**CS 763 Secure Software Development**

**Department of Computer Science**

**Metropolitan College**

**Boston University**

**Spring 2021 Syllabus**

**Instructor Information**

|  |  |  |
| --- | --- | --- |
|  | Name: Yuting Zhang  Office: 1010 Commonwealth ave, Rm 322  Email: danazh at bu dot edu  URL: [http://people.bu.edu/danazh](http://www.merrimack.edu/yzhang) |  |

**Course Information**

**Lecture time and location**

Tuesday 6:00-8:45, FRC L132

**Prerequisites**

At least two 500- level (or above) computer programming-intensive science courses or instructor’s consent. As this is an advanced 700 level course, you should be familiar with programming and software development.

**Reference Books:**

Gary McGraw. Software Security: Building Security In. Addison-Wesley Professional; 1 edition (February 2, 2006)

Michael Howard, David LeBlanc,John Viega . 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them (Networking & Comm - OMG). McGraw-Hill Education; 1 edition (September 24, 2009)

Wenliang Du, Computer & Internet Security: A Hands-on Approach 2nd Edition. May 1, 2019.

Additional Books:

Ross Anderson. Security Engineering. Wiley. 2 edition. (<https://www.cl.cam.ac.uk/~rja14/book.html>)

Mathias Paye. Software Security Principles, Policies, and Protection. (January 2019, v0.33) (<https://nebelwelt.net/SS3P/softsec.pdf>)

*Other Reading Materials*

* Microsoft Secure Development Life Cycle:<https://www.microsoft.com/en-us/sdl/>
* OWASP SAMM Project: <https://www.owasp.org/index.php/OWASP_SAMM_Project>
* OWASP TOP 10:<https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project>
* Developer Guide:<https://www.owasp.org/index.php/Category:OWASP_Guide_Project>
* Testing Guide:<https://www.owasp.org/index.php/Category:OWASP_Testing_Project>
* Secure Coding Practice Guideline:<https://security.berkeley.edu/secure-coding-practice-guidelines>
* Seed Labs: <https://seedsecuritylabs.org/>

**Please find more reference materials on the course blackboard website (**[https://onlinecampus.bu.edu](https://lms.bu.edu/)) **(under the Content/References folder)**

**Description**

Overview of techniques and tools to develop secure software. Focus on application security. Topics include secure software development processes, threat modeling, secure requirements and architectures, vulnerability and malware analysis using static code analysis and dynamic analysis tools, vulnerabilities in C/C++ and Java programs, Crypto and secure APIs, vulnerabilities in web applications and mobile applications and security testing. Hands-on lab and programming exercises using current tools are provided and required. 4 credits.

**Objectives**

At the end of the semester, students are expected to

* Explain secure software development process and activities in the process.
* Explain risk management and threat modeling and identify security risks in real world projects.
* Identify common vulnerabilities and corresponding mitigations in C/C++ and Java programs.
* Explain basic cryptographic mechanisms and use right crypto APIs properly.
* Identify common vulnerabilities and corresponding mitigations in web applications and mobile applications.
* Design and conduct security testing for real world applications.

**Course Requirements**

* Class participation
* Reading and study
* Assignments
  + 4 Labs
  + 3 Written Homeworks
  + Final Project
* Quizzes and Exams

**Class Schedule**

(This is a tentative class schedule. It is subjected to change according to the progress of the class and the feedback of the student.)

|  |  |  |  |
| --- | --- | --- | --- |
| Class  # | Date | Topics | Assignments |
| 1 | 01/26 | Intro, Secure Software Process, Risk management | Written HW1 (01/26-02/09) |
| 2 | 02/02 | Security Concepts, Principles,  Threat modeling, Secure Requirements and design | Final Project is assigned |
| 3 | 02/09 | Code Review, static code analysis, dynamic code analysis | Lab 1  (02/09 - 02/23) |
|  | 02/16 | No class, Monday schedule. | |
| 4 | 02/23 | Vulnerability Taxonomy | HW2  (02/23- 03/09) |
| 5 | 03/02 | C/C++ Programs Vulnerabilities:  memory management, buffer overflow program, integer overflow, string termination problem | Lab 2 (03/02-03/16) |
| 6 | 03/09 | Java Programs Vulnerabilities: visibility issue, reference issue,inner class, reflection, mutability issues, serialization issues |  |
| 7 | 03/16 | Crypto basics: symmetric and asymmetric encryption schemes, key management, how crypto is used to provide confidentiality and authentication | Lab3 (03/16-03/30) |
| 8 | 03/23 | Crypto usage and Misuses: SSL and HTTPS, disk/file encryption, data protection. vulnerabilities (weak passwords, weak random number, insecure crypto functions etc) |  |
| 9 | 03/30 | Browser security mechanism,  Mobile security mechanisms | HW3 (03/30-04/13) |
| 10 | 04/06 | OWASP Top 10, SQL injections, XSS, etc | Lab4 (04/06-04/20) |
| 11 | 04/13 | Penetration Testing |  |
| 12 | 04/20 | Risk-based Security Testing |  |
| 13 | 04/27 | Review/Student Project Presentations | Project is Due |
| 14 | 05/07 | Final Exam |  |

**Spring 2021 COVID-19 Policies**

**Compliance:** All students returning to campus will be required, through a digital agreement, to commit to a set of Health Commitments and Expectations including face coverings, symptom attestation, testing, contact tracing, quarantine, and isolation. The agreement makes clear that compliance is a condition of being a member of our on-campus community.

You have a critical role to play in minimizing transmission of COVID-19 within the University community, so the University is requiring that you make your own health and safety commitments. Additionally, **if you will be attending this class in person, you will be asked to show your Healthway badge on your mobile device to the instructor in the classroom prior to starting class, and wear your face mask over your mouth and nose at all times.** If you do not comply with these rules you will be asked to leave the classroom. If you refuse to leave the class, the instructor will inform the class that they will not proceed with instruction until you leave the room. If you still refuse to leave the room, the instructor will dismiss the class and will contact the academic Dean’s office for follow up.

Boston University is committed to offering the best learning environment for you, but to succeed, we need your help. We all must be responsible and respectful. If you do not want to follow these guidelines, you must participate in class remotely, so that you do not put your classmates or others at undue risk. We are counting on all members of our community to be courteous and collegial, whether they are with classmates and colleagues on campus, in the classroom, or engaging with us remotely, as we work together this fall semester.

**Course Policies**

**Grading Policy**

The grade that a student receives in this class will be based on class participation, in-class exercise, quizzes, project and the exam. The grade is breakdown as shown below. All percentages are approximate and the instructor reserves the right to make necessary changes.

* 5% on the class participation
* 42% on written & lab assignments
* 13% on the final project
* 10% on quizzes
* 30% on the final exam

Letter grade/numerical grade conversion is shown below:

A (95-100) A- (90-94)

B+ (85-89) B (80-84) B- (79-77)

C+ (74-76) C (70-73) C- (65-70)

D (60-65) F (0 – 59)

**Attendance Policy**

Attendance is expected at all class meetings. You are responsible for all materials discussed in class. In general, no makeup quizzes and exams will be given unless an extremely good, verifiable reason is given in advance.

**Assignment Late Policy**

Every assignment has a due date. The late assignments will be penalized within a week with **3 points per day**. No assignments will be accepted one week after the deadline. It is the students' responsibility to keep secure backups of all assignments.

**Academic Integrity**

Academic conduct in general and MET College rule in particular require that all references and uses of the work of others must be clearly cited. All instances of plagiarism must be reported to the College for action. *For the full text of the academic conduct code, please check*<http://www.bu.edu/met/for-students/met-policies-procedures-resources/academic-conduct-code/>.