RITIK AGARWAL

Mail | Website | GitHub | LinkedIn | Security Portfolio

WORK EXPERIENCE

Independent Blockchain & Smart Contract Security Researcher *Jan 2025 - Present*

- Completed a **private security audit** of a **Web3 infrastructure protocol** under NDA; identified and reported multiple valid vulnerabilities.
- Delivered **18 validated security findings** across a broad range of DeFi protocol types, including automated market makers, lending and borrowing markets, ERC-4626 vault architectures, and liquidity management systems.

PERSONAL PROJECTS

Shim - Co-Founder (Live) *May 2026 - Present*

- Built and shipped **Shim**, a **Go-based security proxy** for npm, pnpm, and yarn that **recursively scans direct and transitive** (sub-package) **dependencies** for known vulnerabilities before install.
- Engineered a daemon scanner using **TCP IPC, local vulnerability rules, lifecycle-script analysis**, and **SQLite-backed caching**, adding minimal overhead compared to native npm installs.
- Shipped **cross-platform** release tooling (install/update/uninstall) for Linux, macOS, and Windows, reaching **25+ early users** since launch.

Multisig Smart Contract Wallet - Account Abstraction *Feb 2024 - Mar 2024*

- Built a **multisig smart contract wallet** using ERC-4337 account abstraction, requiring multiple designated signers to jointly authorize and approve a transaction before it executes on-chain.
- Implemented wallet creation, **signer management**, and the **propose-approve-execute** transaction flow using Solidity smart contracts, OpenZeppelin libraries, and ethers.js.
- Built the supporting frontend and backend with **Next.js**, **Prisma**, and **Supabase**, with Alchemy providing blockchain RPC infrastructure.

Uniswap V4 Take-Profit Hooks (GitHub) *Dec 2024 - Jan 2025*

- Built custom Uniswap V4 hooks implementing **automated take-profit order execution**, integrating with the V4 core and periphery contract architecture.
- Developed and tested the hooks in Solidity using Foundry, validating execution logic against Uniswap V4's core and periphery contract interfaces.

TECHNICAL SKILLS

- **Languages:** Solidity, Python, Go, SQL, JavaScript, C++
- **Frameworks & Libraries:** Next.js, ethers.js, OpenZeppelin
- **Databases & Tools:** Supabase, Prisma, SQLite, Git, GitHub
- **Security & Audit Tooling:** Foundry (PoC development), Hardhat, Remix

EDUCATION

Jain University, Bangalore *Aug 2024 – Sept 2026*

Master in Computer Application

Relevant Coursework: Network Security & Cryptography, Database Management Systems, Cloud Computing Foundations, Python Programming

GLS University, Ahmedabad *July 2021 – May 2024*

Bachelor's in Computer Application - 84%

Lions English School, Silvassa *April 2019 – May 2021*

High School, Commerce with Computer Science - 85%

LEADERSHIP & ACHIEVEMENTS

Kuru Smart Contract Security Review *Oct 2025*

- **Ranked 3rd of 723 participants**, with **4 validated findings**, in a smart contract security review.

Cyber Shadez Hackathon - Backend Developer *Feb 2024 – Mar 2024*

- Led team to **2nd place**; built an **Account Abstraction DApp** using Supabase, Prisma, Alchemy, Next.js, Solidity, and OpenZeppelin.

Cyber Shadez Hackathon - Backend Developer *Feb 2023 – Mar 2023*

- Led team to **1st place**; built and shipped an **NFT minting DApp** under competition conditions using OpenZeppelin, ethers.js, and Next.js.