

# IDA Lab Assignment

Date : 30 - 09 - 2025  
Raj Shekhar - 240545002004

Objective : IDA Lab to find the secret password in the exe file of a C program.

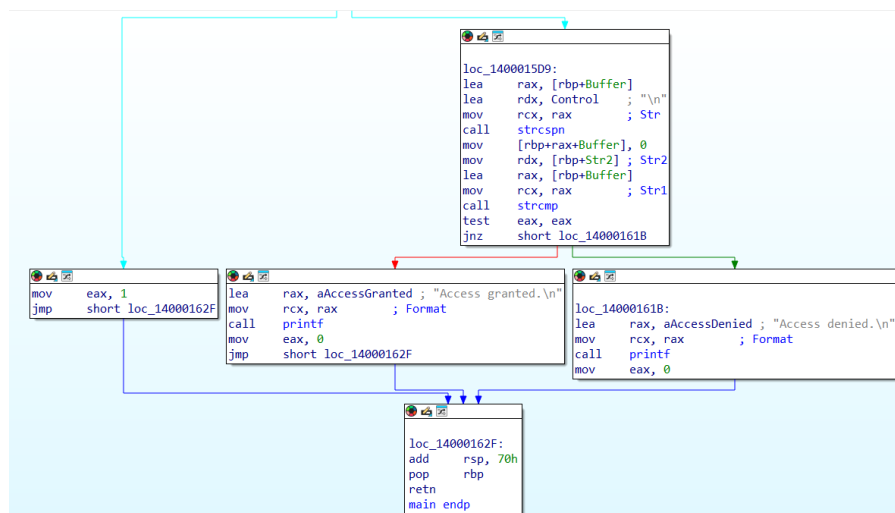
Step 1 : Open IDA pro and Select the file to analyse.

```
public main
main proc near

Buffer= byte ptr -50h
Str2= qword ptr -8

push    rbp
mov     rbp, rsp
sub     rsp, 70h
call    __main
lea     rax, aS3cr3tpSsw0rd ; "S3cr3tP@ssw0rd"
mov     [rbp+Str2], rax
lea     rax, Format          ; "Enter password: "
mov     rcx, rax             ; Format
call    printf
mov     ecx, 0               ; index
mov     rax, cs:__imp__acrt_iob_func
call    rax ; __acrt_iob_func
mov     rdx, rax
lea     rax, [rbp+Buffer]
mov     r8, rdx              ; Stream
mov     edx, 40h ; '@'      ; MaxCount
mov     rcx, rax             ; Buffer
call    fgets
test    rax, rax
jnz     short loc_1400015D9
```

Step 2 : Look for the interested string in the Disassembler window.



Step 3 : Verify the process further.

Step 4 : Check if the key is valid and working.

Step 5 : Report the Leakage of the key.

Conclusion : Hence, Using IDA pro helps reveal hidden insights like passwords, vulnerabilities, etc of a software to rebuild it, here a key was found inside program itself to restrict users from accessing.