## CTF – Capture The Flag

การแข่งขัน CTF ในปัจจุบันมักจะแบ่งเป็นสองแบบใหญ่ ๆ คือ การทำ attack and defense ซึ่งก็คือการแข่งขันในการป้องกันพร้อมทั้งโจมตีฝ่ายตรงกันข้ามโดยพร้อม ๆ กัน และ อีกรูปแบบหนึ่งก็คือการแข่งขันแบบ capture the flag ซึ่งก็คือการแข่งขันในการแก้ไขโจทย์ปัญหา เพื่อหา string ที่เป็นเสมือนคำตอบของโจทย์นั้น ๆ แล้วนำมาขึ้นคะแนน ผู้ใดที่ได้คะแนนรวมสูงสุด ก็จะได้รับชัยชนะไป โดย string คำตอบนี้มักจะอยู่ในรูปแบบต่าง ๆ เช่น FLAG{<md5 string>} หรือแม้กระทั่ง flag{<md5 string>} โดยในโจทย์ข้อนี้ คุณจะทำหน้าที่เป็นผู้เข้าแข่งขันโจทย์ CTF ในข้อหนึ่ง กล่าวว่า มีระบบฐานข้อมูลขอเว็ปไซต์บทความอยู่ โดยบทความจะเก็บไว้ในตารางที่ประกอบด้วย blog id, title และ body และ ผู้เขียนบทความหลาย ๆ ท่านในนั้นได้เผลอเรอ แล้วทำการ copy secret key ตัวเองลงไป paste ใน body ของบทความแล้วอัพโหลดขึ้นระบบ ! โดย key ที่ว่านั้นจะอยู่ในรูปแบบของ FLAG{<md5 string>} หรือ flag{<md5 string>} เท่านั้น โดย <md5 string> หมายถึง string ที่ถูกเข้ารหัสด้วย algorithm md5 มีความยาว 32 ตัวอักษร หน้าที่ของคุณคือการตามหาบทความทุกอันที่มี flag เหล่านี้อยู่

**โครงสร้างข้อมูล**

มี 1 ตารางชื่อดังต่อไปนี้

1. blog มี Column ดังต่อไปนี้
    - bid รหัสบทความ เป็น Primary key ประเภท serial
    - title ชื่อของบทความ ประเภท text
    - body เนื้อหาของบทความ ประเภท text

**ข้อมูลส่งออก**

SQL ที่เขียนนั้นจะต้องมีผลลัพธ์เพียง 3 column ซึ่งคือ รหัสบทความ (bid), ชื่อบทความ (title) และเนื้อหาบทความ (body) โดยมีจำนวน record เป็น 0 หรือ มากกว่านั้น โดย จะเป็น 0 ในกรณีที่ตารางไม่มีข้อมูลเลย และ กรณีที่ไม่มี flag อยู่ในบทความใด ๆ เลย โดยผลลัพธ์ให้เรียงตามรหัสบทความจากน้อยไปมาก

**การส่งโจทย์ใน Grader**

- ให้ส่งมาเป็นคำสั่งภาษา SQL สำหรับ PostgreSQL และให้เลือกภาษาตอนส่งเป็น “postgres”

**ชุดข้อมูลทดสอบ**

- 100% มี flag อยู่ในหลายบทความ

Pro-tips: ILIKE เป็นคำสั่งที่เหมือนคำสั่ง LIKE เพียงแต่สามารถค้นหาแบบ case insensitive ได้