Carson Hedrich

carsonhedrich@gmail.com • chedrich3@gatech.edu • (239) 989-8301 • carsonhedrich.github.io

Education

Georgia Institute of Technology Anticipated Graduation December 2025
B.S. Computer Science Current GPA: 3.85
Relevant Coursework: Perception & Robotics, Systems and Networks, Design & Analysis of Algorithms, Information Cybersecurity, Embedded Systems Design

Experience

Student Training in Engineering Program (STEP) Intern Summer 2023
Google – US-NYC-9TH

- Collaborated as part of a pair to significantly extend the back-end and front-end functionality of a feature that provides information into an advertiser's performance.
- Utilized **asynchronous programming, unit testing, end-to-end testing, and debugging**.
- Participated in software development life cycle by writing design documents, implementation, going through design reviews, and preparing for launch.
- Utilized full stack development, using **Java**, **Dart**, **CSS**, and **Mockito**.

Skills

Technical Skills: Java, C++, C, Python, Assembly, Dart, CSS, JavaScript
Cybersecurity Skills:

- Malware Analysis using **IDApro/Ghidra, Ollydbg**
- Digital Forensics using **Autopsy**
- Web and system security testing: **SSRF, CSRF, XSS, SQL injection, reverse shells, privilege escalation**
- Tools including **ffuf, Gobuster, Hydra, Nmap**

Projects

Information Cybersecurity Semester Project Fall 2024

- Investigated a simulated computer of a fake suspect for signs of illegal activity using **Autopsy**.
- Examined a wide array of clues from the suspect, including messages hidden using steganography, obfuscation, suspicious web activity, and network packet traces.
- Exploited vulnerabilities in the simulated websites to gain more information and gain proof of the suspect's guilt.

Reverse Malware Engineering Project "Harulf" Spring 2025

- Performed static and dynamic analysis on a packed/encrypted virus to determine its method of infection and purpose.
- Applied sandboxing and debugging techniques to safely unpack the virus using **Ollydbg**, extract the unencrypted binary, and analyze it using **IDApro**.
- Conducted assembly-level analysis of the Windows PE file to discover polymorphic capabilities of the virus, which could be used to improve threat definitions.

Professional Development

TryHackMe – Online Cybersecurity Training Platform September 2025 - Present

- Practicing both offensive and defensive techniques through cybersecurity labs that simulate real-world scenarios.
- Developing hands-on skills in ethical penetration testing using common tools (**Nmap, Hydra, Gobuster**, etc.) to discover and exploit security vulnerabilities in simulated attack scenarios.
- Analyzing compromised systems to investigate malicious activity and determine the extent of the breach's impact.