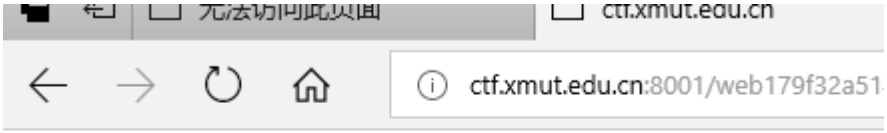
1：第一题手机扫码即可

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

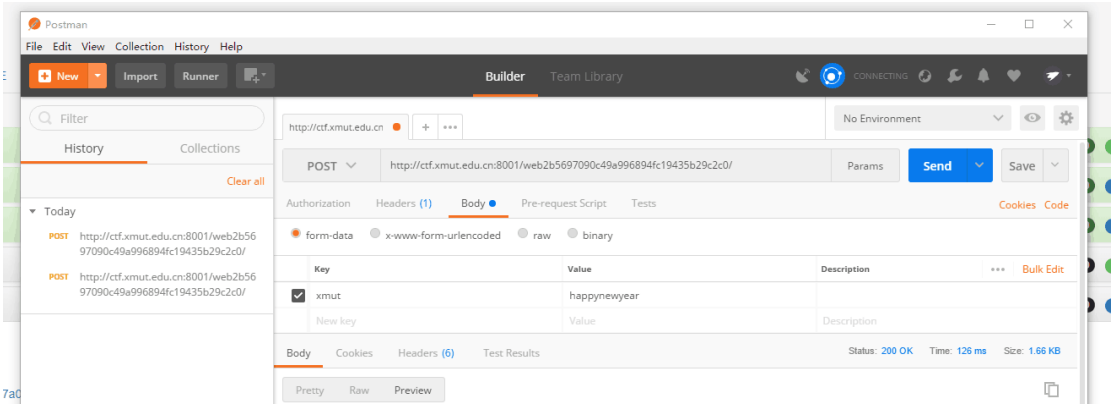



```php
<?php
    include "flag.php";
    highlight_file(__FILE__);

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

3：php 代码审计

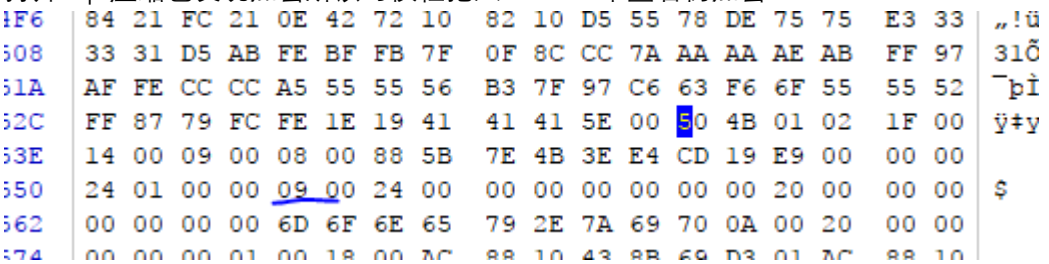
由于用不了 bp 发送 post 所以百度了一个 postman

```php
<?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!
```

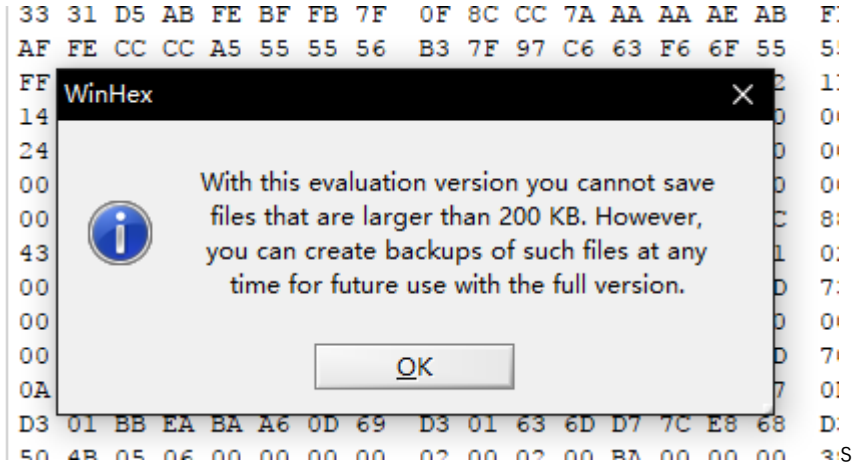


5：杂项

打开 zip 压缩包发现加密所以习惯性拖入 winhex 中查看伪加密

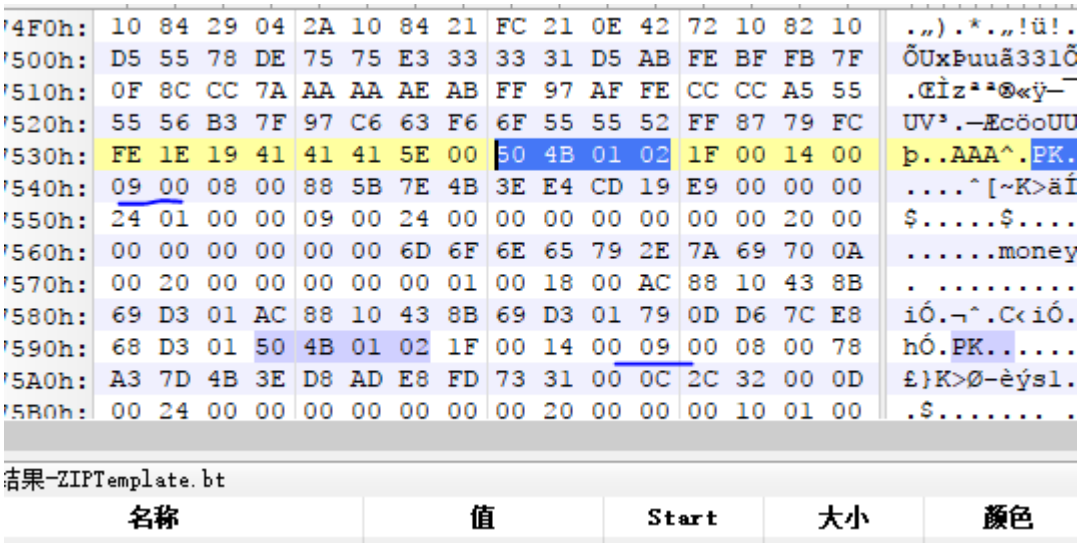


但是修改后发现不行，提示文件太大

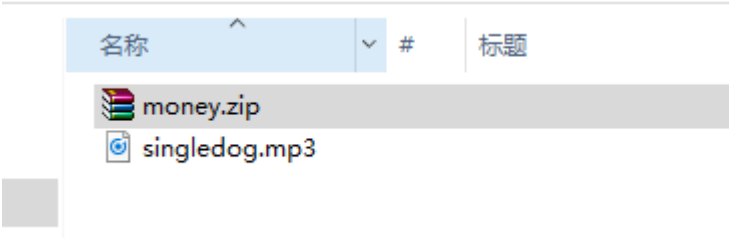


所以想到还可以用 010editer 修改。。。

查找后发现有 2 个疑似伪加密的文件所以全部修改为 00

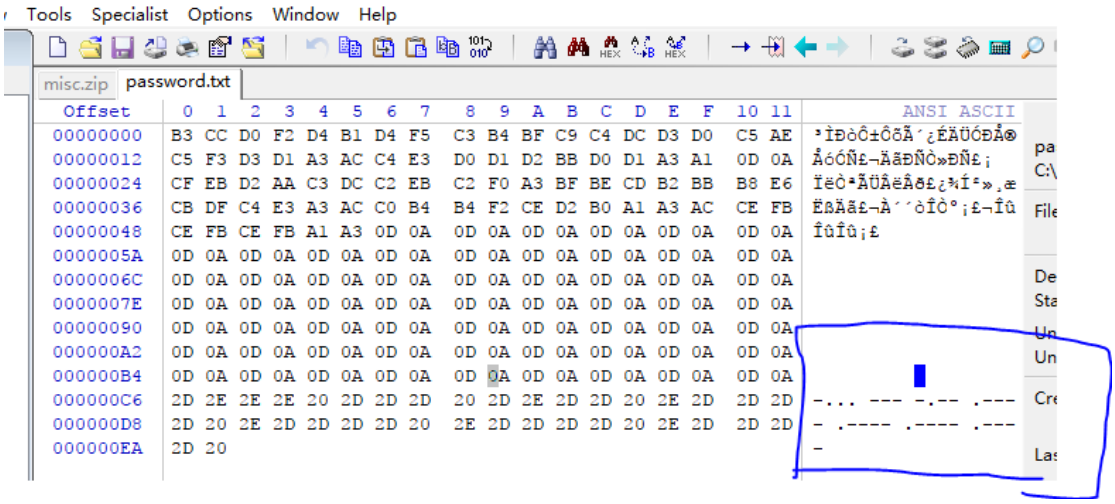


解压文件得到了 2 个文件



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



解密后发现得到了 boy1111,还有一个 MP3 文件没用到所以用 MP3stego 来分离 MP3 文件

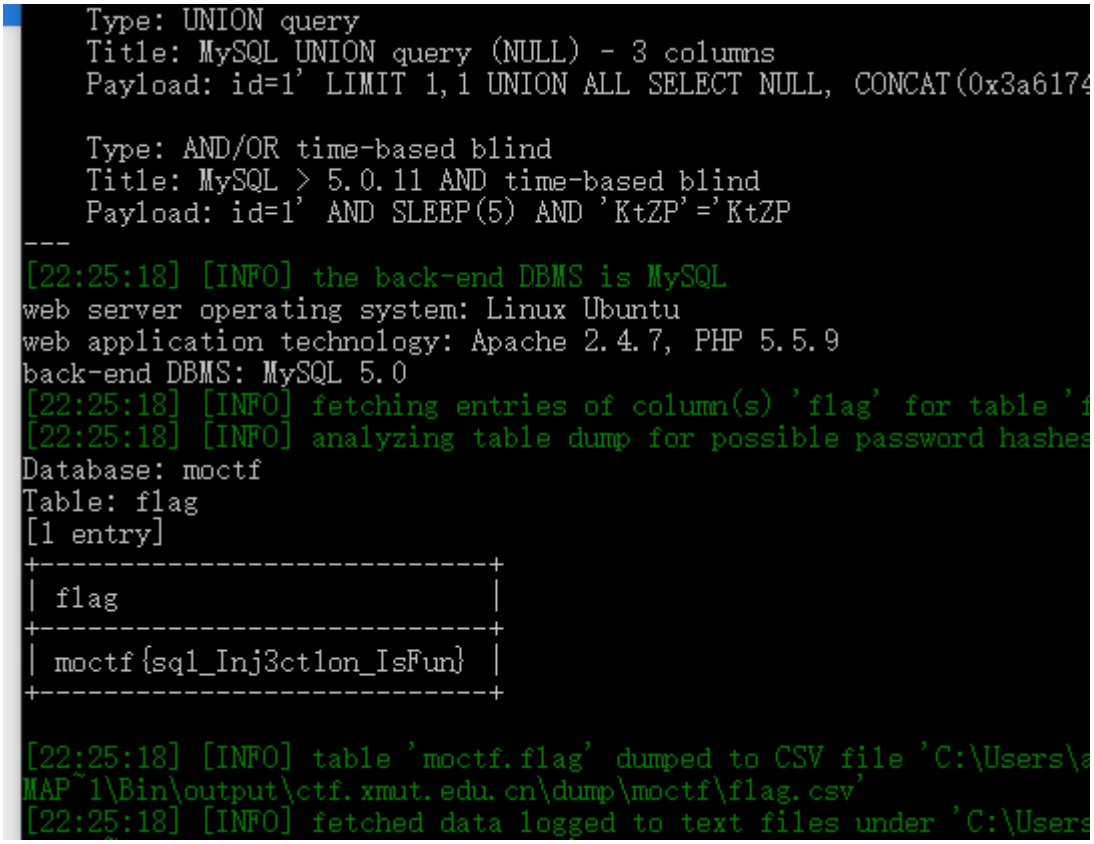
生成了一个 txt 文件 bW9jdGZ7UzFuZ2wzX0QwZ30= base64 解密后即可

6：sql 注入

一开始用 Python 写的 sqlmap 一直连不上数据库，所以又百度找了一个用 c 写的 sqlmap 运行

-u "

http://ctf.xmut.edu.cn:8003/web66d840558c5233f94597a0d92f9eecb9c/sql.php?id=2" -D moctf -T flag -C flag –dump 运行后直接得到 flag



7:颜文字解密

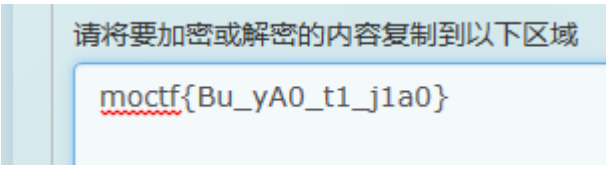
打开 word 文档后发现一堆表情就想起了大佬说的颜文字加密，所以百度在线解密即可

```
ω´ /=·/ ｀m´) /· ~┻━┻. . . //*´∇｀*/·['_'];·o=(ﾟｰﾟ)· · =_=3;·c=(ﾟΘﾟ)·=(ﾟｰﾟ)-(ﾟｰﾟ);·(ﾟДﾟ)·=(
ﾟΘﾟ)=· (o^_^o)/· (o^_^o);(ﾟДﾟ)={ﾟΘﾟ:· '_'·,ﾟωﾟ/·:· ((ﾟωﾟ/==3)· +'_')· [ﾟΘﾟ]· ,ﾟｰﾟ/·:(ﾟωﾟ/+·
'_')[o^_^o·-(ﾟΘﾟ)]·,ﾟДﾟ/:((ﾟｰﾟ==3)·+'_')[ﾟｰﾟ]·};·(ﾟДﾟ)·[ﾟΘﾟ]·=((ﾟωﾟ/==3)·+'_')·[c^_^o];(ﾟДﾟ)·
['c']·=·((ﾟДﾟ)+'_')·[·(ﾟｰﾟ)+(ﾟｰﾟ)-(ﾟΘﾟ)·];(ﾟДﾟ)·['o']·=·((ﾟДﾟ)+'_')·[ﾟΘﾟ];(ﾟoﾟ)=(ﾟДﾟ)·['c']+(ﾟД
ﾟ)·['o']+(ﾟωﾟ/·+'_')[ﾟΘﾟ]+·((ﾟωﾟ/==3)·+'_')·[ﾟｰﾟ]·+·((ﾟДﾟ)·+'_')·[(ﾟｰﾟ)+(ﾟｰﾟ)]+·((ﾟｰﾟ==3)·+'_')·
[ﾟΘﾟ]+((ﾟｰﾟ==3)·+'_')·[(ﾟｰﾟ)·-·(ﾟΘﾟ)]+(ﾟДﾟ)·['c']+((ﾟДﾟ)+'_')·[(ﾟｰﾟ)+(ﾟｰﾟ)]+·(ﾟДﾟ)·['o']+((ﾟｰﾟ
==3)·+'_')·[ﾟΘﾟ];(ﾟДﾟ)·['_']·=(o^_^o)·[ﾟoﾟ]·[ﾟoﾟ];(ﾟεﾟ)=((ﾟｰﾟ==3)·+'_')·[ﾟΘﾟ]+·(ﾟДﾟ)·.ﾟДﾟ/
+((ﾟДﾟ)+'_')·[(ﾟｰﾟ)·+·(ﾟｰﾟ)]+((ﾟｰﾟ==3)·+'_')·[o^_^o·-ﾟΘﾟ]+((ﾟｰﾟ==3)·+'_')·[ﾟΘﾟ]+·(ﾟωﾟ/·+'_')·[
ﾟΘﾟ];·(ﾟｰﾟ)+=(ﾟΘﾟ);·(ﾟДﾟ)[ﾟεﾟ]='\\';·(ﾟДﾟ).ﾟΘﾟ/=(ﾟДﾟ+·ﾟｰﾟ)[o^_^o·-(ﾟΘﾟ)];(oﾟｰﾟo)=(ﾟω
ﾟ/·+'_')[c^_^o];(ﾟДﾟ)·[ﾟoﾟ]='\"';(ﾟДﾟ)·['_']·(·(ﾟДﾟ)·['_']·(ﾟεﾟ+(ﾟДﾟ)[ﾟoﾟ]+·(ﾟДﾟ)[ﾟεﾟ]+(
ﾟΘﾟ)+·((ﾟｰﾟ)·+·(ﾟΘﾟ))+·((ﾟｰﾟ)·+·(ﾟΘﾟ))+·(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+·((ﾟｰﾟ)·+·(ﾟΘﾟ))+·((ﾟｰﾟ)·+·
(o^_^o))+·(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+·(ﾟｰﾟ)+·(o^_^o)+·(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+·((o^_^o)·+(o^_^o))+·(ﾟ
ﾟ)+·(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+·(ﾟｰﾟ)+·((o^_^o)·+(o^_^o))+·(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+·((ﾟｰﾟ)·+·(o^_^o))+·
(o^_^o)+·(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+·(c^_^o)+·(ﾟｰﾟ)+·(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+·((ﾟｰﾟ)·+·(ﾟΘﾟ))+·((ﾟｰﾟ)·+·
(o^_^o))+·(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+·(o^_^o)+·((ﾟｰﾟ)·+·(o^_^o))+·(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+·(o^_^o)+·(ﾟΘ
ﾟ)+·(ﾟДﾟ)[ﾟεﾟ]+((o^_^o)·+(o^_^o))+·(c^_^o)+·(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+·((o^_^o)·+(o^_^o))+·((ﾟｰﾟ)·
+·(ﾟΘﾟ))+·(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+·(o^_^o)+·((ﾟｰﾟ)·+·(o^_^o))+·(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+·((o^_^o)·-·(ﾟ
```

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       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://
115161        0x1C1D9         Zip archive data, at least v2.0 to extract, compre
ssed 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 askii 码的东西所以对应 askii 码表找一下就可以得到 flag 了