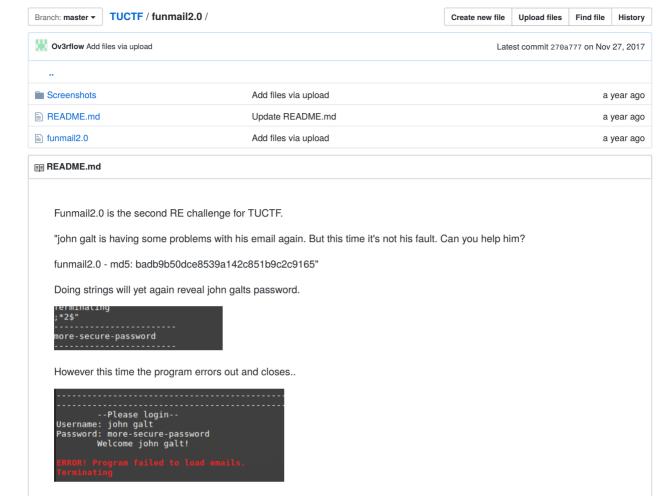
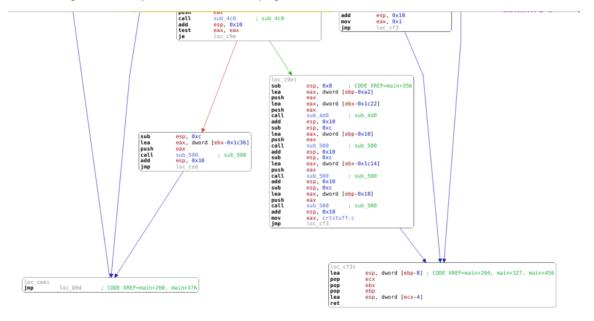
Ov3rflow / TUCTF



Investigating the main function in hopper reveals that the program isnt erroring at all. There are in fact only 2 paths it can take.

- 1. incorrect username/password try again
- 2. correct login credentials, print "error" and close the program



However hopper does show us that the functions to show and print emails do exist. The main function just has no way to call the email functions.

1 of 2 11/22/18, 11:44 AM



Knowing these details it is a simple matter to fire up GDB and find the address that the "showEmails" function is loaded into.

Then we can simply change EIP to point to that function and let the program run to receive our flag!

```
(gdb) set $eip = 0x56555a2c
(gdb) c
Continuing.
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!</pre>
```

2 of 2 11/22/18, 11:44 AM