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>

**CSDN:** <https://blog.csdn.net/qq_43394612/article/details/84900668>

**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'

n The number of characters written so far is stored into the integer indicated by the int \* (or variant) pointer argument. No argument is converted. The format argument must be in write-protected memory if this specifier is used; see SECURITY CONSIDERATIONS below.

**关闭Ubuntu的随机地址**

$ sudo echo 0 > /proc/sys/kernel/randomize\_va\_space

**栈帧**：https://juejin.im/post/5b1560afe51d4506a74d2aeb