Victor Okpukpan

Email | Github | Portfolio | Twitter

PROFILE

Smart contract security researcher and Cyfrin/Updraft ambassador with a background in full-stack Web3 engineering. Focused on adversarial protocol auditing, onchain security analysis, and technical content for Web3 audiences.

EDUCATION

University of Uyo **Akwa-Ibom, Nigeria**
Bachelor of Science, Computer Science 2024

Cyfrin Updraft **Remote**
Blockchain Development and Security 2024

WORK EXPERIENCE

Independent Security Researcher | Freelance **2024 - Present**

- Executed adversarial audits on EVM-compatible protocols, identifying logical inconsistencies, economic exploit vectors, and invariant violations.
- Applied manual review, invariant testing, and static analysis tools including Slither and Aderyn to assess protocol risk.
- Wrote technical pieces around blockchain security to educate both technical and non-technical readers.

Ambassador | Cyfrin Updraft **2024 - Present**

- Mentored developers in smart contract security best practices and audit methodology.
- Created and published technical content on blockchain security and development concepts.
- Engaged with the broader Web3 community to promote secure smart contract development practices.

Full-Stack Web3 Engineer | Freelance **2022 - Present**

- Developed smart contracts and frontends for client projects across Ethereum, Base, and Arweave using Next.js, Wagmi, and Solidity.
- Built responsive, user-facing interfaces for Web3 platforms, integrating wallet connections and onchain transaction flows.
- Worked across the full stack from Solidity contract logic to frontend state management, delivering complete decentralized applications for clients.

WRITING & CONTENT

- Smart Contract Risk Analysis: How to Identify Vulnerabilities Before They Cost Millions — Long-form SEO article for DeFi traders, analysts, and compliance teams.
- How AI Detects Risky Onchain Behavior: Wallet Patterns, Transaction Flags, and What the Data Reveals — Technical explainer on AI-powered onchain risk detection for compliance and analyst audiences.
- Assumptions, Invariants, and Where Exploits Actually Live — Technical thread on audit methodology for security researchers, using the Saga bridge exploit as a live case study.

PROJECTS

- **CallSign:**
  A terminal-style EVM calldata decoder for security researchers and onchain analysts. Decodes raw hex calldata into human-readable function names and parameters, with Safe multiSend support and a shareable URL system. Built with Next.js, React, TypeScript, and ethers.js v6.

SKILLS

- **Security and Auditing:** Smart contract auditing, invariant testing, adversarial review, fund flow tracing, static analysis, vulnerability assessment
- **Audit Tools:** Slither, Aderyn, Solodit, Foundry, Etherscan, Dune Analytics, Arkham
- **Blockchain:** Solidity, Foundry, Wagmi, OpenZeppelin, RainbowKit, ethers.js
- **Frontend:** JavaScript, React, Next.js, TypeScript, Tailwind CSS, Framer Motion
- **Content:** Technical writing, SEO content strategy, Web3 education