codegate ctf reverse easy_serial writeup

原创

charlie_heng 于 2018-02-04 21:25:49 发布 405 收藏

分类专栏： 二进制-逆向工程

本文链接：https://blog.csdn.net/charlie_heng/article/details/79255014

这题拿到，拖进ida，看到ghc之后，我又想起了被haskell统治的恐惧……

首先用hsdecomp来反编译一波，得到如下的代码

```
s1b4_info = unpackCString# "abcdefghijklmnopqrstuvwxyz"
loc_7172600 = I# 9
s1bb_info = !! s1b5_info loc_7172488
loc_7172488 = I# 2
s1b5_info = splitOn $fEqChar (unpackCString# "#") s1dZ_info_arg_0
loc_7172584 = I# 8
loc_7172504 = I# 3
s1b2_info = unpackCString# "1234567890"
loc_7172568 = I# 7
loc_7172552 = I# 6
s1b3_info = unpackCString# "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
loc_7172536 = I# 5
loc_7172520 = I# 4
loc_7172472 = I# 1
loc_7172456 = I# 0
loc_7168872 = C# 48
s1b9_info = !! s1b5_info loc_7172472
s1b7_info = !! s1b5_info loc_7172456
Main_main_closure=>> $fMonadIO
    (putStrLn (unpackCString# "Input Serial Key >>> "))
    (>>= $fMonadIO
        getLine
        (\s1dZ_info_arg_0 ->
            >> $fMonadIO
                (putStrLn (++ (unpackCString# "your serial key >>> ") (++ s1b7_info (++ (unpackCString#
                (case && (== $fEqInt (ord (!! s1b7_info loc_7172456)) (I# 70)) (&& (== $fEqInt (ord (!!
                    <tag 1> -> putStrLn (unpackCString# ":p"),
                    c1ni_info_case_tag_DEFAULT_arg_0@_DEFAULT -> case == ($fEq[] $fEqChar) (reverse s1b
                        False -> putStrLn (unpackCString# ":p"),
                        True -> case && (== $fEqChar (!! s1bb_info loc_7172456) (!! s1b3_info loc_71724
                            <tag 1> -> putStrLn (unpackCString# ":p"),
                            c1tb_info_case_tag_DEFAULT_arg_0@_DEFAULT -> putStrLn (unpackCString# "Corr
                )
        )
    )
```

贼难看懂
于是美化一波

```
mkey_2 = !! mkey 2
mkey = splitOn $fEqChar ("#") s1dZ_info_arg_0
ABCD = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
mkey_1 = !! mkey 1
mkey_0 = !! mkey 0
Main_main_closure=>> $fMonadIO
    (putStrLn ("Input Serial Key >>> "))
    (>>= $fMonadIO
        getLine
        (\s1dZ_info_arg_0 ->
            >> $fMonadIO
                (putStrLn (++ ("your serial key >>> ") (++ mkey_0 (++ ("_") (++ mkey_1 (++ ("_") mkey_2
                (case && (== $fEqInt (ord (!! mkey_0 0)) (70)) (&& (== $fEqInt (ord (!! mkey_0 1)) (108
                    <tag 1> -> putStrLn (":p"),
                    c1ni_info_case_tag_DEFAULT_arg_0@_DEFAULT -> case == ($fEq[] $fEqChar) (reverse mke
                        False -> putStrLn (":p"),
                        True -> case && (== $fEqChar (!! mkey_2 0) (!! ABCD 0)) (&& (== $fEqChar (!! mk
                            <tag 1> -> putStrLn (":p"),
                            c1tb_info_case_tag_DEFAULT_arg_0@_DEFAULT -> putStrLn ("Correct Serial Key!
                )
        )
    )
```

这样就好看很多了，这里首先是用#将输入的字符串分割成三部分
然后三部分分别比较
flag就出来了
S0me0fU5#4r3L00king#AtTh3St4rs