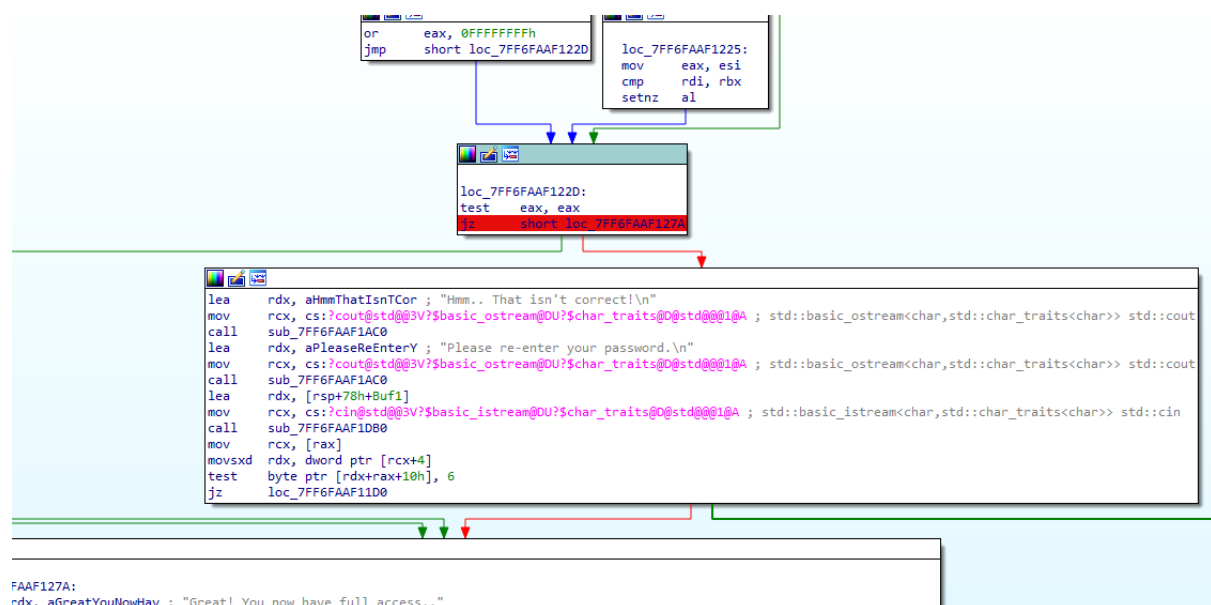


Solution to Lemacs_ez_crack_me by Giblemac

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:

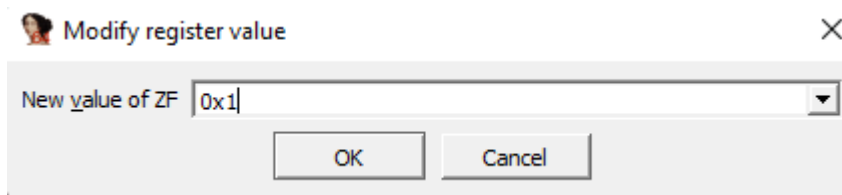
Firstly, I searched for a jump command leading to a "correct" message or to an "incorrect" message. This is when I came across this line.



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).

General registers		
RAX	0000000000000001	NT
RBX	000000000000000A	IOP
RCX	0000004D2EF7FCA8	OF
RDY	0000000000000020	DF
RSI	0000000000000000	IF
RDI	0000000000000004	TF
RBP	0000000000000000	SF
RSP	0000004D2EF7FC80	ZF
RIP	00007FF6FAAF122F	AF
R8	0000000000000004	PF
		CF

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.



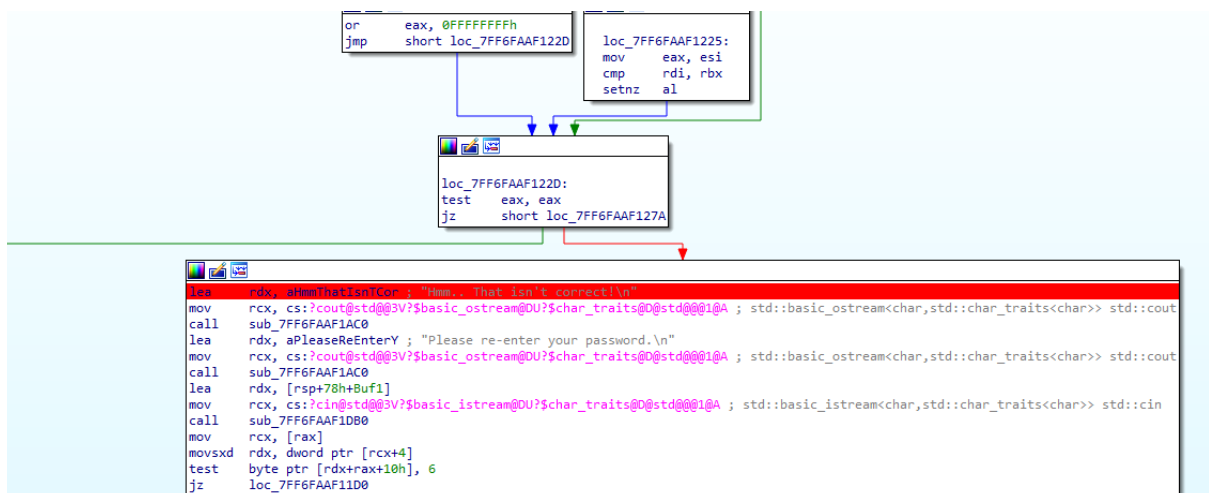
In order to modify the value, change the value from "0x0" to "0x1".

```
Please enter your password
TEST
Great! You now have full access..
```

After that, continue the program and your 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.

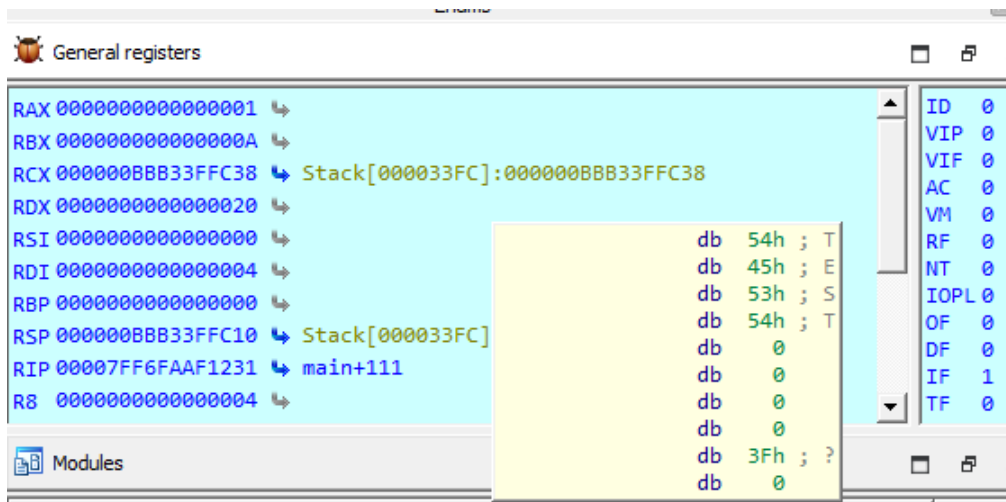
Method 2:

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

Hex View-1

000000BBB33FFBF0	A8 0D 2E E8 FE 7F 00 00	00 00 00 00 00 00 00 00
000000BBB33FFC00	D8 07 2E E8 FE 7F 00 00	14 12 AF FA F6 7F 00 00
000000BBB33FFC10	C0 5E A0 DA FE 7F 00 00	00 00 00 00 00 00 00 00
000000BBB33FFC20	01 07 2E E8 FE 7F 00 00	00 00 00 00 F6 7F 00 00
000000BBB33FFC30	FE FF FF FF FF FF FF FF	54 45 53 54 00 00 00 00TEST....
000000BBB33FFC40	3F 00 00 00 00 00 00 00	04 00 00 00 00 00 00 00	?.....
000000BBB33FFC50	0F 00 00 00 00 00 00 00	43 2B 2B 43 52 41 43 4BC++CRACK
000000BBB33FFC60	4D 45 00 00 00 00 00 00	0A 00 00 00 00 00 00 00	ME.....
000000BBB33FFC70	0F 00 00 00 00 00 00 00	E3 6A 63 99 AD DA 00 00
000000BBB33FFC80	A8 0D 2E E8 FE 7F 00 00	30 23 AF FA F6 7F 00 000#.....
000000BBB33FFC90	D8 07 2E E8 FE 7F 00 00	00 00 00 00 00 00 00 00
000000BBB33FFCA0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000BBB33FFCB0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000BBB33FFCC0	00 00 00 00 00 00 00 00	E0 54 97 E9 FE 7F 00 00
000000BBB33FFCD0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000BBB33FFCE0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000BBB33FFCF0	00 00 00 00 00 00 00 00	EB 48 C6 EA 55 75 00 00

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