# flag_WriteUp(pwnable.kr_flag)软件脱壳反汇编

原创

Hvnt3r 于 2018-07-16 08:56:49 发布 208 收藏

分类专栏： PWN



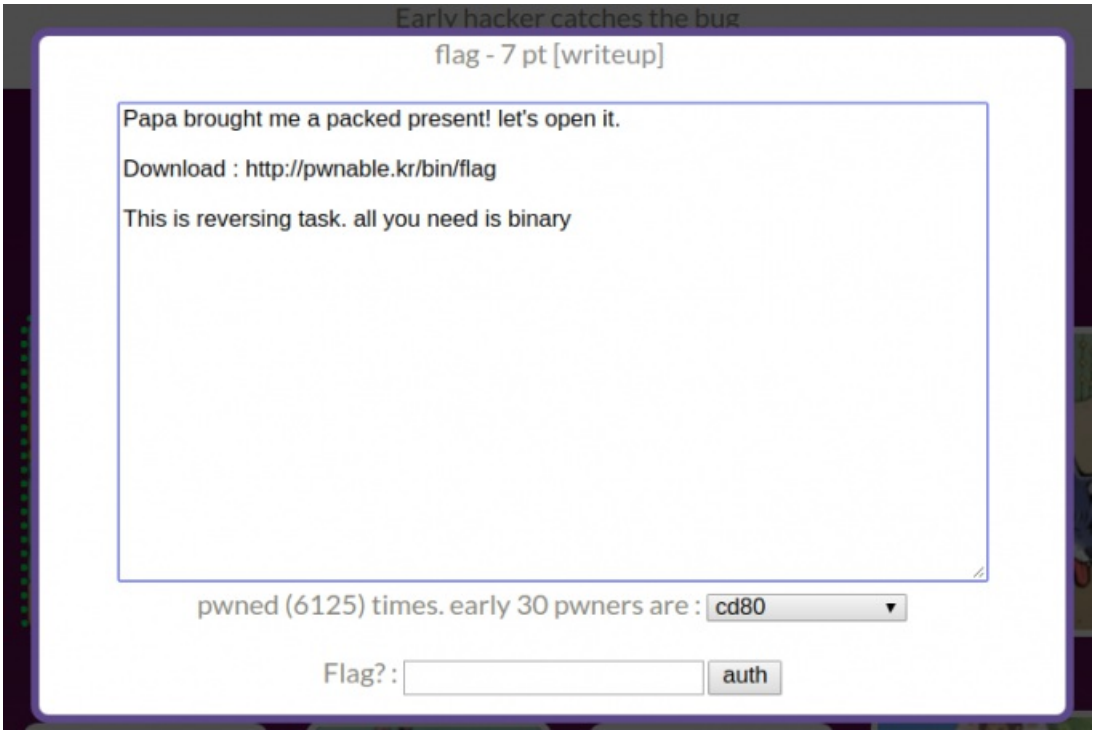
本文链接：https://blog.csdn.net/levones/article/details/81059501





## flag_WriteUp(pwnable.kr_flag)软件脱壳反汇编

题目传送门：http://pwnable.kr/bin/flag




这道题严格意义上考察的是软件查壳和脱壳

根据题目hint：

```
Papa brought me a packed present! let's open it.

Download : http://pwnable.kr/bin/flag

This is reversing task. all you need is binary
```

题目提示我们需要二进制文件，但是他给的文件的不是二进制文件吗

用xdd命令查看flag的16进制数据：

```
root@kali-linux:~/文档/PWN/pwnable.kr/4.flag# xxd flag
...
$.....UPX!
00051d90: 0000 0000 5550 5821 0d16 0807 19cc 204a  ....UPX!...... J
00051da0: dbd8 21c5 3145 0100 5e70 0000 217c 0d00  ..!.1E..^p..!|..
00051db0: 4919 0089 bc00 0000                      I.......
```

看到文件是upx的壳

使用`upx -d flag`命令来去壳

去壳后把文件丢到ida里就可以看到flag了

```
UPX...? sounds like a delivery service :)
```