Pranav Krishna M

Coimbatore, Tamil Nadu | thepranavkrish04@gmail.com | +91-6383-861937 | tourpran.github.io
linkedin.com/in/tourpran | github.com/tourpran

About Me

I am a dedicated security enthusiast with a strong focus on software exploitation in Unix environments. My expertise extends to browser-based exploitation, particularly targeting the V8 JavaScript engine. As an active participant in Capture the Flag (CTF) competitions, I compete with the renowned **team bi0s**, consistently honing my skills and staying at the forefront of cybersecurity advancements.

Education

Amrita Vishwa Vidyapeetham, B.Tech in Computer Science — Oct 2022 – Current

- CGPA: 8.87/10.0 (TO-DO transcript)
- **Coursework:** Data Structures and Algorithms, Computer Architecture, Computational Theory, Operating Systems.

Projects

Pwn Collection — github/pwn-hub

- Curated a comprehensive collection of **beginner-friendly** material on exploitation techniques from various **CTF** competitions.
- Covered topics include:
  - **Stack-Based Exploitation:** Comprehensive guides and practical examples for identifying and exploiting various stack vulnerabilities and effectively bypassing security mitigations.
  - **Heap-Based Exploitation:** Creative exploits targeting the **pt-malloc** implementation and some custom Dynamic Memory Allocators.
  - **Browser Exploitation:** Techniques exploiting the latest **CVEs** for the **V8 engine** and detailed write-ups on multiple CTF challenges involving v8/ quickJS.
- Documented articles for Custom Virtual Machine exploitation, Python interpreter Jails, and **pwnable.tw** challenges.

Bi0s CTF — ctftime.org/bi0sCTF24

- Contributed to bi0sCTF24 by designing an Android challenge centered on exploiting a **dynamic memory allocator** bug via the **WebView** interface. Our efforts led to the competition achieving an impressive rating of **95.48/100**.
- Authored an instructive blog detailing the methodology of exploiting my Custom Dynamic Memory Allocator (DMA) vulnerability, aimed at enhancing participants' understanding of Android-based DMA exploitation techniques.

CTF Events Organizer

- Developed and deployed multiple challenges across various Capture The Flag competitions over the time period, focusing on stack and Heap based exploitation.
  - Bsides CTF, Goa
  - Namibia National Cybersecurity Competition, Southern Africa
  - Zh3r0 CTF, India

Experience

Workshop for School Students — Coimbatore

I helped to organise a workshop for school students, covering essential cybersecurity topics such as **forensics**, **reverse engineering**, **cryptography**, and **web exploitation**, emphasizing the significance of security practices in everyday life.

v8 CVEs v8 Collection

I actively replicate the latest **zero-day** vulnerabilities in the V8 JavaScript engine, focusing on issues such as race conditions, use-after-free (UAF), type confusion, and incorrect range assumptions.

Achievements

RVCE-IITB CTF	: Rank 3 (2 person team, India)
niteCTF 2022 (ARESx)	: Rank 1 (globally)
FooBar CTF 2022 (ARESx)	: Rank 1 (globally)
VolgaCTF 2024 Qualifier (bi0s)	: Rank 2 (globally)
Square CTF 2023 (bi0s)	: Rank 5 (globally) and Rank 1 (India)
UMD CTF 2024 (bi0s)	: Rank 5 (globally) and Rank 1 (India)
b01lers CTF 2024 (bi0s)	: Rank 5 (globally) and Rank 1 (India)
Ugra CTF Quals 2024 (bi0s)	: Rank 5 (globally) and Rank 1 (India)

CTF Teams

bi0s	: Rank 1 (India - Current) University team
ARESx	: Rank 7 (US - 2022) High School team
zh3r0	: Rank 2 (India - 2022) High School team

Technical Skills

Languages: C, C++, x86-64 Assembly, JavaScript, Python.

Tools: Git, Docker, qemu.