Collin Gros
04/01/2020

BUFFER OVERFLOW REPORT

The rsp points to the stack, the rbp points to the stack frame, and the rip points to the current instruction. The stack frame is generated from function calls.

When a function is called, the return address is immediately pushed onto the stack. We can jump to wherever we want in the code by overwriting a buffer all the way up to the address of that return address. Then, when the function is finished, the code returns to wherever you would like, in this case - directly to the 'success' function's address.

I used:
'break "function name"'
'x/x $rbp+8'
'x/x $rbp+4'
'x/x $rbp'

I wasn't able to finish the assignment, as I struggled with gdb commands for far too long.

Checking the bounds of a given input will prevent this whole issue from occuring in the first place.