of some software engineering or coding technique for creating secure software. The exercises will be cumulative, in that each will contribute to a single software artifact that will be complete at the end of the semester. Some exercises will also involve reviewing other students' work. I will drop each student's lowest exercise grade in calculating the final grade for the semester.

Student Disability Services (SDS)

UMBC is committed to eliminating discriminatory obstacles that may disadvantage students based on disability. Services for students with disabilities are provided for all students qualified under the Americans with Disabilities Act of 1990, the ADAA of 2009, and Section 504 of the Rehabilitation Act who request and are eligible for accommodations. The Office of Student Disability Services (SDS) is the UMBC department designated to coordinate accommodations that would allow for students to have equal access and inclusion in their courses.

If you have a documented disability and need to request academic accommodations, please refer to the SDS website at sds.umbc.edu for registration information or visit the SDS office in the Math/Psychology Building, Room 212. For questions or concerns, you may contact us at disAbility@umbc.edu or (410) 455-2459. If you require accommodations for this class, make an appointment to meet with me to discuss your SDS-approved accommodations.

Policies

1. ***Due Dates***
   All assignments are due at the beginning of class on the date listed in the class schedule.

2. ***Missing exams***
   In general, if you miss the deadline to submit an exam, you will receive a grade of 0 for the exam. If you know that you will need an extension in advance, come talk to me about it. **If** I am given sufficient notice, and I agree that the extension is absolutely necessary, then I will extend your deadline. If you miss the deadline due to an unforeseen emergency, then we can arrange an extension **if** I agree that you have a bona fide emergency and you can document that emergency to my satisfaction.

3. ***Missing quizzes***
   If you miss a quiz, you can make it up with a 50% penalty. That is, you will only get credit for half of whatever score you get on the quiz. The quiz must be made up as soon as possible after the class on which it was originally given, ideally the same day or at the latest before the next class. If too much time passes after the quiz was given in class before you request a make-up, I will not allow you to take the make-up and you will get a 0 for the quiz. If you arrive late to class, and a quiz is already in progress when you arrive, you can begin the quiz when you arrive, but must turn it in at the same time as the rest of the class, or you can make it up after class for a 50% penalty, your choice.

4. ***Missing in-class exercises***
   Because of the nature of the in-class exercises, completing them outside of class is more difficult. Generally, exercises will be due at the beginning of the following class period (because it's not always

possible to complete them before the end of a class), and this is true for all students, whether they were in class for the exercise or not. Students absent from class will be responsible for downloading the relevant materials from Blackboard, figuring out how to complete the exercise on their own, and submitting it before the next class. This is more difficult than just coming to class and getting it done.

5. Coming late to class

There is no specific penalty for coming late to class, except the potential to miss quizzes. However, nothing said or done in the first part of the class will be repeated for latecomers. If a student's late arrival to class is disruptive in any way, that student will be asked to leave the classroom.

6. Academic Dishonesty

By enrolling in this course, each student assumes the responsibilities of an active participant in UMBC's scholarly community in which everyone's academic work and behavior are held to the highest standards of honesty. Cheating, fabricating, plagiarism, and helping others to commit these acts are all forms of academic dishonesty and they are wrong. Academic misconduct could result in disciplinary action that may range from a grade of 0 on the relevant assignment or failure of the entire course, to suspension or dismissal from the program. Full policies on academic integrity should be available in the UMBC Student Handbook, Faculty Handbook, or the UMBC Directory.

In particular, for this course:

- No cheating will be tolerated on the exams or on quizzes. Cheating includes gaining specific information about the quiz before taking it (e.g. in the case of a make-up), as well as consulting unauthorized materials during the quiz or exam. It also includes taking an online quiz while absent from class.
- Plagiarism applies to the in-class exercises and exams. All work submitted for these assignments must be created by the students submitting the work. Please see the clarification below about working together.
- Academic dishonesty also includes interfering with another student's work or aiding another student to commit academic dishonesty.

7. Working together

I encourage students to work together on in-class exercises. In this context "working together" means sharing ideas, asking and answering questions, and showing your work to other students. It does NOT include cutting and pasting another student's work into your own exercise, or allowing another student to cut and paste your work. If you use ideas or code suggested by another student, make sure you understand how it works, as you will be responsible for explaining it, and for building on it in future exercises.

In the context of the exams, you are free to discuss the exam, the exam questions, and potential answers with other students, but again, there can be no copying of actual words or text or code from another student. What you turn in on the exam must be your own work.

Schedule

Updates to the schedule over the course of the semester will be announced in class and reflected on the schedule on Blackboard. Below is the initial version of the schedule. I will avoid changes if at all possible, but if I have to make a change I will let you know well in advance.

Last updated 8/25/2017

Date	Topic	Activity	Reading	Due Today
Thursday, August 31, 2017	Course introduction	Syllabus quiz		
Tuesday, September 5, 2017	Tool Environment	In-class exercise		
Thursday, September 7, 2017	Tool Environment (cont.)	In-class exercise		Exercise 1
Tuesday, September 12, 2017	Software engineering basics	Lecture/discussion	Chapter 2	
Thursday, September 14, 2017	Security basics	Lecture/discussion	Chapters 1,3 from Grembi and Chapter 3 from McGraw (on Blackboard)	Application quiz
Tuesday, September 19, 2017	Banking application			
Thursday, September 21, 2017	Requirements gathering	Lecture/discussion	Chapter 5	
Tuesday, September 26, 2017	Use/abuse cases	In-class exercise		
Thursday, September 28, 2017	Design	In-class exercise	Chapters 6-7	Exercise 2
Tuesday, October 3, 2017	Coding practices	Lecture/discussion	Chapters 8-9	Exercise 3
Thursday, October 5, 2017	Blacklist characters	In-class exercise		
Tuesday, October 10, 2017	HTML stripping	In-class exercise		Exercise 4
Thursday, October 12, 2017	SQL Injection	In-class exercise		Exercise 5
Tuesday, October 17, 2017	Build automation and CI	Lecture/discussion		Exam 1; Exercise 6
Thursday, October 19, 2017	Exceptions	In-class exercise		
Tuesday, October 24, 2017	Passing object parameters	In-class exercise		Exercise 7
Thursday, October 26, 2017	Logging	In-class exercise		Exercise 8
Tuesday, October 31, 2017	Testing	Lecture/discussion	Chapter 10	Exercise 9
Thursday, November 2, 2017	Testing	In-class exercise		
Tuesday, November 7, 2017	Guest lecture			Exercise 10
Thursday, November 9, 2017	no class	Work on Exam 2		
Tuesday, November 14, 2017	Standards	Lecture/discussion	Shoemaker and Sigler reading	Exam 2
Thursday, November 16, 2017	Reviews	Lecture/discussion	McGraw	
Tuesday, November 21, 2017	No class			
Thursday, November 23, 2017	No class			
Tuesday, November 28, 2017	Reviews	In-class exercise		
Thursday, November 30, 2017	Maintenance	Lecture/discussion	Chapter 11	Exercise 11
Tuesday, December 5, 2017	Maintenance	In-class exercise		
Thursday, December 7, 2017	TBD	Guest lecture		Exercise 12
Tuesday, December 12, 2017	Wrapping up	Lecture/discussion		Exam 3