

AUTHOR: SANJAY C

Description

What does asm1(0x3fa) return? Submit the flag as a hexadecimal value (starting with '0x'). NOTE: Your submission for this question will NOT be in the normal flag format. [Source](#)

Hints ?

1

assembly conditions

```
asm1 % cat test.S
asm1:
    <+0>:    endbr32
    <+4>:    push    ebp
    <+5>:    mov     ebp,esp
    <+7>:    cmp     DWORD PTR [ebp+0x8],0x2a7
    <+14>:   jg      0x11d3 <asm1+38>
    <+16>:   cmp     DWORD PTR [ebp+0x8],0x28
    <+20>:   jne     0x11cb <asm1+30>
    <+22>:   mov     eax,DWORD PTR [ebp+0x8]
    <+25>:   add     eax,0x15
    <+28>:   jmp     0x11ea <asm1+61>
    <+30>:   mov     eax,DWORD PTR [ebp+0x8]
    <+33>:   sub     eax,0x15
    <+36>:   jmp     0x11ea <asm1+61>
    <+38>:   cmp     DWORD PTR [ebp+0x8],0x48b
    <+45>:   jne     0x11e4 <asm1+55>
    <+47>:   mov     eax,DWORD PTR [ebp+0x8]
    <+50>:   sub     eax,0x15
    <+53>:   jmp     0x11ea <asm1+61>
    <+55>:   mov     eax,DWORD PTR [ebp+0x8]
    <+58>:   add     eax,0x15
    <+61>:   pop     ebp
    <+62>:   ret
```

asm1 % 

ebp diberikan nilai 0x3fa sesuai pada deskripsi, lalu ebp dibandingkan dengan 0x2a7 alhasil ternyata ebp lebih besar sehingga lompat ke baris 38. Pada baris ke 38, ebp (0x2a7)

dibandingkan dengan 0x48b, ternyata tidak sama sehingga lompat ke 55. Pada baris ke 55, ebp disimpan di eax, lalu eax ditambah 0x15 hasilnya 0x40f.