Course Syllabus

Computer Science and Engineering

CS-GY 9163-Application Security

Course Information

Course Pre-requisites

- Graduate Standing

Course Description

This online course addresses the design and implementation of secure applications. Concentration is on writing software programs that make it difficult for intruders to exploit security holes.

Course Objectives

By the end of this course students should be able to:

- Describe security threats faced in different application environments including software, web, database, cloud, and mobile.
- Incorporate measures to reduce the risk of application security breach.
- Locate resources that are up to date to address emerging application security issues.

Course Structure

This course is conducted entirely online, which means you do not have to be on campus to complete any portion of it. You will participate in the course using NYU Classes located at https://newclasses.nyu.edu.

Grading Breakdown

- Unit Assignment 1: 20%
- Unit Assignment 2: 20%
- Unit Assignment 3: 20%
- Unit Assignment 4: 20%
- Unit Assignment 5: 20%

Weekly Structure

Week	Topics	Readings	Assignment
1	Version control, build control, linter, test frameworks, CI/CD, packaging	Text: Ch 1 Common Threads	Unit 1 Part 1
2	Code reviews, fuzzing, static analysis		Unit 1 Part 2
3	Attack basics (Buffer memory, memory, stack) and defences	Text: Ch 5	Unit 1 Part 3

4	Browser security model, HTTP, content rendering, isolation, communication, navigation, security user Interface and cookies	Text: Ch 17 HTTP	Unit 2 Part 1
5	Session management and user authentication, content security policies, web workers, and extensions	Text: Ch 17 State & HTTP Authentication	Unit 2 Part 2
6	Cross Site Scripting, CSRF and metacharacter vulnerabilities	Text: Ch 17 Common vulnerabilities Text: Ch 8 Metacharacter filtering	Unit 2 Part 3
7	Fall Break		

Week	Topics	Readings	Assignment

8	Basics of databases, access control, privileges and views in Databases, techniques for encrypting sensitive information in databases, threats to ecommerce transactions, protecting data integrity and ensuring accessibility.		Unit 3 Part 1
9	Logging and recovery, ARIES & logging, key-value database		Unit 3 Part 2
10	Docker, PID, Mount, Network, UTS, IPC, User; cgroups; capabilities; seccomp; container image scanning and signing and authorization plugins.		Unit 4 Part 1
11	Kubernetes, Notary/TUF, SPIFFE, ISTIO, OPA		Unit 4 Part 2
12	Core security concepts, platform and trends, Threat categories, system architecture and defenses.	Watson (2012)	Unit 5 Part 1
13 & 14	Device controls, privacy controls, system security, encryption & data protection, app security		Unit 5 Part 2

15	Finals Week		

Learning Time Rubric

Please modify the below table to represent the breakdown of learning time in each week of your course.

LEARNING TIME RUBRIC

Learning Time Element	Asynchronous* / Synchronous**	Time on Task for Students (weekly)	Notes
Lecture (Active Module)	Asynchronous	2 - 3 hours	Video and interactive text format. Expect quizzes throughout the module.
Discussions	Asynchronous	0.5 hours	Students discuss instructor's questions for each lesson.
Reading	Asynchronous	1.5 hour	Students complete recommended readings (online journal articles and tutorials).
Assignments	Asynchronous	1.5 hours	Students will read assignments and watch guided solutions. Students will submit a short write-up (1-2 paragraph) of what they learned

Course Communication

Announcements

Announcements will be posted on NYU Classes on a regular basis. You can locate all class announcements under the *Announcements* tab of our class. Be sure to check the class announcements regularly as they will contain important information about class assignments and other class matters.

Email –

You are encouraged to post your questions about the course in the Forums discussions on NYU Classes. This is an open forum in which you and your classmates are encouraged to answer each other's questions. But, if you need to contact me directly, please email me. You can expect a response within 48 hours.

Weekly Virtual Meetings –

On a regular basis, we will hold a virtual class meeting through the video conferencing tool listed on NYU Classes. This meeting is an opportunity for you to ask questions and gain clarification about the course content from myself and your peers. You are highly encouraged to attend these meetings. I understand that not all students will be available to attend these virtual meetings. Due to this fact, the meetings will be recorded so you can watch them when you are available.

Netiquette –

When participating in an online class it is important to interact with your peers in an appropriate manner. Always use professional language (no netspeak) in your discussion board posts and emails. Please be respectful of your classmates at all times even if you disagree with their ideas.

Questions About the Course & Contacting the Instructor

To schedule an appointment with your TA, or to ask any questions about the course content, please post to the discussion forms in NYU Classes.

Readings

The recommended text for the course is:

The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities by Mark Dowd, John McDonald, & Justin Schuh.

Access to free eBook from NYU library:

http://bobcat.library.nyu.edu/primo-explore/fulldisplay?docid=nyu_aleph005548728&context=L&vid=NYU&search_scope= all&tab=all&lang=en_US

You can access NYU's central library here: http://library.nyu.edu/

You can access NYU Tandon's Bern Dibner Library here: http://library.poly.edu/

Assignments and Exams

Refer to **Unit Assignment Guideline** on NYU Classes to complete each weekly portion. The assignments are divided into weekly portions

to help you stay on track. By the end of each week, you are encouraged to place your work-in-progress in the "**File Exchange**" folder on NYU Classes. You will receive feedback from me or teaching assistants and then modify your work accordingly. At the end of each unit, you are required to submit the final version of your project on NYU Classes via "**Submit Coding Assignments**," and "**Submit Written Assignments**" tabs.

Exams Administered and Proctored Online

Exams in this course are administered through NYU Classes. You are required to arrange an online proctor for your exams via ProctorU. More information on ProctorU and scheduling proctoring sessions can be found on [Tandon Online's website](#).

Exams Administered On Paper and Proctored Remotely

Exams in this course are administered via paper and pencil. If you are not able to attend an exam session on-campus, you are required to secure in-person proctoring arrangements near your location. Tandon Online's website

---

University Policies

Moses Center Statement of Disability

Academic accommodations are available for students with disabilities. Please contact the Moses Center for Students with Disabilities (212-998-4980 or mosescsd@nyu.edu) for further information. Students who are requesting academic accommodations are advised to reach out to the Moses Center as early as possible in the semester for assistance.

NYU Tandon School of Engineering Policies and Procedures on Academic Misconduct[1]

A. Introduction: The School of Engineering encourages academic excellence in an environment that promotes honesty, integrity, and fairness, and students at the School of Engineering are expected to exhibit those qualities in their academic work. It is through the process of submitting their own work and receiving honest feedback on that work that students may progress academically. Any act of academic dishonesty is seen as an attack upon the School and will not be tolerated. Furthermore, those who breach the School's rules on academic integrity will be sanctioned under this Policy. Students are responsible for familiarizing themselves with the School's Policy on Academic Misconduct.

B. Definition: Academic dishonesty may include misrepresentation, deception, dishonesty, or any act of falsification committed by a student to influence a grade or other academic evaluation. Academic dishonesty also includes intentionally damaging the academic work of others or assisting other students in acts of dishonesty. Common examples of academically dishonest behavior include, but are not limited to, the following:

    a. Cheating: intentionally using or attempting to use unauthorized notes, books, electronic media, or electronic communications in an exam; talking with fellow students or looking at another person's work during an exam; submitting work prepared in advance for an in-class examination; having someone take an exam for you or taking an exam for someone else; violating other rules governing the administration of examinations.

    b. Fabrication: including but not limited to, falsifying experimental data and/or citations.

    c. Plagiarism: intentionally or knowingly representing the words or ideas of another as one's own in any academic exercise; failure to attribute direct quotations, paraphrases, or borrowed facts or information.

    d. Unauthorized collaboration: working together on work that was meant to be done individually.

    e. Duplicating work: presenting for grading the same work for more than one project or in more than one class, unless express

---

[1] Excerpted from the Tandon School of Engineering Student Code of Conduct

and prior permission has been received from the course instructor(s) or research adviser involved.

f. Forgery: altering any academic document, including, but not limited to, academic records, admissions materials, or medical excuses.