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

Computer Science graduate (CUNY Lehman, May 2026) who builds and breaks software. I run independent bug bounty research on HackerOne, Bugcrowd, and Intigriti, with findings across SSRF to cloud metadata, authentication and access-control bypass, injection and LFI, and email security, alongside full-stack development and customer-facing operations work. I write my own tooling (a REST API over Burp Suite, twelve recon tools merged into an open-source pentesting framework) and document root cause and remediation, not just the bug. Security+ certified and approved through Anthropic's Cyber Verification Program for dual-use security research.

TECHNICAL SKILLS

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

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

Security Tooling: Burp Suite, Metasploit, SQLMap, Nmap, Hydra, John the Ripper, nuclei, httpx, subfinder, ffuf, gobuster, arjun, subzy, waybackurls, Shodan

Detection & Blue Team: SNORT IDS, Splunk, Wireshark, Auditd, NGINX rate limiting, log/traffic analysis

Programming: Python, JavaScript, Bash, Java, SQL; REST API development; security automation

Web & Full Stack: React, Node.js, Express, PostgreSQL, HTML/CSS, Vite; Vercel / Railway / Netlify deployment

Infrastructure & Virtualization: Proxmox, Docker, VMware, Hyper-V, Tailscale, RDP/VNC, Active Directory, Group Policy, TCP/IP, DNS, SSH

Reverse Engineering: Ghidra, Cheat Engine, binary/hex & protocol analysis (SmartFoxServer, SWF/ActionScript), proprietary file-format documentation, Blender Python API

SECURITY RESEARCH & FINDINGS

Independent bug bounty research, January 2024 to Present. Program names are under non-disclosure; available on request. Statuses are reported honestly (triaged-valid, awaiting triage, duplicate, or informational).

Critical, CVSS 9.1 | Parser allowlist bypass to Local File Inclusion | Intigriti (triaged duplicate)

In a monitoring and observability platform's SQL expression engine, the fix for CVE-2026-27876 left 4 of 5 SetOp AST fields skipped by vitess walkSubtree unguarded, enabling Local File Inclusion via load_file() inside an ORDER BY clause. Same primitive class as CVE-2024-9264.

High | Email injection in a Frappe contact form | HackerOne (submitted, awaiting triage)

On a crypto platform, the sender parameter is used as the email recipient rather than the sender, enabling attacker-controlled outbound mail from the platform's legitimate domain with full SPF/DKIM/DMARC alignment and no rate limit. Working end-to-end PoC with a chained phishing payload.

High, CVSS 8.6 | SSRF in a GenAI Knowledge Base crawler | Intigriti (submitted May 2026, awaiting triage)

An HTTP 302 redirect bypass of the crawler's hostname deny-list and IP-resolution check reaches 169.254.169.254 cloud metadata and internal infrastructure.

High, CVSS 7.5 | Admin user enumeration via Cognito ForgotPassword | HackerOne (triaged duplicate)

An unauthenticated GraphQL query leaks the admin client_id; Cognito's ForgotPassword endpoint returns distinct responses for valid versus invalid usernames (CodeDeliveryDetails vs UserNotFoundException), enabling admin email enumeration with a first-letter leak. Patched shortly after testing.

OAuth token exposure to authentication bypass | Bugcrowd (ruled P5/Informational, test user)

Access tokens embedded in window.__STATE__ on a public OAuth authorize page enabled authentication bypass with confirmed account modification (PUT to a user resource returned HTTP 200, first_name modified) and mass user enumeration across IDs 1 to 231M+ via email, name, and query searches without rate limiting.

Hardcoded production API credentials in public JavaScript (CWE-798, CWE-522) | Bugcrowd (triaged duplicate)

Production API credentials hardcoded in a publicly accessible JavaScript config on a domain-registry product granted unauthenticated access to all seven backend API endpoints. Duplicate of an earlier April 2025 report with restricted key scope.

Medium | Unauthenticated mail relay | HackerOne (triaged valid)

Email spoofing with valid DKIM/SPF signatures; provided CVSS analysis and remediation guidance.

PROFESSIONAL EXPERIENCE

Equinox | Manager on Duty

Scarsdale, NY | Nov 2023 to Present

- Promoted from Front Desk Associate (Mamaroneck); flagship rotations at Hudson Yards and Printing House.
- Contribute to strategy meetings with the General Manager, Regional Training Manager, and Facility Manager on member retention, personal-training conversion, facility quality, and staff performance.
- Rebuilt the front desk schedule and shift structure; closed a $1,500 labor budget overrun to zero within three months.
- Run point on in-house club technology: BitLocker recovery, Windows blue screens, POS configuration, audio system faults, member-facing hardware. Diagnose first, escalate to the vendor only when a part has genuinely failed.
- Caught a member accessing the club on someone else's account for nearly a month from a photo-ID mismatch the desk had missed; escalated to the GM, who verified and acted.
- Coach the front desk team on luxury-club standards; trained and onboarded 10+ team members; cross-trained in Pro Shop. CPR/AED certified.

Yonkers Car Wash | Website & Management System

975 Midland Ave, Yonkers, NY | May 2025 to Present

- Developed and support the full-stack membership and billing website, integrating member management, customer inquiries, and remote monitoring of car-wash systems via RDP/VNC over Tailscale.
- Manage ICS infrastructure, the database, and billing automation; increased renewals 35%.
- Supervised and trained a 15-person team; monitor cash registers and site operations remotely.

Central Deli & Convenience | Co-owner

Mamaroneck, NY | Oct 2023 to Feb 2025

- Hired and trained a team of seven and established service standards; owned finances (expense tracking, overhead, profit, forecasting); ran food safety, inventory, and quality control; designed the in-store and digital TV menus.

PROJECTS & ENGAGEMENTS

MCP Kali Server | Open-source AI-pentesting framework (Dec 2024)

Merged pull request #5 after maintainer review, adding 12 recon tools (subfinder, nuclei, httpx, arjun, fierce, byp4xx, subzy, assetfinder, waybackurls, Shodan), SSH session management with file transfer, and reverse-shell handlers.

Burp Suite Automation API (Nov 2024)

Python extension exposing Burp Suite control over a REST API for automated, AI-driven security testing. github.com/sh4faq/burp-suite-api

Flash MMO Protocol Reverse Engineering (Jan 2025)

Network interception (Wireshark), memory inspection (Cheat Engine), SWF decompilation (JPEXS to ActionScript), and DLL analysis (Ghidra); reverse engineered the SmartFoxServer XML/CDATA/JSON protocol and identified a client-side anti-cheat bypass (MD5 with a hardcoded salt).

Game Asset Reverse Engineering Toolkit (Dec 2024)

Reverse engineered Red Alert 2 VXL/HVA/MIX binary formats and shipped a Blender addon for 3D-to-voxel export, with a community guide.

Full-Stack Merchant System (Nov 2024)

PERN-stack CRUD application with search, sort, and dark mode; React on Vercel, Express and PostgreSQL on Railway.

Creative Coding: gesture-tracked apps

A webcam Fruit Ninja clone (MediaPipe fingertip tracking, Three.js parallax) and a TouchDesigner point-cloud destroyed by hand (MediaPipe, GLSL, real-time VFX).

CodePath Blue Team (Oct 2024)

NGINX rate limiting, SNORT IDS, and Splunk/Wireshark analysis.

EDUCATION

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

- Coursework: Data Structures, Full-Stack Web Development, Discrete Math, AI/ML, Robotics, vector calculus, probability.

SUNY Westchester Community College | Computer Programming (Programming I & II)
Valhalla, NY | ~2 years

Self-directed cybersecurity, 2022 to Present

- CTFs, Hack The Box, bug bounty programs, and PortSwigger Web Security Academy.

CERTIFICATIONS

- Anthropic Cyber Verification Program (CVP), approved May 2026, for dual-use security research (vulnerability exploitation, offensive security tooling).
- CompTIA Security+ (SY0-701), July 2024.
- Google Cybersecurity Professional Certificate, August 2024.
- CodePath: Intermediate Cybersecurity & Python Programming, October 2024.