

# pwnable.kr-bof-Writeup

转载

p9bl5byp 于 2017-02-10 10:55:37 发布 948 收藏  
MarkdownPad Document

## pwnable.kr-bof-Writeup

在<http://pwnable.kr/bin/bof.c>得到C代码如下：

```
1 #include <stdio.h>
2 #include <string.h>
3 #include <stdlib.h>
4 void func(int key){
5     char overflowme[32];
6     printf("overflow me : ");
7     gets(overflowme);    // smash me!
8     if(key == 0xcafebabe){
9         system("/bin/sh");
10    }
11    else{
12        printf("Nah..\n");
13    }
14 }
15 int main(int argc, char* argv[]){
16     func(0xdeadbeef);
17     return 0;
18 }
```

在<http://pwnable.kr/bin/bof>下载文件bof，die查壳如下，无壳，为elf文件。

由题目中的提示 *Nana told me that buffer overflow is one of the most common software vulnerability. Is that true?* 可知此题的漏洞为缓冲区溢出，分析C代码：

- 直接把bof拖到IDA中，通过查找关键字字符串跳转到关键函数func。
- 双击a1与s查看地址如下，则二者的地址相差  $+0x00000008 - (-0x0000002C) = 0x34 = 52$

□

- 因为 **0xCAFEBABE**（即IDA中的-889275714）为小端存储，则可以在get(&s)处可构造输入 **'0'\*52+0xBE0xBA0xFE0xCA**，在Linux中检验，可以得到flag为：**daddy, I just pwned a buFFer**。□

构造输入时需要注意用 **cat** - 关闭栈保护；

2017-2-7 19:52:05