

# 攻防世界 Hello, CTF wp

原创

[\\_ys](#) 于 2020-11-14 13:23:37 发布 84 收藏

分类专栏: [RE # 攻防世界](#)

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/qq\\_39214793/article/details/109425578](https://blog.csdn.net/qq_39214793/article/details/109425578)

版权



[RE](#) 同时被 2 个专栏收录

35 篇文章 0 订阅

订阅专栏



[攻防世界](#)

25 篇文章 0 订阅

订阅专栏

## Hello, CTF

从题目可知flag一定加密或者编码过

1. 丢进IDA中分析

```

int __cdecl main(int argc, const char **argv, const char **envp)
{
    signed int v3; // ebx
    char v4; // al
    int result; // eax
    int v6; // [esp+0h] [ebp-70h]
    int v7; // [esp+0h] [ebp-70h]
    char v8; // [esp+12h] [ebp-5Eh]
    char v9[20]; // [esp+14h] [ebp-5Ch]
    char v10; // [esp+28h] [ebp-48h]
    __int16 v11; // [esp+48h] [ebp-28h]
    char v12; // [esp+4Ah] [ebp-26h]
    char v13; // [esp+4Ch] [ebp-24h]

    strcpy(&v13, "437261636b4d654a757374466f7246756e");
    while ( 1 )
    {
        memset(&v10, 0, 0x20u);
        v11 = 0;
        v12 = 0;
        sub_40134B((int)aPleaseInputYou, v6);
        scanf(aS, v9);
        if ( strlen(v9) > 0x11 )
            break;
        v3 = 0;
        do
        {
            v4 = v9[v3];
            if ( !v4 )
                break;
            sprintf(&v8, asc_408044, v4);
            strcat(&v10, &v8);
            ++v3;
        }
        while ( v3 < 17 );
        if ( !strcmp(&v10, &v13) )
            sub_40134B((int)aSuccess, v7);
        else
            sub_40134B((int)aWrong, v7);
    }
    sub_40134B((int)aWrong, v7);
    result = stru_408090._cnt-- - 1;
    if ( stru_408090._cnt < 0 )
        return _filbuf(&stru_408090);
    ++stru_408090._ptr;
    return result;
}

```

[https://blog.csdn.net/qq\\_39214793](https://blog.csdn.net/qq_39214793)

发现

```
sub_40134B((int)aSuccess, v7);
```

通过对程序的分析可以得出v13即为flag

```
asc_408044    db '%x',0
              align 4
```

然后就是将16进制转化为字符串类型，贴一个Python代码（也可在线转化）

```

x='437261636b4d654a757374466f7246756e'
y=''
i=0
while(i<len(x)):
    y+=chr(int(x[i:i+2],16))
    i+=2
print(y)

```

最后得到flag: CrackMeJustForFun