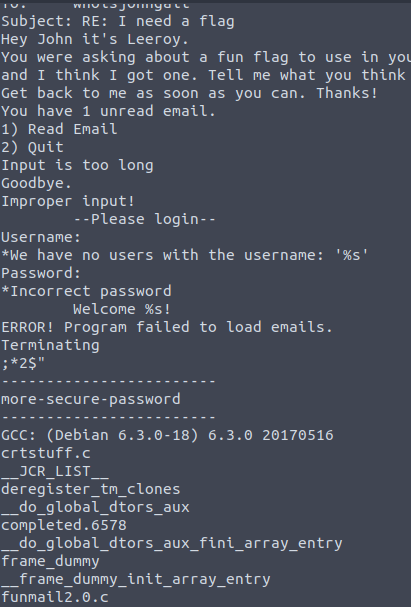
Reverse 6: Funamil 2.0

The description says:

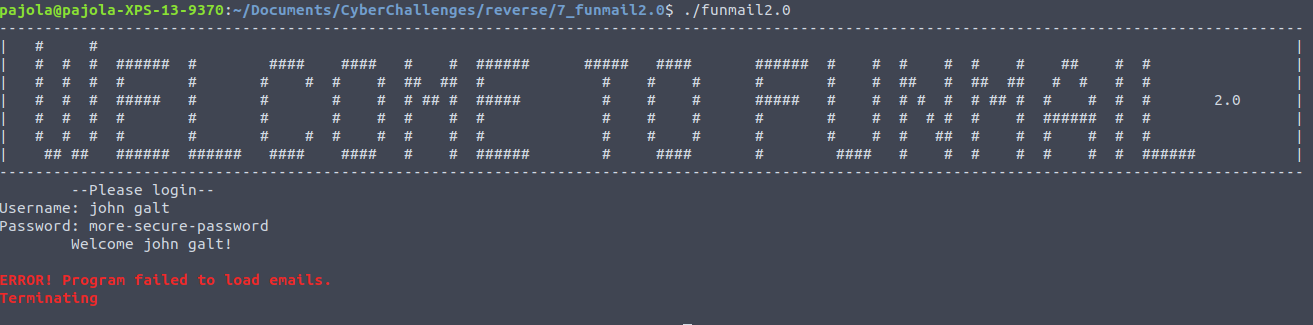
*“john galt is having some problems with his email again. But this time it's not his fault. Can you help him?”*

We know from “funmail” problem that funmail does not store password in a good manner. We can try to reach the password as we did (*strings*).



“More-secure-password” … well, it was easy.

We know username and password, let’s capture this flag.



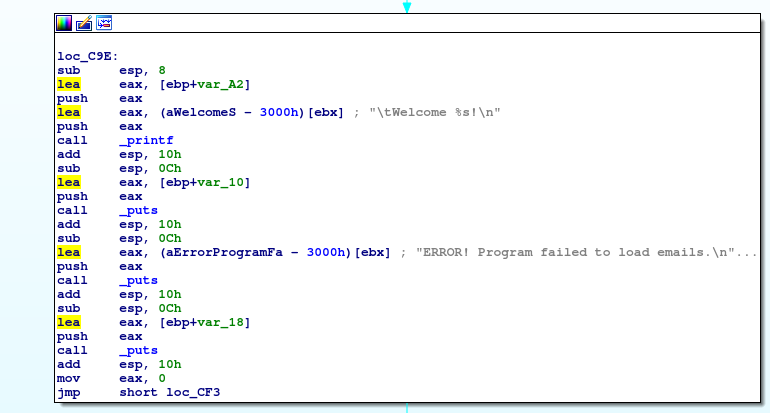
We have a message error. Mmm ….

It seems that there are some issues in the program, since we insert the correct username and password. Let’s open it with IDA.

By checking the possible directions, we see:

1. “We have no user with the username [...]”
2. “Incorrect Password”
3. “Welcome”
4. “Input is too long”

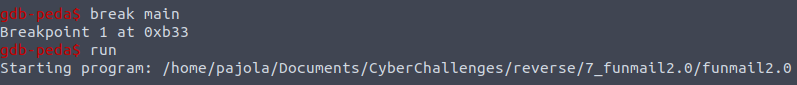
We are interested in the third point; however, as you may notice, the message error is always displayed.



The problem is that here the program never calls the *showEmails* function.

Now I’ll show you a simple approach for solving it: the debugger “gdb”.

By running gdb, we can set a breakpoint:



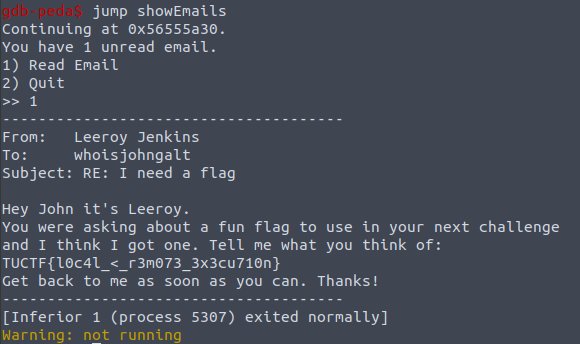
After pressing run we should see several info about the execution.

Now we can do whatever we want, for example call the *showEmails*.

We can just type the following:

Jump showEmails

Which returns the following:



The flag is captured. Of course we could have done something else, like calling directly the function printFlag.