# 格式化字符串漏洞

printf在进行格式化输出时，会根据格式化串中的格式化控制符在栈上取相应参数，按照所需格式进行输出

# 格式化字符串

格式：%[标志][输出最小宽度][.精度][长度][格式字符]

## 标志

- - 结果左对齐，右边填空格
- + 输出符号
- 空格 输出值为正时填入空格，为负值时冠以符号

## 输出最小宽度

用十进制整数来表示输出的最少位数（包括小数点在内）

若实际位数多于定义的宽度，则按实际位数输出；若实际位数少于定义的宽度，则右对齐，左边留空；有负号，则左对齐，右边留空；表示宽度的数字以0开始，则右对齐，左边留空；

## 精度

精度格式符以“.”开头；

若输出为数字，若实际位数大于定义精度，则四舍五入；若不足，则补0；

若输出为字符，若实际位数大于定义精度，则截去超过的部分。

## 长度

长度格式符为h和l两种，h表示按短整型量输出，l表示按长整型输出

## 格式化输出字符

| | |
|---|---|
| %d | 整数的参数会被转成有符号的十进制数字 |
| %u | 整数的参数会被转成无符号的十进制数字 |
| %o | 整数的参数会被转成无符号的八进制数字 |

| | |
|---|---|
| %x | 整数的参数会被转成无符号的十六进制数字，并以小写abcdef 表示 |
| %X | 整数的参数会被转成无符号的十六进制数字，并以大写ABCDEF 表示浮点型数 |
| %f | double 型的参数会被转成十进制数字，并取到小数点以下六位，四舍五入 |
| %e | double 型的参数以指数形式打印，有一个数字会在小数点前，六位数字在小数点后，而在指数部分会以小写的e 来表示 |
| %E | 与%e 作用相同，唯一区别是指数部分将以大写的E 来表示 |
| %g | double 型的参数会自动选择以%f 或%e 的格式来打印，其标准是根据打印的数值及所设置的有效位数来决定。 |
| %G | 与%g 作用相同，唯一区别在以指数形态打印时会选择%E 格式。 |
| %c | 整型数的参数会被转成unsigned char 型打印出 |
| %s | 指向字符串的参数会被逐字输出，直到出现NULL 字符为止 |
| %p | 如果是参数是"void *"型指针则使用十六进制格式显示 |