Hari Priya Muppidi

LinkedIn: linkedin.com/in/hari-priya-muppidi-9a5809336 | Email: haripriyamuppidi02@gmail.com
Phone: +1 (404)-558-9263 | Github: https://github.com/HARIPRIYA02
Portfolio: https://haripriya02.github.io/HARIPRIYA02/

EDUCATION

University of Georgia, School of Computing — Athens, GA
Master of Science in Computer Science — August 2023 – May 2025

- Current GPA : 3.6 / 4.0
- Coursework: Privacy-preserving data analysis, Red-teaming Large Language Models(LLMs), Algorithms, Computer Networks, Database Management, Software Engineering

PROJECT EXPERIENCE

Red Teaming Scientific LLM Agents

- Investigated vulnerabilities in Large Language Model (LLM)-based agents, specifically targeting Cactus (chemical property analysis) and PaperQA (document evidence retrieval).
- Evaluated the robustness of these agents against prompt injection attacks (tool misuse and context ignoring), highlighting potential security risks associated with their instruction-following tendencies using Attack Success Rate(ASR) and Detection Evasion Rate(DER).

Art Gallery Management System

- Designed a modular system using React and Flask, with a scalable architecture for handling customer registrations, events, and transactions.
- Utilized MySQL to maintain a structured, reusable database model aligned with component-based design principles and schema.

Cinema E-Booking System

- Developed a web-based system incorporating secure payment and notification systems using PHP.
- Designed with user-centric features, schema diagrams, and domain classes to enhance scalability and reusability, consistent with shared service bureau environments.

WORK EXPERIENCE

Accenture
(Infrastructure Management - Middleware team for Ross Stores) — Hyderabad, India
Custom Software Engineering Analyst — August 2021 – July 2023

- Applied WebLogic and Log4j vulnerability patch updates across 100+ middleware instances.
- Streamlined security patch updates using automated scripts, reducing downtime significantly.
- Resolved 50+ backup failures and monitored alerts for 200+ application environments to maintain system reliability.

TECHNICAL SKILLS AND CERTIFICATIONS

- **Languages**: Python, JavaScript, React, HTML, CSS, PHP, C++
- **Technologies/Frameworks:** Flask, MySQL, Postgres, TimescaleDB, Git
- **Tools Used:** TimescaleDB, Grafana, Google Colab,

Certifications

Introduction to Databases – Coursera (Meta)
Google Cloud Computing Foundations – Google Cloud and NPTEL

ON CAMPUS INVOLVEMENTS

School of Computing, University of Georgia — Athens, GA
Graduate Teaching Assistant — January 2024 – May 2024
Graded 4 sections of 200+ students for CSCI 2670 - Theory of Computing course and resolved student's queries

Main Library, University of Georgia — Athens, GA
Security Student Assistant — August 2023 – January 2024

- Regulated and ensured the compliance of building and safety for 500+ students.