

CTF实验吧，部分密码学writeup

原创

[0xJoEc001](#) 于 2019-05-23 17:34:16 发布 712 收藏 6

分类专栏: [CTF](#) 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/weixin_43727556/article/details/90484723

版权



[CTF 专栏收录该内容](#)

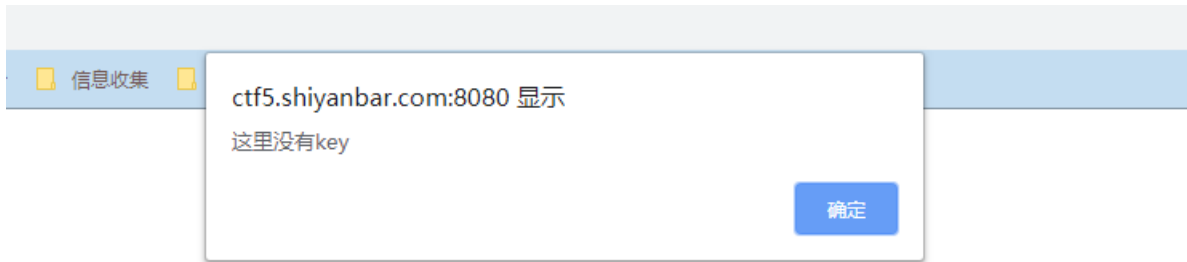
1 篇文章 0 订阅

订阅专栏

1、这里没有key

解题链接: <http://ctf5.shiyanbar.com:8080/4/index.html>

点进去就会有一个弹窗出来



https://blog.csdn.net/weixin_43727556

查看源码, 看到一段密文, 看起来像是VB加密

```
1 <html>
2 <head>
3   <title>大家好</title>
4   <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
5 </head>
6 <body>
7 <br>
8 <br>
9 <center>
10 <script>
11 alert("这里没有key");
12 </script>
13 </center>
14 </body>
15 </html>
16
17 <!-- #0~TgAAAA='[6*1iLa6+pp'aXvfiLaa 6i[[avWi[[a *p[[6*!I'[6 cp'aXvXILa6 fp[:6+Wp[:XvWi[[6+Xi vRIAAA==^#~@ -->
18
```

https://blog.csdn.net/weixin_43727556

VB**解密网站: <https://www.dheart.net/decode/index.php>

JScript/VBScript

JS/VBS/ASP

```
<!--  
#@`TgAAAA=='[6*liLa6++p'aXvfiLaa 6i[[avWi[[a *p[[6*!I'[6 cp'aXvXILa6 fp[:6+Wp[:XvWi[[  
6+XivRIAAA==`#@ -->
```

JS/VBS/ASP

JS/VBS/ASP

```
<!-- Encode@decode -->
```

https://blog.csdn.net/weixin_43727556

**

2、chinese hacker**

解题链接: <http://ctf5.shiyanbar.com/web/2/>

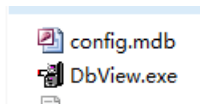
Get The Key
Chinese Hacker

Key Words: 4648

你得到一个数据库 get_the_file
可惜它是加密的, 请解开它并拿到里面的key的内容作为Code1提交。并获得最终KEY1
Check the Code1



自行去下载这个查看数据库的软件



得到文件, 查看数据库, 拿到第一个key: INXW2ZLPNYZDAMJSMJQWE6F=
提交后出现第一个key

Key1: 1GetTheFirst

请返回继续第二题

题目有点坑, 提示的是4648 ——> 46=24 48=32 说明用base32进行解密

用base32对着一段进行解密: INXW2ZLPNYZDAMJSMJQWE6F=

解密后: Comeon2012baby

提交拿到Key2: 2tHEWinNer

chinese hacker 分值: 30

来源: 西普学院 难度: 难 参与人数: 5880人 Get Flag: 1154人 答题人数: 1257人 解题通过率: 92%

那一夜, 你伤害你, 那一夜, 我看见了一堆骷髅头

解题链接: <http://ctf5.shiyanbar.com/web/2/> 通过

1GetTheFirst+2tHEWinNer

提交

https://blog.csdn.net/weixin_43727556

**

3、困在栅栏里的凯撒

**

困在栅栏里的凯撒 分值: 10

来源: 北邮天枢战队 难度: 易 参与人数: 9596人 Get Flag

小白发现了一段很6的字符: NIEyQd{seft}

解题链接: [通过](#)

CTF{tianshu}

https://blog.csdn.net/weixin_43727556

六行二列

N I

E y

Q d

{ s

e f

u }

解到: NEQ{etlydsf}

用凯撒加密位移15位

凯撒密码加密解密

NEQ {etIydsf}

位移

CTF{tiXnshu}

https://blog.csdn.net/weixin_43727556

这里有个坑, 把 CTF{tiXnshu}提交flag不正确
于是他要把里面'X'替换成别的字母。

正确flag: CTF{tianshu}

**

4、我喜欢培根

**

解题链接: <http://ctf5.shiyanbar.com/crypto/enc1.txt>

点进去看到一大串的莫尔斯电码

----- /-----
----- /-----

对其进行解密

莫尔斯电码

Morse code

----- /-----
----- /-----

编码

解码

morse_is_cool_but_bacon_is_cooler_dcdcccdcdcdcccdccccccccddcdcccdcccccdcccdcccdcccdcccdccddcdcd

https://blog.csdn.net/weixin_43727556

回想到题目说道培根, 猜测会不会有这样一种加密方式

用浏览器一查, 果然有这样一种加密方式, 只不过加密的字母只能是a和b

培根密码, 又名**倍康尼密码** (英语: Bacon's cipher) 是由法兰西斯·培根发明的一种**隐写术**。

中文名	培根密码	发明者	法兰西斯·培根
外文名	Bacon's cipher	属性	隐写术
别称	倍康尼密码	学科	密码学

目录

- 1 原理
- 2 特点
- 3 例子
- 4 培根与莎士比亚

原理

编辑

加密时, **明文**中的每个字母都会转换成一组五个英文字母。其转换依靠下表:

A/a	aaaaa	H/h	aabbb	O/o	abbba	V/v	babab
B/b	aaaab	I/i	abaaa	P/p	abbbb	W/w	babba
C/c	aaaba	J/j	abaab	Q/q	baaaa	X/x	babbb
D/d	aaabb	K/k	ababa	R/r	baaab	Y/y	bbaaa
E/e	aabaa	L/l	ababb	S/s	baaba	Z/z	bbaab

H/h	aabab	M/m	abbaa	I/i	baabb		
G/g	aabba	N/n	abbab	U/u	babaa		

加密者需使用两种不同字体，分别代表A和B。准备好一篇包含相同AB字数的假信息后，按照密文格式化假信息，即依密文中每个字母是A还是B分别套用两种字体。

解密时，将上述方法倒转。所有字体一转回A，字体二转回B，以后再按上表拼回字母。

法兰西斯·培根另外准备了一种方法，其将大小写分别看作A与B，可用于无法使用不同字体的场合（例如只能处理纯文本时）。但这样比起字体不同更容易被看出来，而且和语言对大小写的要求也不太兼容。

培根密码本质上是将二进制信息通过样式的区别，加在了正常书写之上。培根密码所包含的信息可以和用于承载其的文章完全无关。

https://blog.csdn.net/weixin_43727556

把原来的字母都替换掉

字符串、文本实时替换

文本替换工具说明：

将文本中的某字符串替换成另外的字符串

原始文本：

daadaaaddadaaaddaaaaaaaaaaddadaaadadaaadadaaadadaadddadaadad
d

需要替换的字符：

d

替换为字符：

b

替换结果：

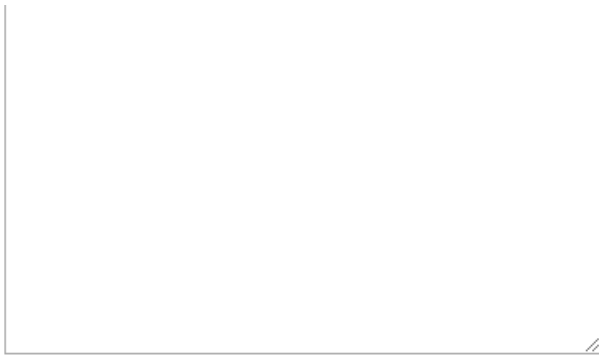
baabaaabbbabaaabbaaaaaaaaaabbabaaaabaaaaabaaabaabaaaabaabbaabbbbaabab
b

https://blog.csdn.net/weixin_43727556

再对培根密码进行解密

在线工具|培根密码加解密

SHIYANBAISCOOL
shiyانبaiscool



解密 加密

https://blog.csdn.net/weixin_43727556

flag: CTF{SHIYANBA IS COOL}

**

5、奇妙的音乐

**

据说flag就藏在这段音乐中，请仔细听。

格式: CTF{}

解题链接: <http://ctf5.shiyanbar.com/crypto/123.zip>

下载后得到两个东西，一个是图片一个是加了密的压缩包

打开图片看到了海伦凯勒的图片，下面有一串密文

我们都知道海伦凯勒是盲人，可以联想到盲文，以前我对盲文也有点印象，见过。

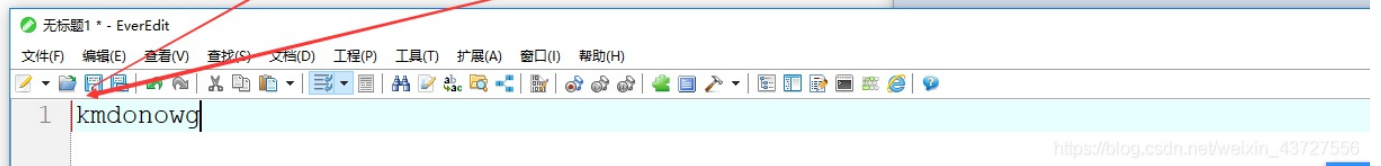
于是查盲文

解读：每个数字的盲文前面都有个“3456”点符形，是数字，表示后面的读作阿拉伯数字。

2. 英语字母盲文（英语一级盲文）



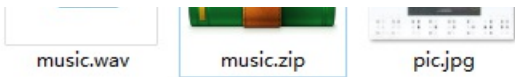
解读：英语盲文 a-j 都只是用了 1245 点位即上半截，和数字的一样；k-t 是 a-j 下面加上了 3 号点位。



https://blog.csdn.net/weixin_43727556

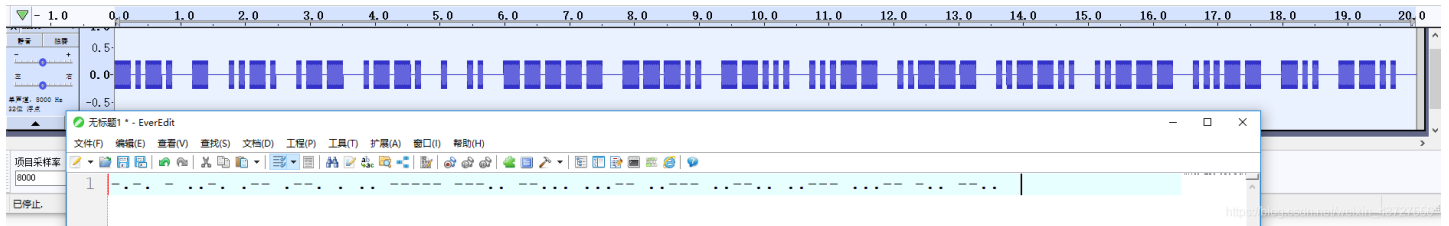
解压出来了一个音频文件





https://blog.csdn.net/weixin_43727556

用Audacity这个工具打开，把莫尔斯电码给搞出来



莫尔斯电码

Morse code



编 码

解 码

ctfwrpei08732?23dz

https://blog.csdn.net/weixin_43727556

**

6、Decode

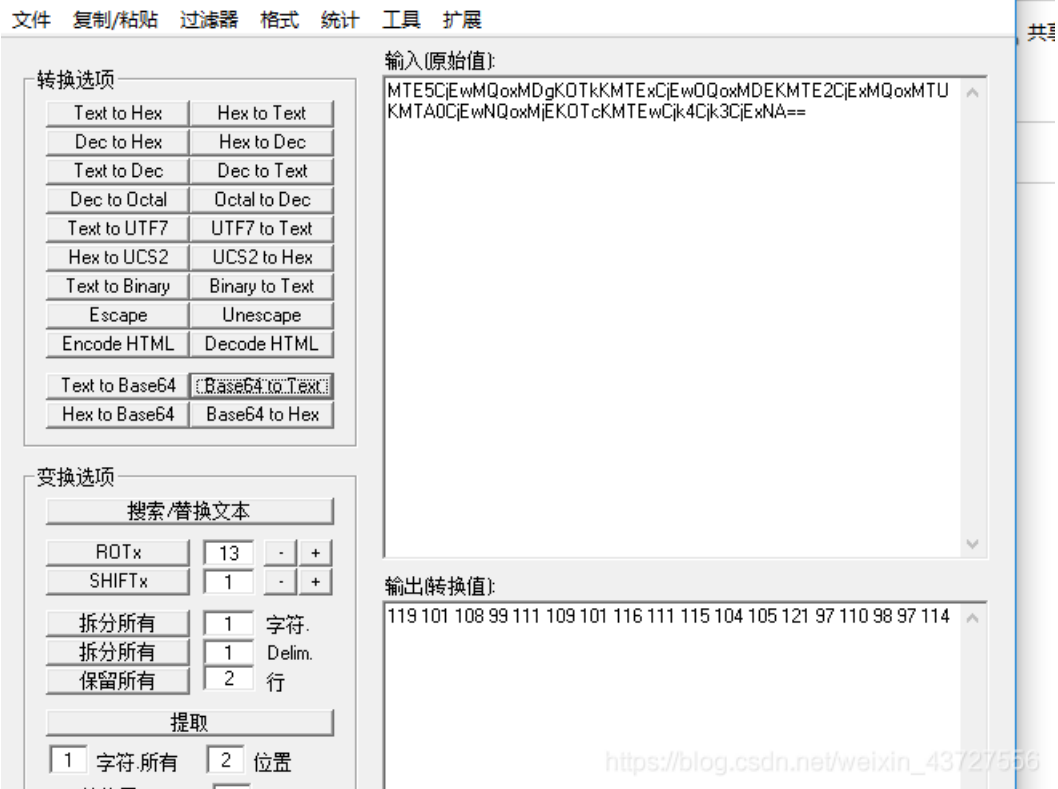
**

flag格式:ctf{}

解题链接: <http://ctf5.shiyanbar.com/crypto/Readme.txt>

点进去是一大串16进制编码

```
0x2534642535342534352533352534332536612534352537372534642535312536662537382534642534342536372534622
534662535342536622534622534642535342534352537382534332536612534352537372534662535312536662537382534
642534342534352534622534642535342534352533322534332536612534352537382534642535312536662537382534642
535342535352534622534642535342534312533302534332536612534352537372534652535312536662537382534642536
612534352534622534662535342536332534622534642535342534352537372534332536612536622533342534332536612
53662253333253433253661253435253738253465253431253364253364
```

ascii码解码，得到flag

