Farhan Almutairi

Security Engineer & Bug Bounty Researcher — Information, Application & AI Security

Founder @ CarbonFlow • Self-Hosted AI & Automation Systems

Al Majma'ah, Saudi Arabia • +966 50 421 1844 • Far7an.o88@gmail.com

linkedin.com/in/carbonflows • bugbounty.sa/profile/farhanawadh • github.com/Farhanward • carbonflows.store

PROFESSIONAL SUMMARY

Security engineer and bug bounty researcher specializing in information security, application security, secure AI infrastructure, and cybersecurity automation. Reported multiple validated vulnerabilities — CSRF, open redirect with WAF bypass, sensitive information disclosure, and broken access control — to major Saudi enterprises through the national bug bounty platform. I build local-first security tooling (SAST, data-loss prevention, runtime threat detection, and prompt-injection defense) with cryptographically signed audit trails, including a DLP gateway that redacts PII and payment keys before data leaves the perimeter. Hands-on with CVE/CWE analysis, CVSS scoring, Linux hardening, malware analysis, and incident response. Strong in Python and secure-by-design engineering.

CORE COMPETENCIES

Offensive Security & Testing: Vulnerability assessment, bug bounty / coordinated disclosure, web application security testing, OWASP Top 10, CSRF, open redirect, WAF bypass, information disclosure, broken access control, API security, CVSS scoring, CWE / CVE (NVD) analysis.

Application & Product Security: Static application security testing (SAST), secure code review, AST-based analysis, secrets detection, data loss prevention (DLP), PII redaction, secure API design, prompt-injection / OWASP LLM Top 10 defense.

Security Operations & Detection: Malware analysis & incident response, MITRE ATT&CK mapping, runtime threat detection (EDR), Sigma / YARA-style rules, SHA-256 file-integrity monitoring, hash-chain / HMAC audit ledgers, Ed25519 digital signatures, Sysinternals.

Infrastructure & Hardening: Linux (Alpine) administration & hardening, SSH key management, Docker, Cloudflare, network / edge security, data classification.

Programming: Python (advanced), Rust, Node.js / TypeScript, Bash, SQL, Kotlin, Dart.

AI Security: Agent governance, prompt-injection immunity, LLM output verification, sovereign local / cloud routing with zero sensitive-data leakage.

BUG BOUNTY & SECURITY RESEARCH

Active researcher on **bugbounty.sa** (Saudi Arabia's national bug bounty platform) — verified profile: bugbounty.sa/profile/farhanawadh

- Reported multiple validated vulnerabilities against major Saudi enterprises (telecom & ISP) via coordinated disclosure.
- Findings include CSRF (CWE-352), Open Redirect with WAF bypass (CWE-601), sensitive information / internal-network disclosure (CWE-200), and broken access control via an over-permissioned API key (CWE-732).
- Targets and technical details withheld under program disclosure policy; findings verifiable through the platform profile.

FEATURED PROJECT — HACKATHON

AL-MUNAA — Collective Immune System for AI Agents

OpenAI Build Week 2026

Developer tool for agent safety · Python · github.com/Farhanward/al-munaa (release v0.1.1)

- Designed a novel **Threat Antibody Protocol**: when one agent detects a prompt-injection attack it emits a signed, privacy-safe **HMAC "antibody"**; other agents in the same trust family verify it and block *mutated* attacks — without ever seeing the original secret-bearing prompt.
- Wraps agent workflows with input/memory scanning, an **action gate**, and output verification; antibody matcher combines Jaccard similarity with padding-resistant containment matching, bounded HMAC sketches (512 entries), and trust-family isolation.
- **Evidence:** 74 tests passing · calibrated matcher **4/4 attacks detected, 0/5 false positives** · live GPT-5.6 action-gate benchmark blocked dangerous tool calls (protected read=0, sink=0).
- Built test-first with Codex (GPT-5.6); integrates GPT-5.6 via the OpenAI Responses API as a bounded intent analyst — deterministic policy remains the final authority, AI advises only on gray cases.

PROFESSIONAL EXPERIENCE

Founder & Security Engineer — CarbonFlow

Self-Hosted AI & Security Systems • Al Majma'ah, Saudi Arabia (Remote) • 2024 – Present

- Built a suite of **22 local-first security & AI-governance microservices** (Python) covering SAST, DLP, EDR, prompt-injection defense, licensing, and compliance — **353 automated tests** passing, hardened with constant-time API-key auth, request-size limits, and structured logging / metrics.
- Engineered a **DLP gateway** that sanitizes PII, API keys, and payment keys (Stripe / Moyasar-style `sk_live_`) before requests reach third-party AI services — **0 leaks over 47,000 checks**.
- Built a **SAST scanner** for source and binaries with AST analysis and CWE mapping, validated against 12,000 NVD CVEs; and an Ed25519-signed, hash-chain audit ledger for tamper-evident logging.
- Operate a self-hosted edge server (Alpine Linux, 17 Docker containers) hardened with SSH key validation, permission trees, and SHA-256 file-integrity monitoring.

KEY SECURITY PROJECTS

Info-Stealer Incident Response & Malware Analysis Self-Directed 2026

- End-to-end analysis and remediation of a real info-stealer intrusion: identified `Trojan:Win32/Malgent`, reconstructed the full kill chain mapped to **MITRE ATT&CK** (T1204, T1562.001, T1547.001, T1053.005, T1546.015, T1539, T1070.006), extracted IOCs (hashes, masquerading persistence, forged code-signing certificate, timestomping), executed containment/eradication/hardening, and verified a clean state with Sysinternals autorunsc.

kashif — SAST Scanner

- Scans source code and binaries using AST analysis and CWE mapping; validated against 12,000 NVD CVEs.

alwaseet — DLP / Enterprise AI Gateway

- Sanitizes PII, API keys, and payment keys before requests reach cloud AI — 0 leaks over 47,000 checks (directly relevant to payments environments).

almunaa & aegis — Agent Security

- Agent immune system for prompt-injection defense (F1 98%) plus a verifiable action-gate with an Ed25519 hash-chain ledger (F1 92%).

alain_alsahira & alqofl — Detection & Crypto

- Lightweight EDR with Sigma / YARA-style rules; and serverless Ed25519 licensing (12k-license benchmark, 705/705 tamper attempts detected).

CarbonFlow & ZEED — Self-Hosted Platforms

- Live AI-automation edge server (17 Docker containers) and a self-hosted RAG system with a 781k-vector Qdrant knowledge base on a single GPU.

CERTIFICATIONS & TRAINING

Tuwaiq Academy — SATR e-Learning Platform (2026) — completed a structured **23-module software-engineering curriculum** across five specialization tracks:

Mobile App Development (Android / Kotlin): Kotlin 101–104 · Android 101–103 · Jetpack Compose · Firebase (Fundamentals + for Android) · Dart 101

Python Programming: Python 101–104

Databases & SQL: SQL 101–103

Data Science & Analysis: Introduction to Data Science · Data Processing & Analysis with NumPy

Software Engineering Practices: Git Fundamentals · Unit Testing 101–102

EDUCATION & LANGUAGES

Health Informatics Technician — Diploma, 2010 • Arabic (native), English (professional working proficiency)