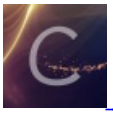
MIPS架构的CTF逆向题--SUCTFbabyre题目writeup

原创

iqiqiya 于 2018-10-18 15:35:14 发布
分类专栏： 我的逆向之路 我的CTF之路 我的CTF进阶之路 文章标签： MIPS架构的CTF逆向题--SUCTFbabyre题目wr
SUCTFbabyre题目writeup



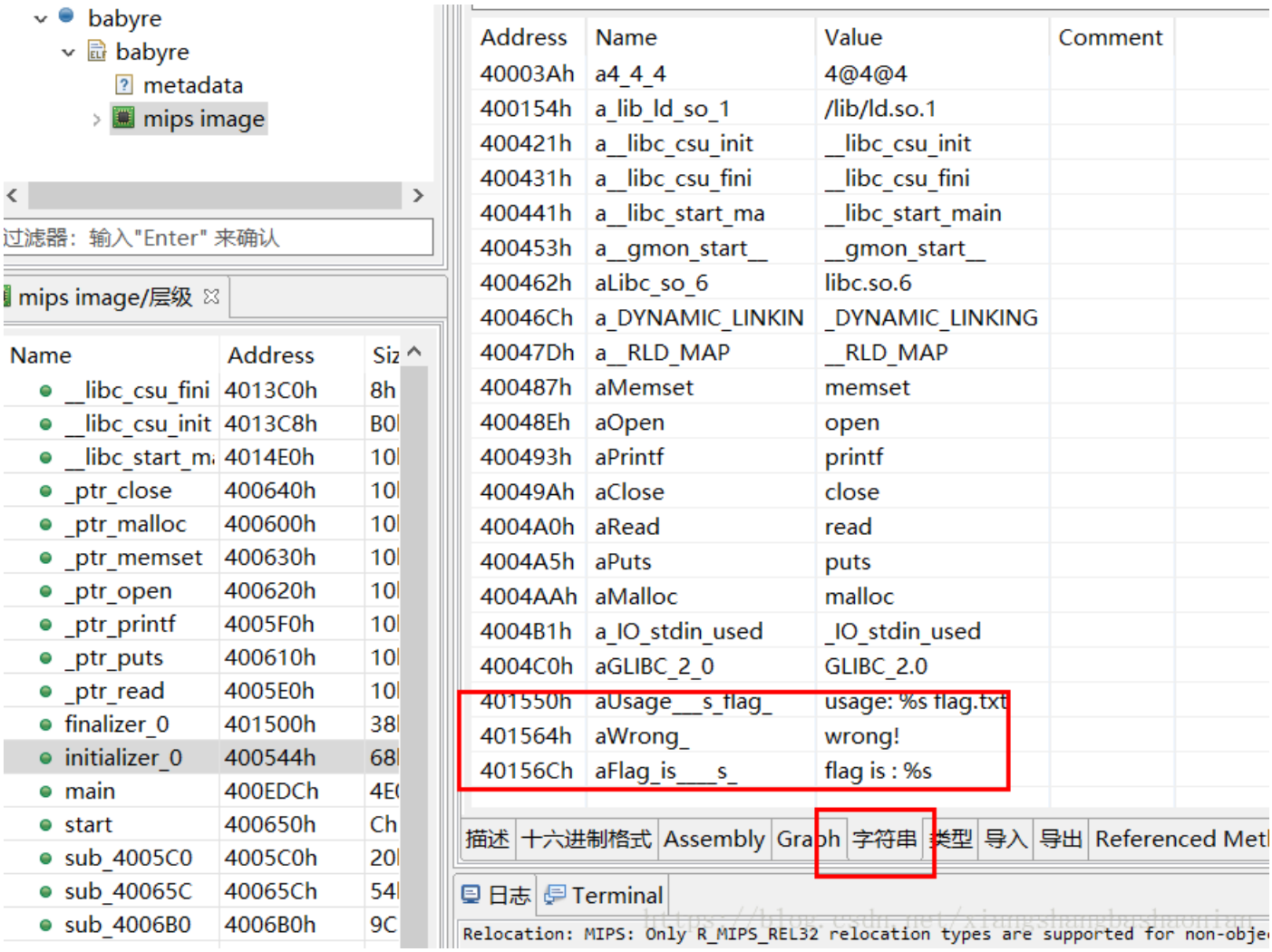
> 一，这道题刚拿到的时候我是直接载入IDA　结果分析的一团糟
>
> 比赛结束之后 看了好多师傅wp 才知道mips架构的专用工具怎么用，比如retdec,jeb-mips
>
> 开始是打算用retdec的，结果在线版的https://retdec.com/decompilation/不能用了　感觉windows下不好装 有时间补坑
>
> 就选择了jeb-mips(试用版)
>
> 扯一点怎样下载　就是https://www.pnfsoftware.com/jeb/demomips这个链接　填写好个人信息　就会发下载地址到邮箱

```
iqiqiya@521:~/Desktop$ file babyre
babyre: ELF 32-bit MSB  executable, MIPS, MIPS-II version 1, dynamically linked
(uses shared libs), for GNU/Linux 2.6.26, BuildID[sha1]=8a245bbb837d4679d7c20df7
ed3cbe1c24b86399, stripped
```


> 二，如果想要在linux里面运行　就必须安装qemu了　我记得好像是直接 sudo apt-get install qemu 就好了
>
> 正常的话直接终端执行qemu-mips babyre
>
> 但是这个文件是32bit 小端序　那么就得用qemu-mips babyre　可是提示我文件损坏。。

```
iqiqiya@521:~/Desktop$ qemu-mipsel ./babyre
./babyre: Invalid ELF image for this architecture
```


> 三，既然运行不了 就直接载入jeb-mips算了
>
> 可以看到关键字符串flag is 等等　双击任意一个进入

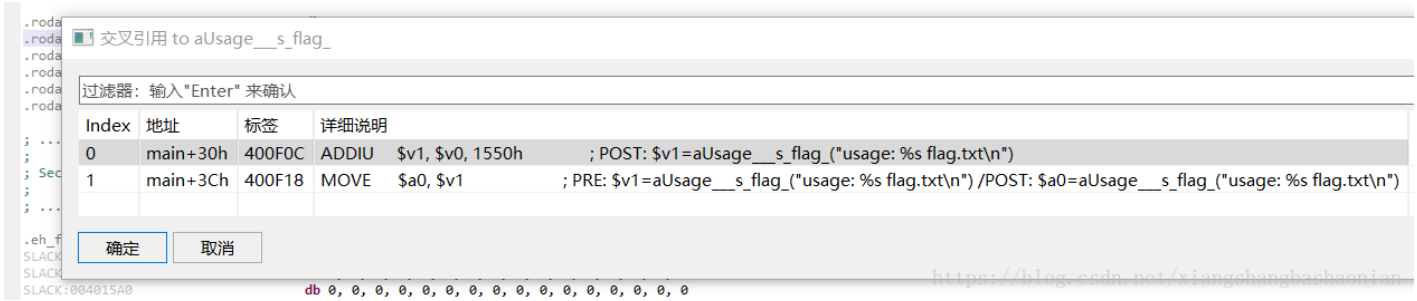


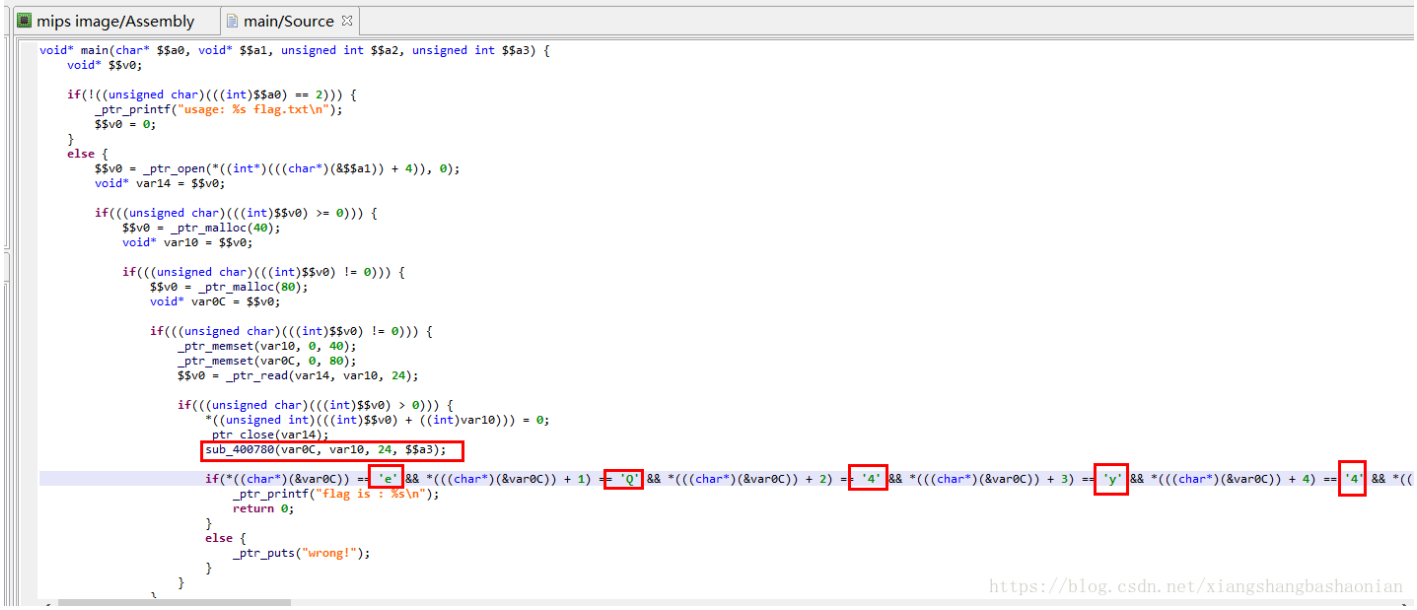
四，接着按大写X 查看交叉引用 可以看到都在main函数 双击任意一个

再按tab键反编译 可以看到sub_400780()就是关键 但是试用版是不支持反编译它的

根据师傅的博客 就是一个替换了base64编码表的加密函数

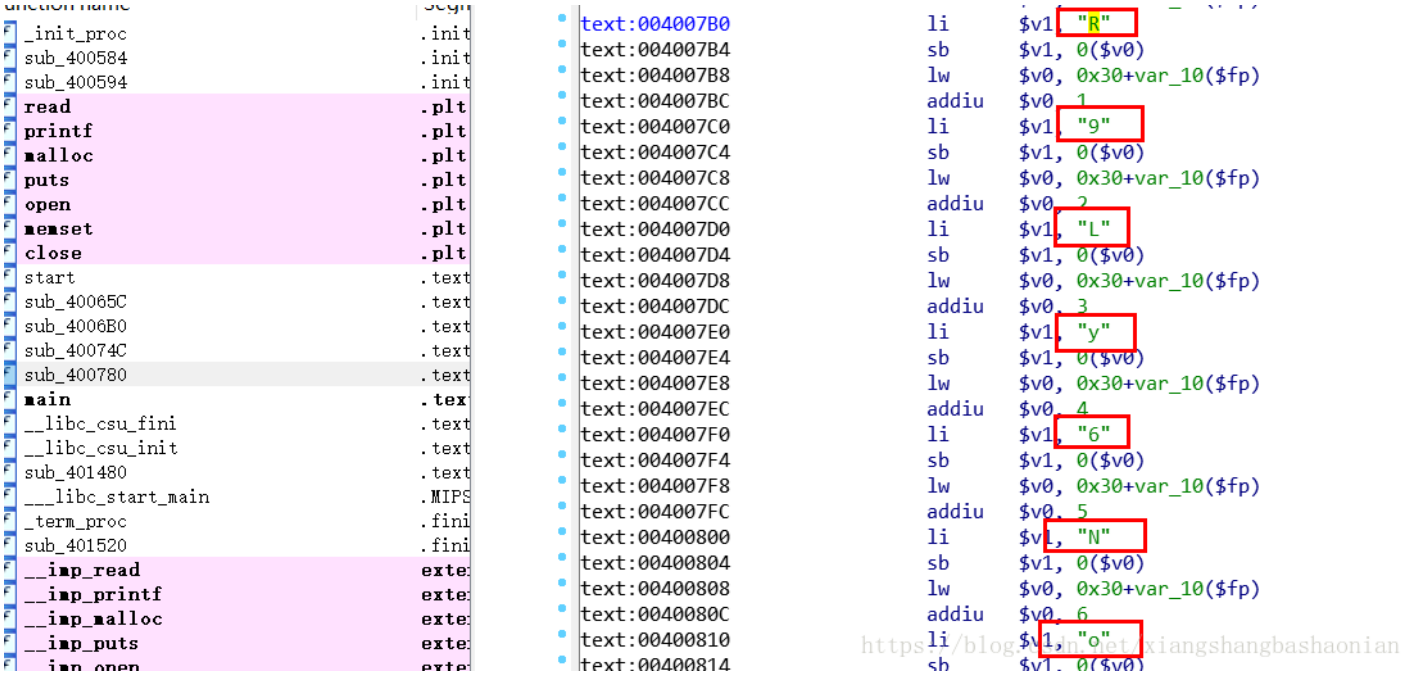
下面那个if判断可以抠出来要解密的**eQ4y46+VufZzdFNFdx0zudsa+yY0+J2m**

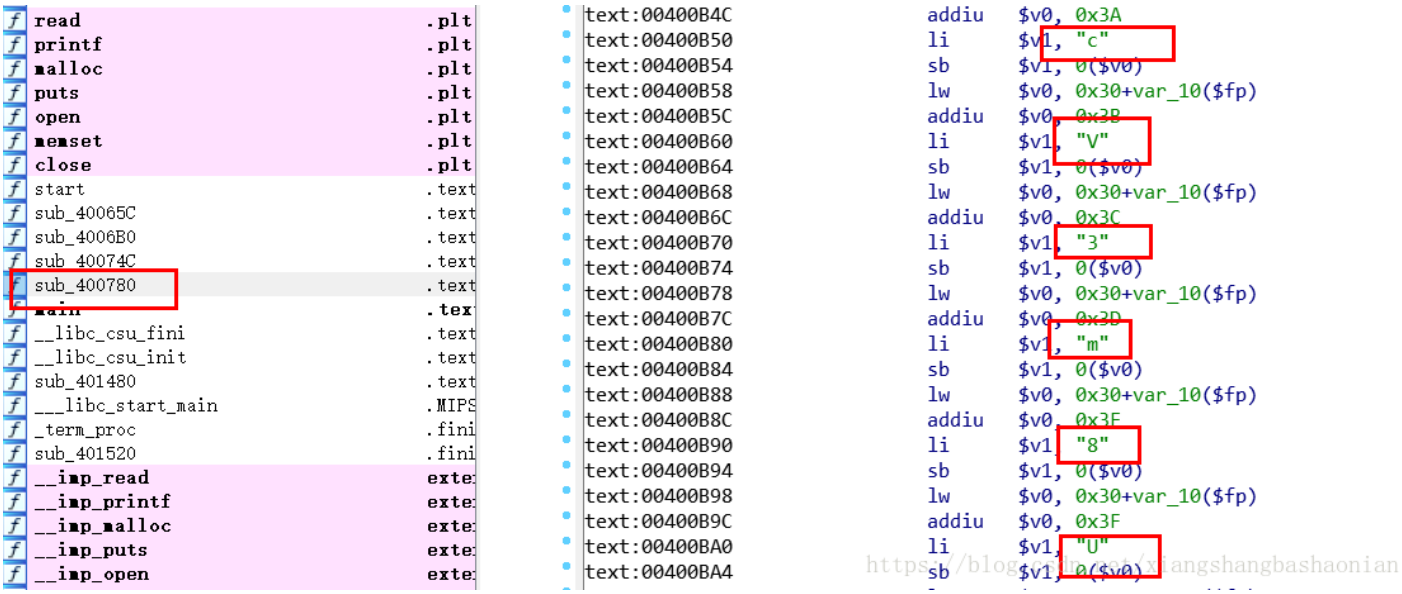




五，那就只好IDA载入 然后找到编码表就好(下边截图省略中间部分)

R9Ly6NoJvslPnWhETYtHe4Sdl+MbGujaZpk102wKCr7/ODg5zXAFqQfxBicV3m8U





最后写个脚本 本来自己写了有 但是发现有师傅https://wangyx-max.github.io/MIPS%E5%90%88%E9%9B%86/有更简单的

```
import string
import base64
my_base64table = "R9Ly6NoJvsIPnWhETYtHe4Sdl+MbGujaZpk102wKCr7/0Dg5zXAFqQfxBicV3m8U"
std_base64table ="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
s = "eQ4y46+VufZzdFNFdx0zudsa+yY0+J2m"
s = s.translate(string.maketrans(my_base64table,std_base64table))
print base64.b64decode(s)
#SUCTF{wh0_1s_{0ur_d4ldy}
```

参考链接：

https://wangyx-max.github.io/MIPS%E5%90%88%E9%9B%86/

https://github.com/Mem2019/Mem2019.github.io/tree/master/writeups/suctf2018#babyre

https://www.cnblogs.com/nww-570/p/8948371.html