

Building Secure Web Applications with Python and Flask



This course is an introduction to building secure, full-stack web applications with Python and Flask. We'll start with Python and Flask, and then subsequent weeks will cover how to add Flask extensions to your applications to implement common web app functionalities, how to protect your website from bad actors, and more! At the end of the course, you'll be able to deploy your app for the world to see.

Course Details

- Course: CMSC388J
- Prerequisites: C- or better in CMSC216 and CMSC250
- Credits: 1
- Seats: 30
- Lecture Time: TBD
- Location: TBD
- Semester: Fall 2020
- Textbook: No textbook, all materials are provided and documentation is online
- Course Facilitators: Yashas Lokesh, Kenton Wong
- Faculty Advisor: Michael Marsh
- Syllabus last updated: February 25th, 2020
- Previously offered: Spring 2020, Fall 2019

Topics Covered

- Python
 - Variables, expressions, operators
 - Iterations, conditionals, collections
 - Functions
 - As first-class objects
 - Decorators
 - "Main" function
 - Built-in functions
- Web Application Security
 - Cross-site scripting (XSS)
 - Cross-site request forgery (CSRF)
 - SQL injections
 - Man-in-the-Middle attacks (MitM)
 - Token & Two-factor authentication
- Flask
 - Routing your web app
 - Templating
 - Adding extensions for more features
 - WTForms
 - SQLAlchemy
 - Talisman
 - Login
 - Creating your own
 - Logging
 - User Management
 - Blueprints
- HTML/CSS/JS
 - Bootstrap
 - Integrating other frameworks
 - Custom CSS/JS configuration
- SQL
 - SQLite
 - PostgreSQL
- Payments Integration
 - Stripe (possibly others, we're open to suggestions)
- App Deployment

- Heroku
- Python Anywhere
- *Possibly*: Google App Engine, AWS
- Version Control
 - Git

Schedule

Week	Topic	Assignment
1	Intro to Python	Python practice (P1) assigned
2	Flask Intro	P1 due, P2 assigned
3	Forms, CSRF	
4	Databases, Injection attacks	P2 due, P3 assigned
5	User Management	
6	Bootstrap & more	P3 due, P4 assigned
7	In-depth CSS & JS*	
8	Flask Extensions (opt., publishing)	P4 due, P5 assigned
9	Logging, Workday	
10	HTTP Headers & Talisman	P5 due, Final project assigned

11	Blueprints	
12	Two-Factor Authentication	
13	Payments with Stripe*	
14	THANKSGIVING BREAK?	
15	Deploying your app	Final Project due

*See Fluid Schedule section below

NOTE: Schedule will be adjusted in the near future to add Thanksgiving break

Fluid Schedule

Weeks 7 and 14 will have a main topic of discussion, but during these weeks, we'll also try to teach topics requested by the students. So if you guys feel like you need more info about a certain topic during class, or just want to learn a new idea altogether, let us know, and we'll try to add it in.

We'll send out information on how you can let us know anonymously; surveys will probably be conducted anonymously on ELMS.

Grading

Grades will be maintained on ELMS. You will be responsible for all material discussed in lecture as well as other standard means of communication (Piazza, email announcements, etc.), including but not limited to deadlines, policies, assignment changes, etc.

Your final course grade will be determined according to the following percentages:

Percentage	Title	Description
------------	-------	-------------

60%	Projects	Weekly projects to test knowledge of topics taught in class
40%	Final Project	Final project - creating app from scratch

Any request for reconsideration of any grading on coursework must be submitted within one week of when it is returned. No requests will be considered afterwards.

Projects

The project is due the day it is scheduled to be due, barring any extensions that may be given out. They will be due at 11:59 PM. Not all of the projects will have tests; they will be graded according to a rubric which will also be provided. All projects must be submitted online on ELMS.

Project weighting will be determined at a later time.

Late Policy: Projects may be submitted up to three days late for 10% off your earned grade, each day. After this, no more projects will be accepted. The highest score you get on the project, counting late and on-time submissions, will be your grade for that project. There are no exceptions unless you've talked with us beforehand or provide a valid excuse.

We will look at your most recent on-time and late (if applicable) submissions when grading.

Final Project

The final project will use everything you have learned in class before and will require you to build a Flask web application from scratch with a group or individually, and deploy the app on a hosting platform. Requirements for the final project will come out towards the end of the semester.

Outside-of-class communication with course staff

We'll communicate through students mainly through Piazza and through office hours.

Office hours: TBD

Please use Piazza as your primary communication with the course staff, we'll get back to you the quickest on Piazza. If you absolutely cannot use Piazza, then email us; if you are emailing Yashas or Kenton, make sure to CC the other. Additionally, please include [CMSC 388J] at the start of your subject line so we don't accidentally ignore your email.

Instructor:

Dr. Michael Marsh - mmarsh@cs.umd.edu

Facilitators:

Yashas Lokesh - yashloke@umd.edu

Kenton Wong - kdubbs0@umd.edu

Excused Absence and Academic Accommodations

See the section titled "Attendance, Absences, or Missed Assignments" available at [Course Related Policies](#).

Disability Support Accommodations

See the section titled "Accessibility" available at [Course Related Policies](#).

Academic Integrity

Note that academic dishonesty includes not only cheating, fabrication, and plagiarism, but also includes helping other students commit acts of academic dishonesty by allowing them to obtain copies of your work. In short, all submitted work must be your own. Cases of academic dishonesty will be pursued to the fullest extent possible as stipulated by the [Office of Student Conduct](#).

It is very important for you to be aware of the consequences of cheating, fabrication, facilitation, and plagiarism. For more information on the Code of Academic Integrity or the Student Honor Council, please visit <http://www.shc.umd.edu>.

Course Evaluations

If you have a suggestion for improving this class, don't hesitate to tell the instructor or TAs during the semester. At the end of the semester, please don't forget to provide your feedback using the campus-wide CourseEvalUM system. Your comments will help make this class better.