

where_is_temp

发表于 2021-03-05 分类于 [Challenge](#) , [2020](#) , [SWPU CTF 2020](#) , [Reverse](#)
[Challenge](#) | [2020](#) | [SWPU CTF 2020](#) | [Reverse](#) | [where_is_temp](#)

[点击此处](#)获得更好的阅读体验

WriteUp来源

[官方WP](#)

题目考点

- lua逆向

解题思路

本题是通过C语言来调用lua脚本，实现flag的获取与验证操作，所以关键点就是要能提取出原始的lua脚本进行分析。

首先是C语言部分比较简单，就是一些垃圾的反调试，然后就是文件操作，将文件释放到临时文件夹中，拿到了这个脚本发现是luac脚本，luac文件转lua文件其实可以选择的工具很多，我自己选择的是luadec，值得一提的是luadec需要确定具体的lua使用的版本，而这可以通过ida查看程序的字符串就可以发现是lua5.3，这样我们基本就能完整还原出lua文件了。

lua脚本中就是一些简单的换位，异或，查表操作等，当然最后两位比较特殊，看似有多解，但根据费马大定理可得其实n只能等于2，而m就等于40，当然熟悉勾三股四弦五的话很容易也可以猜到。

Flag

```
1 flag{luAls_(2_Easy_To_y0u_!!!)}
```

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Challenge/2020/SWPU-CTF-2020/Reverse/tC7YZwqQCJqhVU3q73xazg.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](#) [# SWPU CTF 2020](#)

[Strangeapk](#)

[简陋的VM](#)