[pwn]collision_writeup_pwnable.kr

转载

weixin_30322405 于 2017-05-14 01:46:00 发布 36 收藏
文章标签： python
原文链接：http://www.cnblogs.com/rfhs/p/6852896.html

collision题目如上，连接后有：

源码如下：

程序将输入的char指针强转为int指针，将目标地址的5个int型数据累加后语hashcode做对比，对比结果正确即可得到flag。

20个char型的大小恰好与5个int型的大小相等，要求的输入长度也恰好是20位的字符串，所以即是将输入的20位字符划为5组后累加。

然后将hashcode拆成5组输入即可：

./col `python -c "print '\xc8\xce\xc5\x06' * 4 + '\xcc\xce\xc5\x06"'`

得到flag。

点：

1:不同类型指针的强转：就是指针的值（所指向地址）不变，目标解释结果（char型指针将每个字节的内容解释为一个char，int型指针将每四个字节的内容解释为一个int）改变。

2:不可见字符的打印：此题浪费时间最多的部分。对于不可见字符的输入，采用`python -c `的方法，交互输入到bash中，此处原理不懂，去看python手册。

3:大小端序：x86采用小端序，即输入‘abcd’时，在内存中由低地址（上）到高地址（下）每个字节所存储的内容分别是：0x64,0x63,0x62,0x61。在构造输入时，要按照内存存储的顺序逐字节的输入。

转载于:https://www.cnblogs.com/rfhs/p/6852896.html