What if the buffer is overstuffed?

- ➡ `strcpy` does not check whether the string at `*str` contains fewer than 126 characters

- ◉ If a string longer than 126 bytes is copied into buffer, it will overwrite adjacent stack locations

0x FF FF FF FF

0x 00 00 00 00

0x FF FF FF FF

Args

Return Address

Base Pointer

buf

Overflow

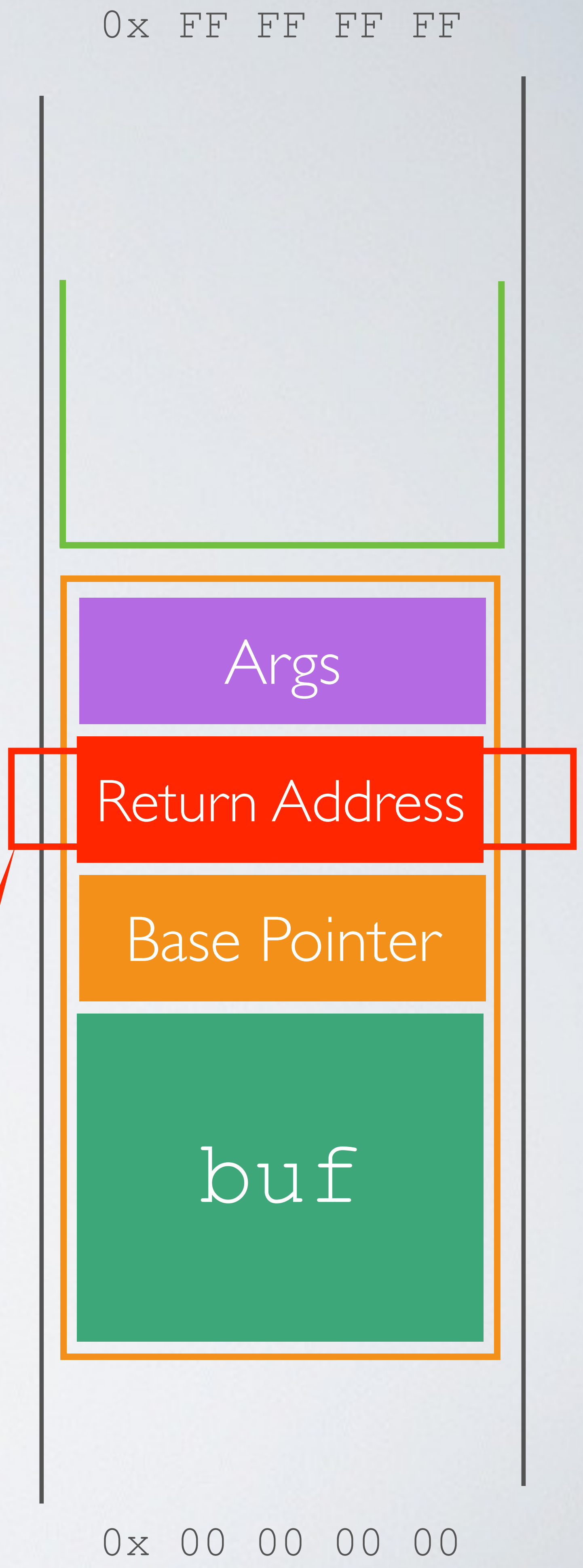
This buffer data will be interpreted as the **return address** (most likely terminating the program with "*Segmentation Fault*")

What if the buffer is overstuffed?

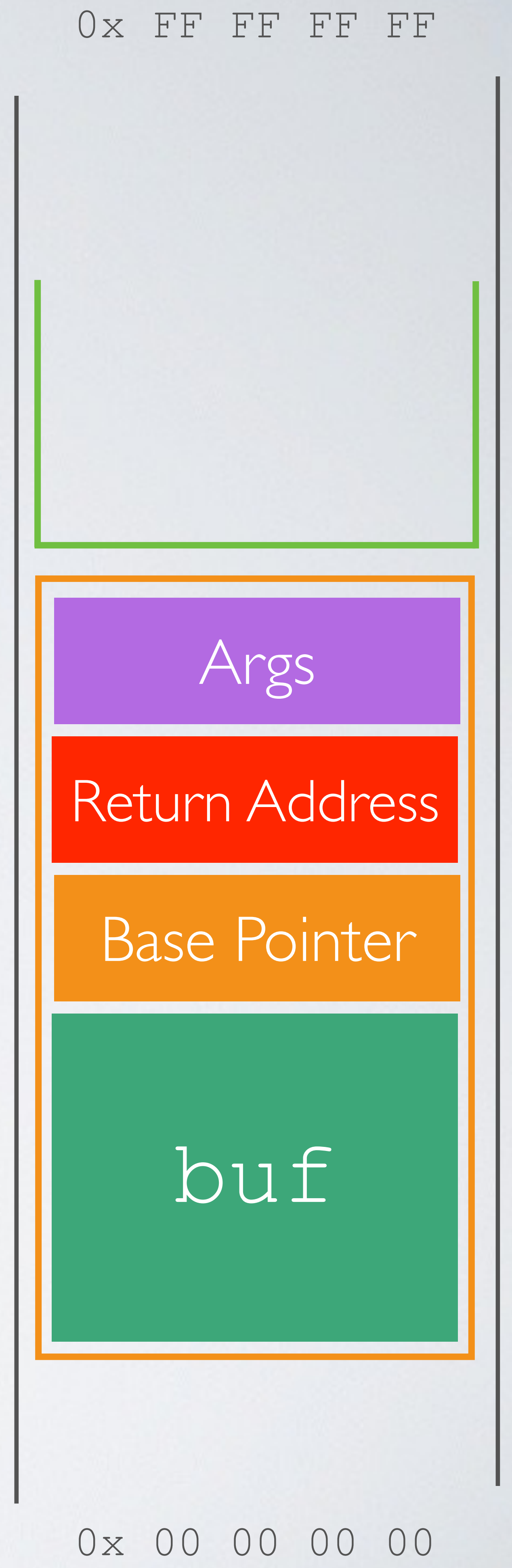
- `strcpy` does not check whether the string at `*str` contains fewer than 126 characters

- If a string longer than 126 bytes is copied into buffer, it will overwrite adjacent stack locations

This buffer data will be interpreted as the **return address** (most likely terminating the program with "*Segmentation Fault*")



Injecting Code


0x FF FF FF FF
Args
Return Address
Base Pointer
buf
0x 00 00 00 00