

writeup-FLAG 实验吧

原创

[charlie_heng](#) 于 2016-11-30 10:47:04 发布 1487 收藏

分类专栏: [二进制-逆向工程](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/charlie_heng/article/details/53405341

版权



[二进制-逆向工程](#) 专栏收录该内容

34 篇文章 3 订阅

订阅专栏

题目如下

请输入 FLAG, 下面的页面会告诉你 FLAG 是否正确

解题链接: <http://ctf5.shiyanbar.com/qwctf/flag-checker.html>

看了下打开的页面, 发现一大串js代码。。。分析了一下发现a[0]给出了, 然后可以一个个地推下去

于是把js代码保存在一个文本下面, 写了个py代码来解

```
import re

content = open("C:/Users/Admin/Desktop/cod1.txt")
list_exp = content.read().split("&&")
flag = ""
now = 0
for k in range(0, 43):
    #print(list_exp)
    for i in list_exp:
        if i.count("a") == 1:
            for w in range(1, 255):
                replace_reg = re.compile(r'a\[\d{1,2}\]')
                num = replace_reg.findall(i)[0].strip('a[').strip(']')
                temp = replace_reg.sub(str(w), i)
                try:
                    if eval(temp) == 1:
                        rep = re.compile(r'a\[' + num + r'\]')
                        for l in range(0, len(list_exp)):
                            list_exp[l] = rep.sub(str(w), list_exp[l])
                        print(str(chr(w) + " " + num))
                        flag += chr(w)
                        break
                except Exception as e:
                    print(temp)

print(flag)
#for i in list_exp:
#    #print(i)
```

解完后得到flag

flag{wh47_my5ter10us-do3s,the+phe45ant/c0nta1n}



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)