

# Jarvis oj 文件数据修复 writeup

原创

charlie\_heng 于 2017-11-25 20:40:46 发布 308 收藏

分类专栏: [二进制-逆向工程](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/charlie\\_heng/article/details/78634051](https://blog.csdn.net/charlie_heng/article/details/78634051)

版权



[二进制-逆向工程](#) 专栏收录该内容

34 篇文章 3 订阅

订阅专栏

感觉这题把逆向玩成了misc。。。。

首先用mfc工具找到处理解密的函数

看了下代码, 是把输入的密码一顿操作之后生成16位的key

然后用这个key异或一波文件的内容, 异或完一次之后+1

但是关键是我们不知道密码是什么。。。虽然提示了8位纯数字, 但是爆破依然很浪费时间

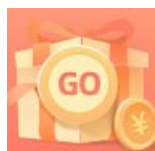
于是就发呆看着屏幕。。。结果看到有几列东西是每一列+1。。。于是大胆猜测全部都是0, 这些就是key加了n异或后的结果

4C	E9	BE	93	DD	6D	01	A6	DA	4F	54	3B	07	19	88	04	Lé*`Ým.¡ÚOT;..^.
4D	EA	BF	94	DE	6E	02	A7	DB	50	55	3C	08	1A	89	05	Mê¿"Èn.ŠÛPU<..%.
4E	EB	C0	95	DF	6F	03	A8	DC	51	56	3D	09	1B	8A	06	NèÀ*Bo."ÛQV=..Š.
4F	EC	C1	96	E0	70	04	A9	DD	52	57	3E	0A	1C	8B	07	OiÁ-àp.©ÝRW>..<.
50	ED	C2	97	E1	71	05	AA	DE	53	58	3F	0B	1D	8C	08	PiÂ-áq.*ÈSX?..Œ.
51	EE	C3	98	E2	72	06	AB	DF	54	59	40	0C	1E	8D	09	QiË"Âr.~RTY&

于是写个脚本, 解出文件, binwalk一波就能拿到一个thumbnail.jpeg 里面就有flag, 脚本如下

```
w=[68, 225, 182, 139, 213, 101, 249, 158, 210, 71, 76, 51, 255, 17, 128, 252]

f=open('CTF_300_1.ctf','rb')
da=f.read()
p=[]
for i in range(len(da)):
    p.append(da[i]^w[i%16])
    w[i%16]+=1
    w[i%16]%=256
f.close()
f=open('dec','wb')
f.write(bytes(p))
f.close()
```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)