

攻防世界crypto高手题之sherlock

原创

[沐一·林](#) 于 2021-09-10 12:35:20 发布 94 收藏 1

分类专栏: [CTF 密码学](#) 文章标签: [ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/xiao__1bai/article/details/120219516

版权



[CTF](#) 同时被 2 个专栏收录

167 篇文章 6 订阅

订阅专栏



[密码学](#)

51 篇文章 1 订阅

订阅专栏

[攻防世界crypto高手题之sherlock](#)

继续开启全栈梦想之逆向之旅~

这题是攻防世界crypto高手题的sherlock

The screenshot shows the header of a CSDN article titled 'sherlock'. It features a dark blue background with white text. At the top left, the title 'sherlock' is displayed in a large font. To its right, there is a thumbs-up icon with the number '6', followed by the text '最佳Writeup由系统战队 • admin提供'. On the far right, there are two green buttons: 'WP' and '建议'. Below the title, the '难度系数' (Difficulty Coefficient) is shown as '★★★2.0'. The '题目来源' (Source) is 'bitsctf-2017'. The '题目描述' (Description) and '题目场景' (Scenario) are both listed as '暂无' (None). The '题目附件' (Attachments) section shows a button for '附件1'. At the bottom right of the header, there is a small text credit: 'CSDN @沐一一沐, 一沐沐一'.

(这里积累第一个经验)

下载附件，是一个txt文档，内容是一篇小说。一开始我以为flag藏在关键字里，我还用百度翻译一个个看内容，现在回想起来真的太傻了，查了资料才发现字符中是有异或点的，大写字母就是要提取出来分析的地方：

```
title: the adventures of sherlock holmes
```

```
author: sir arthur conan doyle
```

```
release date: march, 1999 [ebook #1661]  
[most recently updated: november 29, 2002]
```

```
edition: 12
```

```
language: english
```

```
character set encoding: ascii
```

```
*** start of the project gutenberg ebook, the adventures of sherlock holmes ***
```

```
(additional editing by jose menendez)
```

参考了别人的命令写了自己的提取大写 shell 命令：

```
cat 1.txt | grep -o [A-Z] | tr -d '\n'
```

其中：

grep -o 只显示匹配到的字符串

tr -d 删除指定字符，不删除换行符的话就很长的打竖显示。

结果：

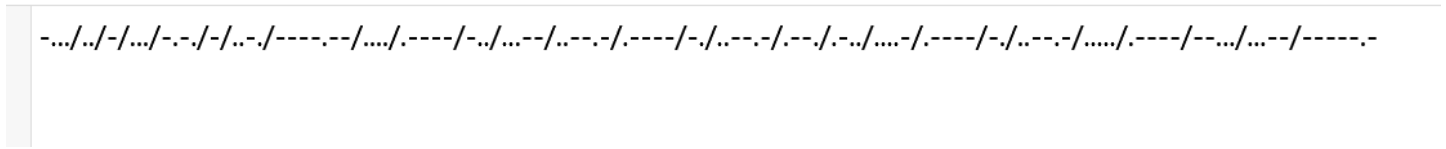
```
$ cat 1.txt | grep -o [A-Z] | tr -d '\n'
ZEROONEZEROZEROZEROZEROONEZEROZEROONEZEROZEROONEZEROZEROONEZEROONEZEROONEZEROZEROZERO
ONEZEROONEZEROZEROONEONEZEROONEZEROZEROZEROONEONEZEROONEZEROONEZEROONEZEROZEROZEROONEZER
OZEROZEROONEONEZEROZEROONEONEONEONEZEROONEONEZEROONEONEZEROONEZEROZEROZEROZEROONEONEZERO
ZEROZEROONEZEROONEONEZEROZEROONEZEROZEROZEROZEROONEONEZEROONEONEZEROONEONEONEONEONE
NEZEROZEROONEONEZEROZEROZEROONEZEROONEONEZEROONEONEONEZEROZEROONEZEROONEONEONEONEONE
NEONEZEROZEROZEROZEROZEROONEONEZEROONEONEZEROZEROZEROZEROONEONEZEROONEZEROZEROZEROONEONE
ZEROZEROZEROONEZEROONEONEZEROONEONEONEZEROZEROONEZEROONEONEONEONEONEZEROZEROONEONEZERO
OONEZEROZEROONEONEZEROZEROZEROONEZEROZEROONEONEZEROONEONEONEZEROZEROONEONEZERO
ONEONEONEONEONEZEROONE
```

CSDN @沐一一沐，一沐沐一

(这里积累第二个经验)

然后可以发现都是ZERO和ONE的单词，不是二进制字符串就是摩斯密码，可是摩斯密码要空格，这里没有，所以是二进制字符串。

附上摩斯密码举例：



然后就是自己写python脚本转换01率，一开始用for语句卡了一下，后来直接换while语句：

```
key1="ZEROONEZEROZEROZEROZEROONEZEROZEROONEZEROZEROONEZEROZEROONEZEROONEZEROONEZEROZEROZEROONEZEROONEZERO
ZEROONEONEZEROONEZEROZEROZEROZEROONEONEZEROONEZEROONEZEROONEZEROZEROZEROONEONEZEROONEONEONEONEONEONEONE
EZEROONEONEZEROONEONEZEROONEZEROZEROZEROZEROZEROONEONEZEROZEROZEROONEZEROONEONEZEROZEROZEROZEROONEONE
ZEROZEROONEONEZEROONEONEONEONEONEONEONEZEROZEROONEONEZEROZEROZEROONEONEZEROONEONEZEROONEONEONEZEROONEONE
EONEONEONEZEROONEONEONEZEROZEROZEROZEROZEROONEONEZEROONEONEZEROZEROZEROZEROONEONEZEROONEZEROZEROZEROONEONEZE
ROZEROZEROONEZEROONEONEZEROONEONEONEZEROZEROONEZEROONEONEONEONEONEZEROZEROONEONEZEROONEZEROONEONEZERO
ZEROZEROONEZEROZEROONEONEZEROONEONEONEZEROZEROONEONEZEROZEROONEONEONEONEONEONEZEROONE"
flag=""
i=0
while i<len(key1):
    if key1[i]=='Z'and key1[i+1]=='E'and key1[i+2]=='R'and key1[i+3]=='O':
        i+=4
        flag+='0'
    else:
        flag+='1'
        i+=3
print(flag)
```

结果:

```
└─$ python 1.py
01000010010010010101010001010011010000110101010001000110011110110110100000110001011001000011
00110101111100110001011011100101111101110000011011000011010000110001011011100101111100110101
00110001001101110011001101111101
```

总结:

1:
(这里积累第一个经验)
下载附件, 是一个txt文档, 内容是一篇小说。一开始我以为flag藏在关键字里, 我还用百度翻译一个个看内容, 现在回想起来真的太傻了, 查了资料才发现字符中是有异或点的, 大写字母就是要提取出来分析的地方。

2:
(这里积累第二个经验)
然后可以发现都是ZERO和ONE的单词, 不是二进制字符串就是摩斯密码, 可是摩斯密码要空格, 这里没有, 所以是二进制字符串。

解毕! 敬礼!