Benchmarking the Security of LLMs Generated Code

Project Description: The goal of this project is to evaluate the security of LLMs generated code. This study involves interacting with different LLMs and crafting prompts to generate code that could be evaluated against any of the TOP 25 CWEs in MITRE framework.

Project Type: Research

Internship Batch:

- **Batch 1:** May 12 to July 12, suitable for Education City students, i.e., CMUQ, TAMUQ and HBKU students
- **Batch 2:** May 26 to July 25, suitable for QU university students

Duties/Activities:

- Implementing an evaluation pipeline for different LLMs.
- Crafting prompts for code generation.
- Designing a dashboard for LLMs evaluation.

Required Skills:

- Proficient in C/C++ and Python.
- Familiarity with program analysis (Abstract Syntax Trees, Control Flow Graphs, etc.)
- Familiarity with the theory of languages and compilers is a plus.

Preferred Intern Academic Level: Senior

Learning Opportunities:

- Learning secure coding practices.
- Learning state-of-the-art tools (i.e., Joern and CodeQL) for vulnerability analysis.
- Exploring the vulnerability analysis research and how it is done in modern software engineering pipelines.
- Exploring prompt engineering and different ways of interaction with LLMs (e.g., Retrieval Augmented Generation).

Expected Team Size: *2*

Mentors

Name: Dr. Ahmed Lekssays email: alekssays@hbku.edu.qa