

# 攻防世界Crypto新手练习

原创

彼岸花苏陌 于 2020-04-14 20:36:30 发布 856 收藏 2

分类专栏: [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/qq\\_42263820/article/details/105519372](https://blog.csdn.net/qq_42263820/article/details/105519372)

版权



[ctf](#) 专栏收录该内容

39 篇文章 1 订阅

订阅专栏

无题

[base64](#)

[Caesar](#)

[Morse](#)

[混合编码](#)

[Railfence](#)

## base64

下得附件, 扔进base64加密解密里面  
就得到flag

```
Y31iZXJwZWJjZXtXZWxjb21  
lX3RvX251d19Xb3JsZCF9
```

请将要加密或解密的内容复制到以下区域

[BASE64加密](#)

[BASE64解密](#)

[https://blog.csdn.net/qq\\_42263820](https://blog.csdn.net/qq_42263820)

## Caesar

读标题，caesar翻译过来就是凯撒，得知是凯撒密码

拿到附件，把文字贴到解密区（不知道位移是多少？一个一个试）最后得知位移为12位

```
oknqdbqmoq{kag_tmhq_xqmdzqp_omqemd_qzodkbfuaz}
```

位移 12



加密

解密

```
cyberpeace{you_have_learned_caesar_encryption}
```

[https://blog.csdn.net/qq\\_42263820](https://blog.csdn.net/qq_42263820)

**Morse**

一看题目就知道是摩斯电码

拿到附件，打开一看，怎么全是0和1组合？

思考一下，0应该代表的是摩斯电码中的圆点，1代表着一杠，那就简单了

文字替换工具替换完成后

需要替换的文字:  (多个可用#号)

替换为:  (多个可用#号,每个对应)

```
11 111 010 000 0 1010 111 100 0 00 000 000 111 00 10 1 0 010 0 000 1 00 10 110
```

批量替换

-- --- .- . . . . - . - . --- - . . . . . --- . . - . - . . . . . - . . . . .

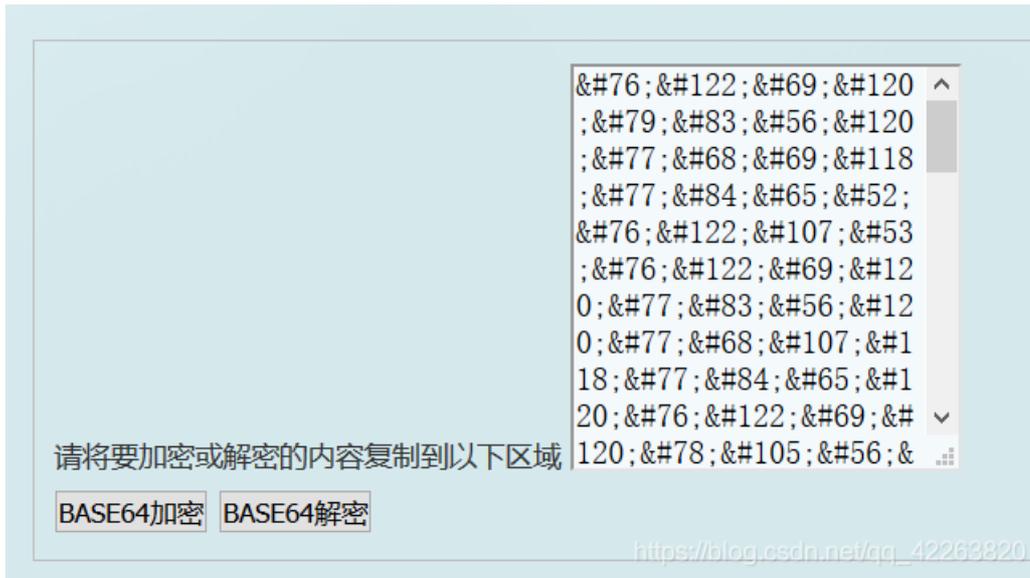
[https://blog.csdn.net/qq\\_42263820](https://blog.csdn.net/qq_42263820)

放进摩斯电码转换中



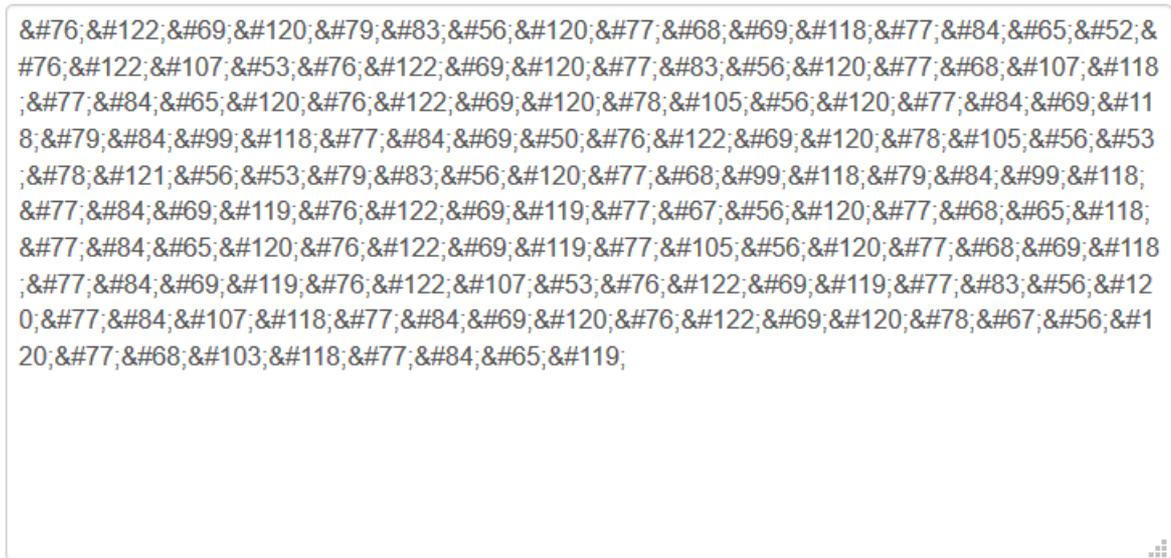
打开文件看一下，知道是base64格式的，放进base64解密

解密完发现这个：



了解到是decode编码后

放进html解码中

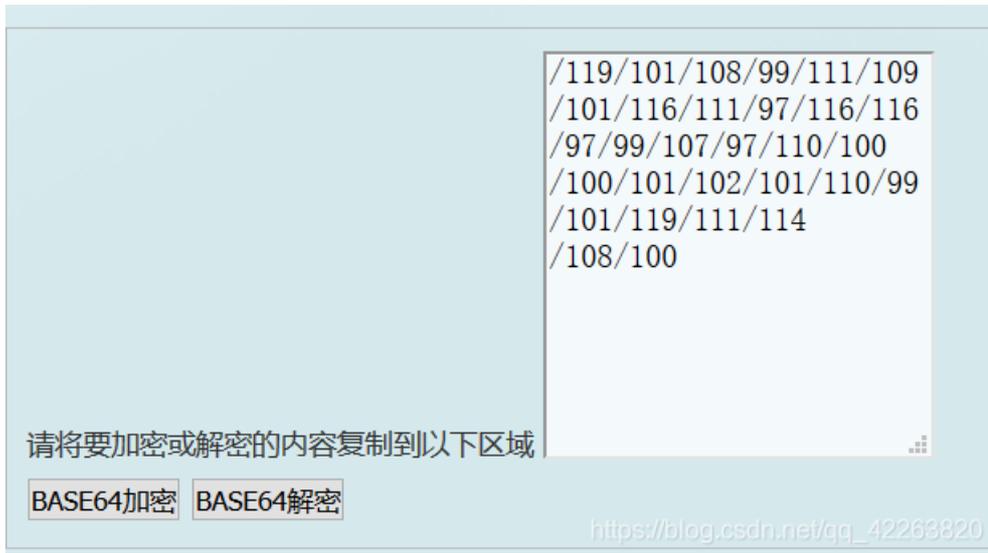


### 复制你的HTML这里解码的文本：



发现解码后好像又绕回base64解码了...

再放进bsase64解密



发现是数字形式，而且都在96-123之间

那就又绕回了html 编码形式，那怎么改呢？

这里可以巧妙一点，把/直接替换成;&#，然后把最前面的;去掉，最后面加个;即可

需要替换的文字:  (多个可用#号)

替换为:  (多个可用#号,每个对应)

```
/119/101/108/99/111/109/101/116/111/97/116/116/97/99/107/97/110/100/100/101/102/101/110/99/101/119/111/114/108/100
```

批量替换

```
;&#119;&#101;&#108;&#99;&#111;&#109;&#101;&#116;&#111;&#97;&#116;&#116;&#97;&#99;&#107;&#97;&#110;&#100;&#100;&#101;&#102;&#101;&#110;&#99;&#101;&#119;&#111;&#114;&#108;&#100
```

[https://blog.csdn.net/qq\\_42263820](https://blog.csdn.net/qq_42263820)

最后再放入HTML解码中

即可得到flag，最后填好cyberpeace{解码后的flag}

Raifence

题目是rail fence，翻译后得知是栅栏，那这题就是栅栏密码

问题

打开文件看一下，把带解码的文字放入栅栏密码解密中题目中也提示了5，那栅栏的每组字数就是5

```
ccehgyaefnpeoobe{lcirg}epriec_ora_g
```

每组字数 5



加密

解密

```
cebgccfe}_en{eohplprgecrayoi}_aoreg
```

[https://blog.csdn.net/qq\\_42263820](https://blog.csdn.net/qq_42263820)

解密完的我：??????

不对吗？

后面考虑了下，栅栏密码的原理就是取一定数字的字母组成一组，然后按每组第一个，每一组第二个依次来排序从而进行加密再回头看源码和flag的标准格式cyberpeace{}，得知c和y一定是每组第一个再看源码，没错啊??????

别急，认真考虑下，是不是不是栅栏密码？

随后百度了解到栅栏密码有传统型和W型，一下释然，

使用W型栅栏解密进行解密，栏数设置为5得到flag、

明文:

```
cyberpeace{railfence_cipher_gogogo}
```

栏数:

5

加密

解密

密文:

```
ccehgyaefnpeoobe{lcirg}epriec_ora_g
```

[https://blog.csdn.net/qq\\_42263820](https://blog.csdn.net/qq_42263820)

## 附Railfence的第二种解法（来源于百度）

不得不说这种方法能想到确实很厉害

在得知c和y间隔是5时，考虑是不是非均匀分组，直接按照c, y, b, e, r把源码分开得到：

ccehg

yaefnpeoo

be{lcirg}

epriec\_o

ra\_g

然后按照第一组第一个类推来排？

显然不对，那按照蛇形来排？，第一组和第五组显然太少了

没错，考虑下回形针式解密：12345 4321 2345的类型

把源码来排的话得到这样的片段

1 9 17 25 33

2 8 10 16 18 24 26 32 34

3 7 11 15 19 23 27 31 35

4 6 12 14 20 22 28 30

5 13 21 29

按照这个顺序排列下来，就得到了flag