ALI RAZA

Vulnerability Researcher
elirazamumtaz@gmail.com | locus-x64.github.io
locus-x64 | locus-x64 | locus_x64

OBJECTIVE

Security researcher with a strong background in C and assembly, focusing on fuzzing, reverse engineering, and code auditing to uncover and remediate software flaws. I develop robust PoCs, collaborate closely with cyber threat experts, and design practical mitigations across userland and kernel to enhance system security.

PROFESSIONAL EXPERIENCE

- **Ebryx (Pvt.) Ltd. [🌐]** *Mar 2023 - Current*
  Vulnerability Researcher Lahore, Pakistan
  - Collaborated with senior threat researchers to investigate vulnerabilities end-to-end and translate findings into actionable detections and mitigations
  - Conducted targeted fuzzing (AFL++, syzkaller) across userland and Linux kernel; triaged crashes, minimized inputs, and authored PoCs
  - Discovered and disclosed a 0-day in `python-socketio` (CVE-2025-61765) [🌐] with PoC and remediation guidance, coordinating with the maintainer
  - Discovered and disclosed CVE-2024-22857 in zlog via AFL++; developed PoC exploit and proposed remediation, working with maintainers through coordinated disclosure
  - Performed secure code reviews and static analysis of C/C++ codebases using CodeQL and manual auditing; hardened CPython against memory corruption classes
  - Performed reverse engineering of firmware and system components with IDA Pro and Ghidra to pinpoint vulnerable code paths and exploitation primitives
  - Designed kernel-level techniques (Netfilter, LKMs) to detect and mitigate path traversal and ASLR brute-force attacks on Linux
  - Built a JVMTI-based userland agent to detect Java deserialization attack primitives at runtime on Linux
  - Conducted n-day research in Linux kernel exploitation, and formalized an attack matrix mapping exploitable kernel objects, prerequisites, and post-exploitation techniques
- **University of the Punjab [🌐]** *Oct 2022 - Feb 2023*
  Teaching Assistant Lahore, Pakistan
  - Designed lab coursework and assessments; provided hands-on guidance and mentorship to students

RESEARCH EXPERIENCE

- **0-day in `python-socketio`: CVE-2025-61765 [🌐]**
  - Identified and reported a security flaw in `python-socketio`; reproduced impact with a PoC and supported mitigation guidance
  - Collaborated with the maintainer for coordinated disclosure and release of a fix/advisory
  - Tools used: Python, pytest, git
- **0-day in Zlog: CVE-2024-22857 [🌐]**
  - Fuzzed zlog and discovered a critical vulnerability enabling arbitrary code execution
  - Built a PoC to demonstrate exploitability and collaborated on mitigation guidance
  - Coordinated disclosure with the maintainer to patch and publish advisories
  - Tools: AFL++, Elixir Bootlin, gdb, git
- **n-day (Dirty Pipe) - CVE-2022-0847 [🌐]**
  - Explored data-only attacks and kernel buffer management internals
  - Traced Linux pipe IPC via Elixir Bootlin and authored a working PoC
  - Tools: Elixir Bootlin, GDB with bata24/gef, QEMU
- **n-day ("Call of Death" in Shannon Baseband) - CVE-2020-25279 [🌐]**
  - Reversed Samsung Exynos modem firmware (Shannon RTOS) with IDA Python and Ghidra
  - Analyzed PAL allocator and identified vulnerable code paths for the CVE statically
  - Emulated the firmware with FirmWire to validate understanding and hypotheses
  - Tools: FirmWire, IDA Pro 9-beta, Ghidra
- **Vulnerability Research & Exploit Development for Android Kernel [🌐]**
  - Final Year Project (FYP) supervised by Dr. Muhammad Arif Butt (arifbutt.me)
  - Progressed from Linux userland exploitation to Android/Linux kernel exploitation
  - Conducted n-day research on CVE-2019-2215

SKILLS

- **Programming:** C (ANSI), Assembly (x86-64/ARM), Bash, Python
- **Security Focus:** Fuzzing, Reverse Engineering, Code Auditing (manual/CodeQL), Exploit Development, Mitigations
- **Domains:** Linux Kernel Internals, Android Kernel/Internals, Mobile Baseband, Python & Java Runtimes (JVMTI)
- **Tools:** QEMU, VMware Workstation, IDA Pro (ost2 certified), Ghidra, GDB+gef, AFL++, Elixir Bootlin, CodeQL, Semgrep, Kali Toolchain, FlareVM Toolchain
- **Operating Systems:** Linux (Ubuntu), Android
- **Open Source Contributions:** zlog (CVE-2024-22857 patch), Elixir Core Reference, Havoc (C2) Framework, pwncollege, Hacktoberfest

EDUCATION

- **PUCIT, University of the Punjab** *Oct 2019 - July 2023*
  Bachelor of Computer Science Lahore, Pakistan
  - Projects:
    - Vulnerability Research & Exploit Development for Android Kernel [🌐]
    - UNIX Shell in C [🌐]
    - Hack Assembler in C++ [🌐]
    - Exploit Scripts in C/Python [🌐]
  - GPA: 3.58/4.00
  - Campus Lead by Google Developer Student Clubs [🌐]
  - President of PUCon23 (National Tech Event by University of the Punjab) [🌐]
- **Punjab Group of Colleges** *Aug 2017 - Oct 2019*
  Intermediate of Computer Science (ICS) Okara, Pakistan
  - Grade: 90.54%
  - Board Topper [🌐]