Reverse 🔖

👤✓

Medium **Reverse Engineering** **picoCTF 2023**

AUTHOR: MUBARAK MIKAIL

Description

Try reversing this file? Can ya?

I forgot the password to this file. Please find it for me?

Hints ❓

(None)

Langsung ketemu flagnya ketika buka filenya di binary ninja

```
int32_t main(int32_t argc, char** argv, char** envp)

    void* fsbase
    int64_t rax = *(fsbase + 0x28)
    int64_t str
    __builtin_strncpy(dest: &str, src: "picoCTF{3lf_r3v3r5ing_succe55ful_9ae8528",
        count: 0x28)
    printf(format: "Enter the password to unlock this file: ", argv, 0x6c75663535656363)
    char var_68[0x30]
    __isoc99_scanf(format: "%s", &var_68)
    printf(format: "You entered: %s\n", &var_68)

    if (strcmp(&var_68, &str) != 0)
    |   puts(str: "Access denied")
    else
    |   puts(str: "Password correct, please see flag: picoCTF{3lf_r3v3r5ing_succe55ful_9ae85289}")
    |   puts(&str)

    if (rax == *(fsbase + 0x28))
    |   return 0

    __stack_chk_fail()
    noreturn
```

picoCTF{3lf_r3v3r5ing_succe55ful_9ae85289}