格式化字符串漏洞
Format String Vulnerability

CWE: https://www.cvedetails.com/cwe-details/134/Uncontrolled-Format-String.html
安全客的相关介绍：https://www.anquanke.com/post/id/85785
GitHub: https://github.com/CTF-Thanos/ctf-writeups/tree/master/2016/CCTF/pwn/pwn3

IDA 软件：https://www.hex-rays.com/

> *IDA is the **I**nteractive **D**is**A**ssembler: the world's smartest and most feature-full disassembler, which many software security specialists are familiar with.*

通过控制输入（写入数据）以修改控制流。那么在哪里寻找输入呢？答案是**数据区**。

测试用例

`from pwn import *` ➡️ `pip install pwn` ➡️ `unicorn 装不上`

安装 Unicorn 中遇到一点问题
Unicorn 的 GitHub 地址：https://github.com/unicorn-engine/unicorn
掘金博客：https://juejin.im/post/5cb69b9951882532a42c0e46

```
ERROR: pthread check failed
         Make sure to have the pthread libs and headers installed.

   make: *** [qemu/config-host.h-timestamp] Error 1
   error: [Errno 2] No such file or directory: 'libunicorn.dylib'
```