MySQL CTF Challenge Guide

Overview:

This Capture the Flag (CTF) challenge is designed around a vulnerable MySQL setup. Players must connect to the database, explore the schema, and retrieve a hidden flag stored in a table.

Challenge Setup:

- A MySQL 8.0 container is used for the challenge.
- The database `ctfdb` is created during initialization.
- Inside this database, a table `hashdump` contains a Base64-encoded flag hash.
- A restricted MySQL user `ptcuser` is created with SELECT-only permissions.
- The objective is to connect using this user and recover the hidden flag.

Player Instructions:

1. Connect to the MySQL container using the provided credentials.

- Username: `ptcuser`
- Password: `Mint@9876543210`
- Host: ``

2. Explore the `ctfdb` database.
3. Identify the `hashdump` table and query its contents.
4. Decode the Base64 string in the `hash` column to reveal the flag.

Notes:

- The challenge is focused only on database enumeration and decoding.
- Players do not have write or administrative privileges.
- Ensure the container is running before participants attempt the challenge.