SYSC 4907 – Fall 2026/Winter 2027

Supervisor	Nafiseh Kahani
Co-supervisor	
Course section	SYSC 4907 Y
Project ID	
Project title	Defensive Security Analysis Pipeline
Project description	This project proposes a multi-agent defensive security analysis pipeline that reviews source code for potential vulnerabilities using a coordinated set of specialized agents. The system analyzes a submitted repository or pull request, identifies the programming language and framework, runs static analysis tools, and enriches the findings by searching existing threat and vulnerability knowledge bases such as CWE, CVE/NVD, OWASP Top 10, and dependency vulnerability databases. Each agent has a focused responsibility, such as understanding the codebase, detecting risky patterns, checking vulnerable dependencies, validating exploitability, and ranking findings by severity and confidence. A key feature of the pipeline is that it goes beyond simply reporting vulnerabilities. After identifying a potential issue, the system generates security-focused regression tests to check whether the vulnerability is actually exposed and to ensure it does not reappear after a fix. For example, if the system detects possible SQL injection, insecure authentication logic, path traversal, or hardcoded secrets, it can generate relevant tests, recommend secure code changes, and re-run verification steps after remediation. The final output is a developer-friendly security report that includes affected files, vulnerability explanation, threat database mapping, severity, generated tests, and suggested fixes.
Program(s)	Computer Systems Software
Maximum number of students	3
Meeting time with supervisor (optional)	
Do you want the student to contact you before the office assign this project to them ? (Yes/No)	Yes