# stegano的writeup

MarcusRYZ 于 2020-02-11 13:33:03 发布 513 收藏

分类专栏： 攻防世界MISC新手练习区 文章标签： 安全

本文链接：https://blog.csdn.net/MarcusRYZ/article/details/104260814

版权

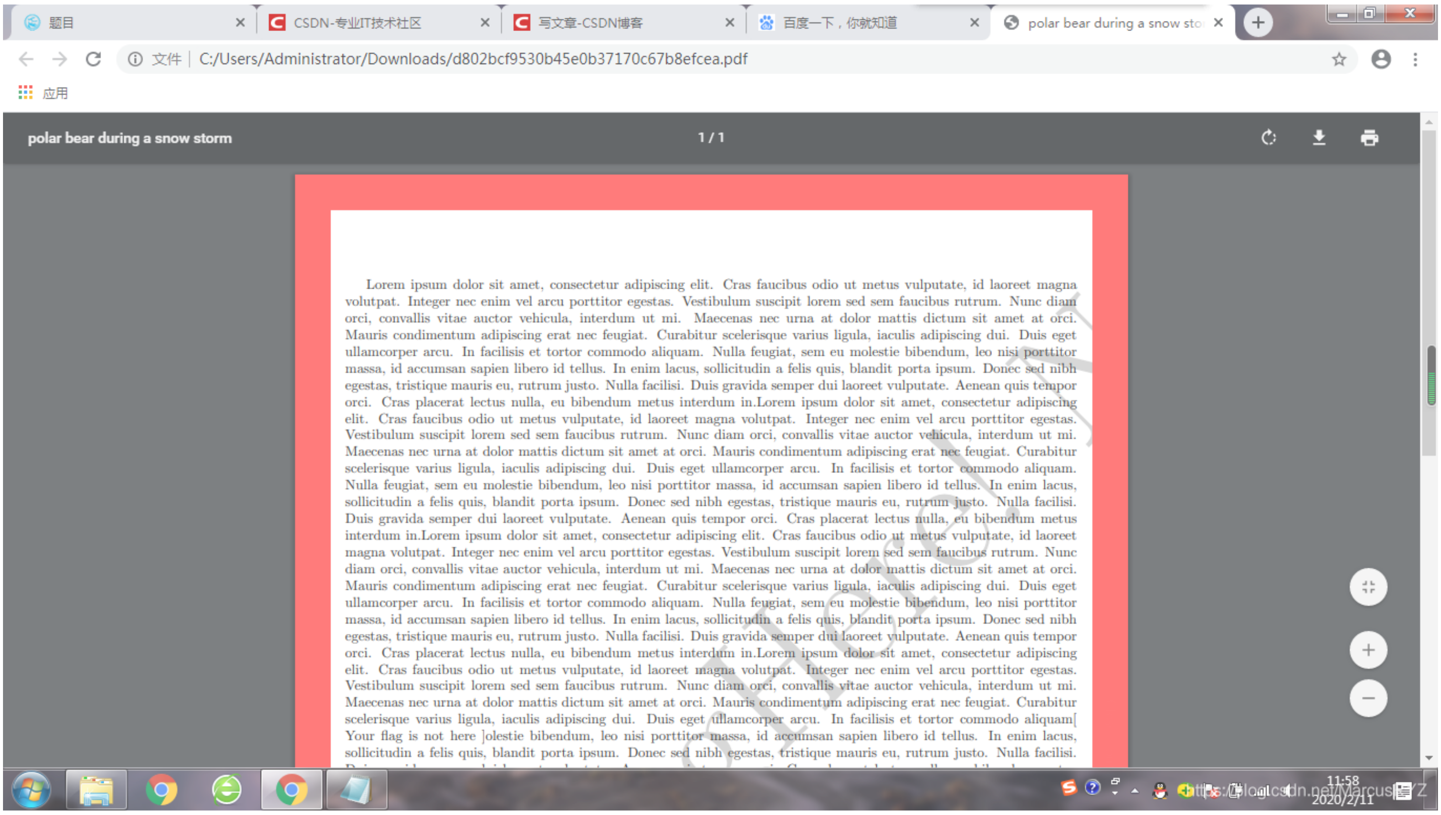
攻防世界MISC新手练习区 专栏收录该内容

12 篇文章 0 订阅

订阅专栏

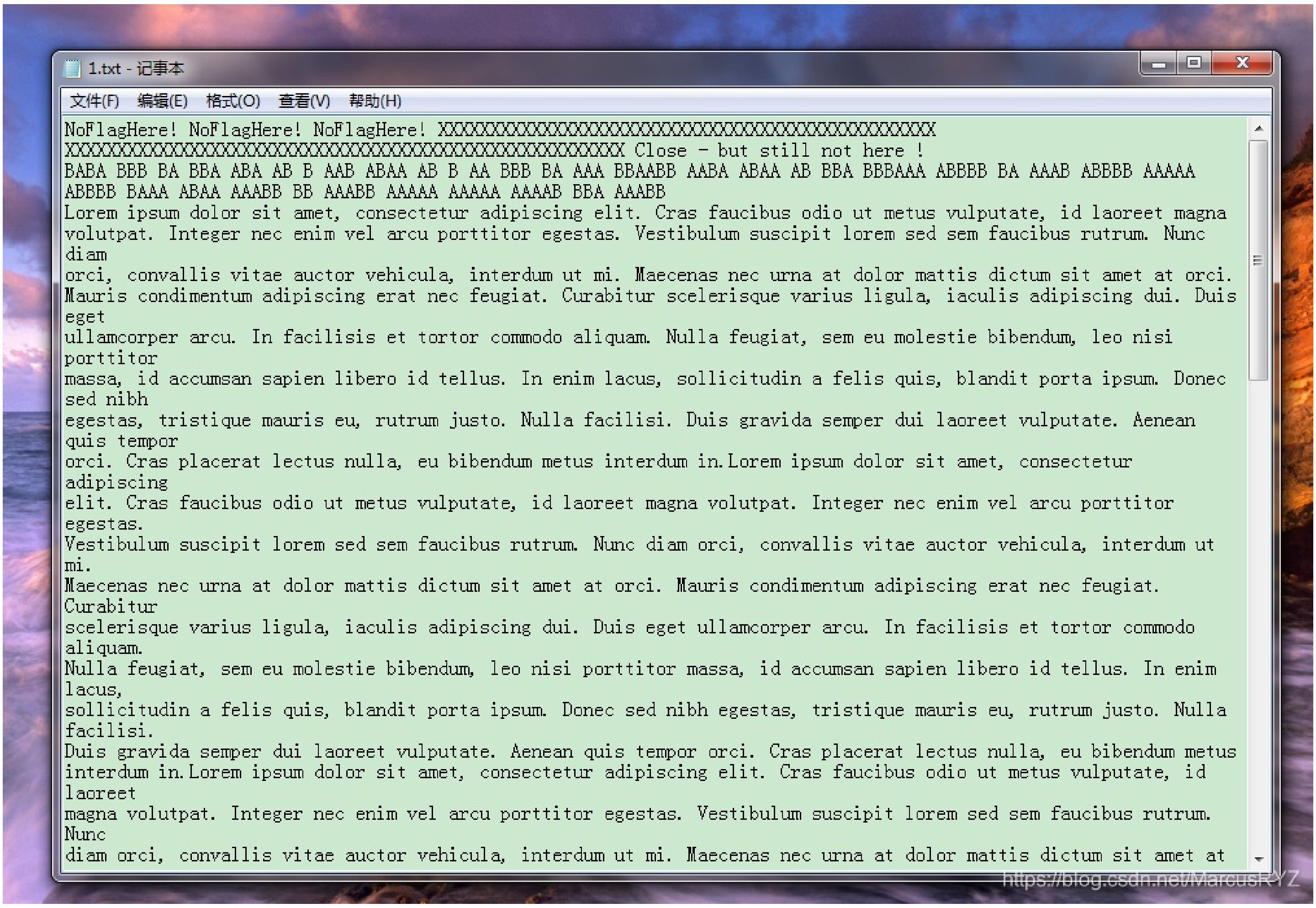
大家好，这次为大家带来的是攻防世界misc部分stegano的writeup。

先下载附件，是一个pdf文件，打开这个文件。


题目
CSDN-专业IT技术社区
写文章-CSDN博客
百度一下，你就知道
polar bear during a snow sto
文件 | C:/Users/Administrator/Downloads/d802bcf9530b45e0b37170c67b8efcea.pdf
应用
polar bear during a snow storm
1 / 1
https://blog.csdn.net/MarcusRYZ
11:58
2020/2/11

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam[ Your flag is not here ]olestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi.

发现这是一篇很普通的英语文章，没有任何关于flag的信息。于是我抱着试试看的心理，全选这个pdf的内容复制，然后粘贴到记事本上。



```
NoFlagHere! NoFlagHere! NoFlagHere! XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX Close - but still not here !
BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA
ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna
volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc
diam
orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci.
Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis
eget
ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi
porttitor
massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec
sed nibh
egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean
quis tempor
orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur
adipiscing
elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor
egestas.
Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut
mi.
Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat.
Curabitur
scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo
aliquam.
Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim
lacus,
sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla
facilisi.
Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus
interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id
laoreet
magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum.
Nunc
diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at
```

果然，发现一串很有特点的字符：BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB。这串字符只由A和B组成，且以空格分开，长短不一。马上想到摩斯密码，即将A看成点，将B看成杠。于是将这串字符复制粘贴到一个新的记事本上，再用python写个脚本解密一下。

```python
def decoding(strings):
    i = 0
    s = ""
    strings += " "
    de = ""
    dict = {"AB": "A", "BAAA": "B", "BABA": "C", "BAA": "D", "A": "E", "AABA": "F", "BBA": "G", "AAAA": "H", "AA": "I", "ABBB": "J", "BAB": "K", "ABAA": "L", "BB": "M", "BA": "N", "BBB": "O", "ABBA": "P", "BBAB": "Q", "ABA": "R", "AAA": "S", "B": "T", "AAB": "U", "AAAB": "V", "ABB": "W", "BAAB": "X", "BABB": "Y", "BBAA": "Z", "ABBBB": "1", "AABBB": "2", "AAABB": "3", "AAAAB": "4", "AAAAA": "5", "BAAAA": "6", "BBAAA": "7", "BBBAA": "8", "BBBBA": "9", "BBBBB": "0"}
    while i <= len(strings) - 1:
        if strings[i] == " ":
            if len(s) <= 5:
                de += dict[s]
            s = ""
        else:
            s += strings[i]
        i += 1
    return de
path = input("输入TXT文档所在文件夹： ")
filename = input("输入TXT文档名： ")
f = open(path + "\\" + filename + ".txt", "r").read().strip()
flag = decoding(f)
f = open(path + "\\" + "result.txt", "w")
f.write(flag)
```

呃，这道题有点小坑，字符串中的BBAABB和BBBAAA是无效的，编脚本时要注意。

运行一下程序，输出一串字符：CONGRATULATIONSFLAG1NV151BL3M3554G3。所以，flag：1NV151BL3M3554G3。