

# Vishvesh Rao

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

## 📄 PROFILE

Passionate about cyber security and especially focus in the field of cryptography and Reverse engineering. 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  
ROLL NO: AMENU4CSE19161  
CGPA: 8.9/10

**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**, Speaker, Organiser, Student mentor 2021 – 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. Created ctf style challenges and mentored students familiarising them with security concepts.

**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.

**Inctf Junior**, Event lead, Challenge creator, Challenge auditor 12/2020  
InCTF Junior is India's First & Premier Hacking & Cyber Security Contest for High School Students, organised by team bi0s. Assigned as the overall events technical lead and in-charge of the Crypto category, responsibilities included creating challenges, auditing challenges of other creators, and challenge deployment/hosting and monitoring the ctf infrastructure.

## 📁 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.

**BltSec**, 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 an improved version of the schnorr musig algorithm.
- Recovering the crypto wallet key by exploiting an insecure implementation of a threshold sharing scheme.

**House Price Prediction**, ML, Data science [↗](#) 11/2021  
An ML model for the purpose of predicting house prices. Extensive feature scaling has been done, missing values filled by using SGDC classifier.

- Analysed the correlation matrix and various individual parameters to understand relationship between features and correspondingly do feature reduction.
- Refined data set was trained on 3 separate algorithms: KNR, Random forest, Linear regression.
- All 3 models accuracy were evaluated and random forest gave the best accuracy of the 3 with a r-square score of 76%.

**YtoMP3**, telegram conversion bot [↗](#) 06/2021  
Simple video search bot for telegram that lets the user search for videos on you tube via inline command.

- Users can take full advantage of telegrams unlimited free storage and built in mp3 player without having to worry about backing up songs or loosing them also comes with support for mp4 format too.

## TECHNICAL ACHIEVEMENTS

---

<b>Runners up in Securinet's CTF Quals 2021</b> , <i>team bi0s</i> Acquired 2nd place internationally and qualified for finals	2021
<b>CSAW CTF Qualifiers/finals</b> , NYU / IITK Ranked 11 internationally and 1st in India in qualifiers and 3rd in finals conducted by NYU and Indian Institute of Technology, kanpur	2021
<b>3rd rank WPICTF 2021</b> , <i>team bi0s</i> Acquired 3rd position internationally in CTF conducted by WPICSC	2021
<b>Black Hat USA 2021</b> , <i>Mandalay Bay, Las Vegas</i> Awarded Student scholarship (1195\$) to attend Black Hat USA 21 held in Las Vegas	2021
<b>Volga CTF 2021</b> , <i>team bi0s</i> Qualified for Volga CTF 2021 finals to be held in Samara, Russia	2021
<b>2nd ISFCR Hackathon 2021</b> , <i>team bi0s</i> Acquired 2nd place internationally	2021
<b>Black Hat Asia 2021</b> Awarded Student scholarship (500\$) to attend Black Hat Asia 21	2021
<b>1st IJCTF 2020</b> , <i>team bi0s</i> Acquired 1st place internationally in CTF organized by warlock_rootx	2020
<b>Black Hat Asia 2020</b> Awarded Student scholarship (500\$) to attend Black Hat Asia 2020	2020
<b>2nd Runners up in CSAW CTF Nationals</b> , <i>team bi0s</i> Ranked 2nd nationally in finals of CSAW organized by NYU Centre for Cyber Security, New York	2020
<b>Runners up in Byte Bandits CTF</b> , <i>team bi0s</i> 2nd position in CTF organized by IIT Indore	2020
<b>1st place DarkCTF 2020</b> , <i>team bi0s</i> Played with the crypto team and won first place internationally	2020

## TECHNICAL SKILLS

---

### Languages

python, C, C++, Java, x86 assembly, solidity, intel 8085, Markdown, LaTeX

### Tools

Docker, Git, VS Code, gdb-gef, Wireshark

### Computer Architectures

MIPS, intel 8085, ARM, intel x86

### Frameworks




Z3, Sagemath, Flask, Ghidra, IDA

### Platforms

GNU/Linux, Windows

## ONLINE PROFILES

---

- **LinkedIn:** [vishvesh-rao](#) 
- **Blog:** [vishvesh-rao.github.io](#) 
- **GitHub:** [Vishvesh-rao](#) 
- **Twitter:** [The\\_Str1d3r](#) 