LLM-VEX: Extending Vulnerability Exploitability eXchange for AI-BOM Security Transparency

Project Description: Software supply chain security increasingly relies on standards such as SBOM and VEX. However, current frameworks do not capture LLM-specific risks.

Building upon guidance from CISA and vulnerability disclosure practices aligned with NIST, this project will:

- Identify LLM-specific vulnerability categories
- Extend VEX schema with LLM-focused records
- Design an AI-BOM format including model, data, and deployment artifacts
- Prototype an automated AI-BOM generator
- Evaluate interoperability with SBOM tooling

The resulting LLM-VEX specification will aim to formalize AI system vulnerability transparency.

Deliverable: specification draft, prototype implementation, and a conference-ready paper.

Project Type: Research + Engineering

Internship Batch: Batch 1 or Batch 2

Duties/Activities:

- Analyze SBOM and VEX specifications
- Model LLM vulnerability taxonomies
- Design JSON schema extension
- Implement AI-BOM prototype generator
- Conduct validation case studies
- Draft conference paper

Required Skills:

- Python
- JSON/schema modelling
- Systems security basics

Preferred Intern Academic Level: Senior undergraduate or MSc

Learning Opportunities:

- Software supply chain security
- AI system risk modelling
- Standards design
- Research publication process

Expected Team Size: 2–3 students

Mentors:

- Dr. Yazan Boshmaf (yboshmaf@hbku.edu.qa)
- Dr. Mohannad Alhanahnah (malhanahnah@hbku.edu.qa)