Shay Mordechai

Security Researcher | Web Security Researcher Candidate

Tel Aviv, Israel | 052-306-4991 | shay.mordechai@proton.me | Portfolio | LinkedIn | GitHub

Summary

> Security Researcher targeting the Web Security Researcher position. Identified 3 Zero-Days via custom AI fuzzing. Expert in Browser Security (V8 JIT) and Protocol Analysis, bridging offensive research and defensive engineering. See full research in my Portfolio.

Professional Experience

DevSecOps Intern | Israel Tax Authority | Aug 2024 – Jul 2025

- Spearheaded Secure SDLC and cloud migration to Checkmarx One (SAST/SCA) across 15+ pipelines, mitigating SQLi and DOM XSS vulnerabilities.
- Hardened gateways via JSON schemas on IBM DataPower, and performed Data Manipulation on 1TB+ daily logs to drive incident response.

Combat Soldier | Combat Intelligence Collection Corps, IDF (Hesder) | Aug 2016 – Nov 2019

- **Executed covert reconnaissance and visual anomaly detection in high-pressure scenarios to build actionable operational target profiles.**

Education

B.Sc. Computer Science | Jerusalem College of Technology | 2021-2025 | GPA: 89

- Coursework: Network Analysis (97), Reverse Engineering (93), Information Security (90).

Technical Projects & Research *(Details in Portfolio)*

Vulnerability Research – SBCL Compiler (3 Zero-Days)

- Engineered a custom Python fuzzer, uncovering 3 Zero-Days (Dynamic Binding Bypass, DoS). Disclosed to MITRE and National CERT (#11265).

Network Protocol & Browser Security Research

- **V8 JIT Internals:** Published analysis on RWX memory allocation & CFI bypasses in browser engines.
- **DNS Rebinding:** Proposed TTL-hardening mitigation, validated by TP-Link PSIRT.
- **RSC Security:** Analyzed Next.js protocols for insecure deserialization vectors.

Automated Trading Engine ("Predator")

- Architected a Python engine fusing XGBoost ML and Gemini LLM for real-time statistical anomaly detection.

TLS 1.2 Handshake & PCAP Simulator

- Engineered a 4,000+ line Python Scapy framework simulating full TLS handshakes, RSA exchanges, and SSLKeyLog generation.

Technical Skills

- **Security:** Web/Browser Security, V8 JIT, Zero-Days, Fuzzing, Memory Corruption, Zero Trust.
- **Dev & Data:** Python, Bash, JavaScript, SQL, Statistical Analysis, Complex Data Sets, Data Manipulation.
- **Networking:** IPv4/IPv6, Raw Sockets, Scapy, DNS Rebinding, Docker/Podman, AWS.