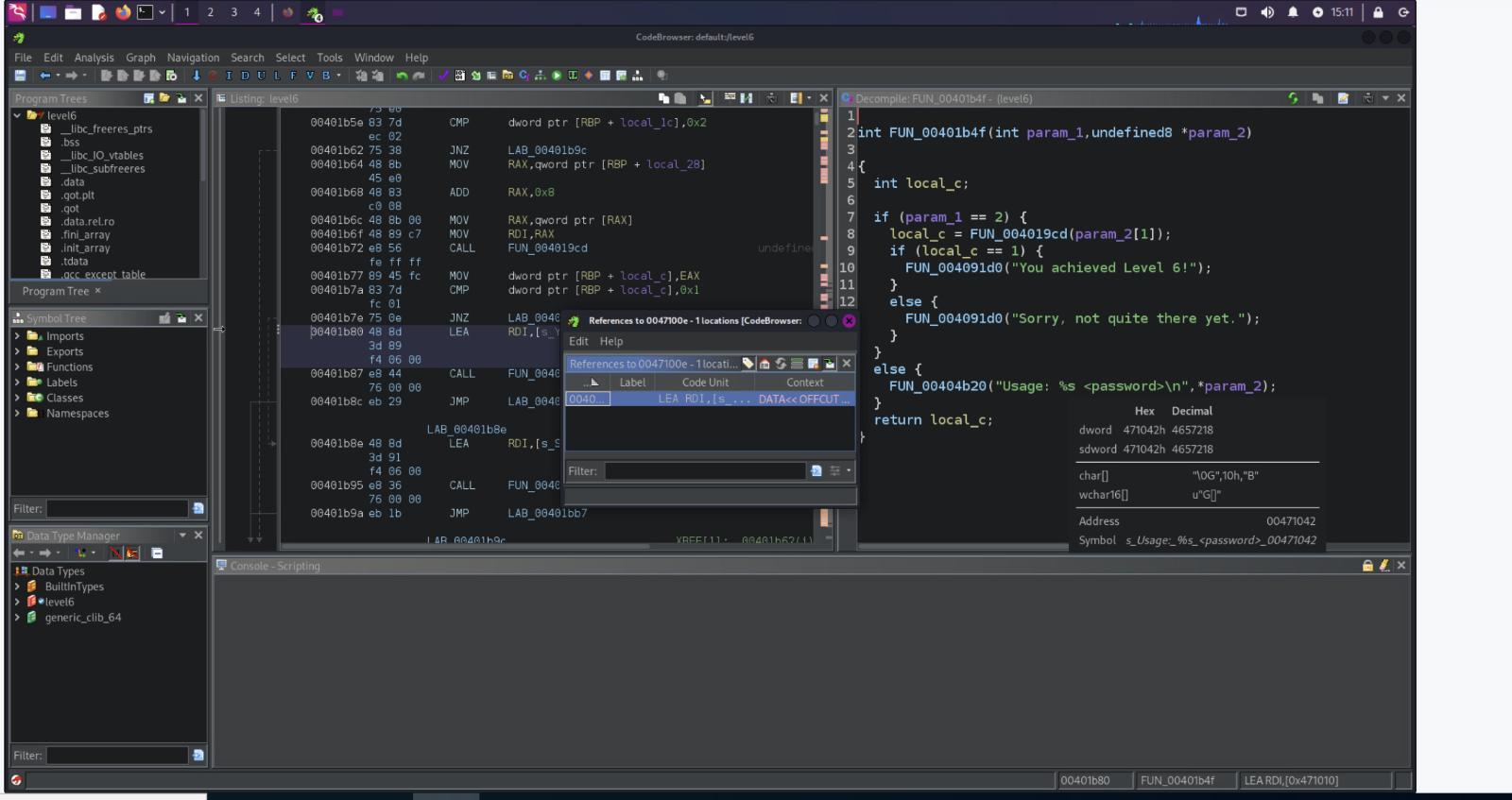
I first searched for strings and found the congrats message

A screenshot of a computer

Description automatically generated

2)And then I showed references to it, and found the “check\_password”



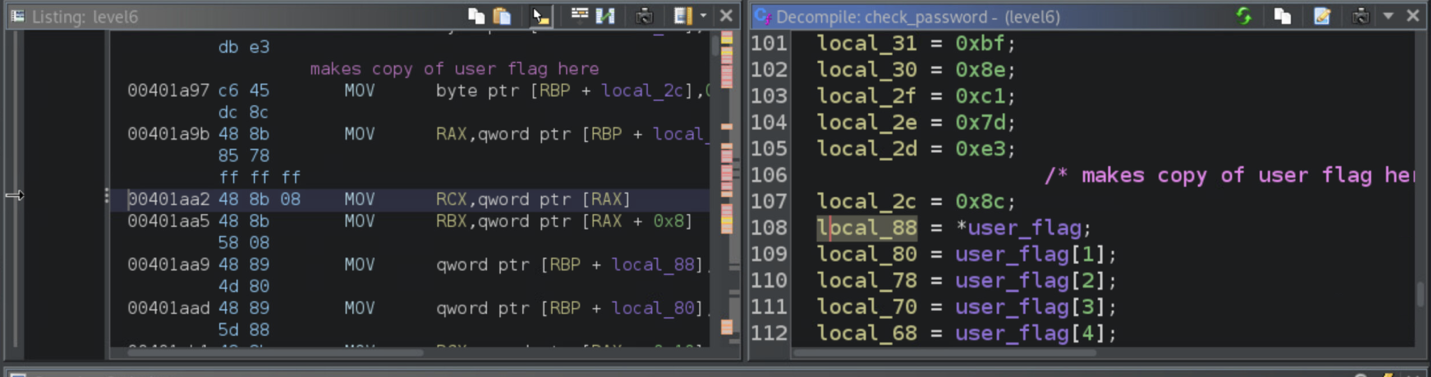
3) I did chmod +x  level6 so i could edit it and then ran gdb with a fake flag

A screenshot of a computer program

Description automatically generated

4)  I then made a breakpoint at 0x401aa2, I made a breakpoint here because that is where the memcopy takes the user\_flag and makes a copy of it, you need to have the flag in the stack before it checks it, and then I ran it

A screen shot of a computer code

Description automatically generated

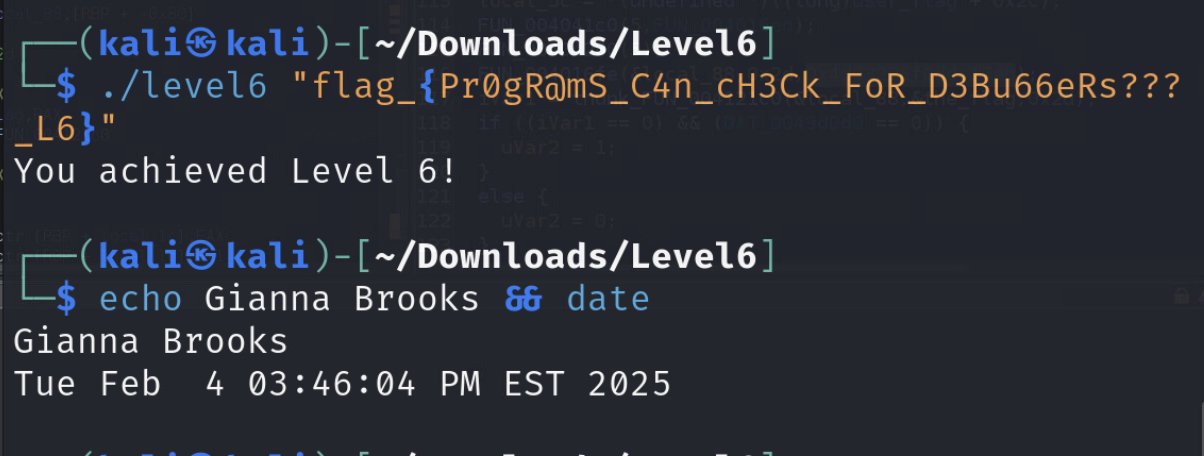
5) I then did I did the call statement for GDB using the encrypt\_decrypt and changed to –0x50 so that I can change it to the real flags decrypted value and then called the rest of the line

A computer screen with white text

Description automatically generatedA screenshot of a computer

Description automatically generated

6)



GDB Script

gdb -- args ./level6 ggb\_fake\_flag\_

b \* 0x401aa2

run

call (void\*) 0x4016fe($rbp-0x50, 0x2d, 0x4d03226f0ddc17eb)

x/s $rbp-0x50