Shay Mordechai

Security Researcher | OS Internals & Network Specialist

❖ 052-306-4991 | ❖ My E-Mail | ❖ My LinkedIn | ❖ My GitHub

Summary

Security Researcher specializing in vulnerability discovery and automated threat hunting. Proven track record in identifying Zero-Day vulnerabilities in complex systems using AI-augmented workflows. Expert in bridging low-level system analysis with high-volume data processing and web-based security architecture.

Professional Experience

DevSecOps Intern | Israel Tax Authority | 2024 - 2025

- **Defense in Depth & AppSec**: Orchestrated a multi-layered security strategy across the SDLC. Conducted Threat Modeling (Design), integrated **SAST/SCA** pipelines (Build), and enforced **JSON**/XML schema hardening *on IBM DataPower (Runtime). Collaboration:* Partnered with SOC/SIEM teams on secure system design, code reviews, and incident response procedures.

Combat Soldier | Intelligence Gathering Unit, IDF

Technical Projects

AI-Augmented Vulnerability Research (SBCL Compiler)

- **Zero-Day Discovery:** Orchestrated an AI-driven fuzzing workflow identifying 3 Zero-Day vulnerabilities; developed full PoC exploits for Memory Corruption and DoS attack vectors.

Predator: Automated Quantitative Trading Engine

- **Intelligence Stack:** Fused XGBoost with **Gemini Pro** to analyze sentiment and automate risk-based liquidation, utilizing a heuristic engine for real-time anomaly detection.
- **Resilience:** Engineered a robust logic layer for API fail-safe stability and dynamic trailing stops.

LeadFlowAI: Secure-by-Design SaaS Platform - Zero Trust: Engineered a "Dark Server" on AWS with zero public ports using Cloudflare Argo tunnels and implemented rootless Podman containers on Fedora.

Network Protocol & Traffic Analysis Toolset - Deep Packet Inspection: Built core protocols (HTTP/DNS/SMTP) from scratch using Raw Sockets and developed a Python-based CTF platform simulating MITM attacks on CAs.

Education

B.Sc. Computer Science | Jerusalem College of Technology | ***2021-2025*** | GPA: 89
Relevant coursework: Network Analysis (97)**,** Reverse Engineering (93), Information Security (90)

Technical Skills

Core Skills: Anomaly Detection, Data Analysis, Network Analysis (L2-L7), Threat Hunting, Research Automation
Languages: Python, JavaScript, C/C++, Assembly (x86), SQL, Bash
Tools & Infra: Burp Suite, Wireshark, Scapy, Docker, Linux (Fedora/Kali), Azure DevOps, AWS Cloud