Michael N LoginKey Challenge Documentation

```
root@0x4261622792058:~/reverseCtf/loginKey/chal# ls -l
total 20
-rwxr-xr-x 1 root root 18528 Sep 10 17:49 CTFChallenge
root@0x4261622792058:~/reverseCtf/loginKey/chal# ./CTFChallenge

        ************************************************
        *        Welcome to 0xDoc Sharing Server       *
        ************************************************

0x999 ~ Please enter in your Login Key: 0x123456789
Login failed!
root@0x4261622792058:~/reverseCtf/loginKey/chal#
```

Verify file in directory
Testing file

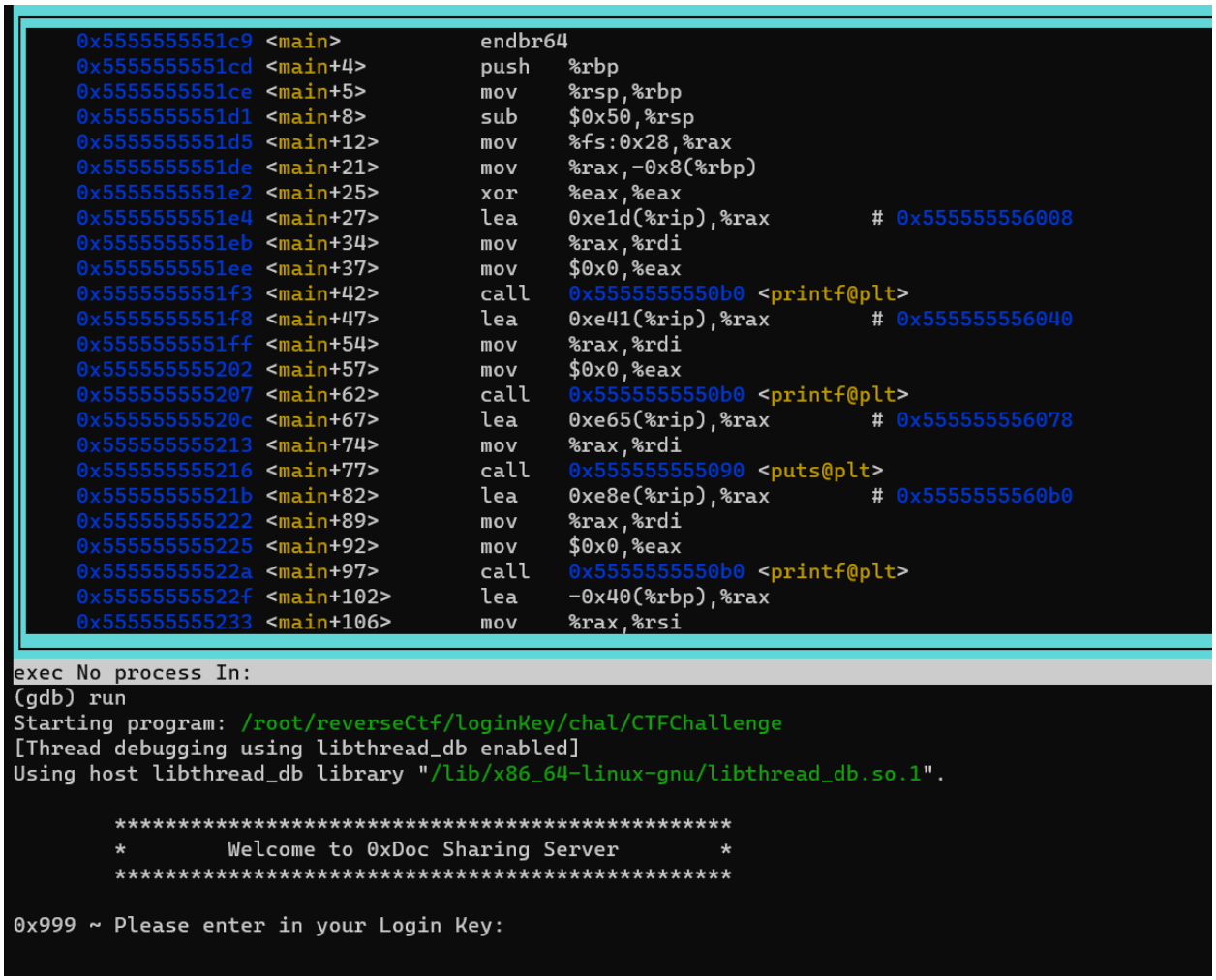
Then open file in GDB

```
root@0x4261622792058:~/reverseCtf/loginKey/chal# gdb ./CTFChallenge
GNU gdb (Ubuntu 12.1-0ubuntu1~22.04) 12.1
Copyright (C) 2022 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./CTFChallenge...
(gdb)
```

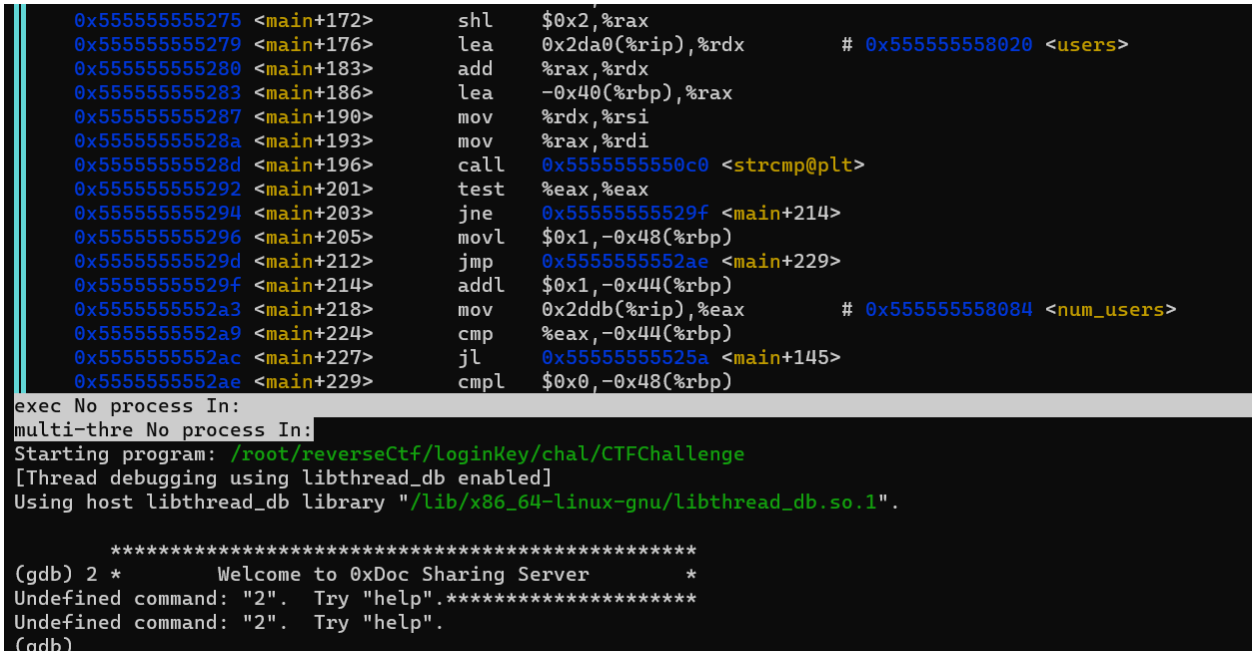
After opening the file in GDB, execute the command layout next. This command sets up the GDB interface to display the assembly output, registers.

Then Type run into the new window to run the program while gdb in analyzing it

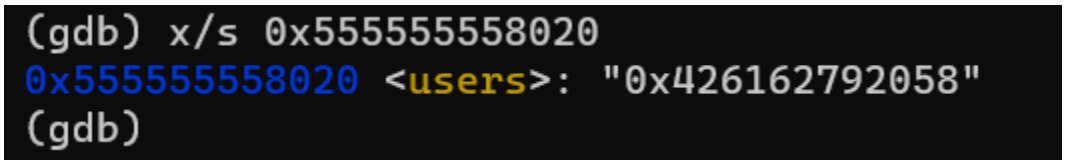


Enter in random input

Notice that something was lea from a external module named users.



Using the memory address in hex 0x555555558020 from module users
You can display what is in that memory address by using command : *x/s 0x555555558020*



Now you have the login key which is my discord user name…

***Now you can copy and paste this into the code running in a netcat server to get the flag*