**Subject Encallment**

***Reverse***

**Challenge:**

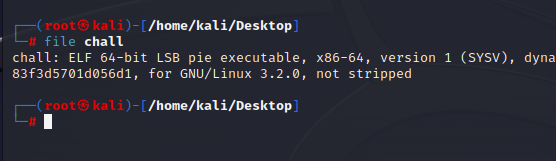
If there's something strange. In your neighborhood. Who you gonna call?

Attached - chall

**Approach:**

The ‘call’ word in the challenge itself gives a very big hint. It might refer to making a function call. Let’s check it out.

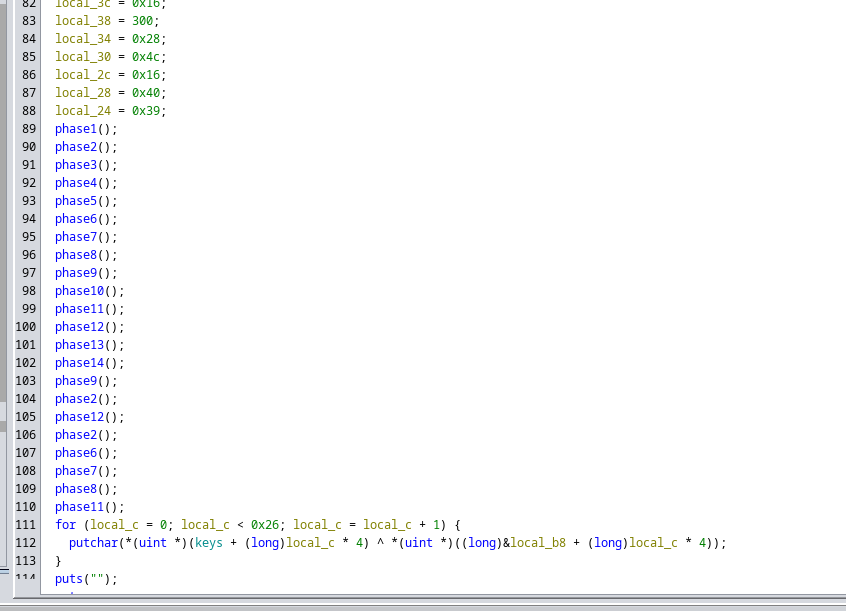
Firstly, using file command on the file tells us its an ELF executable file



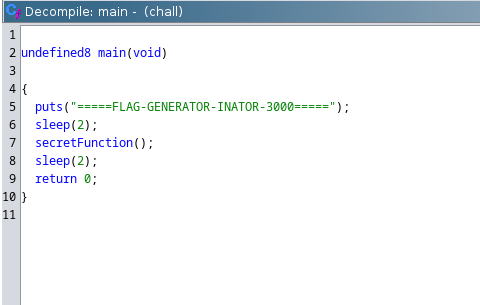
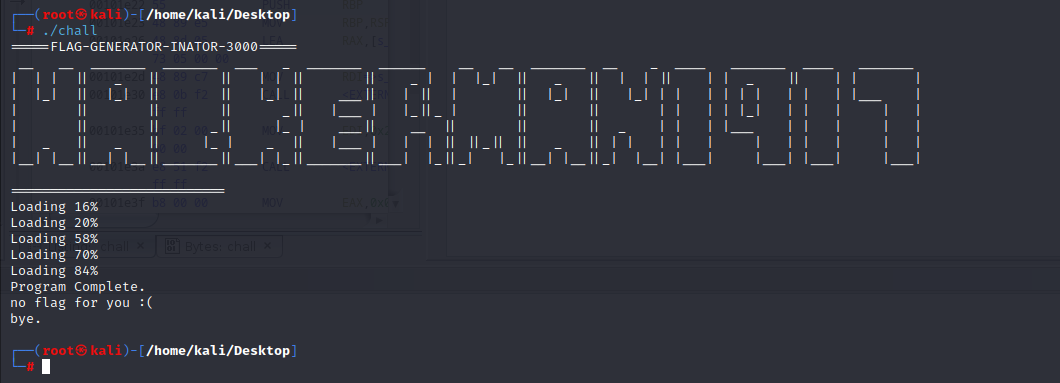
We fire up ghidra and we see the following functions:



We go through the phase 1-14 and doesn’t quite see anything important, not as important of a function that ‘printFlag’ looks like. We open up the function and well, it does make calls to all the phase functions, so we wont need it on a individual basis.

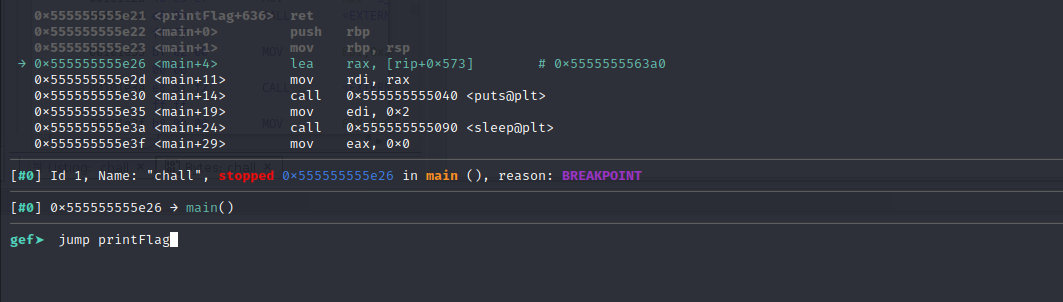


We see the main function and what it does is make a call to the ‘secretFunction’, upon checking the ‘secretFunction’ also there is no call made to the ‘printFlag’ function, which made me more curious about this function.

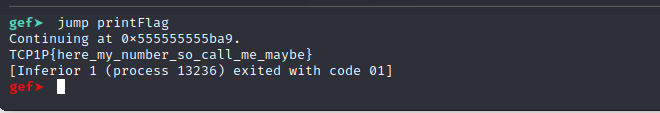


What if we jump our program to this function directly?

We open up our program on gdb (gdb chall) apply a breakpoint at main (b main) and then run the program (run)



When our program stops at the breakpoint, we use the command “jump <fcuntionName>” to jump to that particular function. In this case it’d be “jump printFlag”



…and that’s all!

**Flag: TCP1P{here\_my\_number\_so\_call\_me\_maybe}**

Congrats!!

Happy Hacking!