

GDB baby step 1



Medium

Reverse Engineering

picoGym Exclusive

x86_64

AUTHOR: LT 'SYREAL' JONES

Description

Can you figure out what is in the `eax` register at the end of the `main` function? Put your answer in the picoCTF flag format: `picoCTF{n}` where `n` is the contents of the `eax` register in the decimal number base. If the answer was `0x11` your flag would be `picoCTF{17}`.

Disassemble [this](#).

Hints

1

2

`main` is actually a recognized symbol that can be used with gdb commands.

Kita langsung saja buka dengan Binary Ninja dan langsung ke fungsi main

```
00401129  int32_t main(int32_t argc, char** argv, char** envp) __pure
00401131      int32_t argc_1 = argc
00401134      char** argv_1 = argv
0040113e      return 549698
```

fungsi main langsung mereturn sebuah angka dan itu flagnya

Flag : PicoCTF{549698}