Crackme

发表于 2021-01-04 分类于 Challenge， 2019， SCTF， Reverse
Challenge | 2019 | SCTF | Reverse | Crackme

点击此处获得更好的阅读体验

解题思路

main开头第一个函数进行SMC。先查找区段.SCTF，然后调用DebugBreak下断点。猜测是通过调试器附加的方式来修改。之后进入sub_402450进行SMC。很容易写个脚本还原：

```
from ida_bytes import get_bytes, patch_bytes
st = 0x404000
key = map(ord,list("sycloversyclover"))
for i in range(512):
    tmp = ord(get_bytes(st,1))
    tmp^=key[i%16]
    tmp = ~tmp
    patch_bytes(st,chr(tmp))
    st+=1
```

修改的函数sub_404000在接下来的sub_4024A0中被调用到，可以发现它将之后的一串字符串修改为base64字符串后面加密部分，很容易看出AES CBC，密文密钥初始向量都有

```
from base64 import b64decode
from Crypto.Cipher import AES
key = b"sycloversyclover"
iv = b"sctfsctfsctfsctf"
aes = AES.new(key, mode = AES.MODE_CBC, iv = iv)
res = b"nKnbHsgqD3aNEB91jB3gEzAr+IklQwT1bSs3+bXpeuo="
cipher = b64decode(res)
tmp = aes.decrypt(cipher)
print(tmp)
```

FLAG

```
sctf{Ae3_C8c_I28_pKcs79ad4}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/SCTF/Reverse/5UFwqCkNF7PMZRK78dTJFi.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # Reverse # 2019 # SCTF
babyre
music