Ishaan Sheth

+91-9867776533 ishaanksheth2@gmail.com LinkedIn Github Blogs

Education

University of Mumbai - Dwarkadas Jivanlal Sanghvi College of Engineering **9.46 CGPA**

Bachelor of Technology in Computer Engineering, Honors in Data Science *June 2023 – May 2027*

Experience

Deloitte **May 2024 – July 2024**

Risk Analyst *Proof*

- Analyzed large datasets using Python and Excel to detect anomalies, trends, and control weaknesses, improving the accuracy of **risk assessments**.
- Collaborated with **cross-functional teams** to document internal controls and evaluate their effectiveness in alignment with regulatory and organizational standards.
- Developed reports using **Excel** to communicate **risk insights and key findings** to stakeholders in a clear and actionable manner.
- Supported audit and assurance activities by preparing documentation, performing control testing, and ensuring adherence to frameworks such as SOX and ISO standards.

COE-CNDS Research lab at VJTI **March 2025 – June 2025**

Cybersecurity Research Intern *Proof*

- Conducted **reverse engineering** of **Windows-based binaries** to analyze program behavior, uncover vulnerabilities, and understand low-level system interactions.
- Utilized tools such as **IDA Pro, Ghidra, and x64dbg** to perform static and dynamic analysis, including disassembly, debugging, and control flow tracing.
- Developed **proof-of-concept exploits** and scripts in C and Python to demonstrate identified vulnerabilities and automate analysis workflows.
- Studied **Windows internals**, including **PE file format, memory management, and system calls**, to enhance effectiveness in vulnerability research.

Research Head ACM committee **Feb 2025 – Ongoing**

Research mentee → Research head

- Initially worked under Mihir Panchal and Tirath Bhatiawala as a research mentee learning about the technicalities of writing a research paper.
- After showing consistenc efforts, I was appointed as one of the research head of the ACM student chapter.
- Hosted multiple workshops alongside other heads Aakarshit Saxena,Ankur Vasani Pearl Mody and Rishit Kar.
- Provided **guidance to junior students** in writing their research papers.

Projects

Meltdown attack(yan85 virtual machine) | Github Blog **January 2026**

- Implemented a proof-of-concept Meltdown attack on the **yan85 virtual machine** to demonstrate unauthorized access to sensitive memory regions via **speculative execution**.
- Leveraged **cache side-channel techniques**, specifically **Flush+Reload**, to infer privileged data by observing cache access patterns.
- Developed mechanisms to traverse memory pages and reconstruct kernel-level data from transient execution leakage.
- Analyzed low-level system behavior, including caching effects and speculative execution, to understand and exploit **microarchitectural vulnerabilities**.
- Documented findings and methodology, highlighting the security implications of side-channel attacks on modern processor architectures.

Web server (x86-64 assembly) | Github **March 2025**

- Implemented a minimal HTTP server entirely in **x86_64 assembly** using raw Linux syscalls, eliminating reliance on libc.
- Designed socket lifecycle including **socket**, **bind**, **listen**, and accept to handle TCP connections on port 80.
- Developed process-based concurrency using **fork** to handle multiple client connections simultaneously.
- Built manual **HTTP request parsing** logic to differentiate between GET and POST requests and extract file paths.
- Implemented **GET** handling to read requested files from disk and return contents with a valid HTTP response.
- Implemented **POST** handling to parse request body, compute payload length, and write data to files with appropriate permissions.
- Performed low-level buffer and **memory management** using static **.bss** segments for request and file handling.

Prefetch Side-Channel Attack | Github **January 2026**

- Implemented a microarchitectural side-channel attack using **prefetcht2** and **rdtsc** in x86_64 assembly to leak data from protected memory regions.
- Designed a timing-based probing mechanism that measures **cache latency differences** to identify valid mapped memory without causing faults.
- Developed a **memory scanning routine** over a large virtual address range and used averaged timing samples to reduce noise and improve reliability.
- Engineered **data exfiltration via process exit codes** by reading secret bytes from identified memory locations in the assembly payload.
- Built a C-based harness to dynamically modify shellcode, repeatedly execute the target binary, and capture leaked bytes through exit status.
- Incorporated stability techniques such as repeated sampling and **nanosleep** delays to mitigate timing inconsistencies in **side-channel measurements**.

Research Publications

Quality Analysis of Borewell Water **Published**

IET conference proceedings *February 2026*

QVeriSign- A no-cloning quantum communication framework **Draft completed**

Expected by fall 2026

Prediction of Stock option pricing using Explainable AI techniques **In progress**

Expected by fall 2026

Technical Skills

Languages: Assembly (x86, x86-64), C, C++, Python, Java, Bash, JavaScript, SQL, HTML/CSS
Developer Tools: GDB, Pwntools, IDA Free, Ghidra, Binary Ninja, Radare2, Wireshark, Netcat, curl, Git, Docker,Tmux
Technologies/Frameworks: Linux, FastAPI, TensorFlow, OpenCV, scikit-learn, HuggingFace Transformers, NLTK, Jekyll
Security & Systems: Binary Exploitation (Pwning), Reverse Engineering, Shellcoding, Buffer Overflows, Format String Exploits, Cache Side-Channel Attacks (Flush+Reload), Basic Cryptography
Profiles/Platforms: Pwnable.kr(Top 150), Pwn.college, Pwnable.tw, CTFtime

Technical Writing

Binary Exploitation & Systems Blog | Blog **Ongoing**

- Authored detailed technical writeups on Capture The Flag (CTF) challenges with a focus on binary exploitation and low-level systems.
- Explained vulnerabilities such as buffer overflows, format string bugs, and return-oriented programming (ROP) with step-by-step exploit development.
- Demonstrated practical debugging workflows using tools like GDB, Pwntools, and disassemblers (Ghidra/IDA) to analyze binaries.
- Documented techniques to bypass common protections including NX and ASLR, emphasizing real-world exploitation strategies.
- Structured content to simplify complex concepts like memory layout, syscalls, and shellcoding for better accessibility and learning.

CTF & Competitive Experience

Capture The Flag (CTF) Challenges **Ongoing**

- Actively participated in CTF competitions with a primary focus on binary exploitation (pwn) challenges.
- Solved challenges involving stack and heap buffer overflows, format string vulnerabilities, and basic heap exploitation techniques.
- Developed automated exploit scripts using Pwntools, including payload crafting, remote interaction, and ELF analysis.
- Performed static and dynamic analysis using tools such as GDB, Ghidra, and objdump to identify and exploit vulnerabilities.
- Gained hands-on experience with Linux internals, memory management, and mitigation mechanisms such as NX, ASLR, and PIE.
- Practiced consistently on platforms like pwnable.kr, pwn.college, pwnable.tw, and custom self-hosted challenges to strengthen problem-solving skills.