bugku reverse file writeup

原创

队长啊别开枪了 于 2019-10-08 15:28:08 发布 95 收藏

分类专栏： 逆向 文章标签： CTF 逆向

本文链接：https://blog.csdn.net/weixin_41216733/article/details/102389127

放入ida后看源代码

```
  for ( j = 0; j <= 63; j += 2 )
    v14[v8++] = sub_400EB9((unsigned int)sttr_home[j], (unsigned int)sttr_home[j + 1]); //v14就是将sttr_home每两位转换成了十进制数
  *v12 = encode(flllag);
  for ( k = 0; k < v8; ++k )
  {
    if ( *flllag != (k ^ v15[k] ^ v14[k]) )//目标是逆向出v15[]
    {
      printf("Your file is wrong!! try again", argv);
      result = 0;
      goto LABEL_15;
    }
    ++flllag;
  }
  *v13 = encode(sttr_home);
  printf("the flag is file's MD5 Congratulations!", argv);//提示flag为md5后的值
  result = 0;
```

其中

```
sttr_home 为'664e06226625425d562e766e042d422c072c45692d125c7e6552606954646643'
```

```
flllag为flag{hello_player_come_on_hahah}
```

写python脚本，妹的逆向过来后一直是乱码，老是怀疑自己是哪里出问题了，其实是对的

```
import hashlib
hl = hashlib.md5()
flag='flag{hello_player_come_on_hahah}'

v14=[102,78,6,34,102,37,66,93,86,46,118,110,4,45,66,44,7,44,69,105,45,18,92,126,101,82,96,105,84,100,102,67]
res1=''
for i in range(len(v14)):
 res1+=chr((ord(flag[i])^v14[i])^i)
hl.update(res1.encode(encoding='utf-8'))
c=hl.hexdigest()
print c
```

结果为

914a7b9df69eab5b74b9edb7070e53e8