CIS 311: APPLICATION SECURITY

Class Schedule:	Tuesday, Thursday 2pm to 4pm
Instructor:	Chad Johnson
Office:	SCI B231
Email:	Chad.Johnson@uwsp.edu
Office hours:	Tuesday and Thursday, 1pm to 2pm

COURSE DESCRIPTION

This course is a of the principles, practices, procedures, and methodologies to ensure security of data within applications. It examines secure coding practices and processes, web application security configuration management techniques, and web application security standards.

COURSE OBJECTIVES

- Understand application security testing methodologies.
- Describe threat vectors and attack methods of applications.
- Evaluate application security risks and associated remediations.

TEXTBOOK

- We will be using open-source texts, posted to Canvas.

LECTURES

- Lecture notes will be posted in Canvas. I make every effort to make my notes available, but I may decline to include them at my discretion.
- Students are strongly encouraged to attend each class and actively participate in class discussions.
- In general, I do not believe in taking attendance. However, class attendance may be taken in any class without notification in advance.

GRADING

- 1 Exam: 20%
- 1 Code Audit: 25%
- 5 Labs: 55% (11% each)

Final grades will be assigned according to the following scale:

A: score >= 90	A-: 87 <= score < 90	
B+: 83 <= score < 87	B: 80 <= score < 83	B-: 77 <= score < 80
C+: 73 <= score < 77	C: 70 <= score < 73	C-: 65 <= score < 70
D: 60 <= score < 65		
F: score < 60		

Scale may be adjusted, depending on the overall performance of the class.

ASSIGNMENTS AND DEADLINES

- Labs will be a variety of tasks. Some may require writing a short paper. Others might require completing multiple steps to achieve a goal (as in a CTF.) Each assignment will have those expectations detailed in the assignment instructions.
- Exams are open note/book, and you can use the Internet to search for answers. Please do not collaborate on them. They are not group assignments. You will have the week to complete the exam. Two attempts. Questions will be randomly chosen from a bank. Multiple-choice, multi-select, and true/false only. If you miss an exam, it cannot be made up.

OFFICE HOURS POLICY

- I prefer that you contact me via email.
- Virtual office hours available upon request.

REGRADING

Grades will be posted in Canvas. After the scores are announced, you have 7 days to request regrading by contacting the instructor (office hours or email). Your grade will be final after 7 days.

CANVAS

The Canvas URL is https://canvas.uwsp.edu. Use your UWSP NetID and password to login. We use Canvas for everything from important announcements, instructions, assignment submissions, and grades.

ACADEMIC INTEGRITY

The university cannot and will not tolerate any form of academic dishonesty by its students. This includes, but is not limited to cheating on examinations, plagiarism, or collusion. **Any form of academic dishonesty may lead to F grade for this course.**

STUDENTS WITH DISABILITIES

If you require accommodation based on disability, please let me know. I am willing to provide any reasonable accommodations you require. The sooner you inform me the better.

TENTATIVE SCHEDULE

Week	Lecture Topics	Due	Read
1	Environment setup, pwntools		
2	Application Attacks Overview		
3	Traditional buffers overflow, no protections		
4	Stack Cookies, and bypass techniques	Lab 1	
5	DEP/NX, and bypass techniques		
6	ASLR/PIE, and bypass techniques	Lab 2	
7	Uninitialized variables		
8	TOCTOU, race conditions	Exam	
---SPRING BREAK ---			
9	Heap: internals, heap overflows, and tcache poisoning		
10	Heap: double-free exploitation, and chunk size manipulation	Lab 3	
11	Source code auditing, Scan-build, Weggli		
12	Fuzzing, AFL, Libfuzzer	Lab 4	
13	Web app exploits (XSS, CSRF, SSRF), OWASP		
14	Secure Coding, code reviews	Lab 5	
15	Development Risk Mitigations		
16	FINALS WEEK	Project	