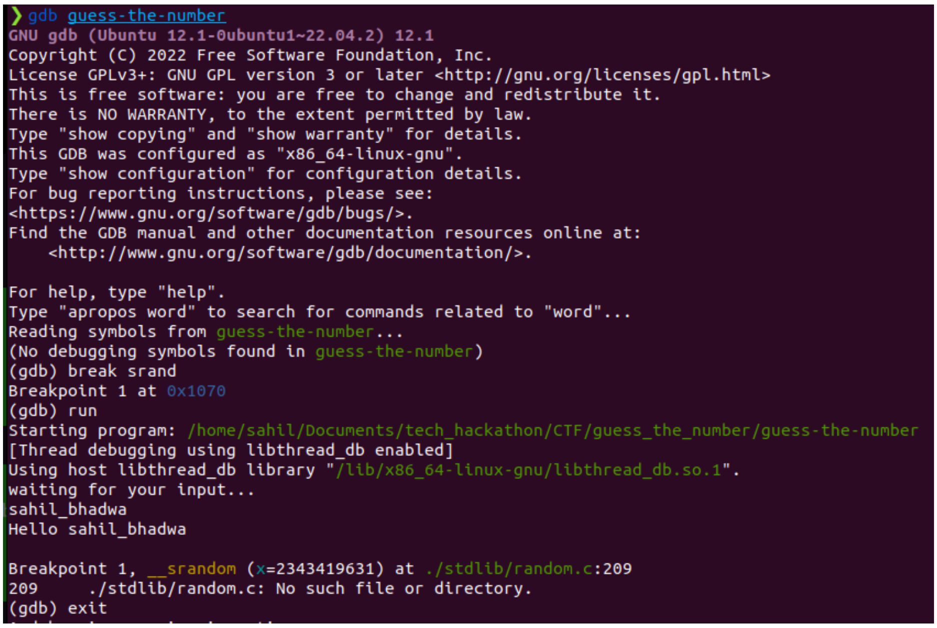
Capture the Flag - CTF

- ## Guess the Number
  - Game? 👀 yay!! Let's go. I can't guess. No ways I have other plans. Hacker hain bhai hacker. Mission Impossible 9 - Find SEED. gdb on the way to save me. gdb ./guess-the-number. break srand. run. BINGO!!

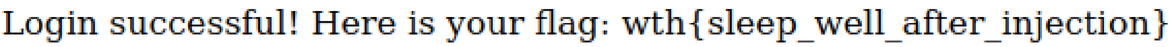
FLAG- wth{tech_council_op}



```
❯ gdb guess-the-number
GNU gdb (Ubuntu 12.1-0ubuntu1~22.04.2) 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 guess-the-number...
(No debugging symbols found in guess-the-number)
(gdb) break srand
Breakpoint 1 at 0x1070
(gdb) run
Starting program: /home/sahil/Documents/tech_hackathon/CTF/guess_the_number/guess-the-number
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
waiting for your input...
sahil_bhadwa
Hello sahil_bhadwa

Breakpoint 1, __srandom (x=2343419631) at ./stdlib/random.c:209
209     ./stdlib/random.c: No such file or directory.
(gdb) exit
```

- ## Login
  - Login! Maybe databases connection exist at the backend. BINGO! It is SQL injection. But wait its not working, lets inspect. Hmmm, JS check function need to bypass, sure open console and define your own function that returns true ONLY and here you **GO.** Gotchaaa….

FLAG- wth{sleep_well_after_injection}



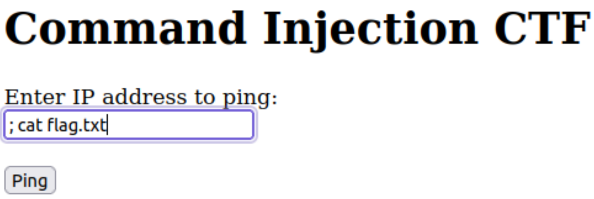
Login successful! Here is your flag: wth{sleep_well_after_injection}

Username- **‘ OR 1=1;--**

[Caution: It is always true beware of SQL injection]

- PING
  - Intersting! OS commands at the back? Let’s check time for command injection, “;ls”. BINGO! Let’s go, “;cat flag.txt”.

FLAG- wth{spread_systems_not_ai}



Command Injection CTF

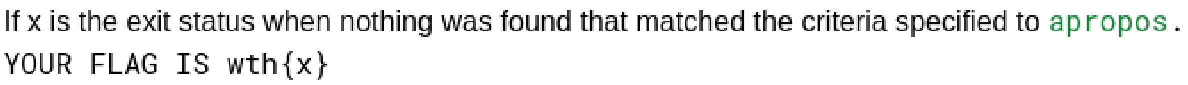
Enter IP address to ping:

; cat flag.txt

- OUR LOGO
  - Steganography? Let’s try the ‘zsteg’ tool. “Zsteg -a ./tech_council_logo.png”. Ohh! I see 👀, extra BYTES. Let’s extract using python script. “.bin” file generated can there be a secret message, conversion on the way to string. NO, result. Done for the day, 1sec away from shutting down the laptop notices something different, opens the bin file. RICKROLL!!!! Bhai yeh ganda wala tha 🙂.

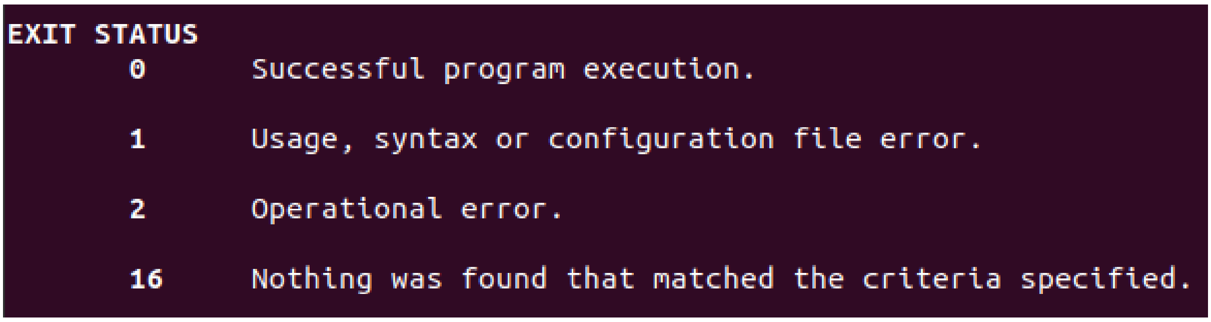
FLAG- wth{salute=o7_hi=o/_hurary=\o/}

- Beyond CTF



If x is the exit status when nothing was found that matched the criteria specified to `apropos`.

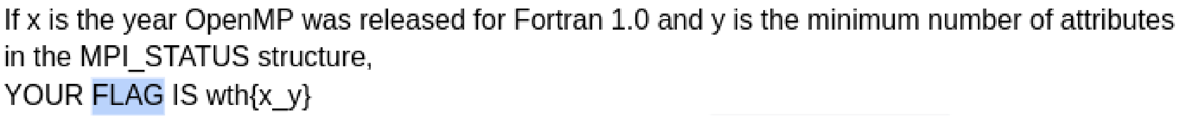
`YOUR FLAG IS wth{x}`



```
EXIT STATUS
       0      Successful program execution.

       1      Usage, syntax or configuration file error.

       2      Operational error.

       16     Nothing was found that matched the criteria specified.
```

FLAG- wth{16}

- Beyond CTF - this time for real.
    - This time for real?????????????????????????????????? Flag le lo yaar.



If x is the year OpenMP was released for Fortran 1.0 and y is the minimum number of attributes in the MPI_STATUS structure,
YOUR FLAG IS wth{x_y}

FLAG- wth{1997_3}