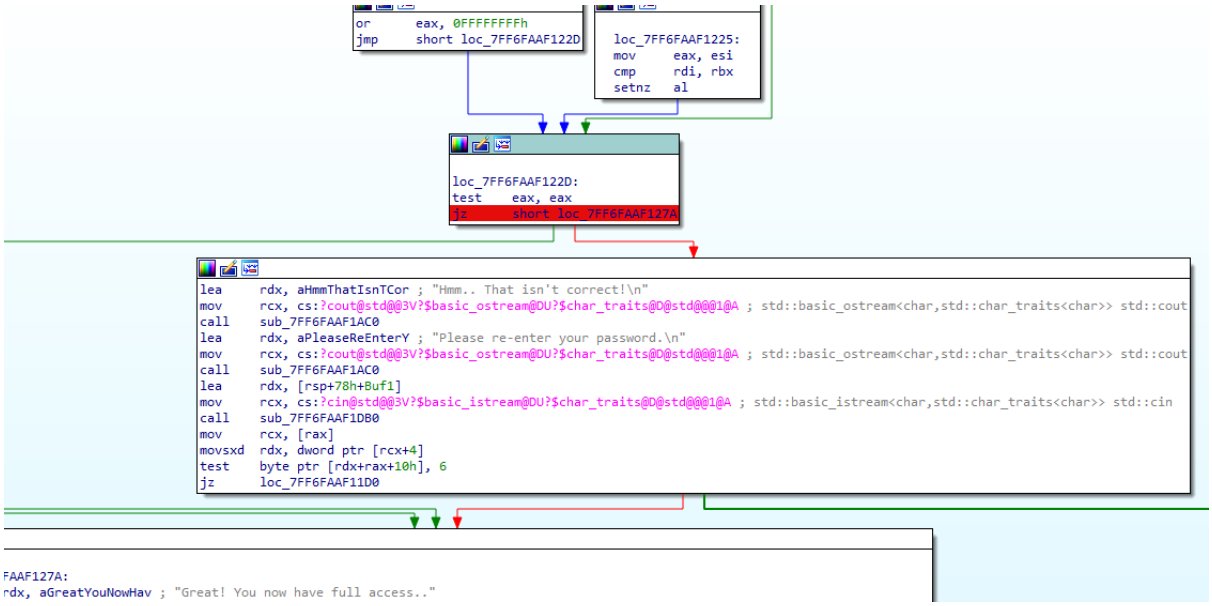
Solution to Lemacs_ez_crack_me by Giblemac

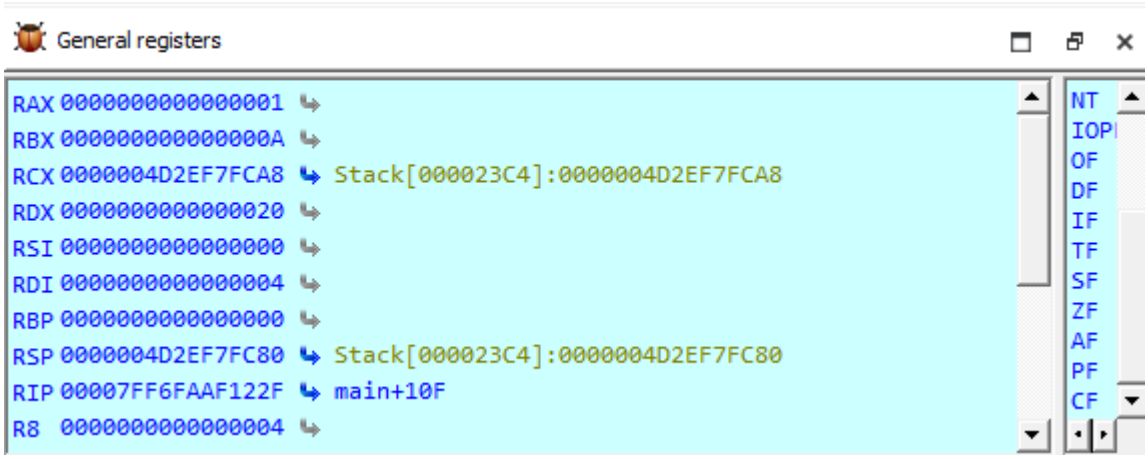
There are two ways to solve this crackme. The first way is to patch the binary, thus allowing for the message "Great! You now have full access.." to appear on the console. The second way is to find the password in the hex dump.

Method 1:

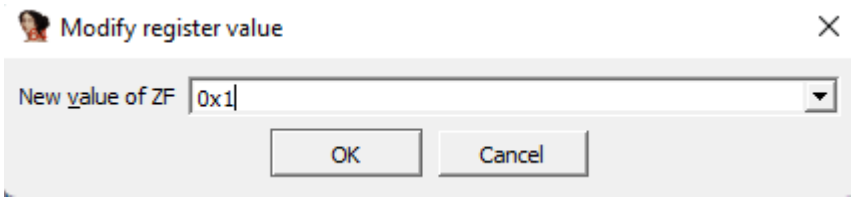
Firstly, I searched for a jump command leading to a "correct" message or to an "incorrect" message. This is when I came across this line.



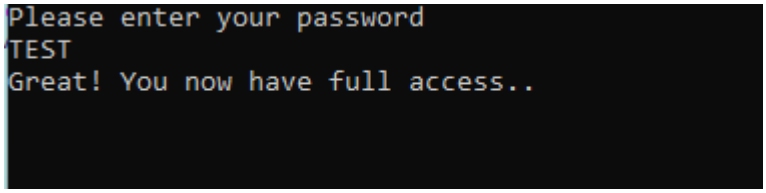
As you can see, I then added a breakpoint to this line so that I can stop the program at that point. I then ran the program as usual (I inputted “TEST”, however you can input any text you like).



Once the program had stopped, Zero Flag (ZF) had a value of 0. This means that the program would go to the incorrect branch. In order to go to the branch we want, the value of the ZF needs to be 1. You can do this by right clicking ZF and modifying the value.



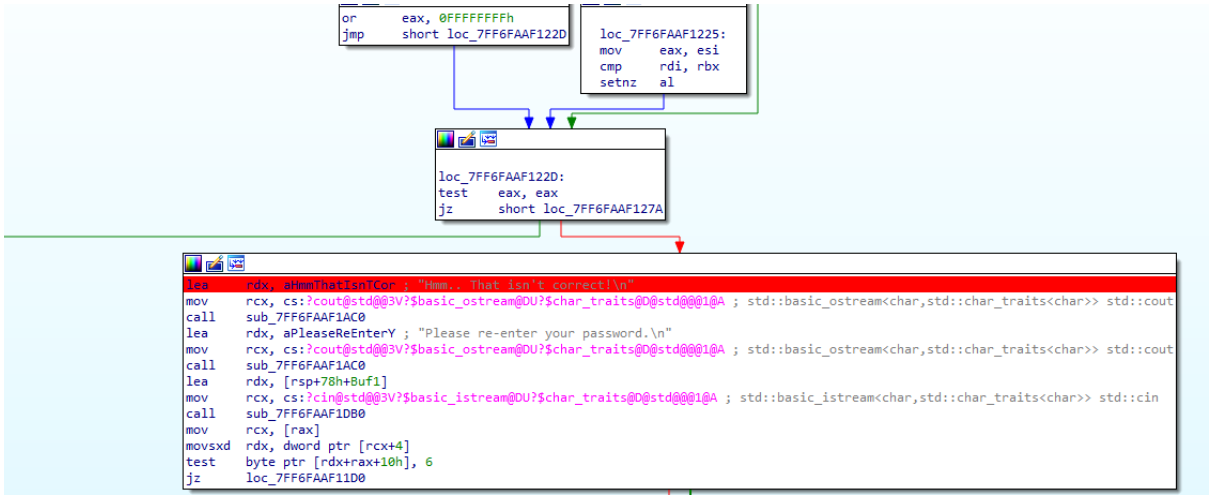
In order to modify the value, change the value from “0x0” to “0x1”.



After that, continue the program and you console should look similar to mine. If the program closes immediately when you try to continue the program, you may want to add a breakpoint at some point after the program outputs the “correct” message.

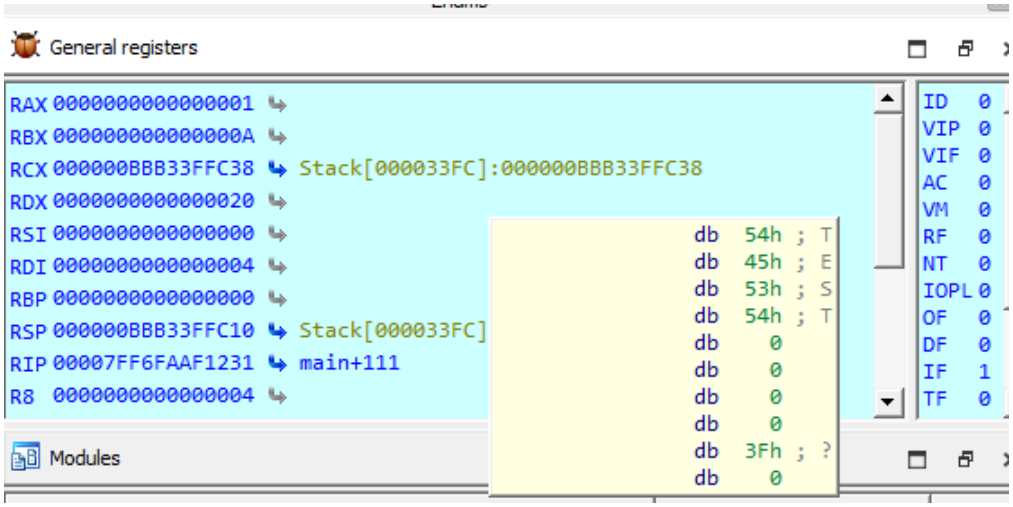
Method 2:

First, add breakpoints on locations that appear to be related to whether the password is correct. For example, I added a break point here:

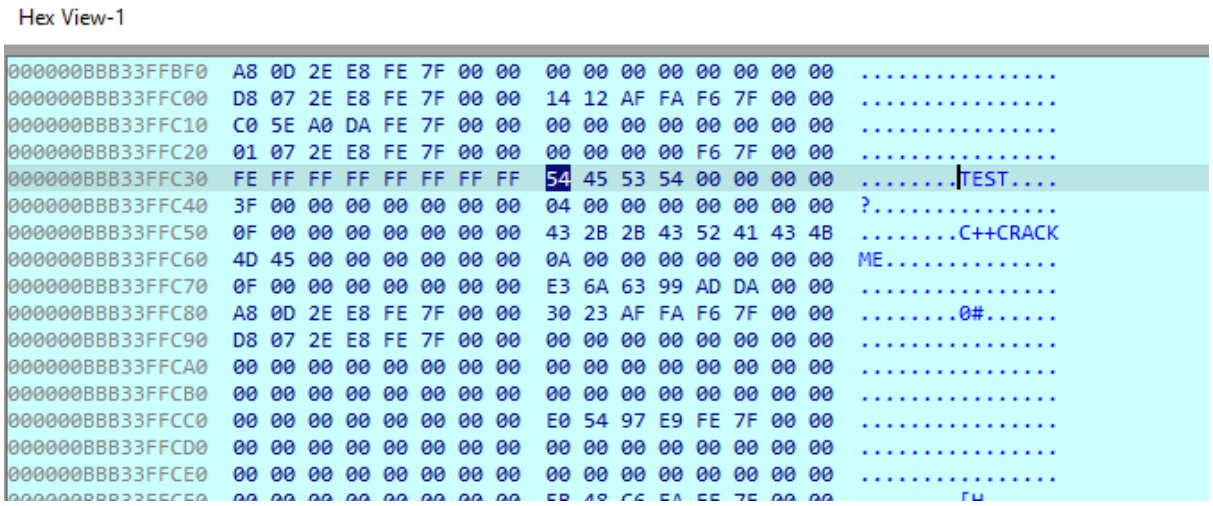


I ran the program whilst debugging and inputted text when prompted to. In this case, I added “TEST”, but you can write whatever you wish.

When the program stopped, I hovered my cursor over Stack[000033FC] and saw my input. This demonstrates that the RCX register is where my input is.



I then opened the hex dump and pressed “g” to jump to an address. I then inputted “000000BBB33FFC38” to jump to the location of “TEST” in the hex dump. This allowed me to find the password.



This shows that the password of the crackme is “C++CRACKME”.