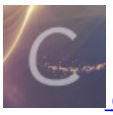
攻防世界Reverse进阶区-tt3441810-writeup

原创

y4ung 于 2020-10-07 09:18:02 发布 304 收藏

分类专栏： ctf 文章标签： ctf

本文链接：https://blog.csdn.net/qq_35056292/article/details/108947359



1. 介绍

本题是xctf攻防世界中Reverse的进阶区的题tt3441810

题目来源： tinyctf-2014

2. 分析

```
$ file rev100
rev100: ASCII text, with CRLF line terminators
```

用vscode打开，是一堆十六进制数

```
00400080  68 66 6C 00 00 48 BF 01  00 00 00 00 00 00 00 48
00400090  8D 34 24 48 BA 02 00 00  00 00 00 00 00 48 B8 01
004000A0  00 00 00 00 00 00 00 0F  05 68 61 67 00 00 48 BF
004000B0  01 00 00 00 00 00 00 00  48 8D 34 24 48 BA 02 00
004000C0  00 00 00 00 00 00 48 B8  01 00 00 00 00 00 00 00
004000D0  0F 05 68 7B 70 00 00 48  BF 01 00 00 00 00 00 00
004000E0  00 48 8D 34 24 48 BA 02  00 00 00 00 00 00 00 48
004000F0  B8 01 00 00 00 00 00 00  00 0F 05 68 6F 70 00 00
00400100  48 BF 01 00 00 00 00 00  00 00 48 8D 34 24 48 BA
00400110  02 00 00 00 00 00 00 00  48 B8 01 00 00 00 00 00
00400120  00 00 0F 05 68 70 6F 00  00 48 BF 01 00 00 00 00
00400130  00 00 00 48 8D 34 24 48  BA 02 00 00 00 00 00 00
00400140  00 48 B8 01 00 00 00 00  00 00 00 0F 05 68 70 72
00400150  00 00 48 BF 01 00 00 00  00 00 00 00 48 8D 34 24
00400160  48 BA 02 00 00 00 00 00  00 00 48 B8 01 00 00 00
00400170  00 00 00 00 0F 05 68 65  74 00 00 48 BF 01 00 00
00400180  00 00 00 00 00 48 8D 34  24 48 BA 02 00 00 00 00
00400190  00 00 00 48 B8 01 00 00  00 00 00 00 00 0F 05 68
004001A0  7D 0A 00 00 48 BF 01 00  00 00 00 00 00 00 48 8D
004001B0  34 24 48 BA 02 00 00 00  00 00 00 00 48 B8 01 00
004001C0  00 00 00 00 00 00 0F 05  48 31 FF 48 B8 3C 00 00
004001D0  00 00 00 00 00 0F 05
```

flag十有八九是在这里头了。写个python脚本提取一下看看：

```
text = """
68 66 6C 00 00 48 BF 01  00 00 00 00 00 00 00 48
8D 34 24 48 BA 02 00 00  00 00 00 00 00 48 B8 01
00 00 00 00 00 00 00 0F  05 68 61 67 00 00 48 BF
01 00 00 00 00 00 00 00  48 8D 34 24 48 BA 02 00
00 00 00 00 00 00 48 B8  01 00 00 00 00 00 00 00
0F 05 68 7B 70 00 00 48  BF 01 00 00 00 00 00 00
00 48 8D 34 24 48 BA 02  00 00 00 00 00 00 00 48
B8 01 00 00 00 00 00 00  00 0F 05 68 6F 70 00 00
48 BF 01 00 00 00 00 00  00 00 48 8D 34 24 48 BA
02 00 00 00 00 00 00 00  48 B8 01 00 00 00 00 00
00 00 0F 05 68 70 6F 00  00 48 BF 01 00 00 00 00
00 00 00 48 8D 34 24 48  BA 02 00 00 00 00 00 00
00 48 B8 01 00 00 00 00  00 00 00 0F 05 68 70 72
00 00 48 BF 01 00 00 00  00 00 00 00 48 8D 34 24
48 BA 02 00 00 00 00 00  00 00 48 B8 01 00 00 00
00 00 00 00 0F 05 68 65  74 00 00 48 BF 01 00 00
00 00 00 00 00 48 8D 34  24 48 BA 02 00 00 00 00
00 00 00 48 B8 01 00 00  00 00 00 00 00 0F 05 68
7D 0A 00 00 48 BF 01 00  00 00 00 00 00 00 48 8D
34 24 48 BA 02 00 00 00  00 00 00 00 48 B8 01 00
00 00 00 00 00 00 0F 05  48 31 FF 48 B8 3C 00 00
00 00 00 00 00 0F 05
"""
res = ""
for each in text.replace("\n", "").split(" "):
    each = each.replace(" ", "")
    if not each:
        continue
    curr_chr = chr(int("0x" +each, 16))
    res += curr_chr

print(res)
```

打印出

来：`hflH¿H 4$HºH,hagH¿H 4$HºH,h{pH¿H 4$HºH,hopH¿H 4$HºH,hpoH¿H 4$HºH,hprH¿H 4$HºH,hetH¿H 4$HºH,h}H¿H 4$HºH,H1ÿH ,<`

看到了个`{`和`}`，ok，尝试只筛选出字母呢？

```
text = """
68 66 6C 00 00 48 BF 01  00 00 00 00 00 00 00 48
8D 34 24 48 BA 02 00 00  00 00 00 00 00 48 B8 01
00 00 00 00 00 00 00 0F  05 68 61 67 00 00 48 BF
01 00 00 00 00 00 00 00  48 8D 34 24 48 BA 02 00
00 00 00 00 00 00 48 B8  01 00 00 00 00 00 00 00
0F 05 68 7B 70 00 00 48  BF 01 00 00 00 00 00 00
00 48 8D 34 24 48 BA 02  00 00 00 00 00 00 00 48
B8 01 00 00 00 00 00 00  00 0F 05 68 6F 70 00 00
48 BF 01 00 00 00 00 00  00 00 48 8D 34 24 48 BA
02 00 00 00 00 00 00 00  48 B8 01 00 00 00 00 00
00 00 0F 05 68 70 6F 00  00 48 BF 01 00 00 00 00
00 00 00 48 8D 34 24 48  BA 02 00 00 00 00 00 00
00 48 B8 01 00 00 00 00  00 00 00 0F 05 68 70 72
00 00 48 BF 01 00 00 00  00 00 00 00 48 8D 34 24
48 BA 02 00 00 00 00 00  00 00 48 B8 01 00 00 00
00 00 00 00 0F 05 68 65  74 00 00 48 BF 01 00 00
00 00 00 00 00 48 8D 34  24 48 BA 02 00 00 00 00
00 00 00 48 B8 01 00 00  00 00 00 00 00 0F 05 68
7D 0A 00 00 48 BF 01 00  00 00 00 00 00 00 48 8D
34 24 48 BA 02 00 00 00  00 00 00 00 48 B8 01 00
00 00 00 00 00 00 0F 05  48 31 FF 48 B8 3C 00 00
00 00 00 00 00 0F 05
"""
res = ""
for each in text.replace("\n", "").split(" "):
    each = each.replace(" ", "")
    if not each:
        continue
    if 97<=int("0x"+each, 16)<=127 or 65 <=int("0x"+each, 16)<=90:
        curr_chr = chr(int("0x"+each, 16))
        res += curr_chr

print(res)
```

打印出来：`hflHHHHHhagHHHHHh{pHHHHHhopHHHHHhpoHHHHHhprHHHHHhetHHHHHh}HHHHHH`

依稀可见`{`前面有flag的样子，看来这里的`h`和`H`是不必要的，让我们把它们去掉看看：

```
text = """
68 66 6C 00 00 48 BF 01  00 00 00 00 00 00 00 48
8D 34 24 48 BA 02 00 00  00 00 00 00 00 48 B8 01
00 00 00 00 00 00 00 0F  05 68 61 67 00 00 48 BF
01 00 00 00 00 00 00 00  48 8D 34 24 48 BA 02 00
00 00 00 00 00 00 48 B8  01 00 00 00 00 00 00 00
0F 05 68 7B 70 00 00 48  BF 01 00 00 00 00 00 00
00 48 8D 34 24 48 BA 02  00 00 00 00 00 00 00 48
B8 01 00 00 00 00 00 00  00 0F 05 68 6F 70 00 00
48 BF 01 00 00 00 00 00  00 00 48 8D 34 24 48 BA
02 00 00 00 00 00 00 00  48 B8 01 00 00 00 00 00
00 00 0F 05 68 70 6F 00  00 48 BF 01 00 00 00 00
00 00 00 48 8D 34 24 48  BA 02 00 00 00 00 00 00
00 48 B8 01 00 00 00 00  00 00 00 0F 05 68 70 72
00 00 48 BF 01 00 00 00  00 00 00 00 48 8D 34 24
48 BA 02 00 00 00 00 00  00 00 48 B8 01 00 00 00
00 00 00 00 0F 05 68 65  74 00 00 48 BF 01 00 00
00 00 00 00 00 48 8D 34  24 48 BA 02 00 00 00 00
00 00 00 48 B8 01 00 00  00 00 00 00 00 0F 05 68
7D 0A 00 00 48 BF 01 00  00 00 00 00 00 00 48 8D
34 24 48 BA 02 00 00 00  00 00 00 00 48 B8 01 00
00 00 00 00 00 00 0F 05  48 31 FF 48 B8 3C 00 00
00 00 00 00 00 0F 05
"""
res = ""
for each in text.replace("\n", "").split(" "):
    each = each.replace(" ", "")
    if not each:
        continue
    if 97<=int("0x"+each, 16)<=127 or 65 <=int("0x"+each, 16)<=90:
        curr_chr = chr(int("0x"+each, 16))
        if curr_chr != "h" and curr_chr!="H":
            res += curr_chr

print(res)
```

打印出来`flag{poppopret}`，看来这就是flag了。

提交上去发现结果不对。。。试了好几次都不行，最后去网上找writeup，发现提交的内容是不包括flag{ }的，也就是最后提交的只有`poppopret`。。

3. 总结

有时候提交上去不对，不是你结果错了，可能是flag的格式不太对。。。