SQL Direct

Web Exploitation

Description:

Connect to this PostgreSQL server and find the flag!
Additional details will be available after launching your challenge instance.

Connect to this PostgreSQL server and find the flag!

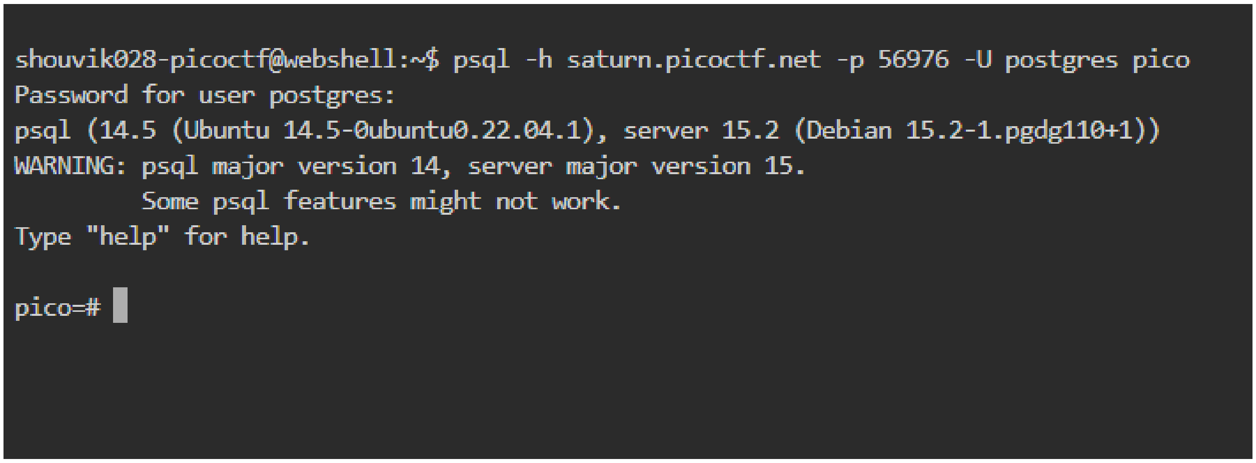
`psql -h saturn.picoctf.net -p 56976 -U postgres pico`

Password is `postgres`

Hints:

1) What does a SQL database contain?

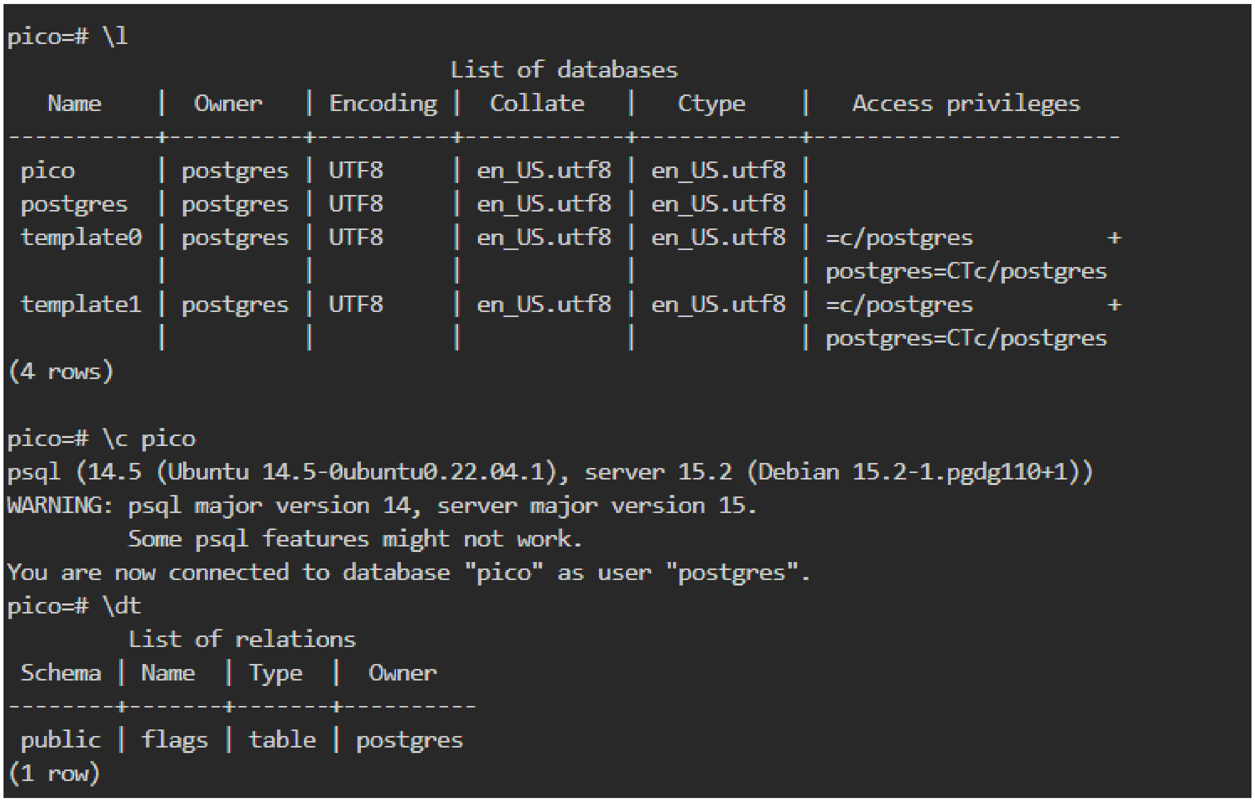
Solution:



```
shouvik028-picoctf@webshell:~$ psql -h saturn.picoctf.net -p 56976 -U postgres pico
Password for user postgres:
psql (14.5 (Ubuntu 14.5-0ubuntu0.22.04.1), server 15.2 (Debian 15.2-1.pgdg110+1))
WARNING: psql major version 14, server major version 15.
         Some psql features might not work.
Type "help" for help.

pico=#
```

1) We use the pico webshell and enter the command in the description with password postgres.
2) We use \l to list the directories.

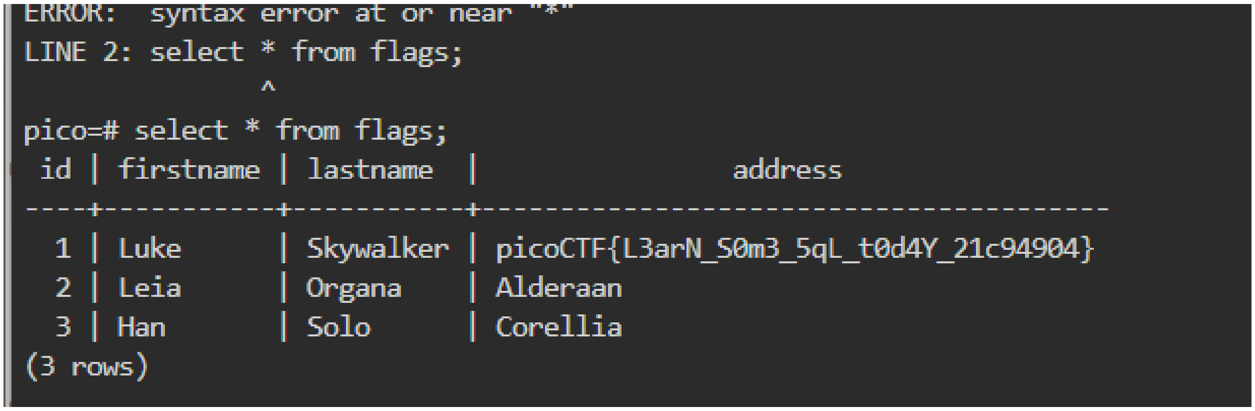


```
pico=# \l
                                List of databases
   Name    |  Owner   | Encoding |  Collate   |   Ctype    |   Access privileges
-----------+----------+----------+------------+------------+-----------------------
 pico      | postgres | UTF8     | en_US.utf8 | en_US.utf8 |
 postgres  | postgres | UTF8     | en_US.utf8 | en_US.utf8 |
 template0 | postgres | UTF8     | en_US.utf8 | en_US.utf8 | =c/postgres          +
           |          |          |            |            | postgres=CTc/postgres
 template1 | postgres | UTF8     | en_US.utf8 | en_US.utf8 | =c/postgres          +
           |          |          |            |            | postgres=CTc/postgres
(4 rows)

pico=# \c pico
psql (14.5 (Ubuntu 14.5-0ubuntu0.22.04.1), server 15.2 (Debian 15.2-1.pgdg110+1))
WARNING: psql major version 14, server major version 15.
         Some psql features might not work.
You are now connected to database "pico" as user "postgres".
pico=# \dt
         List of relations
 Schema | Name  | Type  |  Owner
--------+-------+-------+----------
 public | flags | table | postgres
(1 row)
```

3) Using \dt to list directories we see a directory called flags.

4) We navigate through this directory to find the flag.



```
ERROR:  syntax error at or near "*"
LINE 2: select * from flags;
               ^
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)
```

Flag:
picoCTF{L3arN_S0m3_5qL_t0d4Y_21c94904}