Ziya Azizov

AI Security Engineer · Adversarial ML · Web Security

ziyaazizov9@gmail.com · +994 77 217 23 58 (WhatsApp) · Baku, Azerbaijan
ayfar.dev · github.com/ziko-asm · linkedin.com/in/ziya-azizov-91bba638a

PROFILE

Security engineer who builds and breaks AI systems. I research how LLM agents, prompt-injection filters and ML intrusion detectors fail under attack, publish reproducible benchmarks, and built ProvGuard, an open-source defence that stopped 144/144 AgentDojo banking attacks. I also ship and harden production websites end to end.

EXPERIENCE

Independent Security Researcher · Bugcrowd Oct 2026 – present

- Vulnerability research on public bug bounty programmes; identified and responsibly reported security issues in two different systems, following each programme's disclosure rules.

Founder & Web Developer · ayfar (self-employed) 2026 – present

- Builds, secures and deploys websites and online shops for businesses in Baku; runs authorised security audits of AI chatbots (Agent Audit).
- Hardened client sites to 100/100 security scores (from 77 and 89), incl. removing a leaked bot token and adding CSP/CORS.

AI SECURITY RESEARCH

ProvGuard — prompt-injection defence for LLM agents provguard.vercel.app

Python · LLM agents · AgentDojo · Ollama · MIT open source

- Tracks where every tool argument came from and blocks sensitive calls whose arguments came only from untrusted text — no LLM judge.
- AgentDojo (ETH Zürich), model-free: banking 144/144 attacks stopped, Slack 97/105, workspace 200/240, travel 79/120.
- Live Qwen3 8B agent: attack success 16/48 → 0/48 with no measurable utility drop.

Agent Audit — security audits for AI chatbots and agents agent-audit-ten.vercel.app

LLM red teaming · prompt injection · jailbreaks · data exfiltration

- Service that runs real attacks (prompt injection, jailbreaks, tool misuse, system-prompt leakage) against a client's assistant, only with written authorisation, and delivers an evidence-backed PDF report with fixes.

Prompt Injection Detector Benchmark prompt-injection-detector-snowy.vercel.app

Python · DistilBERT · TF-IDF · Llama 3 (Ollama) · scikit-learn

- Compared keyword rules, TF-IDF + LR, fine-tuned DistilBERT, Llama 3 judges and a cascade on two public datasets, cross-tested.
- Fine-tuned transformer: 0.96–0.98 F1 in-domain, but blocks 97% of harmless text or finds only 23% of injections on the other source.

GraphGuard IoT — robustness of GNN intrusion detection graphguard-iot.vercel.app

PyTorch Geometric · GCN · GAT · GraphSAGE · FastAPI

- Trained GCN, GAT and GraphSAGE to find compromised devices in a 1,500-device IoT graph; attacked with gradient, DICE and PGD; compared DropEdge, cosine pruning and adversarial training over 5 seeds.
- GraphSAGE reaches F1 0.81 (AUC 0.97); coordinated bot evasion drops GCN from 0.70 to 0.01.

Adversarial Robustness of Neural Intrusion Detectors ai-nids-robustness.streamlit.app

PyTorch · FGSM / PGD · Integrated Gradients · Streamlit · CI

- MLP and 1D-CNN on KDD Cup 1999 and UNSW-NB15 under two threat models; PGD adversarial training lifts MLP detection under attack from 0.07 to 0.98 on KDD, but conclusions flip on UNSW-NB15 (attacks 3.7× closer to benign traffic).

SECURITY TOOLS

SaytYoxla — website security and health checker saytyoxla.vercel.app

Python · FastAPI · React · TypeScript · Vercel

- Scores any site 0–100 in seconds (HTTPS, security headers, SPF/DMARC, speed, SEO) with a fix per issue; FastAPI back end with rate limiting, SSRF protection and 43 tests; React + TypeScript front end.

SKILLS

AI / ML	PyTorch, PyTorch Geometric, Transformers, scikit-learn, Ollama, adversarial ML (FGSM, PGD), GNNs, Integrated Gradients
LLM security	Prompt injection, jailbreaks, data exfiltration, tool misuse, AgentDojo, red teaming
Web security	CSP, HSTS, CORS, SSRF protection, SPF/DMARC, secret handling, security headers
Engineering	Python, FastAPI, JavaScript, TypeScript, React, pytest, GitHub Actions, Linux, Docker, Vercel
Low level	C++, x86-64 Assembly (NASM), Kali Linux

EDUCATION

M.Sc., Control in Technical Systems · Baku Higher Oil School (BHOS) 2026 – present

B.Sc., Mechatronics and Robotics (taught in English) · Azerbaijan State Oil and Industry University (ASOIU) 2022 – 2026

LANGUAGES

Azerbaijani (native) · English (C1) · Turkish