

AMIR HOSSEINPOUR

Offensive Security Consultant – Red Team, Application Security & Vulnerability Research

Toronto, ON · amir.m.hosseinpour@gmail.com · github.com/amir-hosseinpour · hackerone.com/mghack123

SUMMARY

Offensive security consultant working across red team, web and API exploitation, and vulnerability research. At White Tuque I deliver penetration tests and red and purple team assessments for 20+ enterprise clients, operate Cobalt Strike and Havoc on red team engagements, and built the red team and penetration-testing pipeline for a major Canadian insurer, with recurring adversary simulations and tabletop exercises. Web applications are my core, the place red teams most often get in and pivot from: 120+ validated vulnerabilities on Fortune 500 programs, including a high-severity race condition at PayPal. On my own time I research hardware. A six-bug chain I found gave root on any robot in Ecovacs' Deebot fleet from any account, with six CVEs filed and disclosure under Safe Harbor, presented at BSides Toronto 2026. Co-organizer of DEFCON Toronto (DC416), where I find the researchers and presenters who speak to Toronto's security community.

CORE COMPETENCIES

Red & Purple Team	C2 operations with Cobalt Strike and Havoc, adversary simulation, tabletop exercises, privilege escalation and lateral movement, findings mapped to MITRE ATT&CK
Web, API & Mobile	External entry and internal pivots through web apps; authorization bypass, IDOR, race conditions and business-logic chains across REST and GraphQL; OAuth2.0/OIDC; iOS and Android
Network & Cloud	External and internal network assessments; AWS attack paths through IAM misconfiguration, overprivileged roles and secrets exposure
Embedded Device & Research	Firmware extraction over UART, reverse engineering, protocol analysis (MQTT), exploit chain development, CVE filing and coordinated disclosure
AI Red Teaming	Prompt injection, insecure tool use and excessive permissions in LLM and agent-based systems
Tooling	Offensive tools and automation in Python, Go and Bash; Burp Suite extensions, custom Nuclei templates, GraphQL schema tooling
Reporting & Delivery	Technical and executive reports, client scoping, presenting findings to engineers and leadership, mentoring junior testers

EXPERIENCE

White Tuque – Offensive Security Specialist

Toronto, ON · October 2024 – Present

- Deliver black-box and grey-box penetration tests, red team and purple team assessments for 20+ enterprise clients plus standalone engagements, across web, API, mobile, internal and external networks, and cloud, for fintech, insurance, manufacturing, and oil and gas clients in Canada and the US.
- Built the red team and penetration-testing pipeline for a major Canadian insurer, with recurring adversary simulations and tabletop exercises so their teams rehearse real attack-and-response scenarios instead of relying on a once-a-year test.
- Operate Cobalt Strike and Havoc C2 on red team engagements for post-exploitation, privilege escalation and lateral movement.
- Find authorization bypass, IDOR and multi-step business-logic flaws across REST and GraphQL APIs that scanners miss, including internal web apps that are often assumed safe behind the perimeter, and work with client engineers on server-side fixes.
- Assess AWS attack paths, red team identity-verification and anti-fraud flows for fintech clients, and review AI and agentic workflows for prompt injection, insecure tool use and excessive permissions.
- Lead engagements end to end, from scoping and rules of engagement through reporting and retest; write technical and executive reports mapped to OWASP and MITRE ATT&CK.
- Mentor interns on the offensive team through live engagements and report writing.

ASEC – Penetration Tester

Toronto, ON · May 2024 – October 2024

- Surfaced critical and high-severity vulnerabilities, including authentication and authorization bypasses, across web application, API and network assessments for fintech and financial-services clients in Canada, the US, Australia and Europe.
- Specialized in API and GraphQL security under the mentorship of Nick Aleks, author of *Black Hat GraphQL* and former Head of Security at Robinhood.
- Wrote a custom Nuclei template for each finding so clients could regression-test the fix in their own CI/CD pipelines.

HackerOne – Security Researcher

Remote · February 2022 – Present

- 120+ validated vulnerabilities across Fortune 500 programs, including severe findings on PayPal, Airbnb, Sony, Booking.com and AT&T; specialty in authorization bypass, privilege escalation, race conditions and multi-step business-logic chains.
- High-severity race condition in PayPal's checkout flow: token and amount verification ran in separate pipelines, so inside a time and value window a payment could be confirmed without the funds being captured.

DEFCON Toronto (DC416) – Co-organizer

Toronto, ON · 2025 – Present

- Find researchers and presenters and program the monthly talks and workshops for Toronto's security community.
- Ran the AI Fight Club at Palo Alto Networks, a hands-on workshop for 200+ practitioners on attacking and defending LLM and agent systems.

VULNERABILITY RESEARCH & DISCLOSURE

- **Embedded device research: Ecovacs Deebot fleet compromise.** Soldered onto the UART, dumped the firmware, recovered cloud credentials and mapped the MQTT topic tree. The broker trusted whatever device identity a client claimed, and the robot ran incoming commands as root with no signature check, so any authenticated account could push a shell to any robot in the fleet. Six-bug chain, six CVEs filed with MITRE, coordinated disclosure under the vendor's Safe Harbor. Presented at BSides Toronto 2026; write-up on defcontoronto.ca.

OPEN-SOURCE TOOLS

- **Eidolon** — AI-driven offensive security workspace orchestrator (MIT): per-engagement isolation, scope tokens, hash-chained audit log and three-tier command gating.
- **graphql_sdl_generator** — rebuilds and extends a GraphQL schema from scattered .gql files into a single SDL for attack-surface mapping.
- **API-Authentication-Checker** — Burp Suite extension that replays proxy-history API calls with Cookie and Authorization stripped, flagging endpoints reachable without authentication.

SPEAKING & COMMUNITY

- **BSides Toronto 2026** — "Who Else Is Cleaning Your Home?": hardware-to-cloud compromise of a robot vacuum fleet, from UART to root on any device.
- **SecTor 2025** — "When Hackers Meet Burglars: Red Teaming the Smart Building."
- **DEFCON Vancouver** (Microsoft-hosted) — API attack chains and OAuth2.0 exploitation. · **InfoSec Hamilton** — speaker.
- Organizing committee, **TASK** (Toronto Area Security Klatch), Toronto's longest-running security community: help plan its meetups and events, and spoke at TASK in 2025 and 2026.

TECHNICAL SKILLS

C2 & Offensive: Cobalt Strike, Havoc, Burp Suite Pro, Nuclei, ffuf, nmap, sqlmap, Metasploit, BloodHound, mitmproxy, Frida / objection

Hardware & IoT: UART, firmware extraction and analysis, MQTT **Cloud:** AWS (IAM, EKS, Lambda, S3)

Programming: Python, Go, Bash, JavaScript / TypeScript **Frameworks:** MITRE ATT&CK, OWASP ASVS / WSTG, PTES

Spoken languages: English, Persian, Mandarin

EDUCATION

Bachelor of Computer Engineering, University of Sistan & Baluchestan