

picoCTF 2021

Hints ?

1

Simple compare

bits, ex. 5614267 would be picoCTF{0055aabb})

Use arguments a and b: 2593949075 and 2233560849

```

.arch armv8-a
.file "chall.c"
.text
.align 2
.global func1
.type func1, %function
func1:
    sub sp, sp, #16
    str w0, [sp, 12] ; simpan argumen a
    str w1, [sp, 8] ; simpan argumen b
    ldr w1, [sp, 12] ; ambil a
    ldr w0, [sp, 8] ; ambil b
    cmp w1, w0 ; bandingkan antara a dan b
    bhs .L2 ; jika a <= b, jump ke L2
    ldr w0, [sp, 12] ; jika a > b, kembalikan (return) nilai a
    b .L3
.L2:
    ldr w0, [sp, 8] ; return b
.L3:
    add sp, sp, 16 ; kembalikan nilai stack pointer (sp)
    ret ; return
.size func1, .-func1
.section .rodata
.align 3
.LC0:
    .asciz "Pilih salah satu: a atau b"

```

```

ARMssembly0 % cat chall.S
.arch armv8-a
.file "chall.c"
.text
.align 2
.global func1
.type func1, %function
func1:
    sub    sp, sp, #16
    str    w0, [sp, 12]
    str    w1, [sp, 8]
    ldr    w1, [sp, 12]
    ldr    w0, [sp, 8]
    cmp    w1, w0
    bls    .L2
    ldr    w0, [sp, 12]
    b      .L3
.L2:
    ldr    w0, [sp, 8]
.L3:
    add    sp, sp, 16
    ret
.size    func1, .-func1

>>> clear
>>> str_angka1 = "2593949075"
>>> str_angka2 = "2233560849"
>>> print(len(str_angka1))
10
>>> print(len(str_angka2))
Traceback (most recent call last):
  File "<python-input-4>", line 1, in <module>
    print(len(str_angka2))
          ^^^^^^^^^
NameError: name 'str_angka2' is not defined. Did you mean: 'str_angka1'?
>>> clear
>>> str_angka1 = "2593949075"
>>> str_angka2 = "2233560849"
>>> print(len(str_angka1))
10
>>> print(len(str_angka2))
10
>>> hex(2593949075)
'0x9a9c8593'
>>> 

```

Flag : picoCTF{9a9c8593}