You have a function call and arguments

When you call printf in c, you are supposed to have format string be

Name = “Nick”;

Printf(“Hi I’m %s”, name);

Will take name off the stack as a string, put in standard out

Format string attacks work when you call variable directly, for example

Printf(x)

Then now you control that function, so if you make it equal to a bunch of %x’s, it will say ok I need to grab that many values off the stack as hex values, then just print memory off the stack.

When you want to own something using a format string, you can use %c that allows you to print that number of characters to the terminal. You can say print %200c to print 200 characters to terminal. %n puts a pointer on stack.

%37$s will print 37 things down the stack as well, can be any number

Now you can control what libc function calls it makes, say exit is a certain value, you can change memory address to be main, and it will just keep running main instead of exiting.