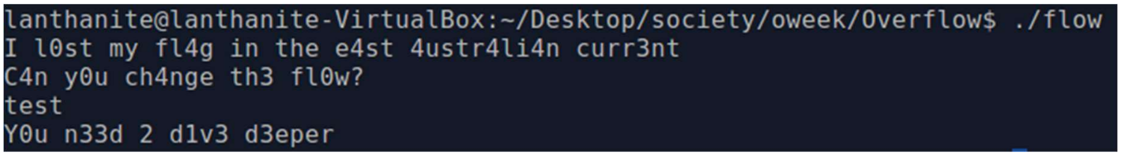
Flow (50 pts)

We're given a binary called *flow*. When we run it, it requests input, and then exits.

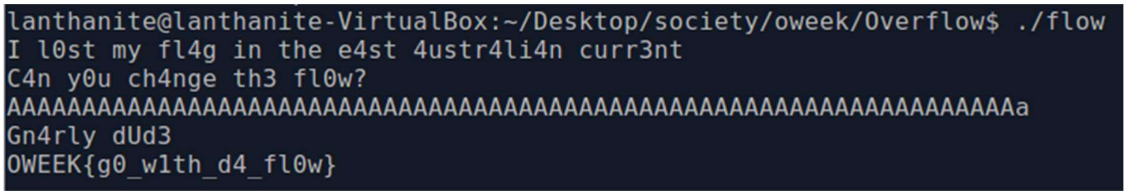


```
lanthanite@lanthanite-VirtualBox:~/Desktop/society/oweek/Overflow$ ./flow
I l0st my fl4g in the e4st 4ustr4li4n curr3nt
C4n y0u ch4nge th3 fl0w?
test
Y0u n33d 2 d1v3 d3eper
```

This challenge relates to a class of challenges called *buffer overflow* vulnerabilities. Specifically, this challenge is a stack-based buffer overflow. For a great explanation, check out LiveOverflow's video here https://www.youtube.com/watch?v=T03idxny9jE. This challenge is functionally identical to the one he solves there – overflowing a stack-based buffer to overwrite a variable value.

In general, it's always a good idea to check for buffer overflow vulnerabilities when doing binary exploitation challenges. How do you do this, you might ask?

Brute force, my friend.



```
lanthanite@lanthanite-VirtualBox:~/Desktop/society/oweek/Overflow$ ./flow
I l0st my fl4g in the e4st 4ustr4li4n curr3nt
C4n y0u ch4nge th3 fl0w?
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAa
Gn4rly dUd3
OWEEK{g0_w1th_d4_fl0w}
```