ISAH DAUDA

+234 810 380 0607 || koinated@gmail.com

https://github.com/trinnode || linkedin.com/in/trinnex

PROFESSIONAL SUMMARY

Security practitioner with a focus on smart contract auditing, web application penetration testing, and blockchain protocol development. I hold certifications in application security, network security, and threat intelligence, and I have applied that knowledge across internships, competitive audit contests, and independent protocol builds. My development background across full-stack Web3 architecture means I audit systems from the same perspective as the engineers who built them, which consistently surfaces logic-level and architectural vulnerabilities that automated tools do not catch.

CERTIFICATIONS

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

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, network security, adversarial AI red teaming, CTF competition, 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,ERC-4337, IPFS, proxy upgrade patterns, on-chain protocol architecture, delegatecall vulnerability analysis, flash loan attack vectors, oracle manipulation, reentrancy and access control auditing.

Development
TypeScript, Python, JavaScript, React, Next.js, Node.js, Fastify, Scapy, Supabase, PostgreSQL, Docker, Docker, Bash scripting

Security Tools

Burp Suite, Metasploit, SQLMap, Nikto, Gobuster, Hydra, John the Ripper, Slither, Mythril, Foundry fuzz testing, Echidna, Manticore, Wireshark, Nmap, Aircrack-ng, Kismet, Tcpdump, Netdiscover, Maltego, Shodan, theHarvester, Recon-ng, Autopsy, Volatility, Binwalk, ExifTool, Kali Linux, Parrot OS, Ubuntu, Windows Server, WSL2, VirtualBox, VMware.

EXPERIENCE

- **Cybersecurity Student Intern**

  CFSS : Cyber and Forensics Security Solutions | Remote (India-based)

  November 2023 to December 2023

Completed an intensive cybersecurity and ethical hacking internship covering penetration testing methodology, information gathering techniques, and vulnerability mitigation strategies. Worked through hands-on scenarios involving digital infrastructure security under the guidance of practicing security professionals.

- **Student Intern : Web3 Developement/ Security**

  Web3Bridge | Ikorodu, Lagos State, Nigeria

  July 2025 to October 2025

Completed a structured Web3 development and security internship covering smart contract development, protocol design patterns, and blockchain security fundamentals.

- **Volunteer : Cybersecurity Awareness Campaign**

  Cybersecurity Education Initiative (CYSED) | Minna, Niger State, Nigeria

  October 2023

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

SECURITY ENGAGEMENTS AND INDEPENDENT PROJECTS

A. Bug Bounty Hunting: Cantina, YesWeHack, Bugcrowd

Active bug bounty hunter across three major platforms covering both Web2 and Web3 targets. On Cantina, participation focuses on smart contract and DeFi protocol security reviews. YesWeHack and Bugcrowd engagements cover web application and API security testing across a range of programme scopes and industries. Work across all three platforms involves manual vulnerability research, responsible disclosure, and writing clear impact-focused reports for programme owners.

B. Sherlock Audit Contest : XRP Ledger C++ Codebase

Participated in a competitive public 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 confidential transfer state correctness.

C. Glider Query Contest : r.xyz

Authored semantic static analysis queries targeting ERC-2771 context spoofing through delegatecall, multicall vulnerability patterns, and unmasked calldata address flows. Submitted to the public r.xyz Glider query database contest.

D. VERIDAQ : ZK Credential Verification Protocol

Designed and shipped a full-stack ZK credential system using Circom circuits, five Solidity contracts, a Fastify API, and a Next.js frontend, deployed on Base Sepolia. Security focus included circuit constraint integrity and proof soundness against witness manipulation.

E. 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.

EDUCATION

Bachelor of Technology in Cyber Security Studies

Federal University of Technology, Minna (FUTMinna) *2021 to 2026*