Iyke - Security Research Resume

CONTACT

eokorie1911@gmail.com · Iyke.dev · github.com/devIykee · @deviykee · Remote, Nigeria

SUMMARY

Smart contract security researcher working on EVM protocols, mostly launchpads and CDP engines. Eleven bugs reported privately, seven rated High, one with a confirmed vendor fix in production. I verify on forks and local Foundry tests, never against live state, and bound severity to what the PoC actually shows.

TECHNICAL SKILLS

Languages Solidity, Rust, Python, TypeScript, Bash

Tooling Foundry (forge, cast, anvil), Slither, Echidna, Sourcify, Blockscout API, bytecode and selector analysis

Protocols Uniswap V2/V3/V4 core and periphery, bonding curves, LP locking, CDP collateral and liquidation, oracle quorum design, flash loans

EVM CREATE address prediction, nonce and revert semantics, storage layout, slot0

SECURITY RESEARCH

Openfair, V3 graduation pool squat (High). Launch seeding ran through `createAndInitializePoolIfNecessary` with no check on the returned price, so a stranger could open the pool first and take the raise into it. Reported privately. Openfair shipped v2.0 and backfilled protection for launches already live. No funds lost.

The Index, flash loanable payout snapshot (High). Distribution weights read live `balanceOf` at a moment anyone could trigger. No checkpoint, no hold period. Reproduced with a Foundry test built from the deployed snapshot and distribute logic.

Merry Men, V4 pre-init bricks the factory (High). `initializePool` returns instead of reverting on an existing pool and the factory ignored that. Claiming the next predicted CREATE address made `createToken` fail during settlement, and the revert rolls the nonce back so retries hit it again. Confirmed on an Anvil fork.

StockDotFun, V4 pre-init freezes graduation (High). Taking the pool key costs gas and no inventory. Graduation then reverts for good, curve trading is already off, and about 4.4 ETH of raise is stuck with no recovery path in the verified source.

HoodRich, no slippage bounds on V2 migration (High). `addLiquidityETH` ran with both minimums at zero. Found by diffing against the same codebase's meme factory, which already checked `slot0`, and a competing pad using 95 percent bounds on the same call.

Also reported. Robinlaunch V3 pool squat and Robinfun pair pollution freeze, both High. xStocks single reporter oracle and unminted borrow fee debt. HoodCash burned reward accrual. SLVR delegate claim redirect.

RESEARCH AND TOOLS

- Bug hunt toolkit, ten scripts covering the repeatable parts of a hunt: chain id gate, creator trace, frontend bundle grep, surface map with Sourcify and selector dump, unauthenticated call triage, Foundry fork scaffold, report and disclosure templates.
- Audit playbook the toolkit implements: intake, per step gates, PoC and report structure, and the rule that I try to disprove a finding before writing it up.
- Reviewed roughly 30 Robinhood Chain protocols. Negative results are written up the same way as positive ones.

EXPERIENCE

Independent Security Researcher, 2026 to present

- Eleven findings across launchpads, CDP engines, mining pools and distribution contracts.
- Most of the work sits in AMM pool initialisation. The same mistake shows up on nearly every bonding curve launchpad, in three different shapes across V2, V3 and V4.

Freelance Blockchain Developer, CribX, Aug 2026 to present

- Audited and finished a multi chain deposit system (BTC, ETH, SOL, USDT, USDC) in a NestJS, Prisma and BullMQ backend.
- Made deposit crediting idempotent so replayed chain events cannot double credit, working inside existing BitGo custody and Tatum monitoring.

Other build work. Covenant, an attestation gated treasury on Stacks, second place in the FlowVault hackathon. Skimflow, x402 micropayments settling in USDC on Arc. Freelance Escrow in Rust and Stylus. Technical audit of CredChain.

EDUCATION

B.Eng. Software Engineering, Federal University of Technology Owerri, 2023 to 2028, in progress