

Caleb Warzocha

warzochaec@gmail.com – [calebwarzocha.dev](mailto:warzochaec@gmail.com) – www.linkedin.com/in/caleb-warzocha/

Education

Worcester Polytechnic Institute (WPI), Worcester, MA
Bachelor of Science in Computer Science

May, 2027
GPA: 3.42

Experience

Undergraduate Research Assistant, Cake Lab (WPI)

Summer 2026

Worked in the WPI Cake Lab under Professor Robert Walls, researching and evaluating the performance of the Bounce Allocator, a kernel and userspace protection against use-after-free attacks, as well as generalizing it to a desktop Linux environment.

- Built a custom Linux kernel from Radxa's kernel source and build environment, enabling MTE support on new ARM hardware with no standard kernel support.
- Deployed the Bounce allocator in both kernel space and userspace on the new hardware.
- Selected and ran SPEC CPU benchmarks validated by prior published research to compare the Bounce allocator against other allocators, debugging Bounce Compiler issues along the way.

Assistant Land Surveyor

Summer 2024

Collected field data using GNSS equipment, total stations, and digital levels.

- Interpreted site plans in order to set proper baseline locations and used specialized tools to take measurements.

Projects

Major Qualifying Project: BSim and Stability, Cake Lab (WPI)

Aug 2026 - Jun 2027

Senior capstone, under professor Robert Walls, researching how to make Ghidra's BSim more robust to compiler, architecture, and optimization-level changes by replacing its usual TF-IDF feature weighting with a stability-aware coefficient.

- Researched how Ghidra's BSim tool generates and matches binary function signatures to identify where custom feature weighting could be applied.
- Built and tested a modified Ghidra/BSim distribution that feeds a stability-coefficient lookup table into BinID computation.
- Developing a script to sweep BSim's hash-table count (L) and bucket-bit-width (K) to identify the configuration that maximizes true-positive function matches.

Buffer Overflow Attack Lab, Machine Org & Assembly Language

April 2025

Developed attacks to expose and understand buffer overflow vulnerabilities.

- Created exploits using x86-64 assembly, debugging tools (GDB, OBJDUMP), and custom utilities.
- Executed code injection and return-oriented programming attacks by chaining gadgets.

TA Application & Management Website, Software Engineering

November 2024

Worked with a team of 5 to develop a full-stack web platform for managing TA applications and class assignments

- Programmed backend logic in C and frontend layout in HTML
- Built user registration, login, and class assignment features with persistent data storage
- Used Git and GitHub for source control, code reviews, and iterative development

Coursework & Skills

Relevant Courses: Algorithms, Software Engineering, Systems Programming, Machine Org & Assembly, Database Systems, Intro to Security, Software Security, Digital Forensics (*Winter 27'*), Reverse Engineering (*Spring 27'*), Web Application Security (*Winter 26'*)

Languages: Java, C, C#, Python, DrRacket, HTML, x86-64 Assembly, x86 Assembly

Tools & Technologies: Visual Studio Code, Git, GitHub, SQL, AWS(EC2), Linux, Matlab

Security: OS security fundamentals (Linux/Windows), authentication & session management, cryptography, Ghidra, Pwntools, buffer-overflow exploitation, Code Injection, Return-Oriented Programming, binary exploitation

Activities

Vice President, WPI Cybersecurity Club (CSC)

Aug 2026 - Present

House Manager, Phi Kappa Theta Fraternity

Jan 2025 – Jun 2026

Student Athlete, WPI Men's Varsity Rowing

Sep 2023 - Jun 2026

Director of Risk, Inter-Fraternity Coalition (IFC)

Dec 2024 - Dec 2025