# **CPS 475/575 - Secure Application Development, Spring 2020**

Dr. Phu Phung

Department of Computer Science,  
University of Dayton

Final Project

Announcement and Tutorial: 3/26/2020

Submission Deadline: TBD

## Introduction

In this final project, you apply all secure programming principles and practices and web development technologies to develop a simple yet secure “**miniFacebook**” web application with the following technical requirements:

* Anyone can register for an account
* Registered users can (if the account is not disabled)
  + Login
  + Change password
  + Add a new post
  + Edit their own posts
  + Add comments on any post, e.g, by their own or others
* Superusers can
  + Login (Database added directly in the database, no registration)
  + Disable (not delete) a registered user
  + Enable a registered user
* Logged-in users can have real-time chat with others

## Security Requirements

* The system must be deployed on HTTPS
* Passwords must be hashed in the database
* No MySQL root account used for the PHP code
* All SQL must be in Prepared Statements
* All inputs must be validated in every layer
  + HTML, PHP, and SQL
* HTML outputs must be sanitized
* Role-based access control for registered users and super users
* Session Authentication and CRSF Protection
* All security principles and practices in the course must be applied, e.g.,
* Security aspects must be integrated at the development phase
  + Defense in depth and defense in breath
* Input/Output must be validated
  + Defensive and Robust Programming

## Project Management

Each team needs to create a team on Bitbucket.org, then create a private repository for the project within that team. You need to add the instructor (email: [pphung1@udayton.edu](mailto:pphung1@udayton.edu)) and the TA (email: [hiremathp1@udayton.edu](mailto:hiremathp1@udayton.edu)) as members of your team so that we can access your repository. **These steps have been covered in Lecture 18 (3/26/2020).**

Your final report should be written in README.md file of the repo following markdown format. A template for your report is available here: <https://bitbucket.org/phu-udayton/secad/src/master/project/README.md>

## Project Submission

**Files to be submitted**

* The report in PDF: Converted from the README.md file
  + URL to your team video demo
* A zip file contains everything from your team repo
  + Should be downloaded from your repository on bitbucket.org

## Grade distribution

The project has 100 points and contributes 15% to your final grade. The grade distribution is as follow:

* Design: 5 points

This part includes:

* + Database design
  + The user interface, e.g., the Web interface and CSS
  + Functionalities of your application, e.g.,
    - How do you separate the roles of regular users (with registration) and super users?
* Implementation, and demos: 50 points:
  + (5p) Anyone can register for an account
  + Logged-in users can (if the account is not disabled)
    - (5p) Change password
    - (5p) Add a new post
    - (5p) Edit their own posts
    - (5p) Add comments on any post, e.g, by their own or others
    - (10p) Chat with other logged-in users
  + Logged-in superusers (5p) can
    - (5p) Disable (not delete) a registered user
    - (5p) Enable a registered user
* Security Requirments: 35 points
  + (2.5p) The system must be deployed on HTTPS
  + (2.5p) Passwords must be hashed in the database
  + (2.5p) No MySQL root account used for the PHP code
  + (5p) All SQL must be in Prepared Statements
  + (5p) All inputs must be validated in every layer
    - HTML, PHP, and SQL
  + (2.5p) HTML outputs must be sanitized
  + Role-based access control for registered users and super users
    - (2.5p) A regular user cannot log in as a superuser
    - (2.5p) A regular user cannot edit/update posts of other users
  + (5p) Session Authentication and Hijacking Prevention
  + (5p) CRSF Protection
* Report: 5 points
  + demonstrate the project meets the requirements, e.g., design, demo, security analysis
  + All source code files must be included in the Appendix
* Organization: 5 points
  + The repository must be accessible on bitbucket.org (shared with the instructor and TA earlier). In addition to the source files, you must have:
    - README.md file under the root folder.
    - database.sql file that creates the database for the application.
  + Zip file downloaded from bitbucket.org