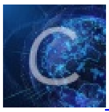
[攻防世界]crypto新手练习区Caesar

原创

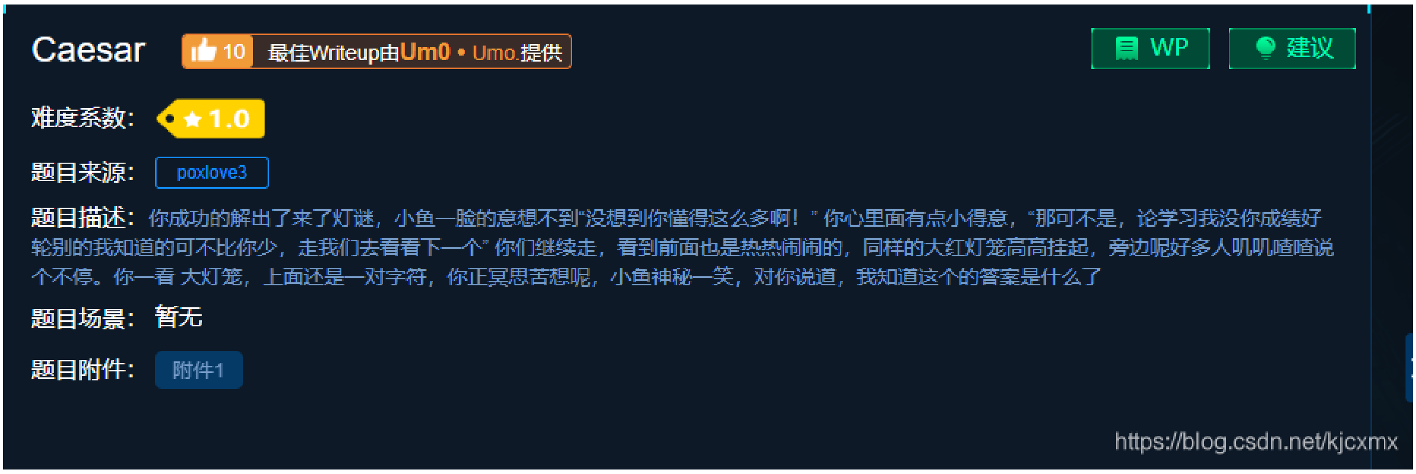
byzf 于 2020-05-03 00:07:15 发布 1449 收藏 3
分类专栏： CTF 安全 文章标签： 攻防世界 密码学 ctf 安全攻防 凯撒密码
kjcxmx
本文链接：https://blog.csdn.net/kjcxmx/article/details/105897544


CTF 同时被 2 个专栏收录
6 篇文章 1 订阅
订阅专栏


安全
9 篇文章 0 订阅
订阅专栏

[攻防世界]crypto新手练习区Caesar

Caesar最佳Writeup由Um0 • Umo.提供



难度系数： 1.0

题目来源： poxlove3

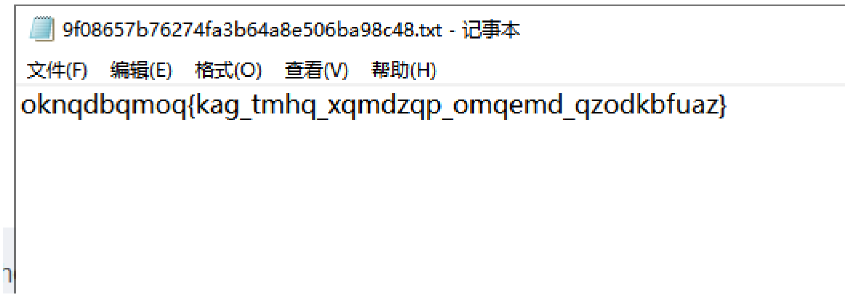
题目描述：你成功的解出了来了灯谜，小鱼一脸的意想不到“没想到你懂得这么多啊！” 你心里面有点小得意，“那可不是，论学习我没你成绩好轮别的我知道的可不比你少，走我们去看看下一个” 你们继续走，看到前面也是热热闹闹的，同样的大红灯笼高高挂起，旁边呢好多人叽叽喳喳说个不停。你一看 大灯笼，上面还是一对字符，你正冥思苦想呢，小鱼神秘一笑，对你说道，我知道这个的答案是什么了

题目场景： 暂无

题目附件： 附件1

附件内容：

```
oknqdbqmoq{kag_tmhq_xqmdzqp_omqemd_qzodkbfuaz}
```



解题

拿到附件内容是一串字母的组合，tiltle提示为凯撒密码。形式像极了flag答案cyberpeace{}，并没有其他编码加密的特征。经过oknqdbqmoq和cyberpeace的对应字母关系，可以推出字母的偏移量是12，如此便得到flag。

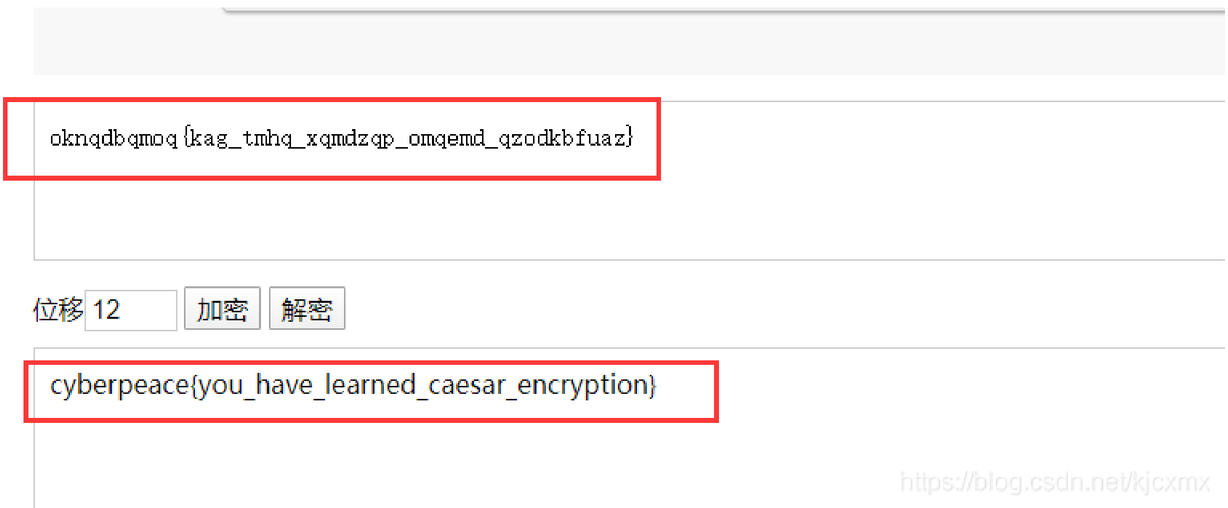
可以选择在线解密

https://www.qqxiuzi.cn/bianma/kaisamima.php

http://www.metools.info/code/c70.html

输入内容和偏移量12后，立即拿到了flag，完成解题。

```
cyberpeace{you_have_learned_caesar_encryption}
```



代码的实现

博主也找了凯撒密码相关的代码实现，如下。

python版本

```
cs= "oknqdbqmoq{kag_tmhq_xqmdzqp_omqemd_qzodkbfuaz}"
b='abcdefghijklmnopqrstuvwxyz'

for key in range(26):
    flag = ''
    for i in cs:
        if i in b:
            num = b.find(i)
            num = num - key

            if num<0:
                num = num + len(b)
            flag = flag + b[num]
        else:
            flag = flag + i
    print('key %s :%s'%(key,flag))
```

什么是凯撒密码呢(百度百科)

在密码学中，**恺撒密码**（英语：Caesar cipher），或称**恺撒加密**、**恺撒变换**、**变换加密**，是一种最简单且最广为人知的加密技术。它是一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。例如，当偏移量是3的时候，所有的字母A将被替换成D，B变成E，以此类推。这个加密方法是以罗马共和时期恺撒的名字命名的，当年恺撒曾用此方法与其将军们进行联系。

博主认为对于凯撒密码，一定要找到偏移量，可以通过字母出现的频率，位置，甚至常用的单词拼音进行求解。用尽办法找出对应的偏移量，即可解题。

特定恺撒密码名称

根据偏移量的不同，还存在若干特定的恺撒密码名称：

偏移量为10：Avocat(A→K)

偏移量为13：ROT13

偏移量为-5：Cassis (K 6)

偏移量为-6：Cassette (K 7)

凯撒密码最早由古罗马军事统帅盖乌斯·尤利乌斯·凯撒在军队中用来传递加密信息，故称凯撒密码。这是一种位移加密方式，只对26个字母进行位移替换加密，规则简单，容易破解。下面是位移1次的对比：

明文字母表	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
密文字母表	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

将明文字母表向后移动1位，A变成了B，B变成了C……，Z变成了A。同理，若将明文字母表向后移动3位：

明文字母表	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
密文字母表	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

则A变成了D，B变成了E……，Z变成了C。

字母表最多可以移动25位。凯撒密码的明文字母表向后或向前移动都是可以的，通常表述为向后移动，如果要向前移动1位，则等同于向后移动25位，位移选择为25即可。

附录：

https://baike.baidu.com/item/%E6%81%BA%E6%92%92%E5%AF%86%E7%A0%81