

CSCI 3330: Format String Exploits by Hand

Consider the following code:

```
unsigned int rng_state = 0x12345678; /* at address 0x0804A02C */

void welcome_user(void) {
    char buf[256];
    printf("What is your name?\n");
    fgets(buf, sizeof(buf), stdin);
    printf("Welcome ");
    printf(buf);
}
```

Now complete the following challenges:

1. Construct a format string that writes the value 0xdeadbeef to the variable `rng_state`. Assume that the machine is 32-bit x86 and that `buf` is located 20 32-bit words above `%ebp+8` at the time that the format string exploit is evaluated in `printf()`.
2. Replace the last two `printf()` calls with a single `printf()` call that prints the welcome message as intended without a vulnerability, i.e., that prints "Welcome [user input]".