Amos Dominion

vielite.github.io | Amosvi247@gmail.com | github.com/vielite | x.com/_vielite_

Profile

Blockchain and systems security researcher specializing in adversarial analysis of smart contracts, distributed systems, and security tooling. Combines static analysis, coverage-guided fuzzing, reverse engineering, and exploit development to turn complex protocol failures into reproducible, high-impact findings. Current work explores AI-assisted formal verification, pairing LLM-guided specification synthesis with SMT-based invariant checking to scale security analysis.

Education

University of Delta
Bachelor's Degree in Cyber Security, CGPA: 4.43

Experience

Independent Security Researcher 2022 – Present
Immunefi, HackenProof, Remedy, and Code4rena

- Discovered and responsibly reported **100+ valid vulnerabilities** across major audit and bounty platforms, earning **$10K+** through accepted findings and competitions.
- Identified **10+ valid vulnerabilities** in the $500K Monad Code4rena contest with keccack_crew, using agentic vulnerability-hunting workflows and coverage-guided fuzzing with **cargo-fuzz** to analyze the Rust codebase at scale.
- Ranked **top 3 in the Glider Security Contest** by engineering offensive Python queries that surface live, high-severity EVM smart-contract candidates.

Penetration Tester & Security Analyst
University cybersecurity research team

- Collaborated with professors and a leading university research team to design and deploy hands-on penetration-testing labs.
- Performed authorized, real-world penetration tests against live systems and translated findings into practical remediation guidance.
- Delivered applied lectures and trained security personnel, including police officers, in digital forensics and penetration testing methodology.

Reverse Engineering & Competitive Security

- Reverse engineer x86/x86-64 binaries, Solana SBF bytecode, and EVM bytecode using GDB, Ghidra, and Binary Ninja; competed in **200+ CTFs** with **50+ top-ten finishes**.
- Led teams to national and international finals, including CYSEC, SECCON, and Black Hat, under production-like time constraints.

Selected Projects & Open Source

z3ro-spec Python · Z3
Developing an agentic CLI for automated EVM formal verification and on-chain vulnerability research, with an emphasis on AI-guided specification and invariant generation.

TheFaultyVendingMachine Static Analysis
Building vulnerability-detection passes for Solana programs and EVM smart contracts.

4naly3er TypeScript
Contributed vulnerability-detection passes to an open-source smart-contract analyzer used across 100+ protocol reviews.

Hound Agentic Security Research
Extended the open-source security agent with a custom workflow for large-scale Rust vulnerability hunting during the Monad audit competition.

Damn Vulnerable DeFi — Foundry Solidity · Foundry
Contributed Foundry-based material to an open-source smart-contract security challenge suite.

Achievements

Top 3, Glider Security Contest (2025) • Ranked **#8 globally on CTFtime** (2025)
1st at Backdoor CTF and L3ak CTF (2025) • 2nd at DaVinci Code CTF (2022) • 3rd at K!nd4susCTF (2025)
Finalist, Black Hat MEA (2023) • Finalist, CYSEC as university team captain (2022) • Finalist, SAS CTF (2025)

Skills

Languages: Solidity, Rust, Python, TypeScript, C, x86/x86-64 Assembly
Security & formal methods: Smart-contract and DLT auditing, AI-assisted formal verification, static analysis, fuzzing, reverse engineering, exploit development
Tools: Z3, Lean 4, Certora Prover/CVL, Foundry, Glider, Hound, Ghidra, GDB, Binary Ninja, Slither, cargo-fuzz, AFL++