Kamdin Bembry Syracuse, NY | kob4035@rit.edu | (315) 813-9115 | Zia-Rashid.github.io

## Education

**Rochester Institute of Technology (RIT)** BS/MS in Computing Security — Expected Graduation: May 2028

- GPA: 3.84 | Dean's List (Fall 2024, Spring 2025)
- Member of RITSEC (Cybersecurity Club – Vulnerability Research, Reversing, Penetration Testing)

## Experience

**Penetration Testing Intern**, Coalfire, Chicago IL — May 2025 – Aug 2025

- Performed security audits across 2 clients engagements to proactively identify security flaws and vulnerabilities.
- Contributed to a security assessment on AI-integrated IDEs, specifically targeting potential vulnerabilities within its AI components and implementation as part of a group research project.
- Collaborated with clients to present findings, explain complex vulnerabilities, and consult on effective remediation strategies.

**Vulnerability Research Interest Group Co-Lead** — Aug 2024 – Present

- Co-lead student security research group specializing in low-level exploitation, vulnerability analysis, and reverse engineering.
- Participated in development of custom operating systems, rehashing of novel heap exploits, and JavaScript browser engine research.
- Wrote detailed technical documentation to help other students learn and contribute.

## Activities

**Fuzzilli Enhancements: AI-Augmented Analysis and Component Targeting** — Aug 2025 – Present

- Enhanced a fork of `Fuzzilli` by integrating AI-augmented plateau solving, complex seed generation, and feedback-aware corpus generation.
- Implemented a component tagging mechanism within the program templates, enabling targeted mutations conditioned on specific engine subsystems.

**Agentic CTF Autosolver** — Aug 2025 – Present

- Developed an LLM-driven challenge autosolver that autonomously triages, analyzes, and solves CTF-style reverse-engineering, binary-exploitation, forensics, and cryptography challenges.
- Achieved a **68% solve rate** on NYU's LLM CTF Benchmark - outperforming competing models by over 30%.

**AI Integrated IDE Security Assessment** — June 2025 – Aug 2025

- Conducted a security assessment of AI-integrated IDEs, rigorously testing for prompt injection, editor-specific vulnerabilities, and inappropriate MCP server access. Discovered and documented a variety of interesting vulnerabilities, such as:
  - Arbitrary File Exfiltration
  - Arbitrary Code Execution
  - Dozens of successful Prompt Injections

**V8 Quarterly Quiz - pwn.college/quarterly-quiz/v8-exploitation** — Feb 2025 – June 2025

- Completed the pwn.college V8 Quarterly Quiz (Username: `ziarashid`).
- Learned about V8 internals including the structure of `HeapObjects`, `Maps`, `Turbofan`, etc.
- Explored the compiler architecture of V8 including Turbofan's sea of nodes, feedback vectors, typing, etc.
- Studied the fundamentals of the V8 sandbox including the pointer compression cage, trusted pointer tables, and code pointer tables.

**Compiler & Browser Research** — Nov 2024 – Present

- Explored LLVM IR(Intermediate Representation) creation and optimization mechanisms by implementing a custom programming language and studying the performance of different optimizations; thus gaining experience in multiple LLVM passes, instruction selection, IR transformations, and various optimization trade-offs.
- Experimented with javascript's V8 engine for exploitation and compiler research by studying the chromium codebase, re-enacting past exploits, and completing custom V8 CTF challenges.

**Kernel and OS for Fuzzing & Vulnerability Research** — Aug 2024 – Dec 2024

- Built a toy operating system designed for fuzzing with LibAFL QEMU, enabling security research and vulnerability discovery in low-level system components.
- Designed a specialized fuzzing harness to detect vulnerabilities in KVMCTF, focusing on hypervisor security, guest-to-host escape detection, and identifying weaknesses in virtualized environments.

**Competitions**

- **CTF Competitions:** Created and Solved various challenges with 'Squid Proxy Lovers' (ctftime.org/team/222966). This includes:
  - Google CTF 2025: 3rd
  - DEFCON 2025 Quals: 10th
- **AI Jailbreak Competitions:** Won $500 by Jailbreaking GPT-5 using creative and minimalist prompt injection strategies.
- **CPTC:** Intercollegiate penetration-testing competition simulating realistic red-team exercises to find and exploit vulnerabilities.

## Technologies

**Programming Languages:** C++, C, LLVM, JavaScript, Swift, Python, x86_64 Assembly, SQL
**Tools:** LLVM, V8, Turbolizer, Fuzzilli, IDA, AFL++, pwntools, BurpSuite, Gen-AI,