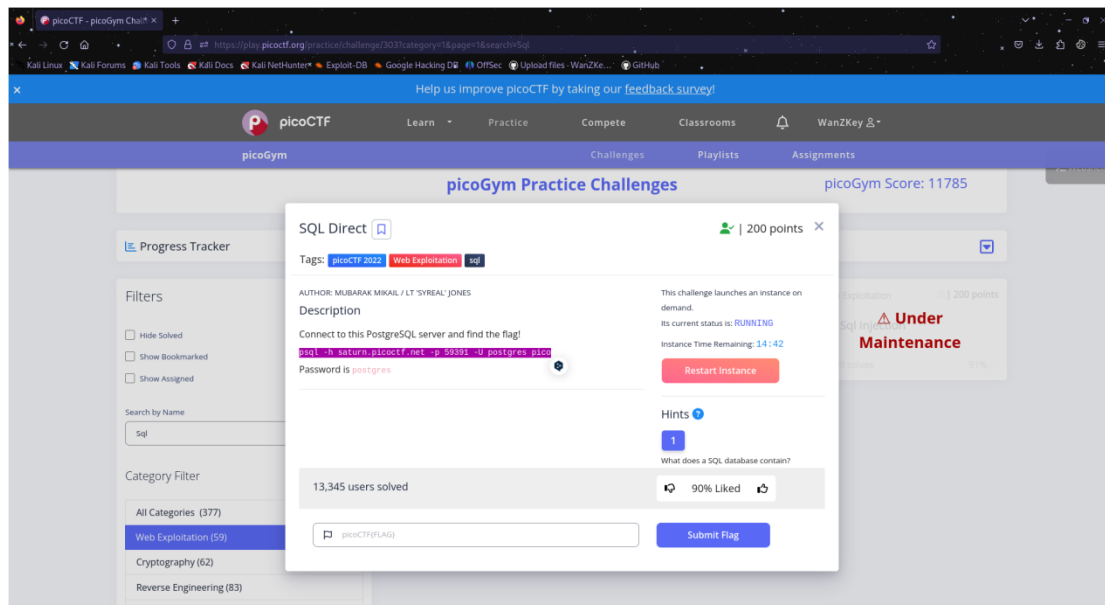


Nama Team : BELMOTI CYBER  
Anggota : Riduan  
: Dikara Syarofunniam

## Web Explotation

### Soal Nomor 1 SQL Direct

#### 1. Tampilan Awal Soal.



Pertama ini kita di berikan Tautan yang disediakan adalah perintah PostgreSQL untuk menyambung ke basis data pada server **saturn.picoctf.net** dengan menggunakan tautan: `psql -h saturn.picoctf.net -p 59391 -U postgres pico` kata sandi: **postgres**.

Cara penyelesaiannya kita menggunakan terminal yg ada di kali linux kita, masuk menggunakan linknya dan masukan password nya seperti yang tertera pada website pico Tersebut. karna untuk mendapatkan flagnya kita harus memasuki direktori database pada PostgreSQL.

#### 2. Tampilan Awal Terminal.



Ini merupakan tampilan awal ketika kita memasuki database psql nya, nah untuk mendapatkan flagnya kita perlu melihat **"Direktori Daftar Tabel Database"** di dalam SQL tersebut, dengan cara mengetik **"\dt"** dalam terminal tersebut.

### 3. Isi Daftar Tabel.

```
lks@LKS: ~
File Actions Edit View Help
zsh: corrupt history file /home/lks/.zsh_history
(lks@LKS)-[~]
$ psql -h saturn.picoctf.net -p 52277 -U postgres pico
Password for user postgres:
psql (16.3 (Debian 16.3-1), server 15.2 (Debian 15.2-1.pgdg110+1))
Type "help" for help.

pico=# \dt
          List of relations
Schema | Name | Type | Owner
-----+-----+-----+-----
public | flags | table | postgres
(1 row)
```

Nah kita sudah masuk ke Direktori Daftar Tabel, dan juga kita menemukan **“Direktori Tabel Flag”** di Tabel tersebutlah berisi flagnya, untuk itu kita harus memilih tabel tersebut menemukan Flag-nya, Dengan cara memasukan sintaks **“Select \* from flags;”** pada terminal linux.

### 4. Isi Flag.

```
lks@LKS: ~
File Actions Edit View Help
zsh: corrupt history file /home/lks/.zsh_history
(lks@LKS)-[~]
$ psql -h saturn.picoctf.net -p 52277 -U postgres pico
Password for user postgres:
psql (16.3 (Debian 16.3-1), server 15.2 (Debian 15.2-1.pgdg110+1))
Type "help" for help.

pico=# \dt
          List of relations
Schema | Name | Type | Owner
-----+-----+-----+-----
public | flags | table | postgres
(1 row)

pico=# select * from flags;
 id | firstname | lastname | address
----+-----+-----+-----
  1 | Luke      | Skywalker | picoCTF{L3arN_S0m3_5qL_t0d4Y_21c94904}
  2 | Leia      | Organa    | Alderaan
  3 | Han       | Solo      | Corellia
(3 rows)
```

Nah kita mendapatkan Flag-nya, yaitu :

**“picoCTF{L3arN\_S0m3\_5qL\_t0d4Y\_21c94904}”**.