2021 XCTF Guesskey

原创

Crazy198410 于 2021-01-19 20:49:58 发布 280 收藏

分类专栏： XCTF 文章标签： 安全

本文链接：https://blog.csdn.net/Crazy198410/article/details/112851943

Guess key

下载附件，是一段代码，分析如下：

```
from random import randint
import os
from flag import flag
N=64
key=randint(0,2**N)  # 0到2的64次方中随机取一整数
print key
key=bin(key)[2:].rjust(N,'0')  # key取二进制，只取64位，左侧补0
count=0
while True:
 p=0
 q=0
 new_key=''
 zeros=[0]
 for j in range(len(key)):
  if key[j]=='0':        #在key中筛选0
   zeros.append(j)    #如果有0，zeros列表就补上0的位置号，最大64，最小0
 p=zeros[randint(0,len(zeros))-1]    #在zeros列表中随机取一个字符串
 q=zeros[randint(0,len(zeros))-1]    #在zeros列表中随机取一个字符串
 try:
  mask=int(raw_input("mask:"))    #输入mask
 except:
  exit(0)
 mask=bin(mask)[2:]               # mask变成二进制
 if p>q:
  tmp=q
  q=p
  p=tmp           #使p<q
 cnt=0
 for j in range(0,N):              # 在key中循环
  if j in range(p,q+1):        # 在p到q中循环
   new_key+=str(int(mask[cnt])^int(key[j]))    #如果j在p到q中，则newkey +=(mask中的值与key中的值异或)
  else:
   new_key+=key[j]          # 如果j不在p到q中，则直接将key赋值给newkey
  cnt+=1
  cnt%=len(mask)
 key=new_key
 try:
  guess=int(raw_input("guess:"))
 except:
  exit(0)
 if guess==int(key,2):
  count+=1
  print 'Nice.'
 else:
  count=0
  print 'Oops.'
 if count>2:
  print flag
```

在下面这段代码中：

```
for j in range(0,N):              # 在key中循环
  if j in range(p,q+1):        # 在p到q中循环
   new_key+=str(int(mask[cnt])^int(key[j]))    #如果j在p到q中，则newkey +=(mask中的值与key中的值异或)
  else:
   new_key+=key[j]          # 如果j不在p到q中，则直接将key赋值给newkey
```

发现只有当j 在p和q之间时，newkey会与原来的key不一样。而且变换机制是由我们的输入决定的，所以我们就要控制我们的输入，尽可能的减少改变。
发现当我们使mask为“0”时，newkey与原来key一致。而且，当我nc连接时，会将原来的key反馈给我们。这样，我们就能得到flag了。