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

Education

Rochester Institute of Technology (RIT) BS/MS in Cybersecurity — Expected Graduation: May 2028
- GPA: 3.84 | Dean's List (Fall 2024, Spring 2025)
- Member of RITSEC (Cybersecurity Club – Vulnerability Research, Reversing, Penetration Testing)
- RIT Wrestling Affiliate

Cicero North Syracuse High School / Syracuse University (STEP) Advanced Regents — Graduated June 2024
Diploma with Honors & Pre-University Program
- Weighted GPA: 99.4/100; Wrestling Team Captain

Experience

Penetration Testing Intern, Coalfire — May 2025 – Aug 2025
- Performed real-world cyberattacks to uncover security flaws. Assisted in ethical hacking engagements, vulnerability exploitation, and reporting. Contributed to securing networks and applications against advanced persistent threats.

Activities

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
  - File System Embedding into System Prompt
  - Lack of Request Throttling (DoS vulnerability)
  - Dozens of successful Prompt Injection Attempts
- Detailed findings and methodology are available in the full write-up on my page.

Pwn College 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.
- Learned key exploitation concepts including `FakeObject` and `AddrOf`, how to construct them, and how to utilize them.

Compiler & Browser Research — Nov 2024 – Present
- Dived into 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 minimalistic operating system and custom kernel designed for fuzz testing with LibAFL's QEMU mode, enabling security research and vulnerability discovery in low-level system components.
- Developed a specialized fuzzing harness to detect vulnerabilities in Google's 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' and '[:](SLICES)'. This includes:
  - Google CTF 2025: 3rd
  - DEFCON 2025 Quals: 10th
- **Red/Blue Team Competitions:** Competed in defensive cybersecurity events such as Hivestorm 2024 (University of Texas San Antonio), UB Lockdown (University of Buffalo), and IRSEC (RIT), focusing on network defense, incident response, and threat mitigation.

Technologies

Programming Languages: C++, C, LLVM, JavaScript, Python, x86_64 Assembly, Java, SQL
Tools: LLVM, V8, Turbolizer, IDA, LibAFL, pwntools, BurpSuite, Gen-AI,

Interests

LLVM compiler and IR research, JS V8 engine exploitation, Learning Japanese & Korean, Backpacking, Snowboarding, Wrestling & Brazilian Jiu-Jitsu, Archery, Spirited driving, Reading books & novels