Nathaniel Good

✉ stanleygvi@gmail.com ☎ (510) 501-4919 github.com/stanleygvi linkedin.com/in/nathaniel-good

EDUCATION

B.S. in Computer Science 06/2026
University of California, Santa Cruz Santa Cruz, CA

- Relevant Coursework: Operating Systems, Computer Networking, Computer Security, Distributed Systems, Data Structures and Algorithms

TECHNICAL SKILLS

Security
MITRE ATT&CK, network traffic analysis, incident response, web application security, system hardening, Windows hardening, Windows event auditing

Systems / Infrastructure
Linux, Windows, Docker, Git, PostgreSQL, Google Cloud Platform

Security Tools
mitmproxy, ModSecurity, WinRM

Languages
Python, Go, C++, C, Bash, SQL, JavaScript

CYBERSECURITY EXPERIENCE

CCDC / WCCDC 2025 – Present
UCSC Slug Security
its.ucsc.edu/its-news/the-next-generation-of-cyber-defenders/

- Hardened compromised Linux and Windows systems during live red-team attacks by removing persistence, securing exposed services, and restoring operational functionality
- Investigated attacker activity during live cyber defense exercises, performing incident response and threat remediation across an 8-person defense team
- Implemented an automated workflow to deploy containerized ModSecurity WAFs protecting exposed web services
- Implemented a WinRM-based Windows registry hardening task to enforce Defender, auditing, and firewall logging baselines across hosts
- Placed 5th in the 2026 WCCDC qualifiers and advanced to regionals

Open Source Contributor 06/2023 – 09/2023
Google Summer of Code at Mitmproxy
mitmproxy.org/posts/har-support/

- Implemented HAR import/export support in mitmproxy to reconstruct HTTP traffic flows for web traffic analysis and debugging
- Developed Pytest coverage for HAR parsing across multiple browser and client formats, achieving 100% code coverage for the feature

SECURITY PROJECTS

MITRE ATT&CK Command Pipeline 12/2025
Security Research Project
github.com/stanleygvi/MITRE_CMD_GEN/blob/main/report/report.md

- Designed a multi-stage pipeline that generates attacker scenarios and OS-specific commands from MITRE ATT&CK tech- niques
- Built retrieval and validation stages to ensure generated commands aligned with MITRE ATT&CK techniques and OS- specific attack behavior
- Packaged 500+ validated commands into a Parquet dataset for adversary emulation and detection research

RELEVANT EXPERIENCE

AppCensus 06/2024 – 08/2024
Data Analyst Intern

- Analyzed network traffic across 200+ mobile apps to identify tracking SDK behavior and expand internal detection coverage
- Built internal Flask and JavaScript tooling to search network analysis artifacts associated with SDK detections

Good Research 05/2021 – 06/2023
Junior Data Scientist

- Developed Python tooling to extract tracker domains from captured web traffic and enrich IP data with GeoLite ASN metadata for attribution and tracking infrastructure analysis
- Built a PyTorch screenshot-classification pipeline for 383 labeled screenshots across 13 mobile apps, achieving 94% accuracy