CS4238 Lab: OllyDbg

The **goal** of this lab is to get familiar **with OllyDbg**.

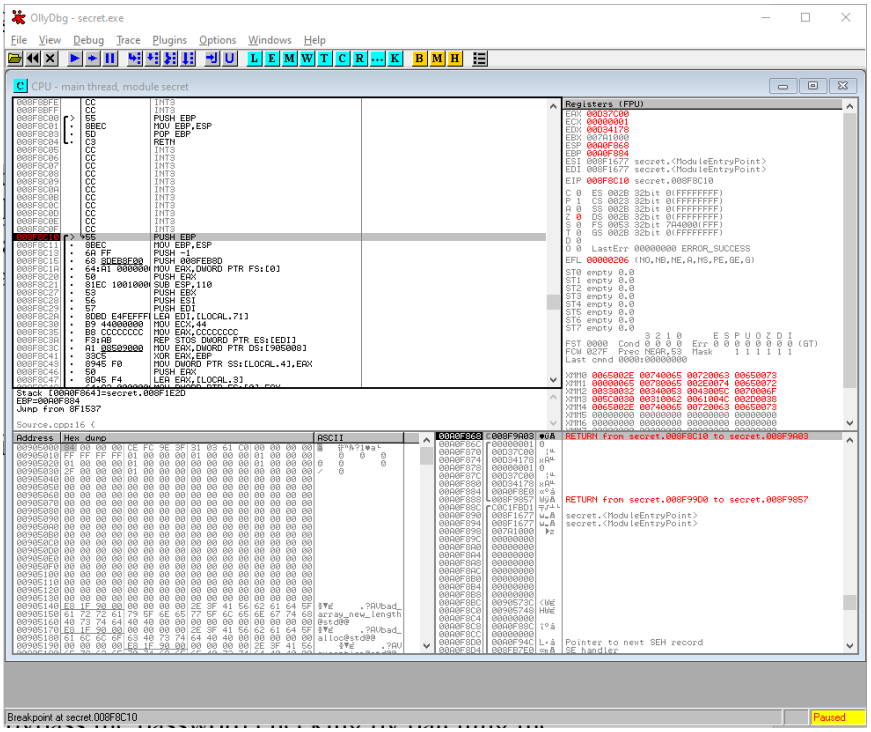
Lab Set-up

You will need the OllyDbg for this lab (already integrated into the Flare VM). You can also install it from the website. A *secret.exe* file will be used for analysis (see this lab's attachments). It is a program which takes a string as input, compares the input with a secret string, and decides whether to accept the input or reject it.

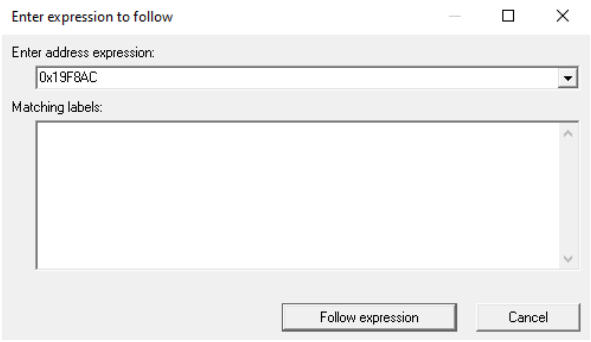
A. Set breakpoints

The goal of this task is to set breakpoints within different methods.

1. (INT 3) Breakpoints at arbitrary instruction by selecting an instruction and pressing F2:



2. (Memory) Choose an address to set a breakpoint, e.g. 0x19F8AC. Press Ctrl+G to follow this address:



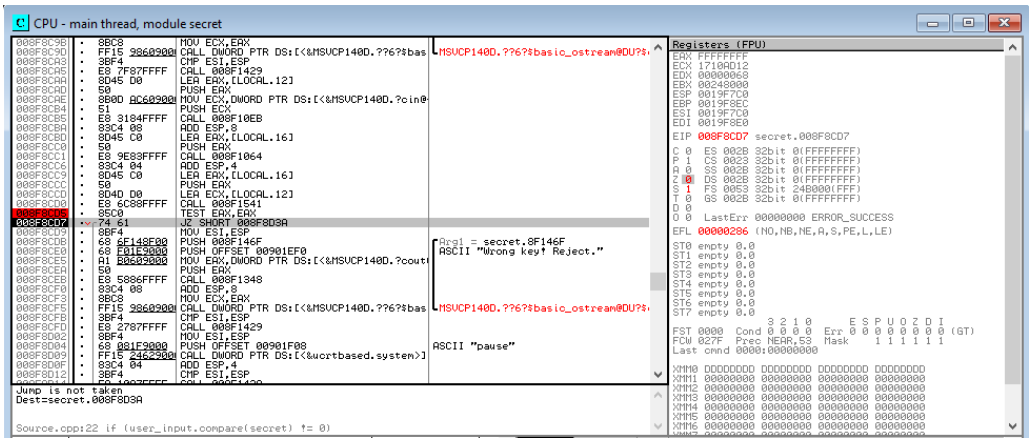
Select the address and press Shift+F3. Choose the type of memory breakpoint.

3. (Hardware) Similar to the memory breakpoint, but press Shift+F5.

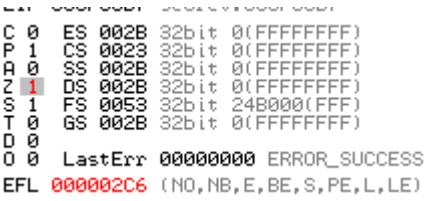
B. Register manipulation

The goal of this task is to bypass the password checking by patching the program permanently.

1. Set a breakpoint at a branch instruction. Run the program to that breakpoint.



2. Here, we demonstrate how to modify the value in *ZF* of the *EFLAG* register. Double click the '0' to the right of "Z".



3. To manipulate other registers (other than EIP), just double-click their values.