Robert Boada

rnb2135@columbia.edu • (787)-672-4256 • GitHub: rboada26 • LinkedIn: linkedin.com/in/robert-boada

EDUCATION

Columbia University | New York, NY

B.A. in Computer Science **May 2026**

Relevant Courses: Data Structures in Java, Advanced Programming, Fundamentals of Computer Systems, Computer Networks, Security I, Security II, Malware and Reverse Engineering, Architecture, System on Chip

TECHNICAL SKILLS

Programming Languages: Java, C/C++, Rust, Python, Javascript, MIPS, Bash, Ocaml
Technologies: Git, Docker, Fuzzing, Google Cloud, Vim, Networking, Flask, AWS
Operating Systems: Linux, Windows

RELEVANT EXPERIENCE

Cyber NYC REU | Summer Research Intern | New York, NY **May 2025 - Aug 2025**

- Worked under Professor Jana and PhD students to develop a fuzzer that uses Gemini LLM to optimize seed expansion with traditional mutation strategies (coverage-guided). Prompt Engineered dynamic coverage aware prompts. Used Magma and FuzzBench to conduct benchmarks on open source targets. Supported by Google's Cyber NYC Institutional Research Program through Columbia Engineering.

Columbia University Department of Computer Science | Student Researcher **Aug 2024 - Present**

- This project aims to build a visualization tool that enables developers to gauge the progress a fuzzer has made while testing a given software and interactively tune the fuzzer's configuration to address observed bottlenecks. This visualization and interactive debugging tool will be built on top of FOX , our recently published state-of-the-art coverage-guided fuzzer. Using C and Python.

Software and Security Engineer Intern | GM SecTec | San Juan, PR **June 2024 - Aug 2024**

- Implemented web application scanning and enumeration tool in Rust and Python.
- Competed in internal company CTF event and got first place
- Gained new exposure to cybersecurity and software development practices such as: Steganography, Reverse Engineering, Release Testing, DevOps, Reverse Shells, and Computer Networking.

PROJECTS

L1es | Personal Project **June 2025 - Present**

- Developed a comprehensive command-line cache simulator implementing multiple cache architectures (direct-mapped, set-associative, fully associative) with configurable replacement policies. Built timing-based side-channel attack demonstrations including Prime+Probe, Flush+Reload, Spectre, and Meltdown simulations. Created professional CLI interface with CSV/JSON data export capabilities for security research and microarchitectural vulnerability analysis. Enables quantitative comparison of cache design security trade-offs and attack effectiveness across different configurations.

Cybersecurity Projects | Personal Projects **Aug 2021 - Present**

- AES file encryption system implemented in C/C++
- Packet Sniffer implemented in Rust
- Created basic keylogger implemented in Rust
- CTF skills: Buffer Overflows, SQL injection, XSS, Malware Analysis/Reverse Engineering, Web App Security, CLI
- Participated in several CTF competitions since high school: PicoCTF, Hack the Box, Try Hack Me, Google CTF