

anxun3

发表于 2021-01-15 分类于 [Challenge](#) , [2020](#) , [安洵杯](#) , [Reverse](#)
[Challenge](#) | [2020](#) | [安洵杯](#) | [Reverse](#) | [anxun3](#)

[点击此处](#)获得更好的阅读体验

WriteUp来源

<https://xz.aliyun.com/t/8582>

题目考点

- MIPS逆向

解题思路

题目分析

这道题是个去了符号表的mips程序

首先建议使用ghidra和ida联合分析

使用的知识点为

strcmp函数,只对比第二个字符串的长度,也就是代表,只对比前面的字符串

strstr,寻找第一个出现字符串的位置

kmp算法,搜索字符串,返回位置,但是比strstr搜索快

test函数,一个简单的异或算法...

过程

首先是strcmp函数,解出对应的第一段d0g3wi11

其次是发现,这里存在寻找m0r3的字符串,并且因为count计数是两次,所以直接记录下来

然后kmp算法,寻找了11b3,和b3tt3r这两个字符串

最后test函数解出来就是

```
1 key = "o3v6d4|}9y"
2 flag = ''
3 for i in range(len(key)):
4     flag += chr(ord(key[i])^(i+2))
5 print flag
```

m0r3b3tt3r

最后根据重复的位置,把字符串拼接完成:

d0g3wi11b3m0r3m0r3b3tt3r

最后输入了这个字符串,就会输出:

d0gewillbem0rem0rebetter

这就是最后的flag了

Flag

1 d0gewillbem0rem0rebetter

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2020/安洵杯/Reverse/juUw7tZJk4DAMqMIECNVbS.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 #安洵杯](#)
[EasyCM_WP](#)
[debugging](#)