HABOOB

BCTF 2018 WRITE-UP

Crypto – Guess Polynomial

CHALLENGE DESCRIPTION

Guess Polynomial

nc 39.96.8.114 9999

The server code is given.

SOLUTION

The server will generate an array of random numbers then will ask to provide a number to guess the array. After reading the code we provide a number that will be the sum of all elements in the array by the following code.

```
def calc(coeff, x):
    num = coeff[0]
    for i in range(1, len(coeff)):
        num = num * x + coeff[i]
    return num
```

After we provide a large number (1e+51) a pattern will emerge that will be possible to reverse the sum of all elements in the array.

As shown in the following screenshots.

```
263635555626195999387428350000000000000000001486130883346470483878
037272629500000000000000000001423055368157062743332140086341000000
000000000000026178400229174400421381149321620000000000000000000364
552243805904445416720886169800000000000000000001739097278065968256
480242786315000000000000000000018628143927644220096253288371471000 0
000000000000015880279248137598856616113959983000000000000000000000
490529552326921512996538526304000000000000000000011040725698102714 6
062260065232980000000000000000000161584432940259423219420967757930 0
000000000000000009090454102207311468263769377587000000000000000000
052968937881858926518015514763800000000000000000015216308897128 74
947963961742544400000000000000000123720654932843615885773584342 27
000000000000000001633967095785797126423577673516 6
```

The last number is highlighted in the figure above and our strategy to guess the array is to subtract the last number from the sum then will divide the remaining sum by the large number provided above. This method will be repeated until there is no remaining number in the sum.

We developed a code to do all these steps.

The code is provided below.

```
from netcat import Netcat
guess_number = long("10000000000000000000000000000000000000000000000000")

def get_last_number(remaining_sum):
    last_number = ""
    y = 0
    for i in xrange(len(remaining_sum)-1, -1 , -1):
        y = i
    # try to figure out the end out an number
    if remaining_sum[i-5:i] == "00000":
            break
        last_number = remaining_sum[i] + last_number
    if(len(remaining_sum) > 37):
        last_number = remaining_sum[y] + last_number

    return long(last_number)
loop = 0
while (loop < 10):
    print "LOOP: " + str(loop)
    if(loop == 0):
    # connect to the server thrugh netcat lib
        nc = Netcat('39.96.8.114', 9999)
        nc.read_until('Please input your number to guess the coeff:')

    nc.write(str(guess_number) + '\n')
    data = nc.read_until("It is your time to guess the coeff!")
    data = data.replace("This is the sum: ", "")
    data = data.replace("It is your time to guess the coeff!", "")

    sum = data
    cof = ""
    for i in range( 0, 120):
        if long(sum) == 0 or long(sum) == -1:
            continue
        last_number = get_last_number(sum)
        cof = str(last_number) + str(" ") + cof
    # eliminate last number by subtract it from the sum then divide by guess
number
    sum = str(long(long(sum) - long(last_number))/long(guess_number))
    print cof
    nc.write( cof + "\n")
    print nc.read(100)
    loop = loop + 1
```

The code file will be attached.

References

Netcat library https://gist.github.com/leonjza/f35a7252babdf77c8421