James Madison University
CS531: Secure Programming
Fall 2024
Syllabus

Instructor Information

Name: **Dr. M. Hossain Heydari**
Email: heydarmh@jmu.edu
Work Phone: 540-568-8745
Office Location: CS/ISAT 225
Office Hours: All my classes are online, so my office hours are mostly via Zoom and by appointment. Please send me an email and let me know if you want to have a Zoom meeting. We can agree on the day and time.

- I am available in my office on **Wednesdays**: 1:00 - 3:00.
- If you have any questions about the program and I am not available, please contact Lucas Hopper (hopperlg@jmu.edu), room 219, 540-568-8772.

Note: Please post your classroom related questions in the appropriate forum, so your classmates may also benefit from the QA.
Personal Link: http://users.cs.jmu.edu/heydarmh

Classroom: https://Canvas.jmu.edu. This is a 100% online course and all instructions are done through the Canvas course delivery System.

Digital Library

Please visit the following link to access JMU's CS digital library subscriptions: https://www.lib.jmu.edu/. Please feel free to contact our librarian for help with other resources.

Course Description

A survey of concepts related to secure and rugged programming. Considers both the theoretical foundations of secure and rugged programming and various issues that arise in practice. Some language-specific and platform-specific issues are addressed. *Prerequisite: Unconditional admission as Computer Science graduate student*.

Course Objectives

Students in this course are expected to learn about various kinds of faults that make computer programs vulnerable to attack and how they can be prevented, detected, and removed. Specifically, they are expected to be able to understand cross-site scripting, cross-site request forgery, session fixation, clickjacking, magic URLS, predictable cookies, string and buffer overflows, memory management vulnerabilities, integer vulnerabilities, command/SQL injection, error/exception handling vulnerabilities, information leakage vulnerabilities and user interface vulnerabilities. In addition, they are expected to understand byte-code loaders and how they can be secured.

Required Textbook

24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them, David Le Blanc, John Viega, and Michael Howard. You have free access to this book through the JMU libraries. There are many other sites on the net that offer this as a free copy, be careful with some of these.

Secure Coding in C and C++, 2nd Edition, Robert C. Seacord (SEI Series in Software Engineering), available as a free PDF.

Secure Programming HOWTO, David A. Wheeler, available in multiple formats. Please note the list of items from the "Related Materials".

Suggested Readings:

From Dr. Bernstein's: Additional readings for this course will come from the following sources, all of which are available on-line to members of the JMU community through Safari Books using the JMU VPN or proxy server.

Flanagan, D. (2011) *JavaScript: The Definitive Guide*, O'Reilly Media , Cambridge, MA.
(Order from amazon , order from Barnes and Noble , compare at bigwords , compare at CampusBooks4Less , order from Chegg , or search eFollett)

Henick, B. (2010) *HTML and CSS: The Good Parts*, O'Reilly Media, Cambridge, MA.
(Order from amazon , order from Barnes and Noble , compare at bigwords , compare at CampusBooks4Less , order from Chegg , or search eFollett)

Oaks, S. (2001) *Java Security*, O'Reilly Media , Cambridge, MA.
(Order from amazon , order from Barnes and Noble , compare at bigwords , compare at CampusBooks4Less , order from Chegg , or search eFollett)

Pauli, J. (2013) *The Basics of Web Hacking*, Syngress , Boston.
(Order from amazon , order from Barnes and Noble , compare at bigwords , compare at CampusBooks4Less , order from Chegg , or search eFollett)

Tatroe, K. , P. MacIntyre and R. Lerdorf (2013) *Programming PHP*, O'Reilly Media , Cambridge, MA.
(Order from amazon , order from Barnes and Noble , compare at bigwords , compare at CampusBooks4Less , order from Chegg , or search eFollett)

Tentative Schedule

Part 1: Secure Coding in C and C++
Part 2: 24 Deadly Sins of Software Security
Part 3: Secure Programming How To

Tentative Programming Sin Presentations:

- Sin1: SQL Injection
- Sin2: Web Server Vulnerabilities

- Sin3: Web Client-related vulnerabilities (DOM XSS)
- Sin4: Use of Magic URLs, Predictable Cookies, and Hidden Form Fields
- Sin5: Buffer Overruns
- Sin6: Format String Problems
- Sin7: Integer Overflow
- Sin8: C++ Catastrophes
- Sin9: Catching Exceptions
- Sin10: Command Injection
- Sin11: Failure to Handle Errors Correctly
- Sin12: Information Leakage
- Sin13: Race Conditions
- SIN 14: Poor Usability
- Sin15: Not Updating Easily
- Sin16: Executing Code with too much Privilege
- Sin17: Failure to protect stored data
- Sin18: The Sins of Mobile Code
- Sin19: Use of weak Password-Based Systems
- Sin20: Weak Random Numbers
- Sin21: Using Cryptography Incorrectly
- SIN22: Network Sins
- Sin23: Improper Use of PKI, Especially SSL
- Sin24 Trusting Network Name Resolution
- Common Secure Coding Principles
- Secure Coding Best Practices
- Static Program Analysis
- Dynamic Program Analysis

Delivery Method

This course will be delivered entirely on-line using Canvas (https://canvas.jmu.edu). Students are expected to log into the classroom few times a week to participate in the classroom discussions, download their projects, PowerPoint slides, course documents, take quizzes, and receive their grades. Please see the discussion forum for details.

Programming assignments have to be submitted to the Student LINUX system.

Methods of Evaluation

All documents submitted for grade are subject to JMU Honor Code. Projects, quizzes, and exams must be your own work. Using any unauthorize source is considered cheating and may cause your dismissal from JMU. If not sure, please check with your instructor ahead of time.

Presentations	35%
Participation	20%
Projects	25%
Moderating	10%
Final Exam	10%

Weighted Total	Grade
92-100%	A
90-92%	A-
87-89%	B+
82-86%	B
79-81%	B-
72-78%	C
<72	F

Discussion Boards

There are several discussion forums on the Canvas for this course, one per topic being discussed. You may either click on the "***Add New Thread***" button to start a new topic for the discussion forum or click on the "Subject" of a message to read and possibly reply to it.

Attendance/Participation Policy:

- Several discussion threads are proposed by the instructor and students for each Forum. Students are expected to log into the classroom several times a week and participate in the discussions.
- Each student must contribute to the discussions in the topical Forums. Only actual contributions would be given discussion points. Things like "I agree" or "I do not agree" in response to a current discussion shall not be counted. Please avoid repeating what has already been said. These waist everybody's time and clutter the discussion forum.
- Only contributions posted during the designated module period shall be graded. You can keep on discussing the issues, but once a forum is graded, your discussion grade will not be change.
- Discussion participation will be graded, using a scale of 0-3:
  0: no participation
  1: posting made
  2: few postings made during the module's period, with some original ideas
  3: several postings made in a timely fashion with original and interesting comments
- The instructor will monitor the students' contributions and provide suggestions/answers.
- These forums remain available for viewing till the end of the course. At the discretion of the instructor, these forums may be moderated by the instructor or selected student(s).

Assignments and Submission Policy

1. Please note that your assignments are due by Sunday midnight of the due date.
2. Late assignments will lose 25% of the grade for each day being late.
3. You will have access to our LINUX server (**student.cs.jmu.edu**) to implement your projects. You are welcome to develop your projects on any platform. But you need to make sure your project works on this machine to get full credit (that is the only place I will test your programs).
4. Faculty help is not generally available over the weekends and holidays. So, please start working on your projects early so you get answer to your questions before the weekend.

Projects

- You will have several projects, most of which will be done on the Virginia CyberRange. We will talk about those in their designated forums.

Final Project

- You will have a final project that will be evaluated by your classmates and myself.

Moderating Discussions:

- Each student chooses/assigned some topics to create a presentation. The student moderates the discussion forum for the topic. The week of a discussion for which you are a leader you must:
  - Post several discussion questions in your discussion board on Canvas relating to your presentation to stimulate discussion.
  - Lead the discussion and encourage students to engage in the discussions in the week's discussions. This means posting the presentations, posting relevant questions, and answering questions.
- Your discussion moderation grade depends on how well the discussion is handled. You can earn up to 20 points for moderating each discussion forum.
- All students are required to participate in these discussions, to earn participation points.

Ask-the-Instructor Forum

This forum is designed for questions that students want answered by the instructor, not covered in a Topical Forum. Questions in this forum should be of logistic nature. Topic questions should be posted in the related discussion forum.

We will have a discussion forum for each of the major programming projects. In this forum, students can:

- Post questions about the project and their deliverables.
- Respond to issues/questions raised by others.
- You are not supposed to post solution to the project. You can only help with how a statement is used and provide small hints.

Open forum

Open forum is available for general discussions related to Information Security. You can post job openings and other topics not directly related to the course. This forum is not graded, but the instructor will monitor the forum. No political discussions please.

Please get involved, ask questions, answer the posted questions, and communicate with your faculty. We are here to help. If you need extra (individual) help, make sure you ask and don't wait till it is too late!

General Policies:

Adding/Dropping Course Policy

Please note that you are responsible for the tuition for all the courses you registered. You can only get a tuition refund, if you drop a course before the add/drop deadline. Students are responsible for adding and dropping courses via e-campus, please talk to Carole Ritchie and your instructor before doing so. I do not give "WP" or "WF" grades to students requesting a drop after the deadline except in extraordinary circumstances. Please see the Registrar Office's website for dates and deadlines:
https://www.jmu.edu/registrar/students/print_dates.shtml

Disability Accommodations: JMU abides by Section 504 of the Rehabilitation Act of 1973 and the Americans with Disabilities Act, which mandate reasonable accommodations be provided for students with documented disabilities. The rights and responsibilities of individuals with disabilities are described in Student Handbook. If you have need of accommodations, you must:

1. File the necessary documentation and supporting evidence with the Office of Disability Services.
2. Obtain an "Access Plan Letter" from the Office of Disability Services.
3. Schedule a meeting to speak with me **at the start of the semester**. (Make sure to bring your "Access Plan Letter" to this meeting.)
4. I will then make every reasonable effort to accommodate your needs. More information can be found at http://www.jmu.edu/accessibility.

Inclement weather: Inclement weather policies are not applicable to Distance Education students.

Religious Observation Accommodations

If you cannot satisfy a requirement of the course for religious reasons you must let me know at least 2 weeks in advance. In some cases you will be required to "make up" the requirement; in other cases the distribution of requirements will be changed.

Plagiarism and Academic Integrity:

Students are expected to comply with the JMU Honor Code as stated in the Student Handbook and available from the Honor Council Web site: http://www.jmu.edu/honor/code.shtml.
Consulting with other students about problems and solutions is not a violation of the Honor Code provided that the ultimate work turned in for an assignment is your own. This means that everything written down and turned in for an assignment must come from your head and not someone else's. When in doubt, ask me.

Have a Great Semester