Alan Cao

Security Engineer

CONTACT

+1 (646) 979-0481

alan.cao@nyu.edu

https://codemuch.tech

ex0dus-0x

SUMMARY

Second-year university student and security engineer with 2+ years of experience in industry and academia. I specialize in architecting and auditing secure systems and software, while also incorporating offensive security research to help protect the digital ecosystem for all.

SKILLS

Security: Offensive Security, Vulnerability Assessment, Threat Detection, Reverse Engineering, Cryptography

Programming: C/C++, Rust, Python, SQL, x86 Assembly, Go, Verilog, JavaScript, HTML/CSS

Software Technologies: Unix Shell, Git, Vim, Docker, Vagrant, Clang/LLVM, CI/CD, AWS, Sentry, Binary Ninja

Hardware Technologies: LTSpice, Xilinx

Other: Technical Writing, Chinese Mandarin

EDUCATION

New York University

B.S Computer Engineering, Class of 2023

WORK EXPERIENCE

OSIRIS Lab @ NYU

Jan. 2020 to Current

Security Researcher

- Conducting security research and bug-hunting efforts in compiler security, specifically in C/C++ obfuscation, WebAssembly and LLVM.
- Maintaining lab infrastructure through internal development pipeline to deliver core backend services for training and research.
- Led security training sessions on reverse engineering and cryptography to engage with aspiring security students.

Trail of Bits

Oct. 2018 to Jan. 2020

Security Engineer (Intern)

- Improved symbolic execution engine Manticore to help support cryptographic software assurance for open-sourced projects.
- Implemented a fuzzing interface API and an ensemble-based fuzzing engine into the DeepState framework to empower security unit testing.
- Engaged in security assessments for corporate vendors, using both industry and in-house security tools to help disclose security issues.
- Published multiple articles on internship research to company blog to share knowledge with security community.

VOLUNTEERING

CSAW @ NYU

Jan. 2020 to Current

- Co-lead and organizer for the collegiate CSAW CTF competition, involved in challenge writing and deployment, technical logistics, and infrastructural maintenance for 1,000+ teams in 90 countries.

PROJECTS

Confine - Containerization tool for dynamic threat analysis (https://github.com/ex0dus-0x/confine).

Boa - Web-based automated reverse engineering platform for black-box Python malware and executables (http://boa.codemuch.tech).

Ghostpass - Privacy-First Secrets Cryptosystem written in Go to prevent rubber-hose cryptanalysis (https://ghostpass.github.io).

Brute - Crowd-sourced credential stuffing engine built for security professionals (https://github.com/ex0dus-0x/brute).

Binsec - The Swiss Army Knife for Binary (In)Security, a cross-platform utility used to detect binary security mitigations (https://github.com/ex0dus-0x/binsec).