

Ali Raza

Lahore, 54590
Punjab, Pakistan

Webiste: locus-x64.github.io
Email: [elirazamumtaz\[at\]gmail.com](mailto:elirazamumtaz[at]gmail.com)

Research Interests

Interested in identifying security vulnerabilities posed by Operating Systems and understanding their potential exploitation. As a Malware Researcher at Ebryx, I specialize in Linux kernel exploitation and mainly focus on n-day research. I aim to transition towards zero-day discovery and adeptly craft Proof of Concepts (PoCs) and exploits for the Linux/Android Kernel.

Research Experience

0day in zlog (Famous C logging library) - CVE-2024-22857

November, 2023 – March, 2024

Ebryx (Pvt.) Ltd.

- Collaborator: [Faran Abdullah](#)
- Found Vulnerability in zlog using AFL++ providing arbitrary code execution
- Responsibaly disclosed the vulnerability to the maintainer
- CVE number - [CVE-2024-22857](#)
- Detailed blog post include Poc : www.ebryx.com/blogs

Vulnerability Research and Exploit Development for Android Kernel, University FYP

July, 2022 – July, 2023

PUCIT - University of the Punjab

- Supervisor: Dr. Muhammad Arif Butt
- Worked on problems related to memory errors in binaries
- Worked on reversing binaries using IDA Freeware
- Worked on chroot jailbreak
- Worked on analyzing Linux kernel
- Worked on analysing msg_msg as exploit primitive
- Done with analysis of CVE-2019-2215

Professional Experience

Malware Researcher

Ebryx (Pvt.) Ltd.

- Working on Kernel nday research
- Tools: IDA Freeware, elixir by bootlin, GDB, QEMU, etc.
- Recognitions: Annual Best Performance Award 2023

March, 2023 – Present

Lahore, Punjab, Pakistan

Teaching Assistant (Operating Systems)

PUCIT - University of the Punjab

- Designed material and coursework for the newly introduced lab component of the subject
- Designed exam papers for the lab
- Assisted students in the lab + other TA responsibilities

October, 2022 – February, 2023

Lahore, Punjab, Pakistan

Skills

Programming Languages: Assembly, C, C++, Python

Security: Binary Exploitation, Reverse Engineering, Vulnerability Research, Fuzzing, Exploit Development, n-day Research

Tools: AFL++, syzkaller, IDA Pro, elixir by bootlin, GDB, GNU/Make

OS: Linux-x64

Education

PUCIT - University of the Punjab

October, 2019 – July, 2023

Bachelor of Science - Computer Science

Lahore, Punjab, Pakistan

- Graduated with CGPA 3.65/4.0
- Campus Lead of Google DSC
- Member of the Cyber Security Society (Cyber@PU)

Punjab Group of Colleges, Okara Campus

August, 2017 - September, 2019

Intermediate of Computer Science with Physics

Okara, Punjab, Pakistan

- Graduated with 3rd position in BISE Sahiwal.

University Projects

Unix Shell

C, Makefile

<https://github.com/locus-x64/unix-shell>

- An effort to write the *nix-based shell to gain an understanding of how the shell works and how OS creates and handles processes and allows processes to communicate with each other through its IPC interface

Exploits Scripts

Python, x86 Assembly

<https://github.com/locus-x64/exploit-development>

- Basic scripts that I have written to solve some exploitation challenges

Hack Assembler

C++

<https://github.com/locus-x64/hack-assembler>

- A 16-bit machine language assembler for the 16-bit Hack Assembly Language. It was done as part of building a complete 16-bit computer during the Computer Organization Assembly Language Course

Courses & MOOCs

Computer Systems Security: pwn.college

- Shellcode Injection
- Sandboxing
- Reverse Engineering
- Memory Errors
- Race Conditions
- Kernel Security
- Program Exploitation

Awards & Honors

Board Topper

2019

Intermediate - BISE Sahiwal

Sahiwal, Pakistan

- (<https://pgc.edu/our-achievers>)
- Awarded with a brass medal and a cash prize by the Board of Intermediate and Secondary Education, Sahiwal