**CS4140 Web Applications Security**

2018 Summer

INSTRUCTOR: Dr. Dabin Ding

PHONE: (660) 543 – 8865 EMAIL: dding@ucmo.edu

OFFICE HOURS: TR 3:20-4:20pm (other times by appointment)

TEXTBOOK: None. Please see reference materials.

PREREQUISITE: CS 1100 or CS1030.

I. Purpose of the Course

Web applications have often been developed with minimal attention to security risks. As a result, many corporate sites have become the targets of cybercrimes. The aim of this course is to help students understand the reason behind common security vulnerabilities in web applications and to introduce proper defense methods. In a tool-driven process, students will take sample web applications and redesign them as secure as possible. This course assumes the knowledge on web basics.

II. Objectives and Desired Student Competencies

At the completion of this course, students will be able to:

• Understand the fundamentals of web security

• Use existing tools to detect security flaws in web applications

• Identify the appropriate defense method to mitigate the security threats

• Rewrite the web applications to eliminate the security vulnerabilities

III. Course Content Outline

A. *Textbooks:*

There is no required textbook for this course. Students are encouraged to study instructional material and tutorials online.

B. *Reference Materials:*

1. The Basics of Web Hacking: Tools and Techniques to Attack the Web, 1st Edition Josh Pauli Syngress, 2013

2. Iron-Clad Java: Building Secure Web Application, 1st Edition Jim Manico, August Detlefsen McGraw-Hill Osborne Media, 2014

3. Online Resources:

Web Fundamental: <https://www.w3schools.com/>

Burp Suite: <https://portswigger.net/burp>

Sqlmap: <http://sqlmap.org/>

ZAP proxy: <https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project>

C. *Topics to be covered (Tentative):*

1. **Web Fundamentals**

HTML

HTTP & HTTPS

Web Server

Javascript

Cookie

Session Management

Browser Security

2. **Secure Authentication and Access**

Basic Authentication

Session Hijacking

Session Fixation Attack

Password Management

Identify and Access Control

Missing Function Level Access Control

3. **Secure User Input**

Reflected Cross-Site Script

Stored Cross-Site Script

DOM-based Cross-Site Script

SQL-Injection

Store Procedure Injection

Cross-Site Request Forgery

User Input Validation

4. **Secure Web Development**

Secure Coding Practice

Secure Development Lifecycle

Functional Programming for Secure Web Apps

IV. Procedures/Assessment

**Attendance**

You are expected to attend all lectures and to complete all work assigned. Advance arrangements for unavoidable absence should be made whenever possible. Neither absence nor notification of absence relieves you of the responsibility of meeting all course requirements.

A sample grade distribution:

**Undergraduate Graduate**

Attendance: 50pts Attendance: 50pts

Assignments: 350pts Assignments: 250pts

Midterm exam: 200pts Midterm exam: 200pts

Final exam: 250pts Final exam: 250pts

Quiz: 150pts Quiz: 200pts

Term Project: 100pts

A sample grading scale:

A 900-1000pts

B 800-899pts

C 700-799pts

D 600-699pts

F 0-599pts

**Graduate-level assessment:** To comply with the university policy regarding courses that can be taken for either graduate or undergraduate credit, a student taking this course for graduate credit will be required to write a *graduate term paper* on a topic assigned by the instructor.

**Course Project**: Students taking this course for graduate credit will be required to do a graduate course project which is different from his/her undergraduate counterparts. The course project for graduate students will emphasize the quantitative analytical aspect of a problem as opposed to qualitative arguments expected from an undergraduate course project.

**Late Policy**

Students are expected to complete work on schedule. The late policy for all assignments is as follows: 10% points off, if submitted within 24 hours after the due date; 20% off, if submitted with 1 week after the due date. Partial credits (up to 70%) will be given if submitted before semester ends. Partially finished assignments will receive partial credit.

**Plagiarism Policy**: Academic dishonesty will not be tolerated in this class. Any form of cheating will be dealt with according to the guidelines on page 196-199 of the UCM Planner/Handbook 2013-2014. You can also find the Academic Dishonesty Policy on-line at <http://www.ucmo.edu/student/documents/honest.pdf>.

**Students with disabilities**: Students with documented disabilities who are seeking academic accommodations should contact the Office of Accessibility Services, Union 222, 660-543-4421.

**Student Outcomes for BS in Computer Science**

The following is a list of student outcomes covered in this course .

**SO1 - Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.**

SO2 - Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program’s discipline.

**SO3 - Communicate effectively in a variety of professional contexts.**

SO4 - Recognize professional  responsibilities  and  make  informed  judgments  in  computing practice based on legal and ethical principles.

**SO5 - Function effectively as a member or leader of a team engaged in activities appropriate to the program’s discipline.**

SO6 - Apply computer science theory and software development fundamentals to produce computing-based solutions.

**Student Outcomes for BS in Cybersecurity**

Outcome 6: An ability to apply security principles and practices to the environment, hardware, software, and human aspects of a system

Outcome 7: An ability to analyze and evaluate systems with respect to maintaining operations in the presence of risks and threats