



Medium Reverse Engineering picoGym Exclusive x86_64

AUTHOR: LT 'SYREAL' JONES

Description

Can you figure out what is in the `eax` register? 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}`.

Download the assembly dump [here](#).

Hints ?

1

PTR's or 'pointers', reference a location in memory where values can be stored.

Kita cat saja filenya.

```
Bit-0-Asm2 % ls
disassembler-dump0_b.txt
Bit-0-Asm2 % file disassembler-dump0_b.txt
disassembler-dump0_b.txt: ASCII text
Bit-0-Asm2 % cat disassembler-dump0_b.txt
<+0>:    endbr64
<+4>:    push    rbp
<+5>:    mov     rbp,rs
<+8>:    mov     DWORD PTR [rbp-0x14],edi
<+11>:   mov     QWORD PTR [rbp-0x20],rsi
<+15>:   mov     DWORD PTR [rbp-0x4],0x9fe1a
<+22>:   mov     eax,DWORD PTR [rbp-0x4]
<+25>:   pop    rbp
<+26>:   ret
```

intinya, kita harus mengetahui apa yang disimpan di `eax`, jadi pada isi file tersebut, `eax` menyimpan alamat `rbp-0x4` dimana `rbp-0x4` juga menyimpan alamat dari desimal(0x9fe1a)

jadi flagnya adalah `picoCTF{654874}`