



Medium Reverse Engineering picoGym Exclusive

AUTHOR: ABHISHEK AGARWAL

Hints ?

1 2

The combined range of hex-ascii for English alphabets and numerical digits is from 30 to 7A.

Description

This program has constructed the flag using hex ascii values. Identify the flag text by disassembling the program.

You can download the file from [here](#).

```
00401169    int32_t main(int32_t argc, char** argv, char** envp)
00401175        void* fsbase
00401175        int64_t rax = *(fsbase + 0x28)
00401184        char var_38
00401184        __builtin_strncpy(dest: &var_38, src: "picoCTF{ASCII_IS_EASY_3CF4BFAD}", count: 0x1f)
00401184        printf(format: "The flag starts with %x\n", 0x70)
00401215        int64_t rax_3 = rax ^ *(fsbase + 0x28)
0040121f
00401228        if (rax_3 == 0)
00401230            return rax_3.d
00401230
0040122a        __stack_chk_fail()
0040122a        noreturn
```

flag : picoCTF{ASCII\_IS\_EASY\_3CF4BFAD}