# CIS 418 (1) - SECURE SOFTWARE ENGINEERING

**Grand Valley State University – College of Computing - Department of Computer Science - Fall 2025**

| **Instructor** | **Contact Info** | **Office Location** | **Office Hours** |
|---|---|---|---|
| Dr. Dimitrios Melissourgos | melissod@gvsu.edu<br>352 278 6777<br>CIS 418 Discord | MAK D-2-232 | Monday 3pm-4pm<br>Wednesday 4pm-5pm<br>Friday 3pm-4pm |

## Course Description

### General Information

This course explores characteristics that make software secure and less vulnerable to attacks. Basic techniques for securing applications such as input validation, output encoding, memory management, race conditions, vulnerability analysis and testing, authentication, access control, and secure database management will be covered in detail.

Credits: 3

Grading scheme: Letter grade

Prerequisite: CIS 350 – Introduction to Software Engineering

Lecture time: Monday, Wednesday, Friday at 1:00pm-1:50pm

Lecture location: MAK B-2-235

### Course Objectives

At the end of the course, students will be able to:

- Describe characteristics of secure software.
- Apply principles of secure software development lifecycle.
- Describe software vulnerabilities such as buffer overflow, format string vulnerability, race condition vulnerability, SQL injection vulnerability, cross-site scripting vulnerability and defense mechanisms.
- Build input validation and output encoding into software.
- Design shellcode to test the presence of vulnerabilities and build countermeasures.

### Required Course Material

Computer Security – A Hands-on Approach, Third Edition, by Wenliang Du

## Exams (Tentative)

| Exam | Date | Time | Location |
|------|------|------|----------|
| Midterm | Monday, October 13 | 1:00pm-1:50pm | MAK B-2-235 |
| Final Exam | Monday, December 8 | 12:00pm-1:50pm | MAK B-2-235 |

## Course Schedule

| Week | Topic |
|------|-------|
| Week 1 | Course Organization |
| | Introduction to Security Engineering |
| | Software Security Fundamentals |
| Week 2 | Software Security Development Lifecycle Processes and Activities |
| | Requirements Engineering for Secure Software |
| Week 3 | Secure Design Principles and Threat Modeling |
| | Ubuntu VM Setup for SEED Labs (https://www.seedsecuritylabs.org) |
| Week 4 | Linux Security Basics (Ch. 1) |
| Week 5 | Set-UID Programs; Environment Variables and Attacks (Ch. 2 & Ch. 3) |
| | SEED Lab 1: Set-UID Programs and Environment Variables |
| Week 6 | Buffer Overflow Attack (Ch. 4) |
| Week 7 | SEED Lab 2: Buffer Overflow Attack |
| Week 8 | Midterm |
| | Secure Coding with Static Analysis |
| Week 9 | *Fall Break* |
| Week 10 | Return-to-libc Attack (Ch. 5) |
| Week 11 | SEED Lab 3: Return-to-libc Attack |
| Week 12 | Handling Input, Errors, and Exceptions |
| | Format String Vulnerability (Ch. 6) |
| Week 13 | SEED Lab 4: Format String Vulnerability |
| Week 14 | Web Security Basics (Ch. 11) |
| | Cross-Site Request Forgery Attack (Ch. 12) |
| | *Thanksgiving Break* |
| Week 15 | SEED Lab 5: Cross-Site Request Forgery Attack |

## Grading Policy

### Grading Scale

| | |
|---|---|
| A | ≥93% |
| A- | ≥90% |
| B+ | ≥87% |
| B | ≥83% |
| B- | ≥80% |
| C+ | ≥77% |
| C | ≥73% |
| C- | ≥70% |
| D+ | ≥67% |
| D | ≥63% |
| F | <63% |

| Assignment / Test | Percentage of Final Grade |
|---|---|
| Attendance | 10% |
| SEED Labs (5) | 50% |
| Midterm | 15% |
| Final | 15% |
| Term Paper or Extra SEED Lab | 10% |

### Attendance Policy

Students are required to attend the class. Sign on sheets will be handed out at 11 randomly selected class meetings (lecture or lab). You will receive the full 10% attendance grade if you sign on for 10 out of the 11. Each additional missing class costs 1%. If you cannot attend a class meeting, you need to notify the instructor **before** the beginning of the class. If you have a serious reason for missing the class (e.g. illness, injury, family emergency, etc.), then you will be excused and you will not lose 1% of the attendance grade. If you notify the instructor of your absence **after** the class has begun, you will be required to provide a doctor's note or similar proof of absence in order to avoid the 1% penalty.

### SEED Labs

The lab work aims to provide practical and hands-on experience in attacks and vulnerabilities. There will be 5 labs over the duration of the semester, each of them worth 10% of your grade. We will run the labs on Ubuntu VMs. We will perform some of the tasks in each lab together, during class, and you will be asked to complete the rest of the tasks at home. For each lab, you have to create a report explaining your work with screenshots and text. The due day for your report will be one week after the assignment has been given out, unless stated otherwise.

Assignments turned in after the due date will receive a 20% late submission penalty per day, including weekends and holidays, with a max of 4 days.

Lab assignments are open book; you are allowed to use books, notes, slides, search the internet, and discuss with the instructor and other students while completing the work. However, you are not allowed to engage in practices that would be considered plagiarism, copying, or cheating. Each student is required to complete lab assignments using their own computers and taking their own screenshots.

## Term Paper or Extra SEED Lab

There is a semester-long term paper or an extra unguided lab that students need to complete by Sunday, November 30th. You will find a list of topics for the term paper below. Although the subject of your term paper is not restricted to the ideas below, if you want to write about something else, the topic must be approved by the instructor before you start working on it.

- Microsoft SDL Threat Modeling Tool: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
- Attack Patterns
- Cryptography topics (see section IV in the textbook)
- Penetration Testing
- WebGoat: https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
- Google's Gruyere: https://google-gruyere.appspot.com/
- OWASP Zed Attack Proxy (ZAP) Tool
  https://owasp.org/www-chapter-dorset/assets/presentations/2020-01/20200120-OWASPDorset-ZAP-DanielW.pdf
- Static Application Security Testing (SAST) Tools:
  https://www.owasp.org/index.php/Source_Code_Analysis_Tools
  - OWASP WAP (Web Application Protection) Tool
    https://wiki.owasp.org/index.php/OWASP_WAP-Web_Application_Protection
  - FindSecBugs: https://find-sec-bugs.github.io/
  - FlawFinder: https://dwheeler.com/flawfinder/
  - SonarQube: https://www.sonarqube.org/
  - SonarLint: http://www.sonarlint.org/

# Additional Information and Resources

## Important Dates

Drop Deadline - Grade "W": November 7th by 5:00pm

Other important dates: Fall 2025 Academic Calendar

## Classroom Protocol

Treat faculty, staff, your fellow students, and university property with respect. Do not use your phone during class. Do not make distractions and be on time for the class meetings. Any regrading requests must be made within a week of the students receiving their grade.

### Integrity and Honesty

All students are expected to adhere to the [academic honesty standards set forth by Grand Valley State University](#). In addition, students in this course are expected to adhere to the [academic honesty guidelines as set forth by the College of Computing](#).

### Course Evaluation

The end-of-semester course evaluation sites are set up in LIFT and maintained by the Academic Department Coordinator. Course evaluation sites become available to students during the last two weeks of the semester (not exam week), unless specified otherwise.

### Accessibility and Special Accommodations

Grand Valley State University strives to provide an inclusive environment across campus that is accessible to all individuals with a diverse range of abilities. As your instructor, it is my objective to facilitate opportunities within all class activities and programs because your success is important to me. If you are encountering difficulties that are interrupting your learning experience, please feel free to make those known to me as soon as possible. If you feel that you need accommodations in this course, you must present a memo to me from Student Accessibility Resources (SAR), indicating the approved accommodations. If the class meets in person, you should schedule a meeting with me during office hours to discuss your accommodations. If your class is online or hybrid, please forward your memo to me in an email and schedule a virtual or phone appointment with me to discuss your accommodations. Accommodations are not retroactive. If you have not already done so, please contact the Student Accessibility Resources office (215 CON) by calling (616) 331-2490 or by email to [access@gvsu.edu](mailto:access@gvsu.edu). You can also visit the SAR website [here](#). Please note that I cannot provide accommodations, until I have received a copy of the SAR issued memo. Furthermore, if you think you will need assistance evacuating this classroom and/or building in an emergency, please make me aware so that the university and I can develop a plan to assist you. All discussions will remain confidential.

### GVSU Course Policies

This course is subject to the [GVSU policies](#).

### Discrimination or Sexual Misconduct

Grand Valley State University is committed to creating and advancing a campus community where individuals feel empowered to raise concerns, ask for help, and be informed about options before making any decisions. If you become aware of any discrimination or sexual misconduct incident, please report it at the [Title IX office](#).

### In Case of Emergency

In Case of Fire: Immediately proceed to the nearest exit during a fire alarm. Do not use elevators.

More information is available on the [University's Emergency website](#).