攻防世界_Crypto_sherlock

原创

好想变强啊 已于 2022-03-31 11:13:58 修改 4255 收藏

分类专栏： 攻防世界刷题记录 文章标签： 网络安全 python

于 2022-03-31 11:03:32 首次发布

本文链接：https://blog.csdn.net/qq_38798840/article/details/123852537

攻防世界刷题记录Crypto篇

文章目录

前言

继续高手进阶区题目~sherlock

咦？夏洛克？

下载题目附件得到的是一个内容很长很长的txt文件，大体看了看就是很常规的英语文章，不过有一些突然大写的字母。感觉可能是需要提取出来什么吧，一看别人写的wp确实是要先筛出来文章里的大写字母。在这里顺便学到了如何在命令行里筛选出文件内容，好在mac和Linux命令可以通用呀。

解题步骤

1.筛选出文中的大写字母

先把题目附件改名为sherlock.txt，在该文件路径下打开终端，输入如下命令：

```
cat sherlock.txt | grep -o '[A-Z]' | tr -d '\n'
```

形如“命令A | 命令B”的这种Linux命令是把A执行的结果作为B的输入，所以这行完整命令的执行过程是将sherlock.txt的文件内容筛选出大写字母再去掉换行显示出来。（个人理解，如有错误欢迎指出）
这行命令也是从别人的wp学来的，好像还看见过更复杂的命令，只要能解题就先怎么简单怎么来吧！
得到的结果如下图所示，观察发现全都是ZERO和ONE这两个单词，所以想到下一步把它们转换成用数字0和1显示。

```
% cat sherlock.txt | grep -o '[A-Z]' | tr -d '\n'
ZEROONEZEROZEROZEROZEROONEZEROZEROONEZEROZEROONEZEROZEROONEZEROONEZEROONEZEROONE
ZEROZEROZEROONEZEROONEZEROZEROONEONEZEROONEZEROZEROZEROZEROONEONEZEROONEZEROONEZ
EROONEZEROZEROZEROONEZEROZEROZEROONEONEZEROZEROONEONEONEONEZEROONEONEZEROONEONEZ
EROONEZEROZEROZEROZEROZEROONEONEZEROZEROZEROONEZEROONEONEZEROZEROONEZEROZEROZERO
ZEROONEONEZEROZEROONEONEZEROONEZEROONEONEONEONEONEZEROZEROONEONEZEROZEROZEROONEZ
EROONEONEZEROONEONEONEZEROZEROONEZEROONEONEONEONEONEZEROONEONEONEZEROZEROZEROZER
OZEROONEONEZEROONEONEZEROZEROZEROZEROONEONEZEROONEZEROZEROZEROZEROONEONEZEROZERO
ZEROONEZEROONEONEZEROONEONEONEZEROZEROONEZEROONEONEONEONEONEZEROZEROONEONEZEROON
EZEROONEZEROZEROONEONEZEROZEROZEROONEZEROZEROONEONEZEROONEONEONEZEROZEROONEONEZE
ROZEROONEONEZEROONEONEONEONEONEZEROONE%
```


2.借助Python处理字符串

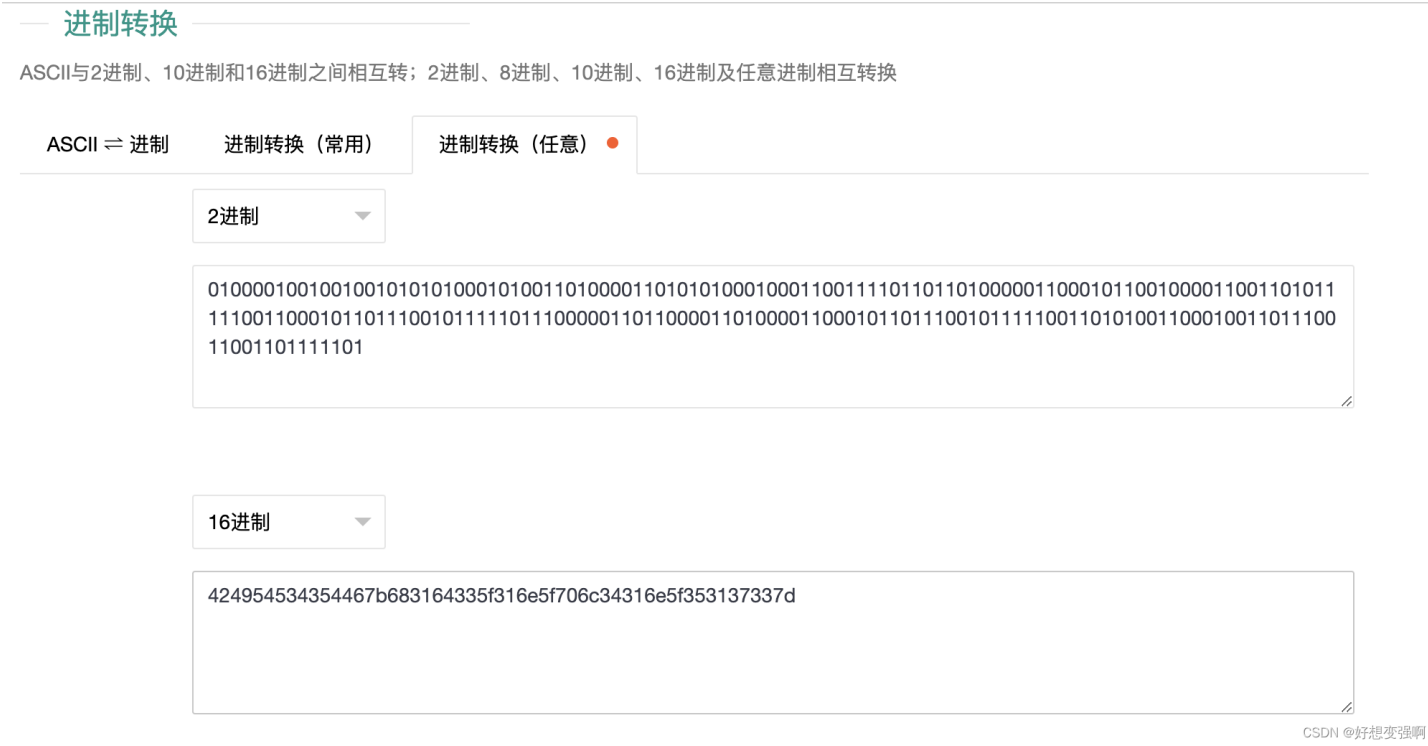
打开Python交互式编程，将ZERO和ONE转换成0和1显示出来：

```
>>> s='ZEROONEZEROZEROZEROZEROONEZEROZEROONEZEROZEROONEZEROZEROONEZEROONEZEROONE
ZEROONEZEROZEROZEROONEZEROONEZEROZEROONEONEZEROONEZEROZEROZEROZEROONEONEZEROONEZ
EROONEZEROONEZEROZEROZEROONEZEROZEROZEROONEONEZEROZEROONEONEONEONEZEROONEONEZERO
ONEONEZEROONEZEROZEROZEROZEROZEROONEONEZEROZEROZEROONEZEROONEONEZEROZEROONEZEROZ
EROZEROZEROONEONEZEROZEROONEONEZEROONEZEROONEONEONEONEZEROZEROONEONEZEROZEROZ
EROONEZEROONEONEZEROONEONEONEZEROZEROONEZEROONEONEONEONEONEZEROONEONEONEZEROZERO
ZEROZEROZEROONEONEZEROONEONEZEROZEROZEROZEROONEONEZEROONEZEROZEROZEROZEROONEONEZ
EROZEROZEROONEZEROONEONEZEROONEONEONEZEROZEROONEZEROONEONEONEONEONEZEROZEROONEON
EZEROONEZEROONEZEROZEROONEONEZEROZEROZEROONEZEROZEROONEONEZEROONEONEONEZEROZEROO
NEONEZEROZEROONEONEZEROONEONEONEONEONEZEROONE'
>>> i=0
>>> while i<len(s):
...     if(s[i] == 'Z'):
...         print(0,end='')
...         i+=4
...     else:
...         print(1,end='')
...         i+=3
...
0100001001001001010101000101001101000011010101000100011001111011011010000011000 1
0110010000110011010111110011000101101110010111110111000001101100001101000001100 1
0110111001011111001101010011000100110111001100110111111 01>>>
```


因为只涉及到两个单词，所以就两种情况用if...else语句即可，关键代码很简单：

```
i=0
while i<len(s):
    if(s[i] == 'Z'):
        print(0,end='')
        i+=4
    else:
        print(1,end='')
        i+=3
```

以0和1显示后，想到借助在线网页工具做一下进制转换，转成16进制比较好用Python恢复成bytes。比较喜欢用的网站在这：http://www.hiencode.com/



然后复制出来16进制数，放到Python的bytes.fromhex中得到flag啦！

```
>>> bytes.fromhex('424954534354467b683164335f316e5f706c34316e5f353137337d')
b'BITSCTF{h1d3_1n_pl41n_5173}'
```

```
bytes.fromhex('424954534354467b683164335f316e5f706c34316e5f353137337d')
```

总结

有时候会懒得去搜索去学新东西，比如暂时还不知道在Python里是不是直接就能做进制转换，只要能解决问题，就想到啥用啥了。继续学习吧。