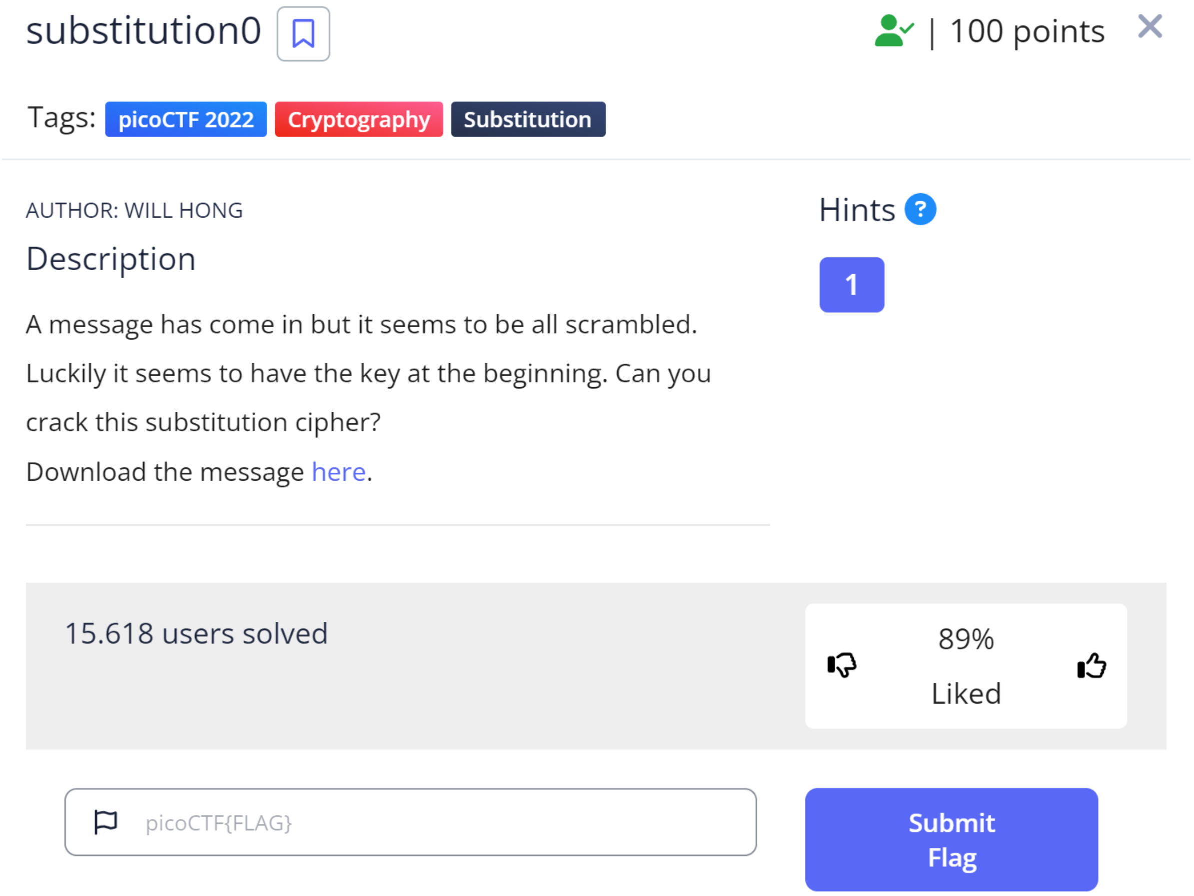
This is a writeup of the picoCTF challenge called substitution0

The challenge is from the picoCTF 2022, and it is worth 100 points.

This is what it looks like



substitution0

| 100 points

Tags: picoCTF 2022 Cryptography Substitution

AUTHOR: WILL HONG

Description

A message has come in but it seems to be all scrambled. Luckily it seems to have the key at the beginning. Can you crack this substitution cipher?

Download the message here.

Hints

1

15.618 users solved

89%

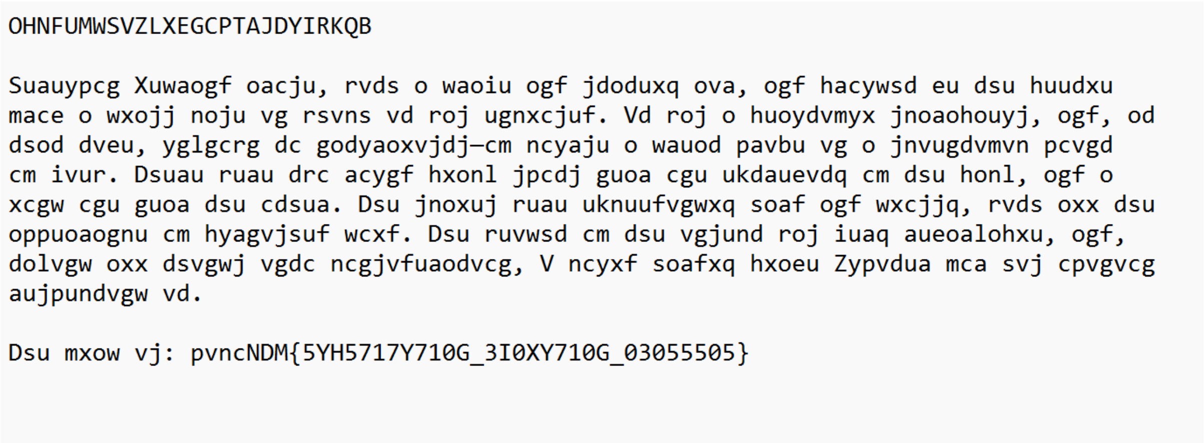
Liked

picoCTF{FLAG}

Submit Flag

As you can see, we have been provided a file with a message, and the description says that there is a key at the beginning of it.

Let’s take a look at the text



```
OHNFUMWSVZLXEGCPTAJDYIRKQB

Suauypcg Xuwaogf oacju, rvds o waoiu ogf jdoduxq ova, ogf hacywsd eu dsu huudxu
mace o wxojj noju vg rsvns vd roj ugnxcjuf. Vd roj o huoydvmyx jnoaohouyj, ogf, od
dsod dveu, yglgcrg dc godyaoxvjdj—cm ncyaju o wauod pavbu vg o jnvugdvmvn pcvgd
cm ivur. Dsuau ruau drc acygf hxonl jpcdj guoa cgu ukdauevdq cm dsu honl, ogf o
xcgw cgu guoa dsu cdsua. Dsu jnoxuj ruau uknuufvgwxq soaf ogf wxcjjq, rvds oxx dsu
oppuoaognu cm hyagvjsuf wcxf. Dsu ruvwsd cm dsu vgjund roj iuaq aueoalohxu, ogf,
dolvgw oxx dsvgwj vgdc ncgjvfuaodvcg, V ncyxf soafxq hxoeu Zypvdua mca svj cpvgvcg
aujpundvgw vd.

Dsu mxow vj: pvncNDM{5YH5717Y710G_3I0XY710G_03055505}
```

As you can see, the text makes no sense, but the key is in the beginning of the text.

Copy the key and open up your linux terminal.

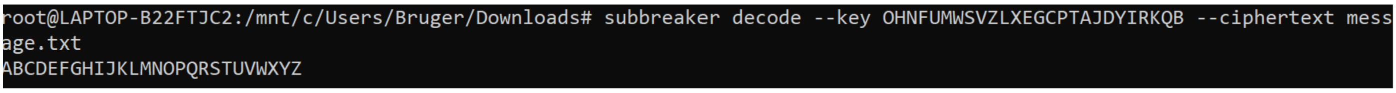
We know it’s a substitution cipher because of the title and the fact that we have a key to decode it. For substitution ciphers, I like to use a tool called subbreaker to decode it.

If you don’t have subbreaker installed, you can install it by using the command:

pip install subbreaker

Once you have the tool, make sure you are in the same directory as the file message.txt, and use this command:

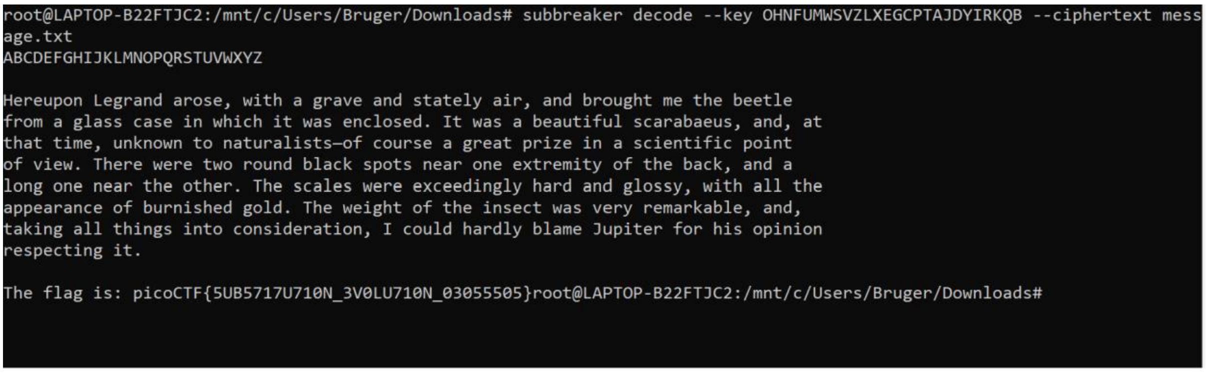
subbreaker decode --key (your key – it might not be the same as mine) --ciphertext message.txt



```
root@LAPTOP-B22FTJC2:/mnt/c/Users/Bruger/Downloads# subbreaker decode --key OHNFUMWSVZLXEGCPTAJDYIRKQB --ciphertext mess
age.txt
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

This tells the subbreaker tool that you want to decode something. It also tells it the key, and the ciphertext to decode.

Now it should give this output:



```
root@LAPTOP-B22FTJC2:/mnt/c/Users/Bruger/Downloads# subbreaker decode --key OHNFUMWSVZLXEGCPTAJDYIRKQB --ciphertext mess
age.txt
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Hereupon Legrand arose, with a grave and stately air, and brought me the beetle
from a glass case in which it was enclosed. It was a beautiful scarabaeus, and, at
that time, unknown to naturalists—of course a great prize in a scientific point
of view. There were two round black spots near one extremity of the back, and a
long one near the other. The scales were exceedingly hard and glossy, with all the
appearance of burnished gold. The weight of the insect was very remarkable, and,
taking all things into consideration, I could hardly blame Jupiter for his opinion
respecting it.

The flag is: picoCTF{5UB5717U710N_3V0LU710N_03055505}root@LAPTOP-B22FTJC2:/mnt/c/Users/Bruger/Downloads#
```

And there at the bottom you can see the flag.

The flag is: picoCTF{5UB5717U710N_3V0LU710N_03055505}