ICS Homework 11

Buffer Overflow

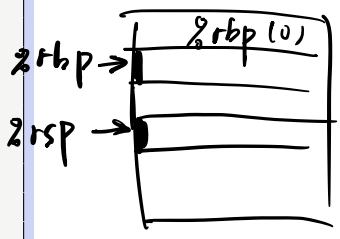
The following C code and assembly code are executed on a **64-bit little-endian** machine. It uses **gets()** function in section 3.10.3 on CSAPP.

```c
void buggy() {
    char buf[0x10];
    gets(buf);
}

int main(){
    buggy();
    return 0;
}
```

```
00000000004004e6 <buggy>:
4004e6: 55                    push   %rbp
4004e7: 48 89 e5              mov    %rsp,%rbp
4004ea: 48 83 ec 10           sub    $0x10,%rsp
4004ee: 48 8d 45 f0           lea    -0x10(%rbp),%rax
4004f2: 48 89 c7              mov    %rax,%rdi
4004f5: e8 17 00 00 00        callq  400511 <gets>
4004fa: c9                    leaveq
4004fb: c3                    retq

00000000004004fc <main>:
4004fc: 55                    push   %rbp
4004fd: 48 89 e5              mov    %rsp,%rbp
400500: b8 00 00 00 00        mov    $0x0,%eax
400505: e8 dc ff ff ff        callq  4004e6 <buggy>
40050a: b8 00 00 00 00        mov    $0x0,%eax
40050f: 5d                    pop    %rbp
400510: c3                    retq
```



Given the following input strings, what's the corresponding address that the function **buggy**() will return to? (**NOTE**: the ASCII number of '0' is 0x30.)

- ""
- "0123456789"
- "01234567890123456789"

0x400509

0x400509

0x400509

-20 → 10

- "012345678901234567890123"
- "0123456789012345678901234567890123456789"