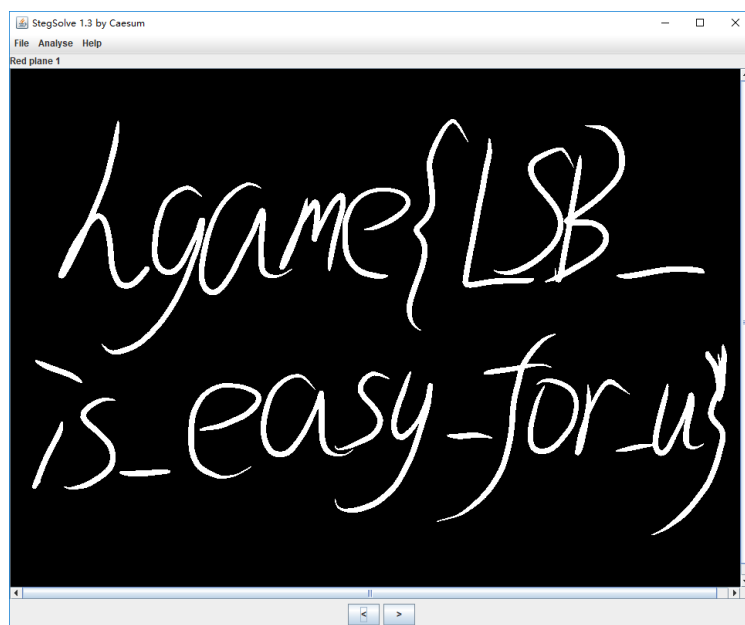


(当初听同学信了他这个目前这个寒假只要 C 语言，打开网站的一瞬间内心是绝望的)

MISC

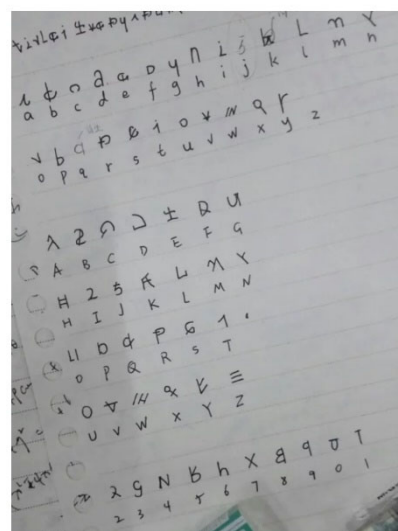
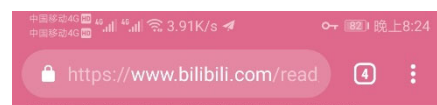
1. Hidden Image in LSB

stegsolve 解决。



2. 打字机

没什么特殊操作，打字机对应键盘按键，对另一张图的 flag 进行翻译，事实上，看到了这个东西。



然后我就开始了持续了半个寒假的字体制作
emm.....

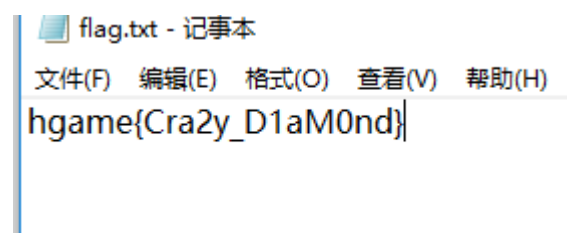
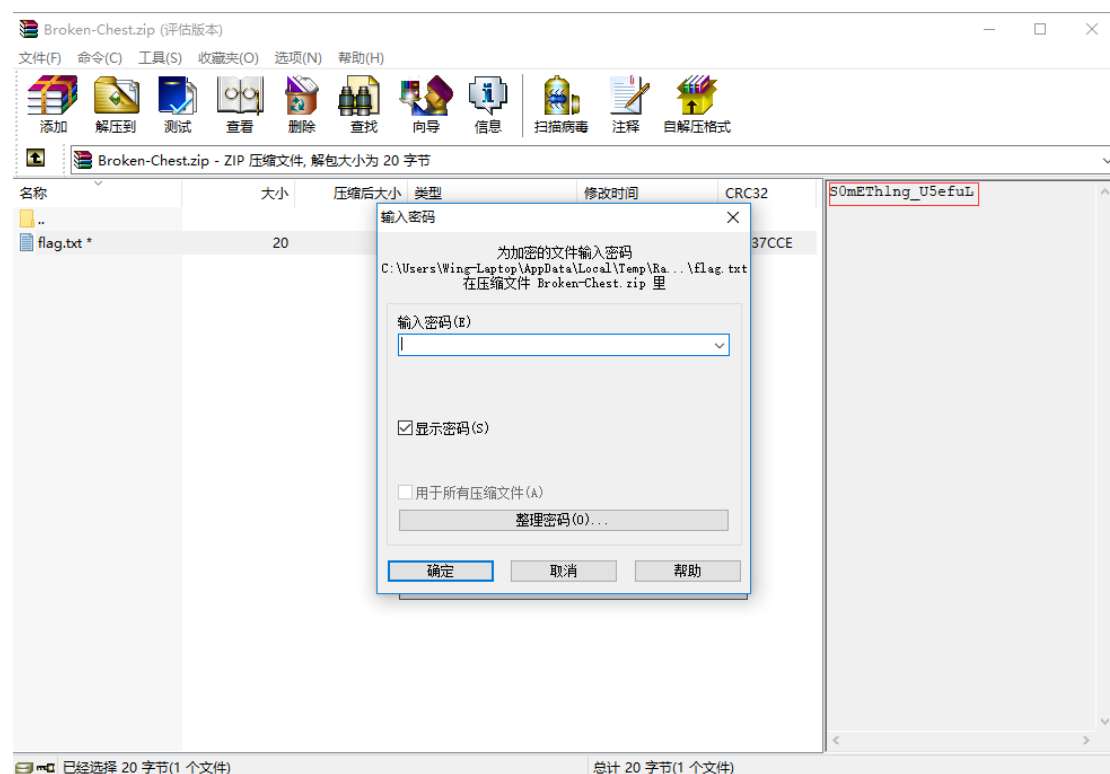


3. Broken Chest

打开压缩包，发现加密的 txt 但无法打开，应该是压缩包损坏（怀疑被篡改了数据），用 010editor 打开，

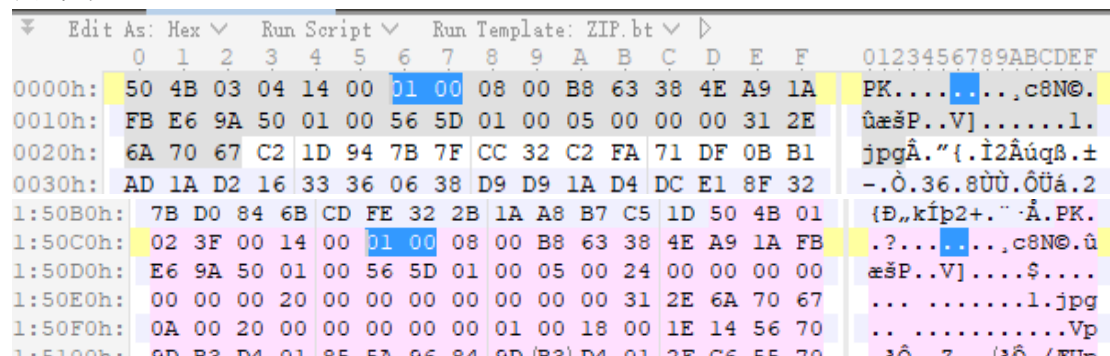
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | 0123456789ABCDEF |
|--------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------------------|
| 0000h: | 4F | 4B | 03 | 04 | 14 | 00 | 09 | 00 | 08 | 00 | 55 | BB | 35 | 4E | CE | 7C | OK.....U»5NÎ |
| 0010h: | B3 | B0 | 22 | 00 | 00 | 00 | 14 | 00 | 00 | 00 | 08 | 00 | 00 | 00 | 66 | 6C | °".....fl |
| 0020h: | 61 | 67 | 2E | 74 | 78 | 74 | 67 | 49 | 3F | 48 | A0 | BE | 53 | 8B | 38 | E4 | ag.txtgI?H %S<8ä |
| 0030h: | 5A | 42 | 49 | 02 | 08 | 5D | 55 | A6 | 4A | 67 | B2 | B3 | CE | B0 | 6E | C1 | ZBI..]U;Jg°³î°nÁ |
| 0040h: | 0B | 85 | DC | EB | 4F | 91 | 4D | BF | 50 | 4B | 07 | 08 | CE | 7C | B3 | B0 | ...ÜeO`M¿PK..î °° |
| 0050h: | 22 | 00 | 00 | 00 | 14 | 00 | 00 | 00 | 50 | 4B | 01 | 02 | 1F | 00 | 14 | 00 | ".....PK..... |
| 0060h: | 09 | 00 | 08 | 00 | 55 | BB | 35 | 4E | CE | 7C | B3 | B0 | 22 | 00 | 00 | 00 |U»5NÎ °°... |
| 0070h: | 14 | 00 | 00 | 00 | 08 | 00 | 24 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 20 | 00 |\$..... |
| 0080h: | 00 | 00 | 00 | 00 | 00 | 00 | 66 | 6C | 61 | 67 | 2E | 74 | 78 | 74 | 0A | 00 |flag.txt.. |
| 0090h: | 20 | 00 | 00 | 00 | 00 | 00 | 01 | 00 | 18 | 00 | 3E | 2C | 76 | B6 | 9D | B1 |>,vq.± |
| 00A0h: | D4 | 01 | 3E | 2C | 76 | B6 | 9D | B1 | D4 | 01 | 1D | F1 | 7E | C5 | 9C | B1 | Ô.>,vq.±Ô..ñ~Åe± |
| 00B0h: | D4 | 01 | 50 | 4B | 05 | 06 | 00 | 00 | 00 | 00 | 01 | 00 | 01 | 00 | 5A | 00 | Ô.PK.....Z. |
| 00C0h: | 00 | 00 | 58 | 00 | 00 | 00 | 10 | 00 | 53 | 30 | 6D | 45 | 54 | 68 | 31 | 6E | ..X.....S0mETHln |
| 00D0h: | 67 | 5F | 55 | 35 | 65 | 66 | 75 | 4C | | | | | | | | | g_U5efuL |

发现头文件的 4F 4B 03 04,而 zip 的头文件应为 50 4B 03 04, 修改并保存。再次打开 zip 文件发现要输入密码，尝试了注释的 S0mETH1ng_U5efuL 直接打开，得到 flag。

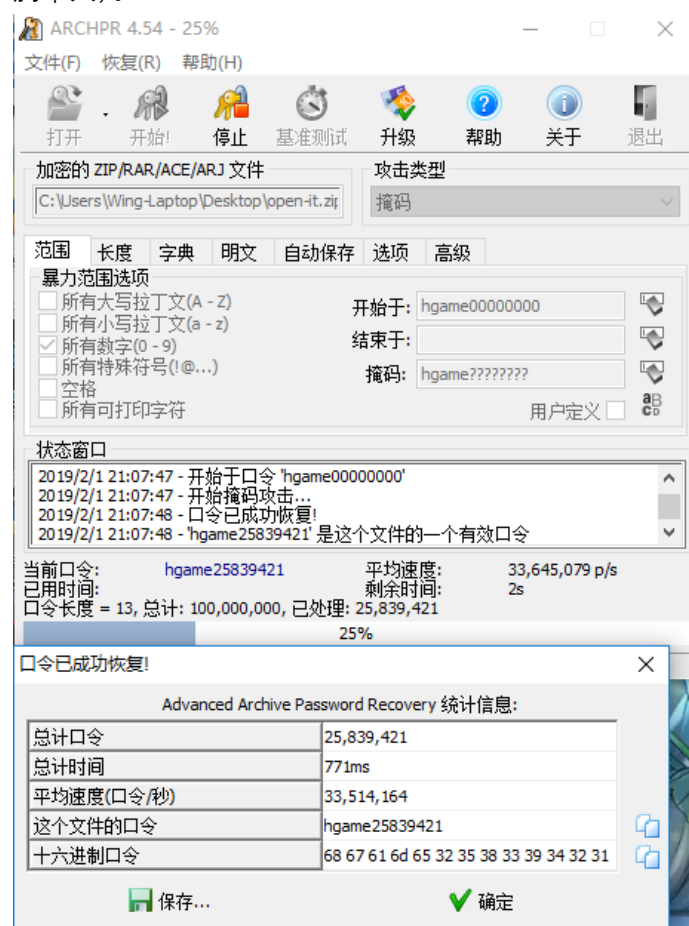


4. Try

最坑的一题，发现后缀为.pcapng，用 wireshark 打开（当初不知道尝试改后缀折腾半天），只有导出 http 对象才有文件，解压压缩包发现 open-it.zip 和 password.txt。发现并没有相同 CRC32 文件，用 010editor 打开 open-it.zip 发现数据区和目录区通用标记都是 01 00 是真密码。



打开 password.txt，猜想 hgame 后八位为数字，使用 archpr 掩码攻击成功得到密码（又折腾半天）。



得到一张 jpg，应该是图片隐写术，尝试使用 stegsolve，flag 没找到，倒是被图片吓得不轻，用 binwalk 扫描文件，发现了是两个文件合成。

WEB

1. 谁吃了我的 flag

hint 提示 vim 编写未保存关机，上网查到了 vim 的著名特点：意外关闭产生备份文件。于是在修改网址，发现 118.25.111.31:10086/.index.html.swp 可以下载备份文件 index.html.swp。用 vim 打开（眼花了），想起 16 进制编辑器查看 flag，将文件转为 16 进制，结尾得到 flag。

```
00002e40: 0000 0000 0000 0000 0000 0000 3c2f 083c .....</!!\
00002eb0: 2f68 746d 6c3e 0009 3c2f 626f 6479 3e00 /html>..</body>.
00002ec0: 0909 3c70 3e74 6865 2066 6c61 6720 6973 ..<p>the flag is
00002ed0: 2068 6761 6d65 7b33 6565 6b5f 6469 5363 hgame{3eek_diSc
00002ee0: 6c30 5375 7265 5f66 526f 6d2b 7745 6273 l0Sure_fRom+wEbs
00002ef0: 6974 407d 0009 093c 2f62 723e 0009 093c it@}...</br>...
00002f00: 703e 6669 6e65 2c20 6e6f 7468 696e 6720 p>fine, nothing
00002f10: 7365 7269 6f75 732c 206a 7573 7420 6769 serious, just g
00002f20: 7665 2079 6f75 2066 6c61 6720 7468 6973 ve you flag this
00002f30: 2074 696d 652e 2e2e 3c2f 703e 0009 093c time...</p>...
00002f40: 2f62 723e 0009 093c 703e 6461 6d6e 2e2e /br>...<p>damn..
00002f50: 2e68 6761 6d65 3230 3139 2069 7320 636f .hgame2019 is co
00002f60: 6d69 6e67 2073 6f6f 6e2c 2062 7574 2074 ming soon, but t
```

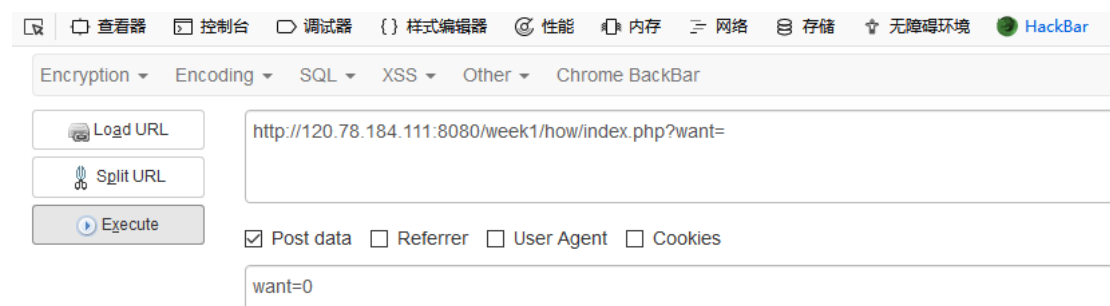
2. 换头大作战

（提示工具要 bp 赶紧下载学习……,设置了火狐）

先尝试了下直接打开，提示 post（post 是啥？学习学习），抓包，send to repeater,go!

想要flag嘛:

用 hackbar 进行 post,



抓包信息 send to repeater, go, 发现

https://www.wikiwand.com/en/X-Forwarded-For
only localhost can get flag

添加 X-Forwarded-For:127.0.0.1,go,发现

t
please use Waterfox/50.0

将 Firefox/65.0 的 UA 改为 Waterfox/50.0,go,发现

the requests should referer from www.bilibili.com

再将 Referer 改为 www.bilibili.com, go,发现，嗯？

r/>you are not admin

不是很懂，思考了一下，修改 cookie: admin=1(当时想到的是布尔值)，go,终于出现了，flag

```
<br/>hgame{hTTp_HeaDeR_iS_Ez}
```

3. very easy web(坑了好久)

看到 php 头皮发麻，不了解，上网找资料，理解为 id 值不为 vidar 会显示“加油”，urldecode 是 url 解码，所以对 vidar 进行 url 编码（对着编码表编码，笑），得到%76%69%64%61%72，输入 id=%76%69%64%61%72，无效，在找资料，发现有个东西叫三元运算符，再试还是不行（绝望）。翻烂了百度和谷歌发现

但是这些函数在遇到urldecode()函数时，就会因为二次解码引发注入。urldecode()函数是对已编码的URL进行解码。引发注入的原因其实很简单，PHP本身在处理提交的数据之前会进行一次解码，例如/test.php?id=1这个URL，我们构造字符串/test.php?id=1%2527，PHP第一次解码，%25解码成了%，于是url变成了/test.php?id=%27；然后urldecode()函数又进行了一次解码，%27解码成了'，于是最终URL变成了/test.php?id=1'，单引号引发了注入。rawurldecode()也会产生同样的问题，因此这两个函数需要慎用。

所以我应该对 vidar 进行二次编码……更改为%id=%2576%2569%2564%2561%2572 得到 flag。

```
hgame{urlDecode_Is_GoOd} <?php
error_reporting(0);
include("flag.php");

if(strpos("vidar",$_GET['id'])!==FALSE)
    die("<p>干巴爹</p>");

$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] == "vidar")
{
    echo $flag;
}
highlight_file(__FILE__);
?>
```

4. can you find me?

源代码发现线索!

```
<a href="f12.php"></a>
```

添加/f12.php,抓包呵呵。如此清晰。

```
>please post password to me! I will open the gate for you!</p>
```

```
password: woyaoflag
```

post 后抓包，在 repeater 里 go 发现

```
<p>please post password to me! I will open the gate for you!</p>
<p>right!</p><a href="iamflag.php"> click me to get flag</a></body>
html>
```

将 f12.php 改为 iamflag.php 得到 flag

```
<body>
  <p>flag:hgame{f12_1s_aMazing111}</p>
</body>
```

PS: 后来发现没用到资料中的 302, flag 藏在跳转网页的情况, 不在 repeater 里试, 直接在火狐里添加, 发现了藏在“302”中的 flag。

| http://47.107.252.17... | GET | /f12.php | 200 | 447 | HTML | can u find me? | 22:49:43 1... |
|-------------------------|------|--------------|-------|-----|------|------------------|---------------|
| http://47.107.252.17... | GET | /toofast.php | 200 | 365 | HTML | can u find me? | 22:49:30 1... |
| http://47.107.252.17... | GET | /iamflag.php | 302 | 342 | HTML | can you find me? | 22:50:01 1... |
| http://47.107.252.17... | POST | /iamflag.php | ✓ 302 | 342 | HTML | can you find me? | 22:49:24 1... |

RequestResponse

RawHeadersHexHTMLRender

HTTP/1.1 200 OK
Server: nginx/1.15.8
Date: Fri, 01 Feb 2019 14:49:31 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.2.14
Content-Length: 181

```
<!DOCTYPE html>
<html>
<head>
  <title>can u find me?</title>
</head>
<body>
  <p>aoh,your speed is sososo fast,the flag must have been left in somewhere</p>
</body>
</html>
```

| http://47.107.252.17... | GET | / | 200 | 424 | HTML | can u find me? | 22:41:13 1... |
|-------------------------|------|--------------|-------|-----|------|------------------|---------------|
| http://47.107.252.17... | GET | /f12.php | 200 | 447 | HTML | can u find me? | 22:45:43 1... |
| http://47.107.252.17... | GET | /toofast.php | 200 | 365 | HTML | can u find me? | 22:49:30 1... |
| http://47.107.252.17... | GET | /iamflag.php | 302 | 342 | HTML | can you find me? | 22:50:01 1... |
| http://47.107.252.17... | POST | /iamflag.php | ✓ 302 | 342 | HTML | can you find me? | 22:49:24 1... |

RequestResponse

RawHeadersHexHTMLRender

HTTP/1.1 302 Found
Server: nginx/1.15.8
Date: Fri, 01 Feb 2019 14:49:24 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.2.14
location: toofast.php
Content-Length: 132

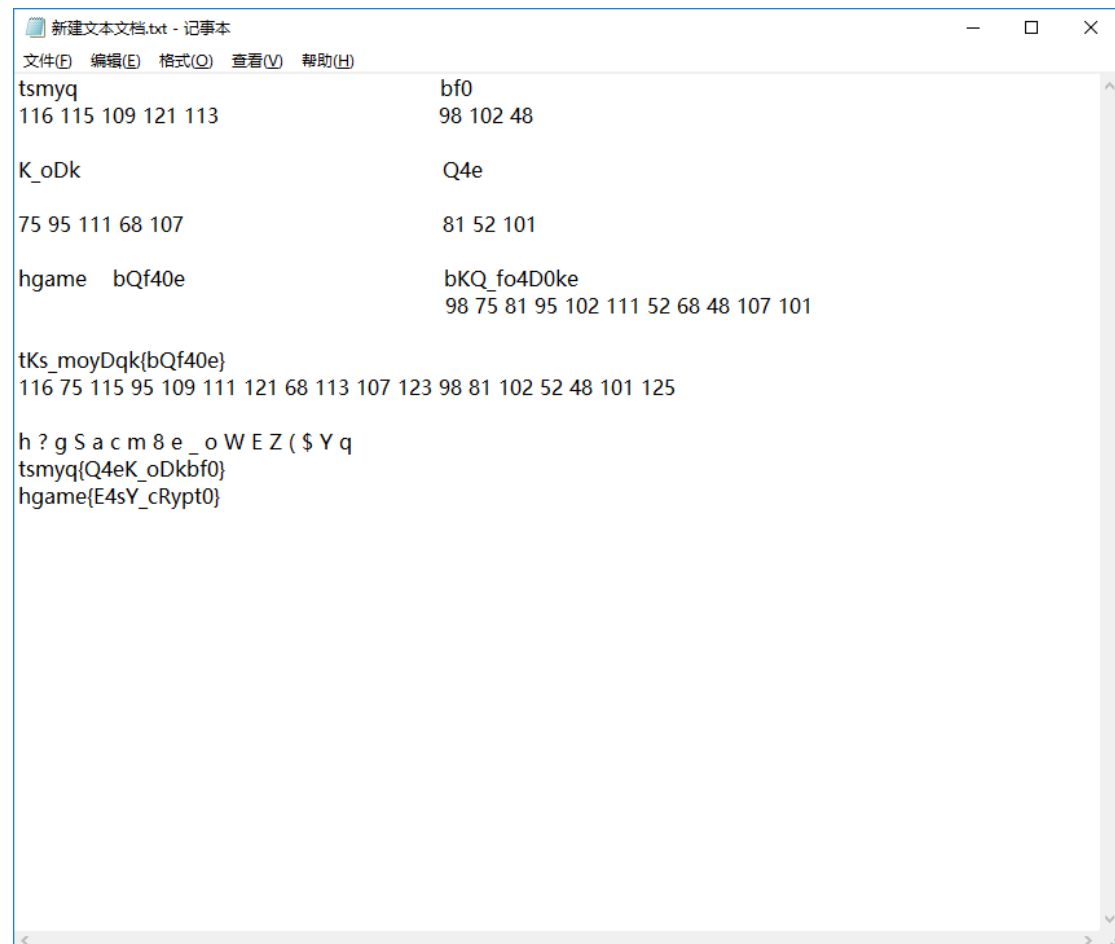
```
<html>
  <head>
    <title>can you find me?</title>
  </head>
  <body>
    <p>flag:hgame{f12_1s_aMazing111}</p>
  </body>
</html>
```

CRYPTO

1. Mix (看到标题心一颤)

题目很显然的摩斯代码，翻译得到 744B735F6D6F7944716B7B6251663430657D。高高兴兴的加上 hgame{} 提交。错误。

还是太年轻，刚看到 mix 就忘了。观察一下发现最大的字母为 F，很有可能是 16 进制，且两个一组刚刚好，对其进行 ascii 转换，得到 tKs_moyDqk{bQf40e}。虽然有花括号，但这次没有激动地提交，没这么简单，太丑了，关键“hgame”的字符都没有。花括号前有 10 个字符，对比“hgame”5 个字符，感觉是栅栏密码，不过不是解密应该是加密，加密后得到 tsmYq{Q4eK_oDkbf0}。嗯，很接近了，把前面的 tsmYq 和 hgame 进行比较，显然 hgame 是 tsmYq 每个字母退 12 位。猜想是字符 ascii 值减一定数字（这一试就是一个小时）。txt 写了好多不行。再想，{} 和 _ 应该不会变了，这样的话数字可能也不变，只有英文字母的话在比较有名的古典密码里应该是凯撒密码了。进行尝试，果然，和 ascii 的猜想不同的是凯撒密码是可以循环的，得到 hgame{E4sY_cRypt0}，错不了，这格式肯定是 flag，提交，正确。



```
新建文本文档.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

tsmyq          bf0
116 115 109 121 113      98 102 48

K_oDk          Q4e
75 95 111 68 107      81 52 101

hgame  bQf40e      bKQ_fo4D0ke
                        98 75 81 95 102 111 52 68 48 107 101

tKs_moyDqk{bQf40e}
116 75 115 95 109 111 121 68 113 107 123 98 81 102 52 48 101 125

h?gSacme_oWEZ($Yq
tsmyq{Q4eK_oDkbf0}
hgame{E4sY_cRypt0}
```