

OLEG LAZARI

US Citizen / Clearance Eligible | Glen Burnie, MD | (929) 400-3442 | ol2764@g.rit.edu | github.com/ol2764RIT

PROFESSIONAL EXPERIENCE

Research Innovations Incorporated

St. Petersburg, FL

Security Researcher I

August 2026–Present

- Continued security research and vulnerability analysis on bleeding edge targets
- Performed reverse engineering and binary analysis using Ghidra and custom static/dynamic analysis tooling in Python/C++
- Collaborated with senior researchers on defensive cybersecurity research and threat modeling initiatives

Research Innovations Incorporated

St. Petersburg, FL

Vulnerability Research Intern

May 2026–Aug 2026

- Conducted security research and vulnerability analysis on bleeding edge targets
- Performed reverse engineering and binary analysis using Ghidra and custom static/dynamic analysis tooling in Python/C++
- Collaborated with senior researchers on defensive cybersecurity research and threat modeling initiatives

Leidos

Columbia, MD

Systems Engineering Intern

May 2024–May 2025

- Automated reverse engineering pipeline using headless Ghidra with Python, extracting CFG and decompiler output, reducing manual analysis by **70%**
- Integrated Ghidra's MCP with local LLaMA for ML-assisted function signature recovery; reverse engineered **4 ICS firmware images** (Cisco IOS, Digi Transport, Phoenix Contact) with automated symbol annotation
- Engineered eBPF kernel security research tooling to explore stealth/persistence techniques including process hiding via `bpf_probe_read` hook interception and syscall table manipulation, informing defensive detection strategies

SECURITY RESEARCH & VULNERABILITY DISCOVERIES

Independent Vulnerability Research – DjVuLibre, CRoaring, ksmdb

Sept 2025–Apr 2026

- CVE-2026-30409** (CRoaring): Discovered integer underflow to out-of-bounds read in bitmap serialization path; developed LibFuzzer harnesses achieving **90%+ code coverage** via structure-aware mutations
- Discovered **RCE-class heap buffer overflow and UAF chain** in DjVuLibre via resource-constrained coverage-guided fuzzing, coordinated disclosure with upstream maintainer within 90-day remediation window
- Identified Linux ksmdb driver heap over-reads and UAF writes using syzkaller customized definitions paired with agentic source code analysis; documentation sent to upstream Linux ksmdb maintainer

FuzzillAI Agentic Fuzzing Framework – RITSEC VRIG [\[github\]](#)

Aug 2025–Apr 2026

- Architected distributed infrastructure with **10+ nodes**, PostgreSQL master database, and in-memory corpus management for real-time synchronization across fuzzing workers
- Implemented **Thompson Sampling** for adaptive mutator selection, achieving **35%+ faster coverage growth** over static-weight baselines by dynamically adjusting exploration-exploitation weights per mutator signal
- Designed automated coverage plateau detection with ML-based corpus generation agents producing novel inputs to escape stagnation in unexplored code paths
- Identified previously undocumented V8 behavioral anomalies including JIT compiler optimization flaws; documented findings for upstream reporting

TECHNICAL PROJECTS

V8 Chrome N-Day Vulnerability Analysis – RITSEC VRIG

Sept 2025–Dec 2025

- Authored **3 published technical writeups** on V8 CVEs: [CVE-2023-4068](#) (WASM/JS null type confusion), [CVE-2025-5419](#) (ITW StoreStoreElimination exploit chain), [CVE-2025-5959](#) (Wasm type canonicalization + MurmurHash64A birthday attack)
- Recreated **3 fully reliable PoC exploit chains** demonstrating end-to-end type confusion primitive through sandbox escape to arbitrary code execution; reverse engineered V8 internals including TurboFan/Maglev pipelines, GC behavior, and JSPI stack switching mechanics

CTF Challenge Design – RITSEC CTF & ISTS CTF

2025–2026

- Designed **5 CTF challenges** across 4 categories for RITSEC CTF 2026 and ISTS 2026
- Grounded designs in 3 current papers (ePrint 2025/376, Tree Borrows PLDI 2025, Bourefis et al. MobiSec 2024) spanning chained CSIDH-512 oracle attacks, Kipnis-Shamir UOV key recovery, Intel TSX anti-debugging RE, SDR/FHSS protocol RE, and deterministic Rust+C CFI bypass; required competitors to implement novel primitives absent from standard tooling

EXTRACURRICULAR ACTIVITIES

RITSEC Vulnerability Research Interest Group

Rochester, NY

Technical Lead

Aug 2025–Present

- Mentored group of 7 students on modern mitigations (PAC, MTE) and how to defeat these mitigations
- Presented on the foundations of how a OS works, syscalls, calling conventions, User Space vs Kernel space
- Weekly technical discussions on CVE disclosures, exploitation techniques, and vulnerability research; collaborative fuzzing campaigns with responsible disclosure focus

TECHNICAL SKILLS

Reverse Engineering: Ghidra, Binary Ninja, GDB, x64dbg, IDA Pro

Vulnerability Research: AFL++, LibFuzzer, Fuzzilli, ASan, UBSan, TSan, MSan, Valgrind

Exploitation: Pwntools, ROP/JOP/SROP, heap exploitation, sandbox escape, type confusion

Vulnerability Classes: Memory corruption, type confusion, integer arithmetic bugs, race conditions, use-after-free

Programming: Python, C/C++, Rust, x86/x64 Assembly, Bash, JavaScript, Go

Infrastructure: Docker, Kubernetes, Git, CI/CD, PostgreSQL

Embedded/Hardware: UART/SPI/I2C, STM32, Saleae logic analyzers, JTAG, firmware analysis

EDUCATION

Rochester Institute of Technology

Rochester, NY

BS Cybersecurity | **GPA: 3.51** | Dean's List (Fall '23, Spring '24, Fall '25, Spring '26)

Expected: May 2027