

# buuctf刷题记录8 [ACTF新生赛2020]rome

原创

ytj00 于 2020-07-30 17:03:43 发布 264 收藏

分类专栏: [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/ytj00/article/details/107694353>

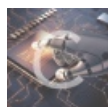
版权



[ctf 同时被 2 个专栏收录](#)

28 篇文章 0 订阅

订阅专栏



[逆向](#)

27 篇文章 0 订阅

订阅专栏

ida打开, 逻辑很清晰

```
v15 = 81;
v16 = 115;
v17 = 119;
v18 = 51;
v19 = 115;
v20 = 106;
v21 = 95;
v22 = 108;
v23 = 122;
v24 = 52;
v25 = 95;
v26 = 85;
v27 = 106;
v28 = 119;
v29 = 64;
v30 = 108;
v31 = 0;
printf("Please input:");
scanf("%s", &v5);
result = v5;
if ( v5 == 'A' )
{
    result = v6;
    if ( v6 == 'C' )
    {
        result = v7;
        if ( v7 == 'T' )
        {
            result = v8;
            if ( v8 == 'F' )
            {
                result = v9;
                if ( v9 == '{' )
                {
```

```

    {
        result = v14;
        if ( v14 == '}' )
        {
            v1 = v10;
            v2 = v11;
            v3 = v12;
            v4 = v13;
            for ( i = 0; i <= 15; ++i )
            {
                if ( *((_BYTE *)&v1 + i) > 64 && *((_BYTE *)&v1 + i) <= 90 )
                    *((_BYTE *)&v1 + i) = (*((char *)&v1 + i) - 51) % 26 + 65;
                if ( *((_BYTE *)&v1 + i) > 96 && *((_BYTE *)&v1 + i) <= 122 )
                    *((_BYTE *)&v1 + i) = (*((char *)&v1 + i) - 79) % 26 + 97;
            }
            for ( i = 0; i <= 15; ++i )
            {
                result = (unsigned __int8)*(&v15 + i);
                if ( *((_BYTE *)&v1 + i) != (_BYTE)result )
                    return result;
            }
            result = printf("You are correct!");
        }
    }
}
}
}
}
}
return result;

```

然后就想去爆破，能穷举就不想动脑子--

```

a=[81,115,119,51,115,106,95,108,122,52,95,85,106,119,64,108,0]
flag=''
for i in range(0,16):
    for k in range(0,127):
        z=k
        if k>64 and k<=90:
            k=(k-51)%26+65
        if k>96 and k<=122:
            k=(k-79)%26+97
        if k==a[i]:
            flag+=chr(z)
print(flag)

```

得到flag: flag{Cae3ar\_th4\_Gre@t}

后来看别人的wp才知道是凯撒加密+大小写转换