

Nick Gregory

nick@nickgregory.me

INTERESTS	Computer security (especially reverse engineering and binary exploitation), meteorology, photography, bowling.
WORK HISTORY	<ul style="list-style-type: none">Software Engineer, Google Jul 2022 – PresentSenior Threat Researcher, Capsule8 (Acquired by Sophos) Jan 2019 – Jul 2022Research Intern, Capsule8 May 2018 – Aug 2018<ul style="list-style-type: none">Researched and implemented strategies to detect zero-day attacksMySQL Production Engineering Intern, Facebook May 2017 – Aug 2017<ul style="list-style-type: none">Rewrote internal tools used to build out new MySQL clustersResearch Intern, M.I.T. Lincoln Lab May 2016 – Aug 2016<ul style="list-style-type: none">Researched techniques to emulate complete embedded systems in the QEMU hardware emulator
EDUCATION	NYU Tandon School of Engineering , Brooklyn, New York, USA <ul style="list-style-type: none">B.S. in Computer Science Sep 2015 – May 2019
OTHER EXPERIENCE	<ul style="list-style-type: none">Vice President & Infrastructure Manager, NYU OSIRIS Lab Sep 2015 – Dec 2018<ul style="list-style-type: none">Oversaw most lab research efforts, and managed all lab infrastructureCo-Lead, CSAW CTF 2016 – 2018<ul style="list-style-type: none">Wrote challenges for, and helped run CSAW CTFDuring this time, CSAW Finals expanded from 1 site to 5 international locations
TALKS	<ul style="list-style-type: none">Uncommon Sense: Detecting Exploits with Novel Hardware Performance Counters and ML Magic, Black Hat USA 2020Using Linux Tracing for Security, CSAW C2 2019
PUBLICATIONS	<ul style="list-style-type: none">Using Undocumented Hardware Performance Counters to Detect Spectre-Style Attacks, CAMLIS 2021<ul style="list-style-type: none">Nick Gregory, Harini KannanSoK: Enabling Security Analyses of Embedded Systems via Rehosting, ACM ASIACCS 2021<ul style="list-style-type: none">Andrew Fasano, Tiemoko Ballo, Marius Muench, Tim Leek, Alexander Oleinik, Brendan Dolan-Gavitt, Manuel Egele, Aurélien Francillon, Long Lu, Nick Gregory, Davide Balzarotti, and William Robertson
PROJECTS	<ul style="list-style-type: none">Holodeck<ul style="list-style-type: none">Assisted rehosting of embedded devices in QEMUIntroduction to Offensive Security<ul style="list-style-type: none">A course I co-created to teach offensive security at NYUDispatch<ul style="list-style-type: none">A Python framework for programmatically disassembling and patching binariesWeather Explorer<ul style="list-style-type: none">A fully open-source website for exploring current weather and forecast dataSnapshot LKM<ul style="list-style-type: none">A kernel module to add a fast snapshot/restore mechanism for fuzzing. Adopted by the AFL++ project.
BUGS	<ul style="list-style-type: none">CVE-2022-25636 2022<ul style="list-style-type: none">A kernel heap out of bounds write leading to privilege escalation
ACHIEVEMENTS & AWARDS	<ul style="list-style-type: none">Bug Bounties 2016 – Present<ul style="list-style-type: none">Found and reported bugs to 4 Alexa top 1000 sites, multiple of which could have led to complete site compromise.10th Place, DEFCON Finals (RPISEC) 201816th Place (10th Academic), iCTF (NYUSEC) 20179th Place, CSAW CTF Finals (NYUSEC) 2015
SKILLS	C, C++, Go, Python, x86 assembly, ARM assembly, SQL