

LinkedIn: [Kelvin KImotho](#)

## Description

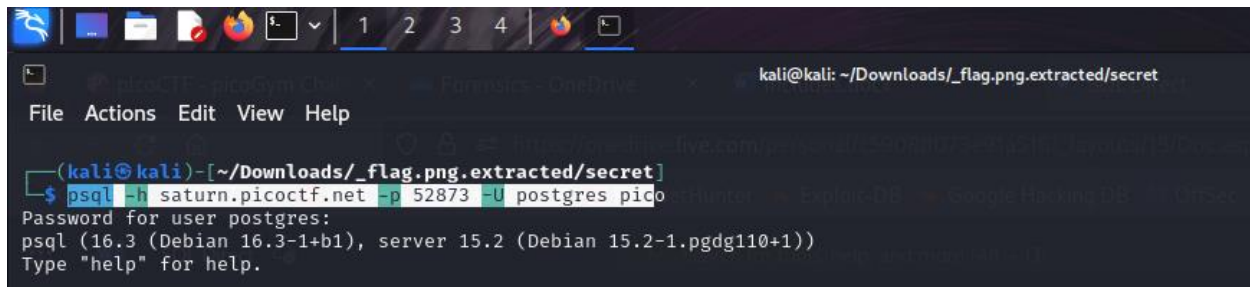
Connect to this PostgreSQL server and find the flag! **psql -h saturn.picocftf.net -p 52873 -U postgres pico** Password is **postgres**

*Hint: What does a SQL database contain?*

## Solution

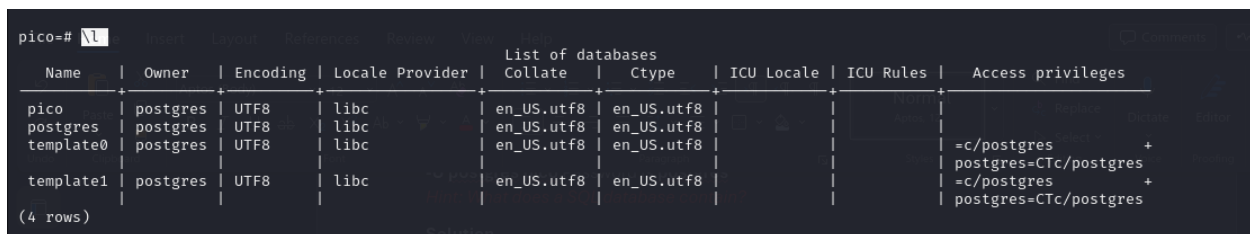
According to the hint, nothing much was required. Just the knowledge of how Postgres database work and SQL language in general.

I went ahead and connected to the Postgres server.



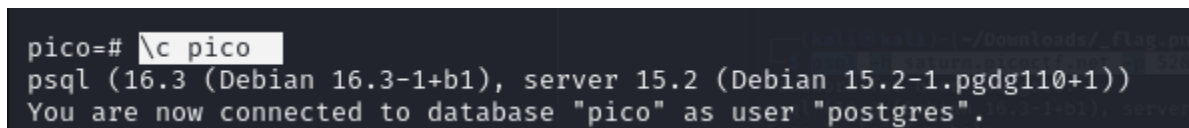
```
kali@kali: ~/Downloads/_flag.png.extracted/secret
(kali@kali)~[~/Downloads/_flag.png.extracted/secret]
$ psql -h saturn.picocftf.net -p 52873 -U postgres pico
Password for user postgres:
psql (16.3 (Debian 16.3-1+b1), server 15.2 (Debian 15.2-1.pgdg110+1))
Type "help" for help.
```

I then used the `\l` flag to list all the databases in the server.



```
pico=# \l
      List of databases
  Name | Owner | Encoding | Locale Provider | Collate | Ctype | ICU Locale | ICU Rules | Access privileges
-----+-----+-----+-----+-----+-----+-----+-----+-----
pico   | postgres | UTF8 | libc | en_US.utf8 | en_US.utf8 | | | |
postgres | postgres | UTF8 | libc | en_US.utf8 | en_US.utf8 | | | |
template0 | postgres | UTF8 | libc | en_US.utf8 | en_US.utf8 | | | |
template1 | postgres | UTF8 | libc | en_US.utf8 | en_US.utf8 | | | |
(4 rows)
```

I found a database named **pico** interesting. I use `\c` flag followed by the database name to connect to it for further analysis.



```
pico=# \c pico
psql (16.3 (Debian 16.3-1+b1), server 15.2 (Debian 15.2-1.pgdg110+1))
You are now connected to database "pico" as user "postgres".
```

After a successful connection to pico database, I used the `\dt` flag to list all the database tables in the pico database.

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

A table named **flags** caught my eyes. I proceeded to examining what flags were stored in there. I ran this command “**select \* from flags**”. This command returns each and every record stored in the flags table, this is possible when **\*** flag is used in SQL which specifies ‘everything’. And That’s how I retrieved the flag “**picoCTF{L3arN\_S0m3\_5qL\_t0d4Y\_21c94904}**”.

```
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)

pico=#
```