AMIR HOSSEINPOUR

Senior Security Engineer – Application & Platform Security

Toronto, ON · amir.m.hosseinpour@gmail.com · +1 437-733-6213 · hackerone.com/mghack123 · github.com/amir-hosseinpour

SUMMARY

Security engineer with 6+ years across application security, secure code review, and securing large distributed systems. Started as the only security person at a retail chain scaling to national coverage, putting security checks into CI/CD pipelines before DevSecOps was a common title. Now run security reviews, threat modeling, and vulnerability management for enterprise clients, and ship the fix in the codebase rather than filing the ticket. 120+ validated findings through HackerOne, including severe issues on PayPal. Lead **DEF CON Toronto (DC416)**, Canada's largest hacker community, and sit on the organizing committee for **TASK**, Toronto's longest-running security community. Build automation first, including Eidolon, an open-source AI-driven security workspace orchestrator. Most recent side project: a robot vacuum, taken apart down to its firmware.

CORE COMPETENCIES

Application Security	Secure code review, architecture review, threat modeling, OWASP Top 10 exploitation and mitigation, secure-by-design, customer data and PII handling
Vulnerability Management	Intake, triage, reproduction, impact assessment, prioritization, remediation tracking, bug bounty and responsible disclosure programs
Secure SDLC & CI/CD	Security checks in developer and CI/CD workflows, SAST and DAST integration, secrets scanning, secure coding guidance, security champions
AI & Agentic Security	Security of agentic architectures and AI-assisted development, LLM tooling failure modes, building security automation with Claude Code and Cursor
Platform & Infrastructure	Multi-site and distributed infrastructure security, network segmentation, hardening and configuration baselines, IAM at scale, endpoint security
Cloud	AWS, GCP, Azure, Docker, Kubernetes, Terraform, PostgreSQL, cloud networking, IAM, OAuth2.0, OIDC
Languages & Frameworks	Python, TypeScript, Go, Bash, SQL · OWASP ASVS and WSTG, MITRE ATT&CK, PTES, NIST 800-53

Security Tools: Burp Suite Pro, Semgrep, CodeQL, Nuclei, Datadog, Cobalt Strike, BloodHound, Frida, MobSF, custom tooling

EXPERIENCE

White Tuque – Offensive Security Specialist

Toronto, ON · October 2024 – Present

- Run security reviews across web applications, APIs, and cloud platforms: secure code review, architecture review, and threat modeling of technical design documents before code ships
- Own the vulnerability management loop for client engagements: intake and triage of VDP and bug bounty reports, reproduction, impact assessment, prioritization, and remediation tracking through to a fix that holds
- Partner directly with engineering teams to embed security earlier in the SDLC, integrating security tooling into developer and CI/CD workflows and writing secure coding guidance
- Test across web, API, mobile, and network surfaces, then trace findings back to root cause in the codebase and ship the patch with the owning team
- Scope and run penetration tests end to end, through rules of engagement, execution, validation, and a retest to confirm the fix actually held
- Identify repeated vulnerability patterns across a codebase and turn a single finding into a framework-level fix and a regression check, rather than a one-off ticket
- Build security automation and tooling in Python, Go, and TypeScript, including Burp Suite extensions and a Nuclei template library used across engagements
- Deliver technical reports and executive readouts across 20+ enterprise clients, and mentor junior engineers on secure code review, testing methodology, and report writing

ASEC – Penetration Tester

Toronto, ON · May 2024 – October 2024

- Delivered application security assessments for fintech and financial-services clients across Canada, the US, Australia, and Europe under Nick Aleks (former Senior Director of Security at Wealthsimple, now Head of Security at Robinhood)
- Tested web applications, REST and GraphQL APIs, and cloud infrastructure. Found 150+ vulnerabilities including IDOR, SSRF, authentication bypass, and privilege escalation
- Reviewed OAuth2.0 and OIDC implementations and IAM configurations for authorization flaws in payment and account systems
- Performed source code review alongside dynamic testing, tracing what was exploitable back to the code that caused it

- Produced technical reports and remediation guidance, presenting findings directly to client engineering teams and translating exploitation chains into code-level fixes

DEF CON Toronto (DC416) – Lead Organizer

Toronto, ON · June 2025 – Present

- Lead Canada's largest hacker community: monthly meetups, speaker programming, and putting local researchers in front of a real audience
- Run sponsorships and partner relationships, including funding the chapter's 10th-anniversary event
- Grew turnout and the speaker pipeline across the Toronto security scene

HackerOne – Bug Bounty Security Researcher

Remote · February 2022 – Present

- 120+ validated vulnerabilities across Fortune 500 responsible disclosure programs, with severe findings on PayPal plus Airbnb, Sony, Booking.com, and AT&T
- Work the researcher side of vulnerability disclosure daily: clear reproduction steps, honest impact assessment, and remediation guidance program owners can act on
- Specialize in authentication and authorization bypass, privilege escalation, and multi-step business-logic chains across web and API surfaces
- Build reusable proof-of-concept frameworks and testing methodologies in Python to scale research across large distributed systems

Ofogh Kourosh Chain Stores – Security Engineer

Tehran, Iran · September 2021 – February 2024

- Owned security for a retail chain scaling from a small footprint toward national coverage, the only security person across corporate systems, store infrastructure, and applications
- Introduced security into the software delivery process as the company built internal tools and a customer-facing online ordering platform: security checks in CI/CD pipelines, application security testing, and fixes worked directly with developers
- Wrote automation and tooling in Python and Bash to replace manual security work that did not scale with the rate of new site openings
- Built network security, hardening baselines, and identity and access management across a growing multi-site estate and a large, high-turnover workforce
- Selected and operated core security tooling including centralized logging, endpoint protection, and vulnerability scanning. Led incident response and assessed third-party and supplier integrations

Ofogh Kourosh Chain Stores – Security Analyst

Tehran, Iran · June 2020 – September 2021

- Monitored security alerts and system logs across corporate and store infrastructure, triaging events and escalating the real ones
- Investigated and responded to incidents including malware, phishing, and account compromise, and ran vulnerability scans with remediation tracked through IT
- Built the company's first security documentation, runbooks, and baseline policies, and administered endpoint protection, email security, and user access reviews

TOOLS & RESEARCH

- **Eidolon:** open-source (MIT) AI-driven security workspace orchestrator built around agent-in-the-loop workflows — github.com/amir-hosseinpour/eidolon
- **API Authorization Testing Extension:** Burp Suite extension for automated OAuth2.0 and OIDC authorization-bypass detection
- **Vulnerability Detection Templates:** Nuclei template library for API and application vulnerability discovery
- **Ecovacs Deebot research:** hardware and firmware security teardown under the vendor's bug bounty program, from UART console access and firmware extraction through cloud API and mobile app analysis

SPEAKING & COMMUNITY

- **SecTor 2025** (Toronto) — "When Hackers Meet Burglars: Red Teaming the Smart Building"
- **DEF CON Vancouver** (Microsoft-hosted) — API attack chains and OAuth2.0 exploitation
- **InfoSec Hamilton** — speaker
- **Organizing Committee, TASK** — Toronto's longest-running security community

EDUCATION

Bachelor of Computer Engineering — University of Sistan and Baluchestan