

Padala Sanjay Vardhan

<https://spektre.in>

Github: [sanjayvardhan](#)

Email : sanjayvardhanpadala@gmail.com

Mobile : +91 7981927996

EDUCATION

- **Amrita School Of Engineering** Kerala, India
Bachelor of Technology in Computer Science; GPA: 7.96 2021 – present
- **FIITJEE Junior College** Andhra Pradesh, India
Board Of Intermediate Education; Percentage: 91% 2019 – 2021

EXPERIENCE

- **Research Intern**
SEFCOM Lab at Arizona State University, USA 2024
 - Worked under the supervision of Dr. Yan Shoshitaishvili.
 - Implemented a Fuzzer for WebAssembly Compiler Pipeline in JavaScript Engines
- **Team Lead**
teambi0s 2023 – present
 - Leading a CTF Team of 30+ players, achieving **Rank 1 in India** and Rank 46 in the World on CTFtime
 - Conducted CTFs, workshops, and trainings for the team and other Universities.
- **CTF Player**
Binary Exploitation / teambi0s 2021 – Present
 - Worked on Linux user-space exploitation(stack and head-based exploitation) and solved challenges based on them during the Capture The Flag competitions.
 - **Browser Exploitation:** worked on JS Engine Internals, specifically **V8 and WebKit** and Wrote exploits for few CVEs.
 - Conducted multiple sessions for freshmen year students in the university on **Reverse engineering and Binary Exploitation**.

PROJECTS

- **WASM Fuzzer**
Author 2024 – Present
 - Developing a Custom Fuzzer for WebAssembly Compiler Pipeline in JavaScript Engines using AFL++
 - Implemented mutation strategies to achieve higher code coverage and uncover deep-seated bugs.
- **bi0sCTF**
Core Management Team and Challenge Author 2022 – Present
 - **bi0sCTF 2024:** Created 2 challenges in Binary Exploitation category for bi0sCTF 2024 based on **V8 Incorrect Map Transition and Bootsector Exploitation**
 - **bi0sCTF 2022:** Created 2 challenges in Binary Exploitation category for bi0sCTF 2022 based on **Race Condition in shared memory access and Unity Game Hacking**.
- **ScareCr0w**
Author 2023 – Present
 - Developing a tool that uses static analysis and OpenAI API to automatically detect and fix memory corruption vulnerabilities
- **Blog Posts on Browser Exploitation**
Author 2022 – Present
 - Wrote Blog Posts on **JS Engine Internals** and **Exploiting V8 and WebKit** CVEs
- **Dynamic Memory Allocator**
Author 2021
 - A Custom Dynamic Memory Allocator written in C language

TECHNICAL ACHIEVEMENTS

- **Winner in Red Team CTF** India
U3F1 *August 2025*
 - Participated in the CTF hosted by Red Team Hacker Academy. Solved Binary Exploitation and Reversing challenges during the CTF based on Format String vulnerability, ROP(Return Oriented Programming), Heap Double-Free and reversing Obfuscated linux binaries.
- **Winner in HSBC x IITB TLCTF Regionals** India
teambi0s *March 2024*
 - Participated in the CTF Finals hosted by Indian Institute of Technology, Bombay in IIT Hyderabad. Solved challenges based on Format String Exploitation, Reversing challenge based on Lexical Parser and few other Binary Exploitation challenges.
- **Winner in IITB TrustLab CTF** India
teambi0s *October 2023*
 - Participated in the CTF hosted by Indian Institute of Technology, Bombay. Solved a challenge based on Spectre Attack, few other the Reversing Engineering and Binary Exploitation Challenges.
- **Runners Up in CSAW Finals** India
teambi0s *November 2022*
 - Participated in the CTF hosted by NYU, New York. Solved a challenge based on PS3 game reversing and few binary exploitation challenges.
- **Winners in Dome CTF** India
teambi0s *September 2022*
 - Participated in the CTF hosted by Beagle Security. Solved challenges from Binary Exploitation category based on UAF(Use After Free) and Race Condition vulnerabilities.
- **Runners Up in BSidedSF CTF** June 2022
teambi0s
 - Participated in the CTF hosted by BSides San Francisco. Solved challenges from Binary Exploitation category based on Format String Exploitation and few other Reverse Engineering challenges.
- **5th in SquareCTF** November 2023
teambi0s
 - Participated in the CTF hosted by Square. Solved Binary Exploitation challenges based on ROP(Return Oriented Programming) and Game Hacking

RESEARCH INTERESTS

- Binary Exploitation
- Browser Security
- Fuzzing
- Automated Binary Analysis
- Reverse Engineering

TECHNICAL SKILLS

- **Languages:** C, Python, Assembly(x86,ARM,MIPS), C++, SQL
- **Tools:** GDB, radare2, IDA, Binary Ninja, Turbolizer, lldb
- **Platforms:** Linux, Windows, MacOS