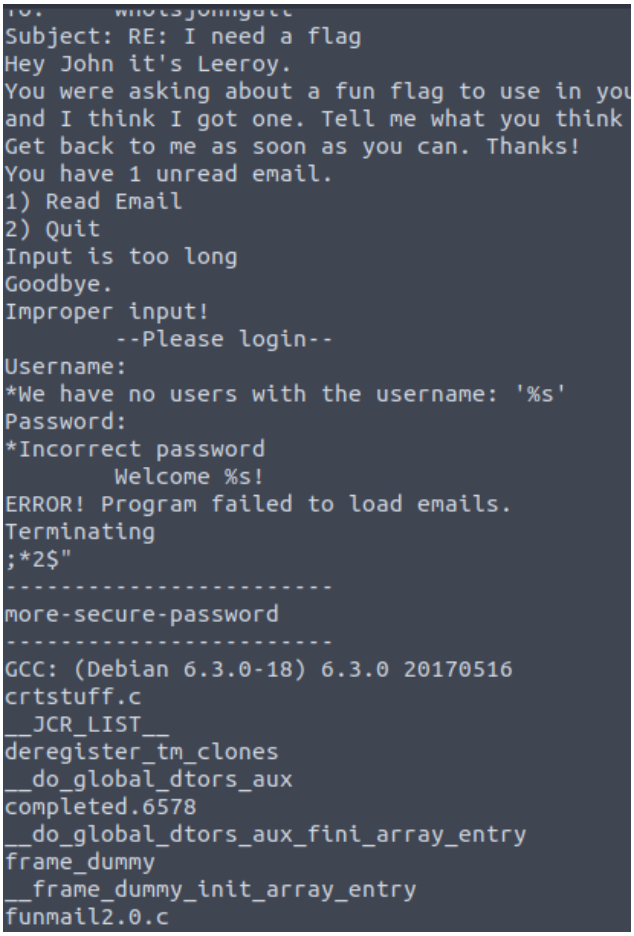
Reverse 6: Funamil 2.0

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.

```
pajola@pajola-XPS-13-9370:~/Documents/CyberChallenges/reverse/7_funmail2.0$ ./funmail2.0
-----------------------------------------------------------------------------------------------------------------------
|   #     #                                                                                                           |
|   #  #  #  ######  #       ####    ####   #    #  ######      #####   ####      ######  #    #  #    #  #    #    ##    #  #                |
|   #  #  #  #       #      #    #  #    #  #   #   #             #    #    #     #       #    #  ##   #  #   #    #  #   #  #                |
|   #  #  #  #####   #      #       #    #  ####    #####         #    #    #     #####   #    #  # #  #  ###      #    #  #                |
|   #  #  #  #       #      #       #    #  #  #    #             #    #    #     #       #    #  #  # #  #  #     ######  #                |
|   #  #  #  #       #      #    #  #    #  #   #   #             #    #    #     #       #    #  #   ##  #   #    #    #  #                |
|    ## ##   ######  ######  ####    ####   #    #  ######        #     ####      #       #    #  #    #  #    #   #    #  ######           |
-----------------------------------------------------------------------------------------------------------------------
       --Please login--
Username: john galt
Password: more-secure-password
       Welcome john galt!

ERROR! Program failed to load emails.
Terminating
```

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.

```
loc_C9E:
sub     esp, 8
lea     eax, [ebp+var_A2]
push    eax
lea     eax, (aWelcomeS - 3000h)[ebx] ; "\tWelcome %s!\n"
push    eax
call    _printf
add     esp, 10h
sub     esp, 0Ch
lea     eax, [ebp+var_10]
push    eax
call    _puts
add     esp, 10h
sub     esp, 0Ch
lea     eax, (aErrorProgramFa - 3000h)[ebx] ; "ERROR! Program failed to load emails.\n"...
push    eax
call    _puts
add     esp, 10h
sub     esp, 0Ch
lea     eax, [ebp+var_18]
push    eax
call    _puts
add     esp, 10h
mov     eax, 0
jmp     short loc_CF3
```

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:

```
gdb-peda$ break main
Breakpoint 1 at 0xb33
gdb-peda$ run
Starting program: /home/pajola/Documents/CyberChallenges/reverse/7_funmail2.0/funmail2.0
```

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:

```
gdb-peda$ jump showEmails
Continuing at 0x56555a30.
You have 1 unread email.
1) Read Email
2) Quit
>> 1
---------------------------------------
From:   Leeroy Jenkins
To:     whoisjohngalt
Subject: RE: I need a flag

Hey John it's Leeroy.
You were asking about a fun flag to use in your next challenge
and I think I got one. Tell me what you think of:
TUCTF{l0c4l_<_r3m073_3x3cu710n}
Get back to me as soon as you can. Thanks!
---------------------------------------
[Inferior 1 (process 5307) exited normally]
Warning: not running
```

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