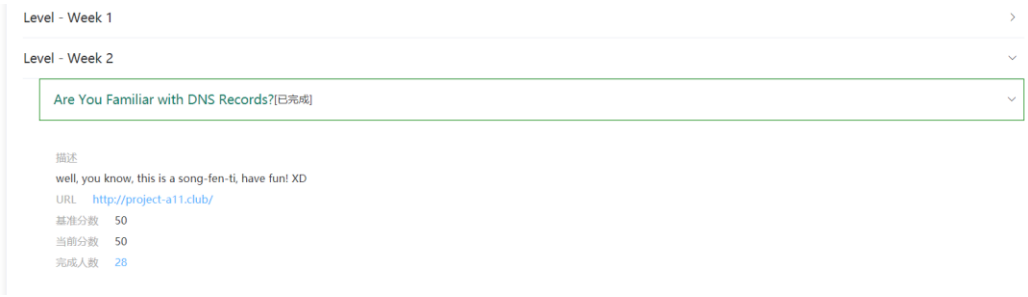
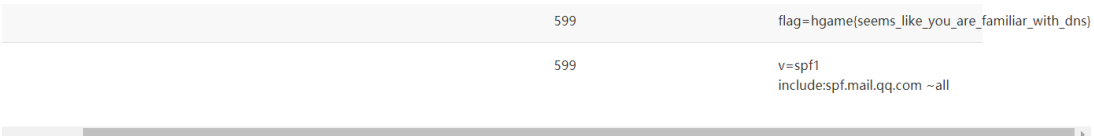
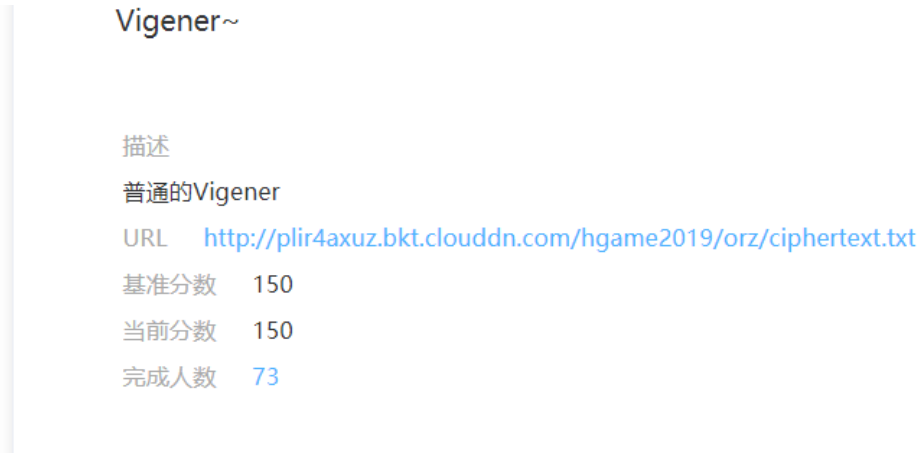
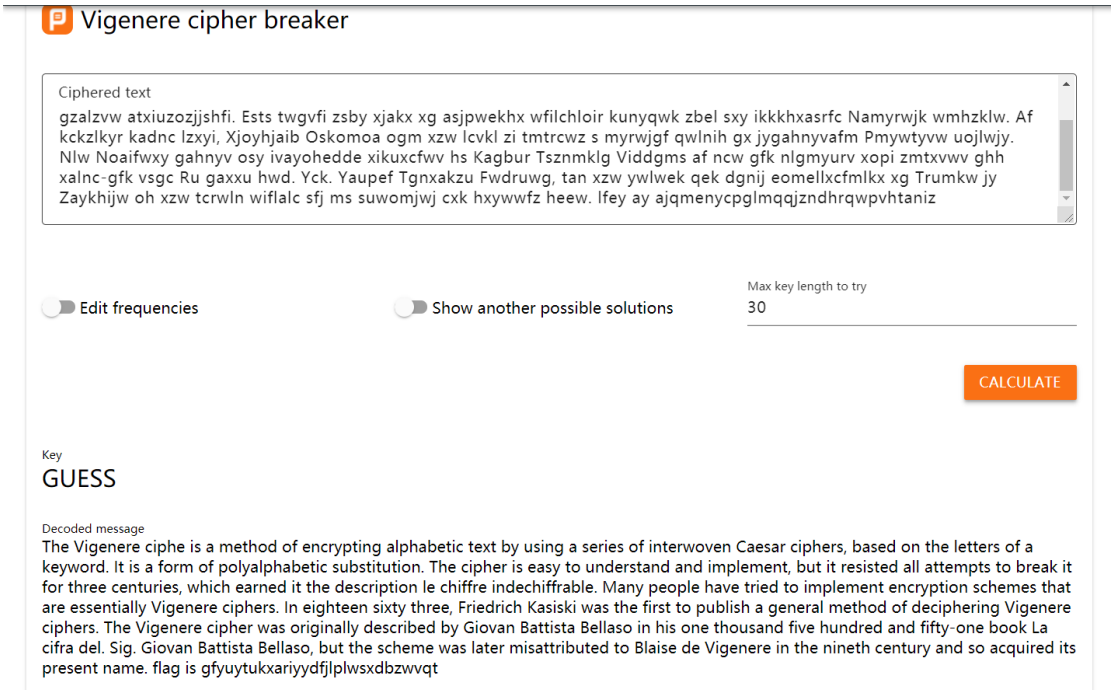


如题就是去查一下他的解析记录（注意网站有些查不到）







浪漫的足球圣地[已完成]

描述

无

URL http://plir4axuz.bkt.clouddn.com/hgame2019/orz/enc.txt

基准分数 150

当前分数 150

完成人数 27

带你去看浪漫的曼城（土耳其）

Google 一下，发现是曼城，再一下 曼城 ctf 发现是个加密方式

966A969596A9965996999565A5A59696A5A6A59A9699A599A596A595A599A569A5A99699A56996A596A696A996A6A5A696A9A595969AA5A69696A5A99696A595A59AA56A96A9A5A9969AA59A9559

一看16进制，转一下2进制（曼彻斯特的格式）

Online Manchester encoder/decoder

Decode and encode Manchester Code (Wikipedia) in your browser.
This may be helpful when manually looking at data transferred by RFID, infrared remote control transmissions, or other protocols.

Terms of use / privacy:

- This service is provided free of charge, without warranty
- The data entered is not transferred back to the server, all operations are done inside your browser
  - You may save this page for personal, off-line use

Usage/Settings:

Accepts a text string with "raw" data in binary representation (e.g. "10101001").
Phase convention:

G. E. Thomas	IEEE 802
0 is encoded as 01 (low-high transition) 1 is encoded as 10 (high-low transition) 01 (low-high transition) is decoded as 0 10 (high-low transition) is decoded as 1	0 is encoded as 10 (high-low transition) 1 is encoded as 01 (low-high transition) 01 (low-high transition) is decoded as 1 10 (high-low transition) is decoded as 0

Encoded

Decode ↓ Encode ↑ Invert ↕

Decoded

-->

http://eleif.net/manchester.html

注意标准，乱选会错的。

2再转16 16就是ascii，解一下

加密或解密字符串长度不可以超过10M

6867616d657b336632346535363735393165396362616232613764326631663734386131643647d

16进制转字符 字符转16进制 清空结果

hgame{3f24e567591e9cbab2a7d2f1f748a1d4}

找得到我嘛？小火汁[已完成]

描述

ε=ε=ε=ε=ε=ε= r(;￣◇￣)┘

hint: Https

URL http://plir4axuz.bkt.clouddn.com/hgame2019/orz/safe.pcapng

基准分数 150

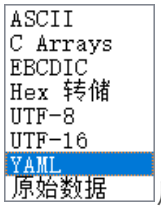
当前分数 150

完成人数 29

https://imlonghao.com/51.html 这题的魔改版

使用过滤器 "ftp || ftp-data"

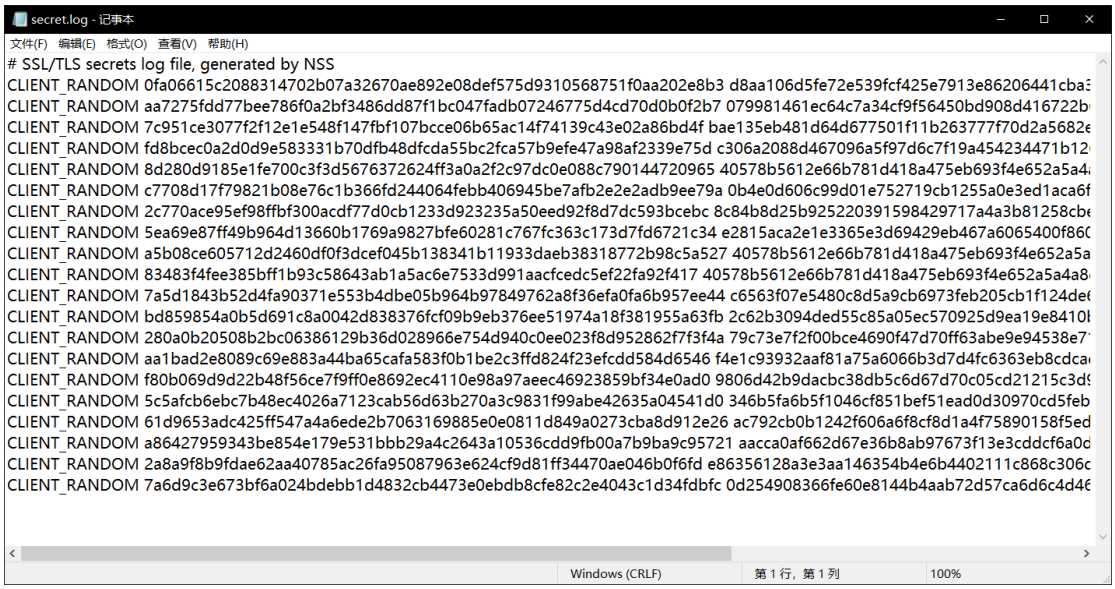
追踪 ftp-data 的 TCP 流，另存为 binary 来提取文件（灰常重要原始格式）



原始数据

提取出个东西（你看那个 50 4B）zip(之前就一直卡在那个原始格式里)（各种错误还以为又是 zip 的魔改）

解 压 出 来 个



之前又中坑了（以为是什么 RSA 的那种类型，去算哪个.key 文件）

就 是 个

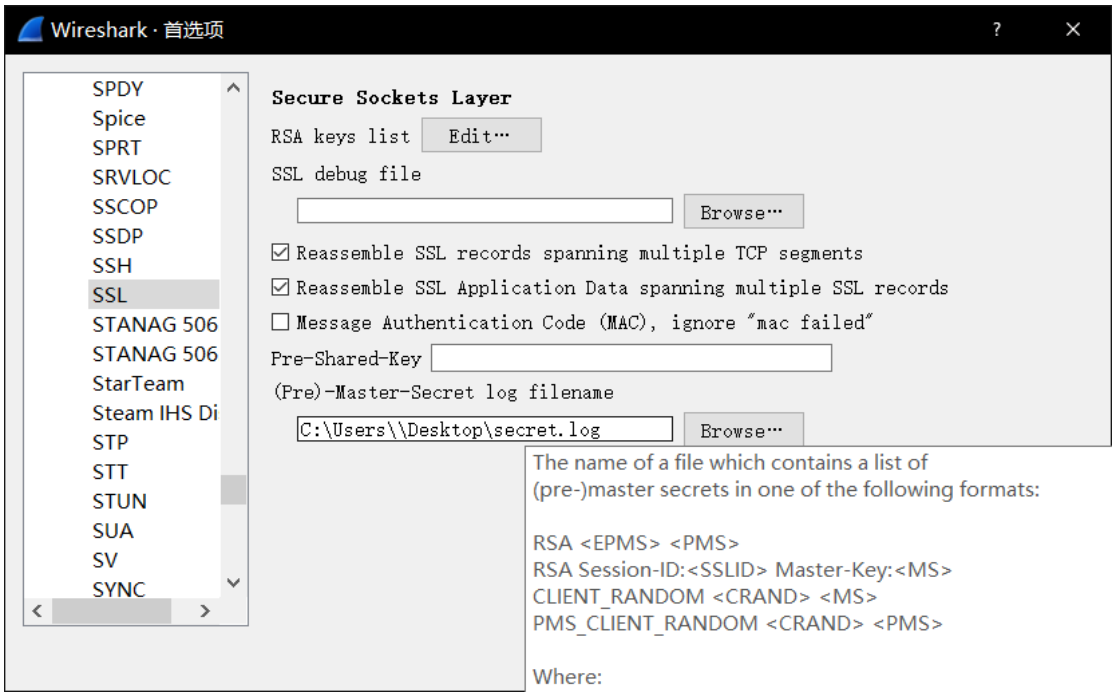
能发现这是一份 `NSS Key Log Format` 的文件，而这个文件是能解密出 Wireshark 里面的 https 流量的。

> Firefox、Chrome 可以通过设置 SSLKEYLOGFILE 环境变量导出所有的会话密钥，估计是为了方便调试。Wireshark 可以通过这种格式的密钥来解密。

资料参考：

NSS Key Log Format - Mozilla | MDN

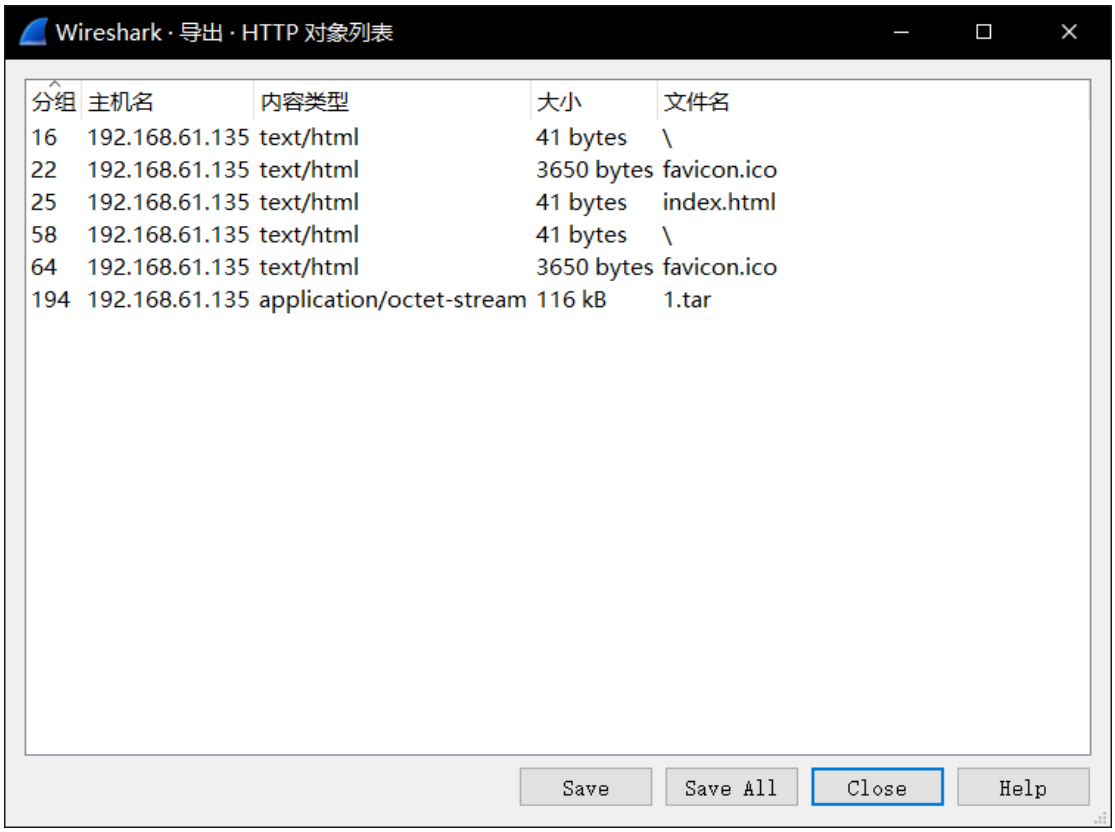
你搞到那个 ssl 里去



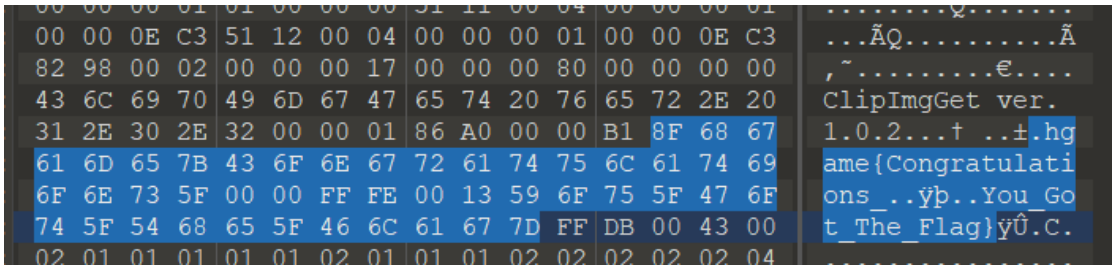
之前一直在搞上面那个文件。。。

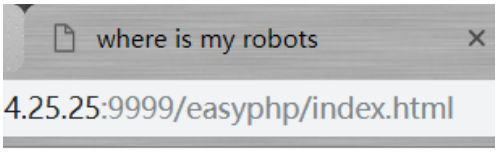
刷新一下。

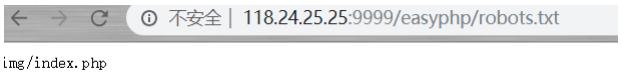
导出 tar



还以为是 java 打开，解压一下 010 打开，我觉得原意肯定不是用 010 看的


00 00 0E C3 51 12 00 04 00 00 00 01 00 00 0E C3
...ÃQ.....Ã
82 98 00 02 00 00 00 17 00 00 00 80 00 00 00 00
,˜.....€....
43 6C 69 70 49 6D 67 47 65 74 20 76 65 72 2E 20
ClipImgGet ver.
31 2E 30 2E 32 00 00 01 86 A0 00 00 B1 8F 68 67
1.0.2...† ..±.hg
61 6D 65 7B 43 6F 6E 67 72 61 74 75 6C 61 74 69
ame{Congratulati
6F 6E 73 5F 00 00 FF FE 00 13 59 6F 75 5F 47 6F
ons_..ÿþ..You_Go
74 5F 54 68 65 5F 46 6C 61 67 7D FF DB 00 43 00
t_The_Flag}ÿÛ.C.



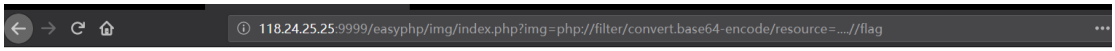


##草莓社区-2

依照上面一题的方式，我们发现，我们在这题中并不能通过../flag.php直接获得flag.php中的内容，这是因为在这一题中使用的include函数在加载../flag.php会解析flag.php文件导致不能显示flag.php的内容。这时候我们就得通过PHP伪协议，**php://filter。**

这样我们就可以构造我们的payload了*http://118.25.18.223:10012/show_maopian.php?mao=php://filter/read=convert.base64-encode/resource=../flag.php*

得到flag:hgame{!m4o_pi4n_ChaO_hao_kan!}



PD9waHAKICAgIC8vJGZsYWcgPSAnaGdhbWV7WW91XzRyZV9Tb19nMG9kfSc7CiAgICBlY2hvICJtYXliZV95b3Vfc2hvdWxkX3RoaW5rX3RoaW5rIjsK <?php

```
        error_reporting(0);
        $img  =  $_GET['img'];
        if(!isset($img))
                $img  =  '1';
        $img  =  str_replace('../',  '',  $img);
        include_once($img.".php");
        highlight_file(__FILE__);
```

Base64.一下就是啦

php trick[已完成]

描述

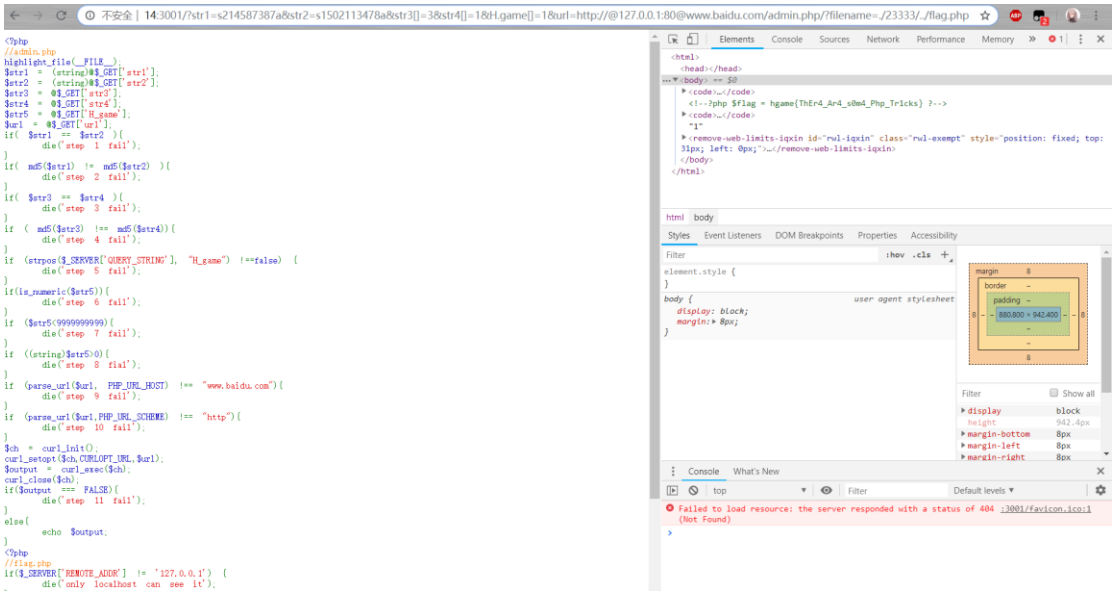
some php tricks

URL http://118.24.3.214:3001

基准分数 200

当前分数 200

完成人数 78



这么多 if，怕了怕了

一点点搞，他叫你干啥你就查啥。。。

PHP Is The Best Language[已完成]

描述

var_dump了解一下

URL http://118.25.89.91:8888/flag.php

基准分数 150

当前分数 150

完成人数 58

```php
if ((md5($_POST['key'])+1) == (md5(md5($_POST['key'])))+1) {
        echo "Wow!!!";
        echo "</br>";
        echo $flag;
}
```

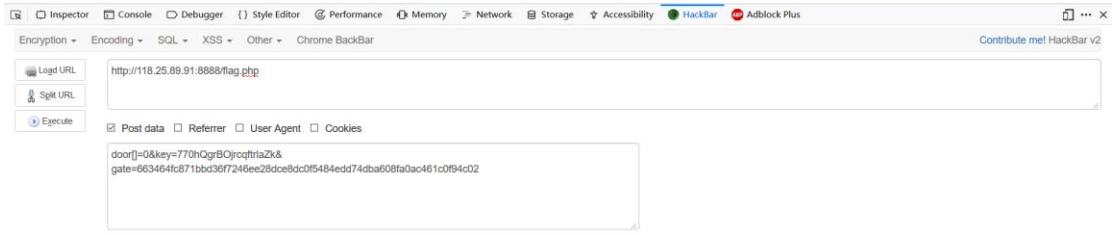
md5弱比较，为0e开头的会被识别为科学记数法，结果均为0

```php
<?php

if (empty($_POST['hmac']) || empty($_POST['host'])) {
    header('HTTP/1.0 400 Bad Request');
    exit;
}

$secret = getenv("SECRET");

if (isset($_POST['nonce']))
    $secret = hash_hmac('sha256', $_POST['nonce'], $secret);

$hmac = hash_hmac('sha256', $_POST['host'], $secret);

if ($hmac !== $_POST['hmac']) {
    header('HTTP/1.0 403 Forbidden');
    exit;
}

echo exec("host ".$_POST['host']);
?>
```

```php
if (empty($_POST['gate']) || empty($_POST['key'])) {
    highlight_file(__FILE__);
    exit;
}

if (isset($_POST['door'])){
    $secret = hash_hmac('sha256', $_POST['door'], $secret);
}

$gate = hash_hmac('sha256', $_POST['key'], $secret);

if ($gate !== $_POST['gate']) {
    echo "Hacker GetOut!!";
    exit;
}
```

像吗？看一下查一下就会了。

Warning: hash_hmac() expects parameter 2 to be string, array given in **/code/flag.php** on line **14**
Wow!!!
hgame{Php_MayBe_Not_Safe}



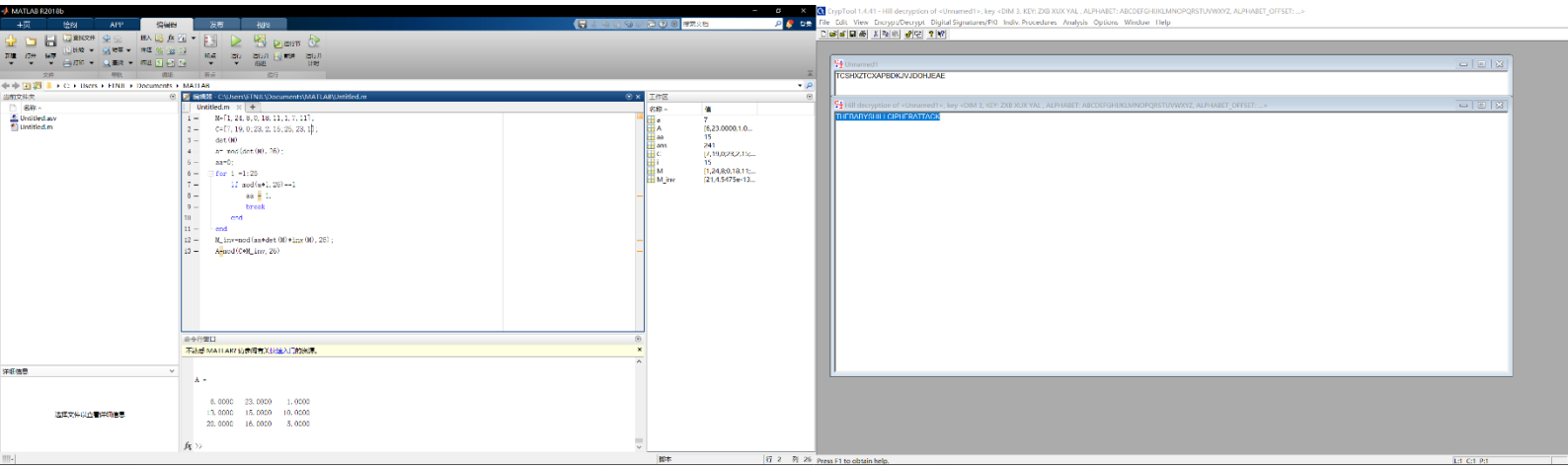
找个搞 pyc 的网站放一下


```
print 'Plz Input Your Flag:\n'
enc = raw_input()
len = len(enc)
enc1 = []
enc2 = ''
aaa = 'ioOavquaDb}x2ha4[~ifqZaujQ#'
for i in range(len):
    if i % 2 == 0:
        enc1.append(chr(ord(enc[i]) + 1))
        continue
    enc1.append(chr(ord(enc[i]) + 2))

s1 = []
for x in range(3):
    for i in range(len):
        if (i + x) % 3 == 0:
            s1.append(enc1[i])
            continue

enc2 = enc2.join(s1)
if enc2 in aaa:
    print "You 're Right!"
else:
    print "You're Wrong!"
```

读一下发现就是个 ascii 变一下抓住格式 hgame{}的变体 iibof} ~
抓住，看一下 123123 的顺序。那个 in 开始让我是子字符串就是是 aaa 的截断部分
后来一搞发现是 9+9+9 抓住中间的标蓝那一串。好，解。

二维码，你查一下，定位码，矫正码，看到中间有个矫正码，想到补外面的定位码（别补里面去了）

HILL



千万不要手算，千万千万。

多翻翻文章（这题好像是个 matlab 的实验改的？）