



# Software Security

## CSE 5474

**Credit Hours:**

3.00

---

**Course Levels:**

Undergraduate (1000-5000 level)

Graduate

---

**Course Components:**

Lecture

---

**Course Description:**

Software security fundamentals, secure coding principles and practices, common software vulnerabilities, memory exploits (shell code), vulnerability analysis (e.g., reverse engineering, fuzzing and symbolic execution), and defenses against common vulnerability exploitation.

---

**Prerequisites and Co-requisites:**

Prereq: 2431, or Grad standing.

---

**Course Goals / Objectives:**

- Be competent with software vulnerability understanding and assessment
  - Be competent with program analysis for software vulnerability discovery
  - Be competent with software hardening countermeasures
  - Be familiar with secure coding principles and practice
  - Be familiar with software threats in new emerging platforms
- 

**Course Topics:**

- Secure software principles and practice
  - Memory safety, memory corruption & vulnerabilities
  - Vulnerability identification (fuzzing, symbolic execution)
  - Exploit development (Shellcode, Return oriented programming)
  - Defenses: Canary, address space layout randomization (ASLR), data execution prevention (DEP), control flow integrity (CFI), software fault isolation (SFI)
-

**Designation:**

Elective