Hamzah Uzzama

(929) 494 - 5056 | hamzahuzzama@gmail.com | www.linkedin.com/in/hamzah-uzzama/ | github.com/hamzahu1589

EDUCATION

CUNY Queens College, GPA, 4.0, **BS in Computer Science, Honors Business & Liberal Arts Minor** **Dec 2025**

- **Relevant Coursework:** Data Structures and Algorithms, Object-Oriented Programming Java, C++
- **Activities and Clubs:** Accenture Early ID Program, Point72 Data Scholars Program, CodeForAll

CodePath, **Cybersecurity Fellow** **Sep 2023 - Dec 2023**

- Implemented industry-standard protocols to enhance overall system security utilizing SSH for password encryption, and utilized Ubuntu Linux for penetration testing to detect and mitigate network vulnerabilities.

SKILLS

- **Technical Skills:** C++, HTML, CSS, JS,SQL, Tableau, Python, Java, Kali Linux, Splunk
- **Certifications:** CompTIA Security+ (Expected 10/15), Bloomberg Market Concepts & ESG, Google IT Fundamentals

PROFESSIONAL EXPERIENCE

Air Force Research Labs, **Cybersecurity Intern** **July 2024 - Aug 2024**

- Spearheaded the implementation of Retrieval-Augmented Generation (RAG) in a two-agent conversational AI setup, increasing conversation history utilization by 30% beyond the context window.
- Designed and developed 3 abstract classes in Python to support the integration and testing of 5 different memory strategies for conversational agents.
- Conducted extensive background research and leveraged over 10 coding examples to implement advanced memory capabilities, enhancing AI agent performance by 25%.

Webacy, **Cybersecurity Extern** **Mar 2024 - Apr 2024**

- Engaged in an immersive externship focused on enhancing digital security within the Web 3.0 ecosystem, applying theoretical knowledge to practical scenarios, and strengthening overall cybersecurity skills.
- Acquired in-depth knowledge of secure coding practices, blockchain designs, and network security protocols through weekly lessons from the Security Manager, improving understanding of secure development methodologies.
- Conducted analysis of wallet safety and panic buttons, across 3 platforms, within a detailed presentation to the CEO and 3 Senior Managers that received praise for clearly highlighting market standing and innovative security measures.

Accenture Immersive Labs, **Cybersecurity Program Participant** **Jan 2023 - March 2024**

- Trailed log analysis and defense security protocols to learn best practices for eliminating computer viruses, enhancing the organization's ability to respond to cyber threats effectively.
- Completed modules on system threat resolution using Windows PowerShell, gaining hands-on experience in identifying and mitigating vulnerabilities to strengthen overall security posture.
- Dedicated over 25 hours to operating on Metasploit, Burp Suite, Nessus, and Linux on platforms like Azure, improving penetration testing, vulnerability assessment, and secure system management skills.

Computer Care and Learning, **Tech Intern** **Jul 2023 - Aug 2023**

- Shadowed a lead technician to solve, understand, and meticulously document client issues with computer hardware and software, improving troubleshooting skills and ensuring accurate record-keeping for future reference.
- Cleaned and optimized 300k+ client records in MySQL, resulting in a 10% increase in data retrieval efficiency, which improved data management processes and facilitated quicker access to critical information.

TECHNICAL PROJECTS

Run2VM, **Tech Stack: Virtual Machines, MSFvenom** **Oct 2023**

- Gained practical experience in creating test files by developing malware designed to bypass detection systems, enhancing the ability to understand and counter cybersecurity threats.
- Conducted detailed malware analysis by downloading and isolating malware onto a virtual machine (VM), allowing for a safe examination of malicious behavior and improving detection and response techniques.
- Developed a single payload malware using MSFvenom, to target the computer's operating system and security protocols, providing valuable insights into system vulnerabilities and defenses.

Run2VM, **Tech Stack: Virtual Machines, MSFvenom** **Oct 2023**

- Utilized Ubuntu as the virtual machine to create a secure environment for password cracking exercises, enhancing understanding of Linux-based security operations and improving system security protocols.
- Cracked a password file with 1k+ employee passwords within 25 minutes using John the Ripper commands, to drive focus on vulnerabilities and risks associated with real-world data breaches such as Yahoo and LinkedIn.

Interactive Chat Assistant, **Tech Stack: Python, integrated OpenAI GPT-3** **Sept 2023**

- Used Python, LLMs, and ML to extract embeddings from 100MB+ multimedia files (Video, Documents) in <10 sec process
- Identified 10+ core intents per file, created a GPT use case, and built a pipeline using retrieval augmented generation
- Worked with external APIs, handling responses, and managing the streaming interface