weird_lua

发表于 2021-03-15 更新于 2021-05-21 分类于 Challenge ， 2020 ， XCTF高校网络安全专题挑战赛 ， 华为云专题赛 ， Reverse
Challenge | 2020 | XCTF高校网络安全专题挑战赛 | 华为云专题赛 | Reverse | weird_lua

点击此处获得更好的阅读体验

WriteUp来源

官方WP

题目考点

- *Lua*

解题思路

本题考点主要是对lua-5.3源码做了部分修改，根据luac生成了二进制文件。

修改了lundump.c中的LoadByte函数，将结果与0xff做了异或，如下

```
static lu_byte LoadByte (LoadState *S) {
  lu_byte x;
  LoadVar(S, x);
  x ^= 0xff;
  return x;
}
```

修改了部分opcode序列的顺序，随机修改，具体见如下：

```
 0  0 1 MOVE -> MOVE
 1  1 1 LOADK -> LOADK
 2  2 1 LOADKX -> LOADKX
 3  3 1 LOADBOOL -> LOADBOOL
 4  4 1 LOADNIL -> LOADNIL
 5  5 1 GETUPVAL -> GETUPVAL
 6 32 1 GETTABUP -> LT
 7 38 1 GETTABLE -> RETURN
 8  7 1 SETTABUP -> GETTABLE
 9 35 1 SETUPVAL -> TESTSET
10 12 1 SETTABLE -> SELF
11 11 1 NEWTABLE -> NEWTABLE
12 33 1 SELF -> LE
13 13 1 ADD -> ADD
14 14 1 SUB -> SUB
15 15 1 MUL -> MUL
16 16 1 MOD -> MOD
17 17 1 POW -> POW
18 18 1 DIV -> DIV
19 19 1 IDIV -> IDIV
20 20 1 BAND -> BAND
21 21 1 BOR -> BOR
22 22 1 BXOR -> BXOR
23 23 1 SHL -> SHL
24 24 1 SHR -> SHR
25 25 1 UNM -> UNM
26 26 1 BNOT -> BNOT
27 27 1 NOT -> NOT
28 28 1 LEN -> LEN
29  6 1 CONCAT -> GETTABUP
30 30 1 JMP -> JMP
31 34 1 EQ -> TEST
32  8 1 LT -> SETTABUP
33 41 1 LE -> TFORCALL
34 40 1 TEST -> FORPREP
35 46 1 TESTSET -> EXTRAARG
36 36 1 CALL -> CALL
37 39 1 TAILCALL -> FORLOOP
38 43 1 RETURN -> SETLIST
39 29 1 FORLOOP -> CONCAT
40 37 1 FORPREP -> TAILCALL
41 42 1 TFORCALL -> TFORLOOP
42 45 1 TFORLOOP -> VARARG
43 10 1 SETLIST -> SETTABLE
44  9 1 CLOSURE -> SETUPVAL
45 44 1 VARARG -> CLOSURE
46 31 1 EXTRAARG -> EQ
```

破解方法：

通过逆向，可以发现头部各种标志不对，从而发现LoadByte的问题，重新编译lua代码修复该问题，修完后继续发现还修改了LUA_SIGNATURE,由\1b改成了\1c。然后继续发现操作码对不上。

自己编写lua脚本，调用lua子代码的string.dump函数，可以找到生成的lua二进制脚本，与正常生成的作对比，可以找到操作码的对应关系。参考https://bbs.pediy.com/thread-250618.htm

更新lua5.3中的opcode顺序（lopcode，具体看.c和.h文件，有三个数组要修改），重新编译luadec（github可以搜索到），然后对check_license_out.lua进行反汇编，反编译会失败。

根据lua反汇编代码逆向分析，即可得到flag。

附上Vidar-Team队求flag的脚本：

```
#!/usr/bin/env python
# coding=utf-8
tb=[81, 138, 85, 142, 185, 35, 229, 83, 8, 225, 92, 223, 222, 47, 182, 158, 17, 74, 34, 100, 43, 103, 102, 147, 237, 88, 73, 28, 224, 23, 44, 40, 154, 127, 16, 169, 160, 1
x=[172, 25, 60, 95, 5, 27, 49, 58, 171, 5, 253, 45, 87, 246, 197, 12, 97, 234, 159, 119, 157, 169, 121, 54, 242]
ans=[94, 117, 57, 37, 54, 110, 15, 223, 163, 133, 99, 237, 8, 128, 27, 54, 233, 181, 242, 55, 230, 62, 42, 252, 116]
for i in range(25):
  print(chr(tb.index( ans[i]) ^ x[i]), end='')
```

Flag

```
flag{th15_15_v3r7_c0mm3n}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/XCTF高校网络安全专题挑战赛/华为云专题赛/Reverse/bWtfisyAVovqRtbbPzbWfT.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # Reverse # XCTF高校网络安全专题挑战赛 # 华为云专题赛

divination
文件包含