ALI RAZA

elirazamumtaz@gmail.com | locus-x64.github.io | LinkedIn | GitHub

January 13, 2026

Dear Hiring Manager,

I spend most of my days breaking things, finding bugs in C code, fuzzing Linux kernel subsystems, and reversing firmware that ships with zero documentation. Safety-critical security is where I want to be because here, the bugs I find actually matter beyond just a CVE number.

I'm looking for a role where I can dig deep into complex systems, reverse engineer components others haven't touched, and turn what I find into real fixes. My background is in kernel internals, baseband security, and low-level systems work. I'm happiest when I have a disassembler open and a problem that takes weeks, not hours.

What I bring:

Reverse engineering without a manual: I spent months inside Samsung's Shannon baseband firmware (Exynos modem, Shannon RTOS). No docs, just IDA Pro and patience. Found vulnerable paths in their PAL allocator and validated everything by emulating with FirmWire.

Finding and reporting bugs: Three 0-days so far: CVE-2025-68472 (MindsDB), CVE-2025-61765 (python-socketio), CVE-2024-22857 (zlog). All found through fuzzing or manual auditing, all coordinated with maintainers, all patched.

Writing it up: I document everything. PoCs, root cause analysis, remediation guidance. Wrote a public blog post on the python-socketio bug for BlueRock. I know that a finding nobody can understand is a finding nobody will fix.

Kernel work: Built LKMs and Netfilter-based detection for path traversal and ASLR brute-forcing. Did n-day research on Dirty Pipe (CVE-2022-0847) and put together an attack matrix mapping kernel objects to exploitation techniques.

Native code: C and x86-64/ARM assembly are my daily drivers. I've built a JVMTI agent to catch Java deserialization attacks at runtime and contributed patches to harden CPython.

Portfolio: My zlog research (CVE-2024-22857) shows how I worked with AFL++, triaged the crash, built a PoC for arbitrary code execution, proposed the fix, and coordinated disclosure. Full write-up: locus-x64.github.io

I'd like to talk about how I can contribute to your team. Happy to walk through any of my research in more detail.

Sincerely,

Ali Raza
Vulnerability Researcher @ Ebryx