ISAH DAUDA

koinated@gmail.com · github.com/trinnode · linkedin.com/in/trinnex · trinnode.tech

PROFESSIONAL SUMMARY

Security researcher and blockchain developer with hands-on experience across smart contract auditing, web application penetration testing, and DeFi protocol development. My work spans competitive audit contests, bug bounty programmes, and the independent design and deployment of production Web3 protocols. A background in full-stack blockchain engineering means I approach security assessments from the inside out, tracing vulnerabilities through architecture and business logic rather than just running automated scans. I am comfortable operating across both Web3 and Web2 attack surfaces and have produced written security reports, proof-of-concept scripts, and remediation guidance across multiple engagements.

PROFESSIONAL EXPERIENCE

Web3Bridge Ikorodu, Lagos State, Nigeria
Student Intern, Web3 Security and Development Track *July 2025 – October 2025*

- Completed a structured cohort programme covering Solidity development, smart contract security patterns, and on-chain protocol architecture as part of Web3Bridge Cohort XIII.
- Worked through real contract codebases, examining common vulnerability classes including reentrancy, access control gaps, and unsafe external calls.
- Contributed to open-source repositories under the Bloceducare organisation on GitHub as part of the cohort track.

CFSS: Cyber and Forensics Security Solutions (Remote, India-based)
Cybersecurity and Ethical Hacking Intern *November 2023 – December 2023*

- Completed an intensive internship in penetration testing methodology, information gathering, and vulnerability mitigation, working through structured scenarios on live digital infrastructure.
- Applied hands-on techniques in reconnaissance, enumeration, and exploitation under the guidance of practicing security professionals.

Cybersecurity Education Initiative (CYSED) Minna, Niger State, Nigeria
Volunteer, Cybersecurity Awareness Campaign *October 2023*

- Participated in a public cybersecurity awareness campaign, communicating digital safety practices and threat awareness to non-technical community members.

CERTIFICATIONS

- Certified AppSec Practitioner (CAP)
- Certified Network Security Practitioner (CNSP)
- Certified Cyber Security Analyst (CS3A)
- Certified Cyber Threat Intelligence Analyst (CTI 101)

SELECTED RESEARCH AND TECHNICAL PROJECTS

Sherlock Audit Contest: XRP Ledger C++ Codebase
Participated in a competitive public security audit covering five live protocol amendments: Batch Transactions, Permission Delegation, MPT DEX, Confidential Transfers, and Sponsored Fees.

Reviewed amendment interaction logic, delegation boundary enforcement, front-running exposure in the DEX layer, and state handling correctness across the Confidential Transfers amendment.
Stack: *C++, XRP Ledger protocol internals, competitive audit methodology*

Glider Query Contest: r.xyz

Authored semantic static analysis queries targeting ERC-2771 context spoofing via delegatecall, multicall vulnerability patterns, and unmasked calldata address flows. Queries submitted to the public r.xyz Glider database contest.
Stack: *Glider query language, ERC-2771, Solidity vulnerability patterns*

VERIDAQ: ZK Credential Verification Protocol

Designed and shipped a full-stack zero-knowledge credential verification system. The security focus was on circuit constraint integrity and proof soundness against witness manipulation attacks. Deployed on Base Sepolia.
Stack: Circom, Solidity, Fastify, Next.js, Base Sepolia

SealBid: FHE Sealed-Bid Auction Protocol

Developed a sealed-bid auction protocol on Fhenix using CoFHE encrypted integer types, ensuring bid values remain encrypted throughout the entire auction lifecycle. The design eliminates front-running at the contract level without relying on commit-reveal schemes. Submitted to the Fhenix buildathon.
Stack: Solidity, CoFHE, Fhenix, FHE primitives

StakeSafari v2: DeFi Staking Interface (Live)

Built and deployed a production DeFi staking frontend with a React and Vite stack, currently live at stake-safari-v2.vercel.app. Developed with a security-conscious frontend architecture, separating wallet interaction logic and on-chain read/write operations cleanly across components.
Stack: React, Vite, Tailwind CSS, ethers.js

ProofArena: On-Chain Bug Bounty Marketplace

Designed a three-layer bug bounty protocol on Initia comprising Solidity smart contracts, a TypeScript AI triage agent, and a React interface. Built submission handling, severity scoring, and trustless payout logic entirely on-chain.
Stack: *Solidity, TypeScript, React, Initia*

NigeriaTI: Automated Threat Intelligence Pipeline

Built an OSINT aggregation system that automates threat indicator collection, IP reputation enrichment, domain intelligence processing, and structured threat feed output, scoped specifically to the Nigerian th*reat landscape.*
Stack: Python, OSINT APIs, threat feed formatting

Evil Twin Detection IDS

Developed a passive wireless intrusion detection system in Python using Scapy, identifying evil twin access points through RSSI fingerprinting and MAC anomaly correlation. Ships with 21 passing pytest tests and runs on live wireless interfaces.
Stack: *Python, Scapy, pytest*

Judgement Day: AI Red Teaming Competition

Produced adversarial attack artifacts across AI triage and suppression scenario tracks for the AIM Intelligence and Korea AI Safety Institute red-teaming competition.

BUG BOUNTY

Active bug bounty hunter across three platforms covering both Web2 and Web3 targets. On *Cantina*, work focuses on smart contract and DeFi protocol security reviews.

YesWeHack and *Bugcrowd* engagements cover web application and API security testing across varied programme scopes and industries. All platform work involves manual vulnerability research, responsible disclosure, and structured impact-focused reporting for programme owners.
Platforms: *Cantina · YesWeHack · Bugcrowd*

TECHNICAL SKILLS

Security and Auditing
Smart contract auditing (Solidity), web application penetration testing, API security testing, bug bounty hunting, threat intelligence and OSINT, social engineering awareness, wireless intrusion detection, Active Directory enumeration and exploitation, adversarial AI red teaming, privilege escalation, reconnaissance and threat modeling, vulnerability disclosure and report writing

Blockchain and Web3
Solidity, Circom (ZK circuits), FHE via CoFHE and Fhenix, Hardhat, Foundry, Base, Initia, ERC-20, ERC-2771, ERC-4337, IPFS, proxy upgrade patterns, on-chain protocol architecture, delegatecall vulnerability analysis, flash loan attack vectors, oracle manipulation, reentrancy and access control auditing, ethers.js, Web3.js, OpenZeppelin

Development
TypeScript, Python, JavaScript, React, Next.js, Vite, Node.js, Fastify, Scapy, Supabase, PostgreSQL, Docker, Bash scripting, Rust (familiar)

Penetration Testing and Exploitation
Burp Suite, Metasploit, SQLMap, Nikto, Gobuster, Hydra, John the Ripper, Netcat, Impacket, Certipy, BloodyAD, nxc

Smart Contract Security Tools
Slither, Mythril, Glider (r.xyz), Foundry fuzz testing, Echidna, Manticore, Aderyn, 4naly3er

Network and Traffic Analysis
Wireshark, Nmap, Aircrack-ng, Kismet, Tcpdump, Netdiscover

OSINT and Threat Intelligence
Maltego, Shodan, theHarvester, Recon-ng, MISP, OpenCTI

Digital Forensics
Autopsy, Volatility, Binwalk, ExifTool

Operating Systems and Environments
Kali Linux, Parrot OS, Ubuntu, Windows Server, WSL2, VirtualBox, VMware

EDUCATION

Federal University of Technology, Minna Niger State, Nigeria

B.Tech in Cyber Security Science *2021 – 2026*

COMMUNITY AND OPEN SOURCE

Web3Bridge Cohort XIII: Completed structured Web3 development and security programme; contributed to open-source Bloceducare repositories on GitHub.

Build Wave (drips): Open source contributor under @trinnode on Stellar and Soroban TypeScript SDK repositories.