

# CIS 751 Lecture Assignment 5

Chuck Zumbaugh

October 8, 2025

Let's assume we have a stack that looks something like the below:

Lower Addresses
EBP
EIP
Format string address
<i>addr</i>
Rest of input
Higher addresses

And also we have a program with the following:

```
int i = 0; // Some variable used in printf()
printf(input, &i); // Input is some user created data
```

We could then overwrite *i*, say with 11, using the string "**Hello world%n**". However, we can also overwrite arbitrary stack locations provided we know the address we want to write to. When `printf()` encounters a format specifier it will call `va_arg()` and return the argument pointed to by `va_list`. Thus, we can specify an address to write to, and a number of format specifiers to move the `va_list` pointer to the address we want to write to. Thus, we would need to move the pointer from somewhere in *Rest of input* to *addr* using input specifiers. Then, when `%n` is encountered, it will write the number of bytes in `printf()` to that address.