### <https://www.anquanke.com/post/id/181019#h2-14>

### Who is he

基于unity开发的游戏，实际只有一个视频播放器，输入框和一个确认框。

找了下资料，默认<Game>\_dataManagedAssembly-CSharp.dll应该是存放主逻辑的地方。dnspy一把梭。

只是一个DES CBC模式的加密，密文密钥都有，初始iv和key相同。注意C#里面字符串默认是Unicode，密钥是”1234“，每个字符后面都要加”x00”。

**import** base64**from** Crypto.Cipher **import** DES

key = b"1x002x003x004x00"

des = DES.new(key, mode = DES.MODE\_CBC, iv = key)

cipher = b"1Tsy0ZGotyMinSpxqYzVBWnfMdUcqCMLu0MA+22Jnp+MNwLHvYuFToxRQr0c+ONZc6Q7L0EAmzbycqobZHh4H23U4WDTNmmXwusW4E+SZjygsntGkO2sGA=="

cipher = base64.b64decode(cipher)

plain = des.decrypt(cipher)[0:-8].decode("utf-16")

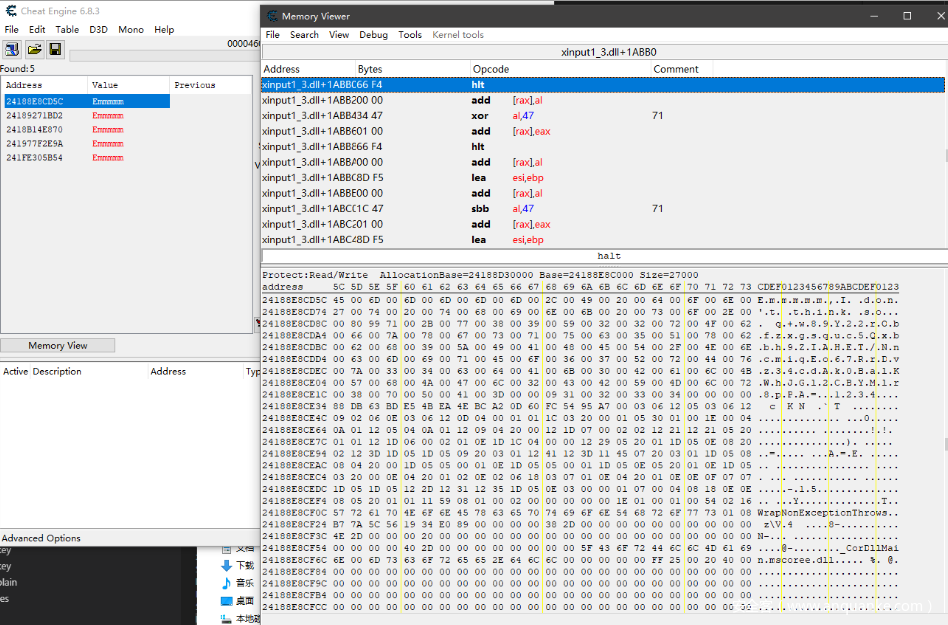
print(plain)

解出来得到

He\_P1ay\_Basketball\_Very\_We11!Hahahahaha!

交一下发现不对，找了半天好像这个dll里没什么奇怪的地方了。

后面用ce，直接暴力搜索”Emmmmm”

[](https://p5.ssl.qhimg.com/t01ccf147ae27749bdd.png)

搜到不止一个结果，在内存中查看一下有新的收获，这里base64的部分和之前dll里的不一样！一共有两个地方不同，先尝试直接解密。第一个得到：

Oh no!This **is** a trick!!!

第二个不知base64改了，key也改成了test。

解密之后得到：

She\_P1ay\_Black\_Hole\_Very\_Wel1!LOL!XD!

提交正确。脚本：

**import** base64**from** Crypto.Cipher **import** DES

key = b"tx00ex00sx00tx00"*# print(a)# print(key)*

des = DES.new(key, mode = DES.MODE\_CBC, iv = key)

a = b"xZWDZaKEhWNMCbiGYPBIlY3+arozO9zonwrYLiVL4njSez2RYM2WwsGnsnjCDnHs7N43aFvNE54noSadP9F8eEpvTs5QPG+KL0TDE/40nbU="

a = base64.b64decode(a)

res = des.decrypt(a)[0:-6].decode("utf-16")

print(res)

继续在ce的内存中翻找，可以看到pe头。把整个dll dump下来，再丢尽dnspy，可以看到内容基本一致。