




## (ii) ARMssembly 0:

ARMssembly 0 


 | 40 points 

Tags: picoCTF 2021 Reverse Engineering

AUTHOR: DYLAN MCGUIRE

Description



What integer does this program print with arguments 266134863 and 1592237099? File: chall.S Flag format: picoCTF{XXXXXXXX} -> (hex, lowercase, no 0x, and 32 bits. ex. 5614267 would be picoCTF{0055aabb})


Hints 

1

Simple compare

6,631 solves / 8,090 users attempted (82%)

 53% Liked 

 picoCTF{FLAG}

Submit Flag

Its given as a hint that we simply have to compare the hexadecimal forms of the given numbers, which we can get easily by running a python script.

I converted the first integer to hex:

```
print(hex(266134863))
```

Output:

```
Tanay Aggarwal@LAPTOP-2A3UP0LM MINGW64 ~  
$ "C:/Users/Tanay Aggarwal/AppData/Local/Microsoft/windowsApps/python3.11.exe" "c:/Users/Tanay Aggarwal/Downloads/temp.py"  
0xfdce54f
```

When I passed this as an argument in the picoCTF{}, it returned the flag as incorrect. So I tried the next integer.

```
print(hex(1592237099))
```

Output:

```
Tanay Aggarwal@LAPTOP-2A3UP0LM MINGW64 ~  
$ "C:/Users/Tanay Aggarwal/AppData/Local/Microsoft/windowsApps/python3.11.exe" "c:/Users/Tanay Aggarwal/Downloads/temp.py"  
0x5ee79c2b
```

When I passed the following:

picoCTF{5ee79c2b} as the flag,

Reverse Engineering

ARMssembly 0

6,633 solves

53% 

 | 40 points

[I could not understand the assembly language code, so I tried this to see if I could cross the level]

This completes this level.