Vishvesh Rao

☎ +91 7306242702 Kochi, India ✉ vishveshsrao@gmail.com vishvesh-rao.github.io

PROFILE

Passionate about web3 security and especially focus in the field of block chain security and cryptography. Actively try to improve skills in security by playing and learning from CTF's as a part of Team bi0s . Also seek to contribute to the open source community.

EDUCATION

B.Tech in Computer Science and Engineering, *Amrita Vishwa Vidyapeetham* 2019 – 2023 | Kollam, Kerala, india
CGPA: 9.02/10

CBSE AISSCE, *Navy Children school* 2017 – 2019 | Kochi, India
Boards, Percentage obtained: 95.6%

CBSE AISSE, *Navy Children school* 2016 – 2017 | Delhi, India
CGPA: 10/10

EXPERIENCE

Inctf Nationals/Juniors, *Event lead, Speaker, Student mentor* 2020 – present
Hacking & Cyber Security contest organized by team bi0s, in association with Amrita Vishwa Vidyapeetham and Amrita Centre for Cyber Security. Gave a talk on security of JWT with, emphasise crypto-related JSON vulnerabilities, forging tokens and manipulating key-value pairs present in jwt to verify tokens. Responsibilities included creating challenges, auditing challenges of other creators, and challenge deployment/hosting and monitoring the ctf infrastructure using docker and ctfd.

Member, Team bi0s, *Cryptanalyst/Reverse engineer* 2019 – present
Team bi0s is the no. 1 ranked CTF team in India. An active member of the team focusing primarily on Cryptography/ Block chain security and related concepts and also do reverse engineering occasionally. Also in-charge of organising events hosted by our club.

Nethermind, *Smart Contract Developer, Security Researcher, Code Reviews* 05/2022 – 08/2022
As part of Netherminds auditing team, participated in code reviews, auditing defi apps deployed on ethereum/Starknet written in solidity (layer 1) and cairo (Layer 2) identifying vulnerabilities ranging from low level bugs to critical issues jeopardising the entire daap. Researched on the best security practices for writing smart contracts and conducted workshops explaining the use automated static analysis tools like slither, amarna. Developed a layer 2 plugin for the truffle framework to allow solidity contracts to be deployed to starknet as layer 2 cairo contracts.

PROJECTS

Traboda, *Cybersecurity Startup* 2020 – present
Designed security challenges for Traboda, an ed-tech startup providing innovative & scalable solutions for tackling cybersecurity threats.

- Lead content creator- Produced content related to cybersecurity topics for traboda academy and for bi0s wiki.
- Developed challenges based on RSA attcaks, Number theory, matrix algebra, repeated xor, homomorphic encryption , modified Diffie-hellman key exchange.

Warp transpiler box, *Truffle box to deploy layer 2 contracts* 07/2022
Developed a truffle Warp-transpiler Box which provides the boilerplate Truffle structure necessary to start coding for StarkWare's Ethereum L2 solution, StarkNet. It allows the developer to write solidity contracts and the compiler will automatically transpile these contracts to cairo contracts and deploy them on strakent without the user having to do any extra work.

BItSec, *EC-Schnorr Signature, Threshold Sharing Schemes* 01/2022
Conducted a security analysis of the EC-schnorr algorithm specified in the bitcoin Taproot upgrade (BIP0340) and analysed vulnerability in threshold sharing scheme used to secure crypto wallet keys.

- Acquiring the account private key via Nonce Reuse in Schnorr Signature Algorithm.
- Exploiting the linear relationship between nonce's generated by an insecure PRNG.
- Taking control of a multi signature process in a two-of-two Naïve Signature Aggregation scheme via a rouge attack on shared public Keys without the knowledge of other participant.
- Detailed analysis on mitigating the rouge key cancellation attack through Bellare-Neven scheme, an improved version of the schnorr musig algorithm.
- Recovering the crypto wallet key by exploiting a threshold sharing scheme, reconstructing the polynomial by finding the lagrange points via polynomial interpolation.

Postmortem of Uniswap v2-Schnoodle attack, *Ethereum, Defi exploit* 08/2022
An in depth analysis of a defi attack that occurred on the ethereum blockchain on Jun-18-2022 resulting in fund loss from a UniswapV2Pair token contract

- The blog post details every aspect of the attack listing all affected addresses that were involved in in the execution of the exploit.
- Analyses the series of interactions with the liquidity token and ERC-777 smart contract, breaking down each transaction to understand its purpose and resulting affect it had with regards to successful exploit implementation.
- Explaining the vulnerability which resulted in the loss of the eth held in the token contract.

TECHNICAL ACHIEVEMENTS

Code Arena, *web3 bug bounties* 07/2022
Won around 500$ as bug bounty auditing codes of multiple decentralized protocols reporting multiple bugs/code optimizations as part of netherminds team.

Runners up in Securinets CTF Quals 2021, *team bi0s* 2021
Acquired 2nd place internationally and qualified for finals

CSAW CTF Qualifiers/finals, *NYU / IITK* 2021
Ranked 11 internationally and 1st in India in qualifiers and 3rd in finals conducted by NYU and Indian Institute of Technology, kanpur

3rd rank WPICTF 2021, *team bi0s* 2021
Acquired 3rd position internationally in CTF conducted by WPICSC

Black Hat USA 2021, *Mandalay Bay, Las Vegas* 2021
Awarded Student scholarship (1195$) to attend Black Hat USA 21 held in Las Vegas

Volga CTF 2021, *team bi0s* 2021
Qualified for Volga CTF 2021 finals held in Samara,Russia

2nd ISFCR Hackathon 2021, *team bi0s* 2021
Acquired 2nd place internationally

Black Hat Asia 2021 2021
Awarded Student scholarship (500$) to attend Black Hat Asia 21

1st IJCTF 2020, *team bi0s* 2020
Acquired 1st place internationally in CTF organized by warlock_rootx

Black Hat Asia 2020 2020
Awarded Student scholarship (500$) to attend Black Hat Asia 2020

2nd Runners up in CSAW CTF Nationals, *team bi0s* 2020
Ranked 2nd nationally in finals of CSAW organized by NYU Centre for Cyber Security, New York

Runners up in Byte Bandits CTF, *team bi0s* 2020
2nd position in CTF organized by IIT Indore

TECHNICAL SKILLS

Languages
python, C++, solidity, Cairo, Markdown, LaTeX

Frameworks
Z3, Sagemath, Flask, Ghidra, IDA, Truffle, Brownie

Tools
Docker, Git, gdb-gef, Wireshark, Slither, Amarna

Platforms
GNU/Linux, Windows

Computer Architectures
MIPS, *intel* 8085, ARM, *intel x86*

ONLINE PROFILES

- ***Linkedin:*** *vishvesh-rao*
- ***Blog:*** *vishvesh-rao.github.io*
- ***GitHub:*** *Vishvesh-rao*
- ***Twitter:*** *The_Str1d3r*