buuctf————[GKCTF 2021]QQQQT

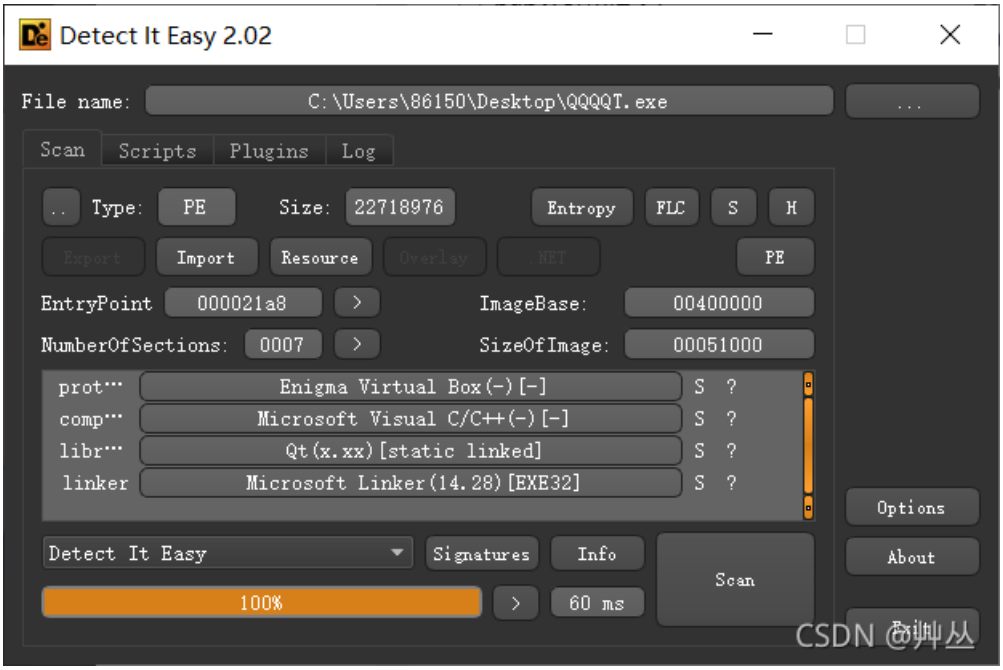
原创

re3sry 于 2021-10-07 21:13:34 发布 321 收藏
文章标签： buuctf reverse

1.查壳。

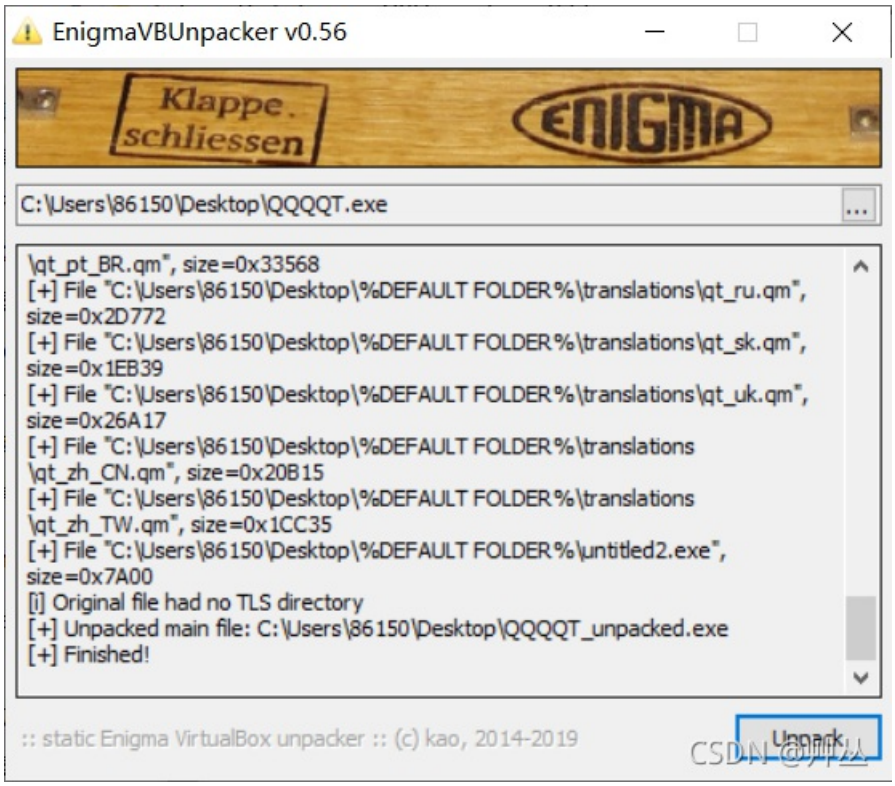
32位

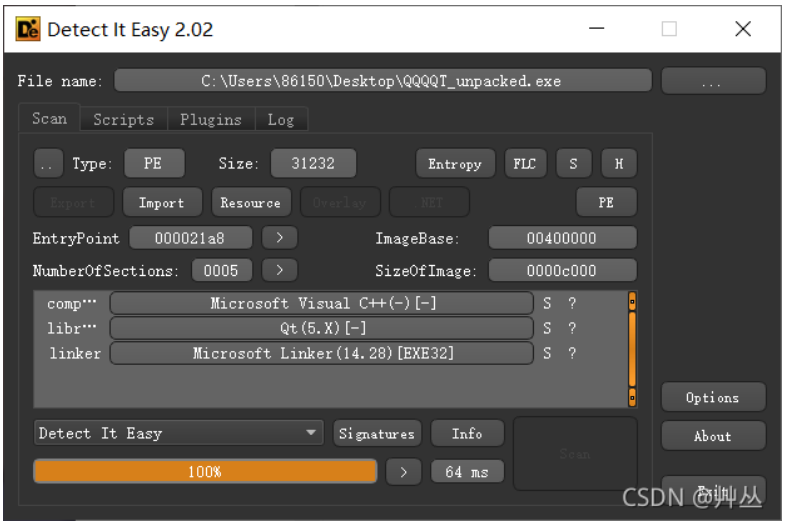
Enigma Virtual Box打包的QT程序



2.解包Enigma Virtual Box。

（这个不解包也可以得出flag）





3IDA反编译。

可以很明显的看出是base58加密。直接解密就可以。

```
30  QString::toLatin1(v15, v16);
31  LOBYTE(v25) = 1;
32  v18 = QByteArray::data((QByteArray *)v16);
33  memset(v23, 0, sizeof(v23));
34  v24 = 0i64;
35  strcpy(v22, "123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz");
36  v20 = 138 * strlen(v18) / 0x64;
37  v13 = v20 + 1;
38  v1 = 0;
39  v21 = malloc(v20 + 1);
40  v2 = v21;
41  memset(v21, 0, v13);
42  v3 = v18;
43  v19 = (int)(v18 + 1);
```

```
87    }
88    while ( v8 <= v9 );
89  }
90  if ( !qstrcmp((const char *)v23, "56fkoP8KhwCf3v7CEz") )
91  {
92    if ( v18 )
93      v12 = strlen(v18);
94    else
95      v12 = -1;
96    v21 = (_BYTE *)QString::fromAscii_helper(v18, v12);
97    LOBYTE(v25) = 2;
98    v20 = QString::fromAscii_helper("flag", 4);
99    LOBYTE(v25) = 3;
100   QMessageBox::warning(this, &v20, &v21, 1024, 0);
```


4.get flag

flag{12t4tww3r5e77}