




攻防世界-reverse Hello, CTF

原创

影子019  于 2019-09-22 15:21:35 发布  2660  收藏 1

分类专栏: [ctf_re](#) 文章标签: [ctf 逆向](#)

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/qinying001/article/details/101159438>

版权



[ctf_re](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

0x01

Hello, CTF

难度系数:  ★ 1.0

题目来源: [Pedy CTF 2018](#)

题目描述: 菜鸡发现Flag似乎并不一定是明文比较的

题目场景: 暂无

题目附件: [附件1](#)

<https://blog.csdn.net/qinying001>

从题目分析, flag一定加密或者编码过。

0x02 IDA分析

```
strcpy(&v13, "437261636b4d654a757374466f7246756e");
```

```
do  
{  
    v4 = v9[v3];  
    if ( !v4 )  
        break;  
    sprintf(&v8, asc_408044, v4);  
    strcat(&str, &v8);  
    ++v3;  
}  
  
while ( v3 < 17 );  
if ( !strcmp(&str, &v13) )  
    sub_40134B((int)aSuccess, v7);  
else  
    sub_40134B((int)aWrong, v7);  
}
```

IDA中主要看这三部分，第一部分是我们需要的flag，第二部分则是将我们输入的字符串转化为16进制，然后再将其转化为字符串储存在str中，第三部分则是判断输入的字符串转换之后是否和flag一样。

0x03

接下来，只要将16进制转化为字符串就可以拿到flag了。

```
>>> bytes.fromhex('437261636b4d654a757374466f7246756e')  
b'CrackMeJustForFun'
```

网络安全公众号，欢迎各位关注！

