



stackexchange

Allocate local buffer  
(126 bytes in the stack)

A dark gray speech bubble with rounded corners and a pointed tail at the bottom center. The bubble contains white text. The tail points downwards towards the bottom center of the image.



Copy argument into local buffer

```
void foo(char *str) {  
    char buf[126];  
    strcpy(buf, str);  
}
```

02 EEE EEE EEE EEE



OXFORD



Stack

grows down



















10 of 10

# Args

Return Address

# Base Pointer

buf

# Stack execution

```
void foo(char *str) {  
    char buf[126];  
    strcpy(buf, str);  
}
```

Copy argument into local buffer

Caller Frame

foo Frame

Stack  
grows down

0x FF FF FF FF

Args

Return Address

Base Pointer

buf

0x 00 00 00 00

0x FF FF FF FF

# 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

