Format String

格式化字符串漏洞

printf这种可变数量参数的函数，将第一个参数作为格式化字符串，根据第一个参数来解析后面的参数。

printf(”%d%4.2f%s”, 100, 1.1, “hello”);

如果第一个参数可以被用户控制，并且不做限制那么就有可能会出现问题，攻击者可以精心构造格式化字符串，完成任意地址读或任意地址写的攻击原语。

一些常用的格式化字符串pattern

%p，以地址形式打印参数值

%s，以字符串形式打印参数指针指向内存

%n$，获取指定位置参数

hh，输出一个字节

h，输出一个双字节

%n，不输出字符，将已经成功输出的字符个数写入对应的整型指针参数所指的变量。