writeup-DASCTF2020七月赛crypto第一题bullshit

原创

拾光、 于 2020-07-25 20:45:03 发布 804 收藏
文章标签： python

bullshit 题目如下：

```
from flag import flag
def pairing(a,b):
    shell = max(a, b)
    step = min(a, b)
    if step == b:
        flag = 0
    else:
        flag = 1
    return shell ** 2 + step * 2 + flag

def encrypt(message):
    res = ''
    for i in range(0,len(message),2):
        res += str(pairing(message[i],message[i+1]))
    return res

print(encrypt(flag))
#1186910804152291019933541010532411051999082499105051010395199519323297119520312715722
```

分析代码得知计算方式为：flag每两个字节分别计算，较大者的平方+小者的2倍+标志，结果转成十进制字符串。逆向解出flag没想到算法，选择暴力破解。

flag一般均为可见字符，一开始手动构造了[a-z,A-Z,0-9,_,{,}]，遍及求解即可。a**2+2b+1的取值范围大体计算了下3-5位数之间。

构造代码如下：

```
result = "11869108041522910199335410105324110519990824991050510103951995193232971195203127157 22"
a=['{','}','a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', '
b=a
flag=""
def pairing(a,b):
    shell = max(a, b)
    step = min(a, b)
    if step == b:
        flag = 0
    else:
        flag = 1
    return shell ** 2 + step * 2 + flag
def check(n):
    for i in range(0, len(a), 1):
        for j in range(0, len(b), 1):
            if (str(pairing(ord(a[i]), ord(b[j]))) == n):
                #print("%c%c" % (a[i], b[j]))
                return a[i], b[j]
    return 0,0

p=0
while p<len(result):
    for x in range(3,6):
        n=result[p:p+x]
        r1,r2 = check(n)
        if r1!=0:
            p+=x
            flag += r1+r2
            break;
print(flag)
```

a数组其实简化构造成 a= [i for i in range(48,128)] 字节更全面一些。