1A screenshot of a computer

Description automatically generated

I clicked on check password function and I found the flag at local\_68.

2A screen shot of a computer

Description automatically generated

I walked through the functions and labeled them based off of what they do. I made sure to note where the base pointer addresses for the user copy and the flag.

3A screen shot of a computer

Description automatically generated

I want to change this line because I want to have the actual flag pass through the encrypt\_decrypt rather than the user flag copy.

4. I moved into cutter nextA screen shot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

I changed the encrypt\_decrypt line to now encrypt\_decrypt the flag instead so I changed it from leas rax, [rbp -0x30] to lea rax, [lea rax, [rbp -ox60]

5

A screenshot of a computer program

Description automatically generated

I decided to make my breakpoint here. This makes sure that loops.

A screen shot of a computer code

Description automatically generated

6

A screenshot of a computer

Description automatically generated

Next, I ran ./level8\_copy with a fake flag and let it get caught in the loop, in another terminal I ran edb and then attached level 8 to it.

7

A screenshot of a computer screen

Description automatically generated

Here is where I found the flag in the dump

8A screenshot of a computer

Description automatically generated

I copied the flag from the dump and ran it. Here is my congrats message with the flag!