

Karl Seryani

Toronto, ON | (647) 618-9007 | karlseryani@gmail.com | karl-seryani.github.io
linkedin.com/in/karlseryani | github.com/Karl-Seryani

EDUCATION AND CERTIFICATIONS

Western University

Bachelor of Science in Computer Science

Sept. 2022 – April 2026

London, ON

- **HTB Certified Web Exploitation Specialist (CWES)**, July 2026
- Two-time Dean's Honour List recipient

EXPERIENCE

Independent Security Researcher (Bug Bounty)

Bugcrowd, HackerOne, Intigriti, Google VRP

April 2026 – Present

Remote

- **Ranked in the Top 15 researchers** on Keeper Security's Bugcrowd program through validated findings
- **Discovered a high-severity Google Cloud flaw** in the Backup and DR product that exposed private data across separate cloud projects
- **Achieved account takeover** on NASA's GLOBE platform through stored XSS; validated as High (P2)
- **Bypassed Keeper's device-approval control**, which let unapproved devices reach authentication; drove a fix within 24 hours of validation and earned **public credit in Keeper's release notes**
- **Found a SQL injection** in Keeper Gateway's password-rotation plugins that enabled **database-account takeover** of any user; validated as High (P2), fixed, and rewarded
- **Reported 30+ vulnerabilities across 4 programs**, each with CVSS 3.1 scoring and fix guidance

Kaimz Inc.

SOC Analyst

Jan. 2025 – April 2025

Waterloo, ON

- **Built a Python integration** between Wazuh and the Jira REST API that auto-created tickets for high-severity alerts with their severity and a short summary, removing manual ticket entry
- **Configured Wazuh firewall rules** to block malicious IP addresses on monitored endpoints
- **Analyzed suspicious attachments** in VirusTotal, ANY.RUN, and Hybrid Analysis to confirm malware

OPEN SOURCE

OWASP ZAP

Contributor | Java, JUnit 5, Gradle

Jan. 2026 – June 2026

Open-Source DAST Scanner

- **Merged 3 pull requests** adding example alerts for the LDAP injection, username enumeration, and SQLite injection scan rules to ZAP's alert documentation
- **Wrote JUnit 5 tests** for alert content and built reusable alert builders that removed duplicate code

PROJECTS

Multi-Agent Security Testing Workflow

Python, SQLite, Claude Code

April 2026 – Present

- **Built a multi-agent workflow** that maps cloud APIs, runs tests, and challenges every positive result, turning 1,500+ test hypotheses into **11 Google Cloud vulnerability reports** (3 triaged, 1 accepted)
- **Cut false positives** by requiring a critic agent to fail to disprove each finding before it reaches a report; researcher, hunter, and critic roles each run on a separate AI model
- **Replaced a large Markdown context file with a SQLite state store** that tracks findings and hypotheses by unique ID, so agents query only what they need, cutting token usage and cost
- **Enforced scope and blocked duplicate tests** with a Python request tool that checks a 220-rule host allowlist and logs 3,100+ experiments as replayable evidence

TECHNICAL SKILLS

Languages: Python, Java, C, JavaScript, Bash, SQL (PostgreSQL, MySQL, SQLite)

Security: Burp Suite, Caido, OWASP ZAP, ffuf, Gobuster, Nmap, sqlmap, Nuclei, Ghidra, Wazuh

Developer Tools: Git, GitHub, Docker, Linux, Google Cloud, Jira, JUnit 5, Playwright, Gradle

AI Tooling: Claude Code, Codex, multi-agent workflows