ARSHDEEP SINGH

New York, NY 10038 | arshdeep.singh4@pace.edu | (551) 689-1852 | linkedin.com/in/ar33h | arshdeepsingh.me

PROFESSIONAL EXPERIENCE

Cerence Inc., Pune, India | Software Engineering Intern January 2023 – July 2023

- Interned at AI Automotive Startup focusing on tour guide application, developing JSON-based tour generation & stateful geo-fencing modules, enabling efficient creation of interactive guided tours, enhancing responsiveness by 25%.
- Diagnosed app crashes, patching key bugs within POI audio triggering and email system, increasing product reliability by 40%, decreasing crash times by 7 minutes.
- Led project to enhance overall experience through implementing GenAI features, designing wireframes and visuals for POC applications, collaborating with researchers to integrate a LLM into the UI.
- Streamlined release documentation, detailing changes, enhancements, and bug fixes to ensure clarity across stakeholders, leading to 15% decrease in post-release support inquiries.
- Automated audio generation for way-point description, utilizing Text-to-Speech services to obtain mp3 responses for 8 diverse routes, gauging word recognition rates & minimizing loss percentages.
- Initiated gathering customer insights on tour experiences, integrating feedback API, doubling form submissions from 500 to 1000 & driving actionable improvements for product evolution.

PROJECTS & COMPETITIONS

AI Prompt Injection Challenge: HackLLM July 2024

- Designed a 5-level security challenge utilizing Streamlit & LLaMa3 AI Model, facilitating hands-on learning experience, and educating users on the implications of prompt injection attacks on large language models.
- Incorporated API to respond to system prompts, setting the difficulty for all 5 levels, challenging the user to adopt exploitation strategies, demonstrating malicious inputs bypassing AI safeguards.

Data Privacy versus National Security Debate April 2024

- Awarded with the most valuable debater title for constructing arguments in favor of data privacy emphasizing the importance of individual privacy rights and the potential dangers of excessive government surveillance.
- Influenced judges and over 50 audience, advocating constitutional principles, highlighted public sentiments, 63% of Americans, regarding loss of control over personal data, supported by federal laws.

Qakbot Malware Analysis March 2024

- Conducted static and behavioral analysis of Qakbot malware using IDA & PEStudio, documenting malware capabilities, identifying 14+ key indicators of compromise and recommending mitigation strategies.
- Presented findings on evasion tactics, including DLL hijacking & registry manipulation, recommending use of email filtering systems & unauthorized execution prevention to reduce the malware attack surface.

One-Time Password Vulnerability Assessment February 2024

- Leveraged BurpSuite to analyze critical vulnerability allowing OTP bypass via response manipulation on organization's website, prompting implementation of robust security measures.
- Crafted structured bug report highlighting absence of encryption standards leading to ability of users to tamper with booking values, recommending input validation & 2-factor authentication to secure user access.

TECHNICAL SKILLS

Programming Languages: Python, JavaScript, Java, SQL
Databases & Cloud: MySQL, PostgreSQL, Firebase
Web Security Testing: BurpSuite, Metasploit, Nmap, Wireshark, SQLMap, Linux, XSS, CSRF
Malware Analysis: Remnux, Flare, IDA, VirusTotal, PEStudio, Regshot, Procmon
Cyber Intelligence: Google Dorking, Maltego, Tor, Wayback Imagery, FOCA

EDUCATION

Pace University, Seidenberg School of Computer Science & Information Systems **New York, NY**
Master of Science (MS) in Cybersecurity | **GPA:** 4.0 December 2024
Relevant Coursework: Ethical Hacking, Malware Analysis, Information Security Management, Cyber Intelligence, Network Security

Symbiosis International University, SIU **Pune, India**
Bachelor of Technology (B.Tech) in Computer Science & Engineering | **Honors:** Security & Privacy June 2023