Name: UID:

1. What do I need to do if I want to access a function through buffer overflow (what needs to be done to the stack)? The function's address is 0x500142.

The function Gets is similar to the standard library function gets—it reads a string from standard input (terminated by '\n' or end-of-file) and stores it (along with a null terminator) at the specified destination (such as a char array previously declared). Functions Gets() and gets() have no way to determine whether their destination buffers are large enough to store the string they read.

```
Dump of assembler code for function getbuf:
=> 0x0000000000601748 <+0>:     push   %rax
   0x000000000060174c <+4>:     sub    $0x40,%rsp
   0x000000000060174f <+7>:     mov    %rsp,%rdi
   0x0000000000601754 <+12>:    callq  0x40198a <Gets>
   0x0000000000601759 <+17>:    add    $0x40,%rsp
   0x000000000060175d <+21>:    pop    %rax
   0x000000000060175f <+23>:    retq
```

What do I need to do if I want some instructions to be executed before the function is accessed? (Assume the value of %rsp right before getbuf is called is 0xabcd0000)

2. What are some optimizations that can be made to the following function?

```
void cs33fun(char* Midterm, char* Grade, int* Final, int n) {

      for (int i = 0; i < (strlen(Midterm)); i++) {
            strcat(Grade, Midterm);

            for (int j = 0; j < n; j++)
                  for (int k = 0; k < i; k++)
                        Final[j] += strlen(Grade);
      }
}
```