pwnable.kr-flag-Writeup

转载

baikeng3674 于 2017-02-07 20:57:00 发布 69 收藏
原文链接：http://www.cnblogs.com/WangAoBo/p/6375901.html

MarkdownPad Document

pwnable.kr-flag-Writeup

- 根据题目提示：*This is reversing task. all you need is binary*，可知此题实际上应归为reverse；
- DIE查壳，发现为upx加壳，直接使用upx工具脱壳。
- Linux下运行该文件，发现关键字符串。
- IDA中***shift+F12***找到关键字符串，并双击关键字符串跳转到对应的函数，得到伪代码如下：

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3   __int64 v3; // rax@1
4
5   puts("I will malloc() and strcpy the flag there. take it.", argv, envp);
6   LODWORD(v3) = malloc(100LL);
7   sub_400320(v3, flag);
8   return 0;
9 }
```

- 由提示***I will malloc() and strcpy the flag there. take it.***以及代码的流程，直接查看flag，得到字符串：***UPX...? sounds like a delivery service :),提交检验正确，则flag即为 UPX...? sounds like a delivery service :)***。事实上，**shift+F12**查找关键字符串时已经出现了flag 2017-2-7 20:54;45