

Pagilla Manohar Reddy

Member of team bi0s, Category lead,
Cryptography,
Team bi0s.

 poimnbmpoff@gmail.com
 [@victim1307](https://github.com/victim1307)
 [@Manohar Reddy Pagilla](https://www.linkedin.com/in/Manohar-Reddy-Pagilla)

Research Interests

Cryptography, Cybersecurity and Networking.

Education

Amrita Vishwa Vidyapeetham, Amritapuri

2020-2024

Bachelor of Technology in Computer Science and Engineering, CGPA: 9.2

Professional Experience

Sinn3rB0y5

March 2021 - September 2021

Team Lead

- We are India's top 7th CTF team in the year 2021.
- It is a team of 2 people, and have participated in more than 50 ctf's in the span of 6 months. Mostly have done Forensic, OSINT & Cryptography in various CTFs.

bi0s Pentesting

September 2021 - March 2022

Team Member, CTF Pentesting team | Mentor: Abhishek

- Learnt Android Development for reverse engineering android applications.
- Learn Selenium and Web automation and build a web automation tool for automatically emailing.

Team bi0s

March 2022 - Present

Category Lead, Cryptography

- bi0s is a team of cybersecurity enthusiasts who actively plans & organising sessions, talks and CTF contests.
- Played Capture The Flag contests almost every weekend and my contribution in the team is to solve crypto challenges which includes Computer Science and Higher Order Mathematics.
- Mentored juniors in the path of cryptography.

Atlassian

May 2023 - July 2023

Product Security Intern | Mentor: Raghavendra Karthik D

- Have built a recon tool called Code Spyder. Code Spyder helps in identifying underlying tech stacks, frameworks and security sensitive code patterns
- This Recon tool can help the pentesters to smart pentesting than usual pentesting

Projects

Sage Implementation for Elliptic Curve Attacks | *Self Project*

January 2023

Wrote a paper presenting the summary of the various attacks that have been discovered on the implementation of Elliptic Curve Cryptography (ECC) in SageMath, a widely used open-source mathematics software. Paper has yet to be submitted for publication.

CryptoLearn | *Self Project*

January 2023

Build a learning platform for cryptography where it starts from basics. It's a friendly platform to learn cryptography for beginners. Also it not only covers the concepts of the cryptographic system but also has the implementation of the cryptographic encryption system in python, sage and more.

CLI Chat Application | *Self Project*

October 2022

A chat application using socket programming. Establishing Connection over sockets and sending message/data to the server side/receiver side . Receiving connection and sending a message/response back . Which includes the Symmetric key encryption for confidentiality.

Automatic Email Login | *Self Project*

October 2022

Automatically logs in into the given email and sends N' number of mails for the list of email ids. I have automated stuff in a web browser.Done automating a file upload feature using selenium web driver.

Admission Management System | *Group Project*

August 2022

The admission management system that assists educational institutions in efficiently managing the student enrolling process. Students can also apply online, check their application progress and submit papers using the admission management system.

Movie Information Application | *Self Project*

February 2022

Movie Information Application, App which shows information about movies and details related to it. Networking using Retrofit. Image Loading using Libraries such as Picasso. Used shared preferences. Listing movies with RecyclerView. Saving favourite movies using Room Database.

Awards & Achievements

- Secured **2nd** place in Securebug.se CTF Loki 2021 *(2021)*
- Secured **4th** in RTLxHA CTF *(2021)*
- Secured **4th** in WinjaCTF *(2021)*
- Secured **5th** place in S.H.E.L.L. CTF *(2021)*
- Secured **6th** place in wtfctf *(2021)*
- Secured **8th** place in NorzhCTF 2021 *(2021)*
- Secured **4th** in WinjaCTF Goa - *team achievement* *(2022)*

- Qualified to CSAW finals and bagged **2nd** place in CSAW Regionals - *team achievement* (2022)
- Qualified to ISITDTU finals which was in Vietnam, bi0s is the only India team which got selected (2022)
- Secured **1st** in DomeCTF 2022 - *team achievement* (2022)
- Secured **2nd** place in BSidesSF 2022 - *team achievement* (2022)
- Secured **5nd** place in nullcon Goa HackIM CTF 2022 - *team achievement* (2022)
- Secured **1nd** place in infoCTF 2023 (2023)

Research Experience

Worked on different attacks in elliptic curve

November 2022

Mentor: *Abhishek Bharadwaj*

Explored and worked out on different types of elliptic curve cryptography. Implemented new type elliptic curve challenges based on the existing attacks. Analysis on different conditions of groups, fields, and the order of each curve for an attack to be possible. Analysis and implementation of lattice based attacks in the elliptic curve cryptography.

Generating Elliptic Curves with any given order

December 2022

Implemented the generation of elliptic curves with a specified order. Analysed on hilbert class, generation of trace and order of the curve on the specified order. Implemented CM discriminant along with curve generation in python and sagemath.

Technical Skills

Programming	Python, Java, SageMath, bash, C, C++, Haskell
Development Tools	Git, GitHub, Docker, GitLab, GCP
CTF Tools	Wireshark, Nmap, Z3, pwntools
Software Tools	Android Studio, Matlab

Extracurriculars

- Amongst **top 20** players at **cryptohack.org** in India
- **Best Programmer** award in DevCTF which is conducted by IIT Delhi
- Participation in **50+** international Capture The Flag events in 2021 and **30+** in 2022
- Built and designed challenges in bi0s CTF which is an **80** rated CTF in **ctftime.org**
- **Mentoring juniors** in cryptography from September 2022
- Finished Cryptography and Information Theory & Mathematical Foundations for **Cryptography** courses
- Conducted workshops on **Cyber Security Awareness** of government school students
- Organised a workshop on different types of **Cyber Attacks** in Amrita Vidyalayam
- Attended conference **NULLCON goa** and also have attend many many conferences virtually
- Active member in **AYUDH** amritapuri