# CIS 518 - SECURE SOFTWARE ENGINEERING (2)

**Grand Valley State University - School of Computing - Fall 2023**


| Instructor | Contact Info | Office Location | Office Hours |
|---|---|---|---|
| Dimitrios Melissourgos | melissod@gvsu.edu<br>352 278 6777 | MAK D-2-232<br><br>DCIH 530H | Tuesday 10am-noon<br>Thursday 10am-noon<br>Tuesday 2:30pm-3:30pm<br>Thursday 2:30pm-3:30pm |


## 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 500 – Fundamentals of Software Practice

Lecture time: Tuesday and Thursday 4:00pm-5:15pm

Lecture location: DCIH 210

### 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.

### Optional Course Material

- James N. Helfrich, Security for Software Engineers, Chapman and Hall/CRC.
- Gary McGraw, Software Security – Building Security In, Addison-Wesley.
- Brian Chess and Jacob West, Secure Programming with Static Analysis, Addison-Wesley.
- Michael Howard and David LeBlanc, Writing Secure Code, 2nd ed., Microsoft Press.
- Patrick Engebretson, The Basics of Hacking and Penetration Testing, Syngress.

## Exams

| Exam | Date | Time | Location |
|---|---|---|---|
| **Midterm** | Thursday, October 12 | 4:00pm-5:15pm | DCIH 210 |
| **Final** | Tuesday, December 12 | 4:00pm-5:50pm | DCIH 210 |

## Course Schedule (Tentative)

| Week | Topic |
|---|---|
| **Week 1** | Course Organization<br>Introduction to Security Engineering<br>Software Security Fundamentals |
| **Week 2** | Software Security Development Lifecycle Processes and Activities<br>Requirements Engineering for Secure Software |
| **Week 3** | Secure Design Principles and Threat Modeling<br>Ubuntu 20.04 VM Setup for SEED Labs (https://www.seedsecuritylabs.org) |
| **Week 4** | Linux Security Basics (Ch. 1)<br>Set-UID Programs; Environment Variables and Attacks (Ch. 2 & Ch. 3)<br>SEED Lab 1: Set-UID Programs and Environment Variables |
| **Week 5** | Buffer Overflow Attack (Ch. 4)<br>SEED Lab 2: Buffer Overflow Attack |
| **Week 6** | Secure Coding with Static Analysis<br>Return-to-libc Attack (Ch. 5)<br>SEED Lab 3: Return-to-libc Attack |
| **Week 7** | Handling Input, Errors, and Exceptions<br>Midterm Exam |
| **Week 8** | Format String Vulnerability (Ch. 6)<br>SEED Lab 4: Format String Vulnerability |
| **Week 9** | Fall Break |
| **Week 10** | Software Security Testing<br>Race Condition Vulnerability (Ch. 7)<br>SEED Lab 5: Race Condition Vulnerability |
| **Week 11** | Shellcode (Ch. 9)<br>SEED Lab 6: Shellcode |
| **Week 12** | Reverse Shell (Ch. 10)<br>SEED Lab 7: Reverse Shell |

| Week | Topic |
|---|---|
| **Week 13** | Web Security Basics (Ch. 11)<br>Cross-Site Request Forgery Attack (Ch. 12)<br>SEED Lab 8: Cross-Site Request Forgery Attack |
| **Week 14** | Cross-Site Scripting Attack (Ch. 13)<br>SEED Lab 9: Cross-Site Scripting Attack |
| **Week 15** | SQL Injection Attack (Ch. 14)<br>SEED Lab 10: SQL Injection 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 |
|---|---|
| **Term Paper or SEED Lab** | 10% |
| **SEED Labs (10)** | 40% |
| **Midterm** | 25% |
| **Final** | 25% |

### SEED Labs

The lab work aims to provide practical and hands-on experience in attacks and vulnerabilities. There will be 10 labs over the duration of the semester, each of them worth 4% of your grade. We will run the labs on Ubuntu 20.04 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 and your findings. You will be graded on these reports.

### Term Paper or SEED Lab

There is a semester-long term paper or an extra unguided lab that students need to complete by Sunday, December 3rd. 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://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- 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 10th by 5:00pm

Other important dates: Fall 2023 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 School of Computing and Information Systems.

### 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.

## Disabilities 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, as early planning is essential. If you feel that you need accommodations in this course, you must present a memo to me from Disability Support Resources (DSR), indicating the existence of a disability and 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 Disability Support Resources office (215 CON) by calling (616) 331-2490 or by email to dsrgvsu@gvsu.edu. You can also visit the DSR website here Disability Support Resources. Please note that I cannot provide accommodations based upon disability, until I have received a copy of the DSR issued memo. Furthermore, if you have a disability and 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.