Hamzeh Emreish

Security Researcher and Full-Stack Developer

Yonkers, NY | 914-335-5761 | hamzehemreish37@gmail.com
linkedin.com/in/hamzeh-emreish | github.com/sh4faq | hamzehemreish.netlify.app

Anthropic Cyber Verification Program | Approved for dual-use security research, May 2026

SUMMARY

CS graduate (CUNY Lehman, May 2026) who both builds and breaks software. Independent bug bounty researcher on HackerOne, Bugcrowd, and Intigriti, Security+ certified, and approved through Anthropic's Cyber Verification Program for dual-use security research.

TECHNICAL SKILLS

Offensive Security: Web & API pentesting (REST, GraphQL), SSRF & cloud metadata (AWS IMDS), OAuth/auth & access-control flaws, injection & LFI, source code review, CVSS/CWE, PoC development

AI / LLM Security: GenAI attack surface, prompt injection, agentic AI testing, MCP tool development, AI-driven recon automation

Tooling: Burp Suite, Metasploit, SQLMap, Nmap, nuclei, httpx, subfinder, ffuf, gobuster, Shodan, Ghidra, Wireshark; SNORT, Splunk, Auditd (blue team)

Programming & Full Stack: Python, JavaScript, Bash, Java, SQL; React, Node.js, Express, PostgreSQL; REST API development; security automation

Infrastructure: Proxmox, Docker, VMware, Hyper-V, Tailscale, Active Directory, TCP/IP, DNS, SSH

SECURITY RESEARCH

Independent Security Researcher | Bug bounty: HackerOne, Bugcrowd, Intigriti

Jan 2024 to Present

- Critical (CVSS 9.1): parser allowlist bypass enabling Local File Inclusion via load_file() in an ORDER BY clause, root-caused to 4 of 5 SetOp AST fields left unguarded in vitess walkSubtree after the CVE-2026-27876 fix. Intigriti (triaged duplicate).
- High (CVSS 8.6): SSRF in a GenAI knowledge-base crawler, bypassing the hostname deny-list and IP check via an HTTP 302 redirect to reach 169.254.169.254 cloud metadata and internal infrastructure. Intigriti (submitted, awaiting triage).
- OAuth token exposure to authentication bypass: tokens in window.__STATE__ on a public OAuth page allowed account modification (PUT returned HTTP 200) and mass user enumeration across IDs 1 to 231M+ with no rate limiting. Bugcrowd (ruled P5/Informational, test user).
- Medium: unauthenticated mail relay enabling email spoofing with valid DKIM/SPF; delivered CVSS analysis and remediation guidance. HackerOne (triaged valid).

EXPERIENCE

Equinox | Manager on Duty

Scarsdale, NY | Nov 2023 to Present

- Run point on in-house club technology (BitLocker recovery, Windows crashes, POS configuration, member-facing hardware); diagnose first, escalate to the vendor only on genuine part failure.
- Closed a $1,500 labor overrun to zero in three months; caught a month-long account-sharing fraud from a photo-ID mismatch; trained 10+ teammates; CPR/AED certified.

Yonkers Car Wash | Web & Operations

Yonkers, NY | May 2025 to Present

- Built and run the full-stack membership/billing site with remote ICS monitoring via RDP/VNC over Tailscale; raised renewals 35%; supervised and trained a 15-person team.

PROJECTS

- MCP Kali Server (2024): merged pull request #5 to an open-source AI-pentesting framework after maintainer review, adding 12 recon tools (subfinder, nuclei, httpx, arjun, subzy, Shodan, and more), SSH session management with file transfer, and reverse-shell handlers.
- Burp Suite Automation API (2024): Python extension exposing Burp's proxy, scanner, and repeater over a REST API so scans can be scripted and driven by AI tooling.

EDUCATION & CERTIFICATIONS

CUNY Lehman College, B.S. in Computer Science (Concentration in Artificial Intelligence), GPA 3.4. Bronx, NY. Graduated May 2026.

Certifications: Anthropic Cyber Verification Program (May 2026); CompTIA Security+ SY0-701 (Jul 2024); Google Cybersecurity Certificate (Aug 2024); CodePath Intermediate Cybersecurity & Python (Oct 2024).