

Level - Week 1
Level - Week 2

Are You Familiar with DNS Records?(已完成)

描述

well, you know, this is a song-fen-ti, have fun! XD

URL <http://project-a11.club/>

基准分数 50

当前分数 50

完成人数 28

如题就是去查一下他的解析记录（注意网站有些查不到）

599	flag=hgame(seems_like_you_are_familiar_with_dns)
599	v=spf1 include:spf.mail.qq.com ~all

Vigener~

描述
普通的Vigener
URL <http://plir4axuz.bkt.cloudcdn.com/hgame2019/orz/ciphertext.txt>

基准分数 150
当前分数 150
完成人数 73

Vigenere cipher breaker

Ciphertext text

gzalzvz atxiuzozjshfi. Ests twgvfi zsby xjaks xg asjpwekhx wfilchloir kunyqwk zbel sxy ikkkhxsrfc Namyrwjk wmhzkIw. Af kckzlkYr kadnc lzxyi, Xjoyhjaib Oskomoa ogm xzw lcvkl zi tmtrcwz s myrwjgf qwlnih gx jygaahnyvafm Pmywtyvw uojlwjy. Nlw Noaifwxy gahnyv osy ivayohedde xikuxcfwv hs Kagbur Tsznmklg Viddgms af ncw gfk nlgmyurv xopi zmtxvww ghH xalnc-gfk vsgc Ru gaxxu hwd. Yck. Yaupef Tgnxakzu Fwdruwg, tan xzw ywlwek qek dgnij eomellxcfmIxx xg Trumkw jy Zaykhijw oh xzw tcrwln wiflalc sfj ms suwomjwj cxx hxywwfz heew. Ifey ay ajqmenycpgImqqjzndhrqpvtaniz

Edit frequencies
Show another possible solutions

Max key length to try
30

CALCULATE

Key
GUESS

Decoded message
The Vigenere ciphe is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It is a form of polyalphabetic substitution. The cipher is easy to understand and implement, but it resisted all attempts to break it for three centuries, which earned it the description le chiffre indechiffable. Many people have tried to implement encryption schemes that are essentially Vigenere ciphers. In eighteen sixty three, Friedrich Kasiski was the first to publish a general method of deciphering Vigenere ciphers. The Vigenere cipher was originally described by Giovan Battista Bellaso in his one thousand five hundred and fifty-one book La cifra del. Sig. Giovan Battista Bellaso, but the scheme was later misattributed to Blaise de Vigenere in the nineth century and so acquired its present name. flag is gfyuytukxariyydfjlplwsxdbzvwqt

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

帶你去看浪漫的曼城（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

[illegible]

Decoded

```
0110100001100111011000010110110101001010111101100110011011001100011001000110100011001010011011000110111001101010011100110101001110010011000101100101001110010110001101100010011000010110001000110010011000010011011011001000011001001100011000110001101100110100001110000110000100110001011001000011010001111101
```


<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

6867616d657b33663234653536373539316539636261623261376432663166373438613164347d

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

$\epsilon = \epsilon = \epsilon = \epsilon = \epsilon = r(\overset{\frown}{\circ})^J$

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)

ASCII
C Arrays
EBCDIC
Hex 转储
UTF-8
UTF-16
YAML
原始数据

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

```
secret.log - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
# SSL/TLS secrets log file, generated by NSS
CLIENT_RANDOM 0fa06615c2088314702b07a32670ae892e08def575d9310568751f0aa202e8b3 d8aa106d5fe72e539fcf425e7913e86206441cba3
CLIENT_RANDOM aa7275fdd77bee786f0a2bf3486dd87f1bc047fadfb07246775d4cd70d0b0f2b7 079981461ec64c7a34cf9f56450bd908d416722b
CLIENT_RANDOM 7c951ce3077f2f12e1e548f147fbf107bce06b65ac14f74139c43e02a86bd4f bae135eb481d64d677501f11b263777f70d2a5682e
CLIENT_RANDOM fd8bce0a2d0d9e583331b70dfb48dfcda55bc2fca57b9efe47a98af2339e75d c306a2088d467096a5f97d6c7f19a454234471b12
CLIENT_RANDOM 8d280d9d185e1fe700c3f3d5676372624ff3a0a2f2c97dc0e088c790144720965 40578b5612e66b781d418a475eb693f4e652a5a4
CLIENT_RANDOM c7708d17f79821b08e76c1b366fd244064febb406945be7afb2e2e2adb9ee79a 0b4e0d606c99d01e752719cb1255a0e3ed1aca6f
CLIENT_RANDOM 2c770ace95ef98ffbf300acd77d0cb1233d923235a50eed92f8d7dc593bcebc 8c84b8d25b925220391598429717a4a3b81258cb
CLIENT_RANDOM 5ea69e87ff49b964d13660b1769a9827bfe60281c767fc363c173d7fd6721c34 e2815aca2e1e3365e3d69429eb467a6065400f86c
CLIENT_RANDOM a5b08ce605712d2460df0f3dcef045b138341b11933daeb38318772b98c5a527 40578b5612e66b781d418a475eb693f4e652a5a
CLIENT_RANDOM 83483f4fee385bf1b93c58643ab1a5ac6e7533d991aacfcedc5ef22fa92f417 40578b5612e66b781d418a475eb693f4e652a5a4a8
CLIENT_RANDOM 7a5d1843b52d4fa90371e553b4dbe05b964b97849762a8f36efa0fa6b957ee44 c6563f07e5480c8d5a9cb6973feb205cb1f124de
CLIENT_RANDOM bd859854a0b5d691c8a0042d838376fcf09b9eb376ee51974a18f381955a63fb 2c62b3094ded55c85a05ec570925d9ea19e8410f
CLIENT_RANDOM 280a0b20508b2bc06386129b36d028966e754d940c0ee023f8d9528627f7f3f4a 79c73e7f2f00bce4690f47d70ff63abe9e94538e7
CLIENT_RANDOM aa1bad2e8089c69e883a44ba65cfa583f0b1be2c3ff824f23efcdd584d6546 f4e1c93932aaf81a75a6066b3d7d4fc6363eb8cdca
CLIENT_RANDOM f80b069d9d22b48f56ce7f9f0e8692ec4110e98a97aeec46923859bf34e0ad0 9806d42b9dacbc38db5c6d67d70c05cd21215c3d
CLIENT_RANDOM 5c5afcb6ebc7b48ec4026a7123cab56d63b270a3c9831f99abe42635a04541d0 346b5fa6b5f1046cf851bef51ead0d30970cd5feb
CLIENT_RANDOM 61d9653adca25ff547a4a6ede2b7063169885e0e0811d849a0273cba8d912e26 ac792cb0b1242f606a6f8cf8d1a4f75890158f5ed
CLIENT_RANDOM a86427959343be854e179e531bbb29a4c2643a10536cd9fb00a7b9ba9c95721 aacca0af662d67e36b8ab97673f13e3cddcf6a0d
CLIENT_RANDOM 2a8a9f8b9fdae62aa40785ac26fa95087963e624cf9d81ff34470ae046b0f6fd e86356128a3e3aa146354b4e6b4402111c868c306c
CLIENT_RANDOM 7a6d9c3e673bf6a024bdebb1d4832cb4473e0ebdb8cfe82c2e4043c1d34fdbfc 0d254908366fe60e8144b4aab72d57ca6d6c4d4f
```

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

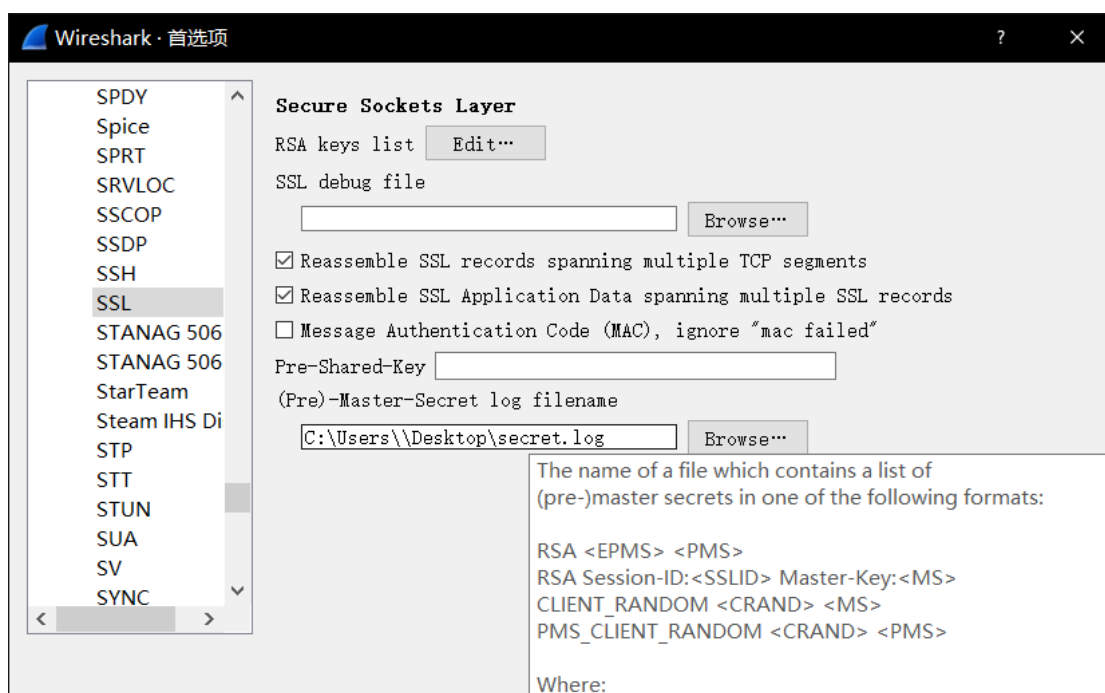
能发现这是一份 **NSS Key Log Format** 的文件, 而这个文件是能解密出 Wireshark 里面的 https 流量的。

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](#)

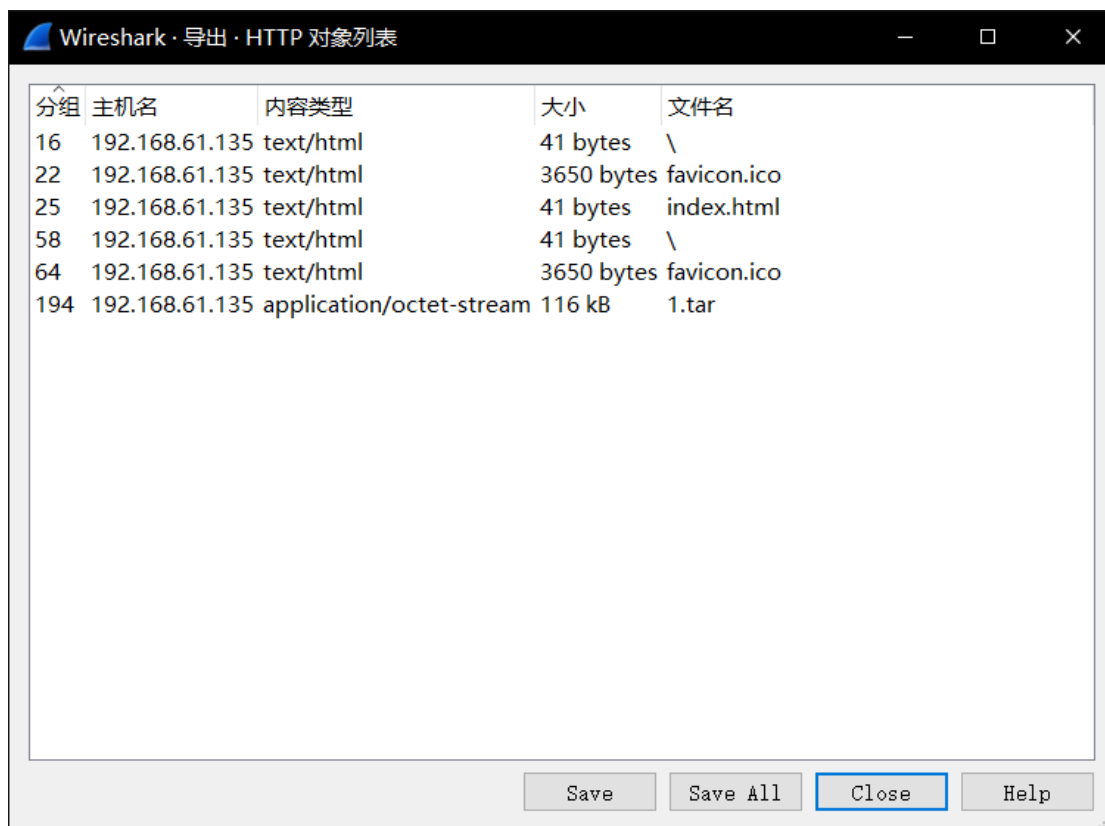
你搞到那个 ssl 里去



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 00 01	01 00 00 00	51 11 00 04	00 00 00 01	00 00 00 01Q.....
00 00 0E C3	51 12 00 04	00 00 00 01	00 00 0E C3	00 00 0E C3	...ÃQ.....Ã
82 98 00 02	00 00 00 17	00 00 00 80	00 00 00 00	00 00 00 00	,~.....€....
43 6C 69 70	49 6D 67 47	65 74 20 76	65 72 2E 20	65 72 2E 20	ClipImgGet ver.
31 2E 30 2E	32 00 00 01	86 A0 00 00	B1 8F 68 67	B1 8F 68 67	1.0.2...† ..±.hg
61 6D 65 7B	43 6F 6E 67	72 61 74 75	6C 61 74 69	6C 61 74 69	ame{Congratulati
6F 6E 73 5F	00 00 FF FE	00 13 59 6F	75 5F 47 6F	75 5F 47 6F	ons_..ýþ..You Go
74 5F 54 68	65 5F 46 6C	61 67 7D FF	DB 00 43 00	DB 00 43 00	t_The_Flag}ýÛ.C.
02 01 01 01	01 01 02 01	01 01 02 02	02 02 02 04	02 02 02 04	

easy_php

描述

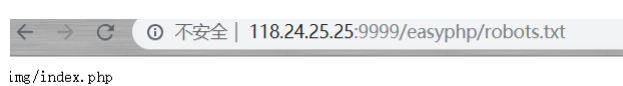
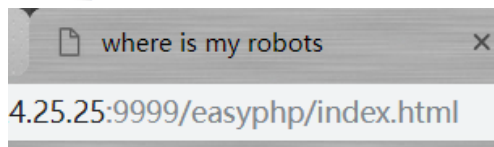
代码审计♂第二弹

URL <http://118.24.25.25:9999/easyphp/index.html>

基准分数 150

当前分数 150

完成人数 98



##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!}

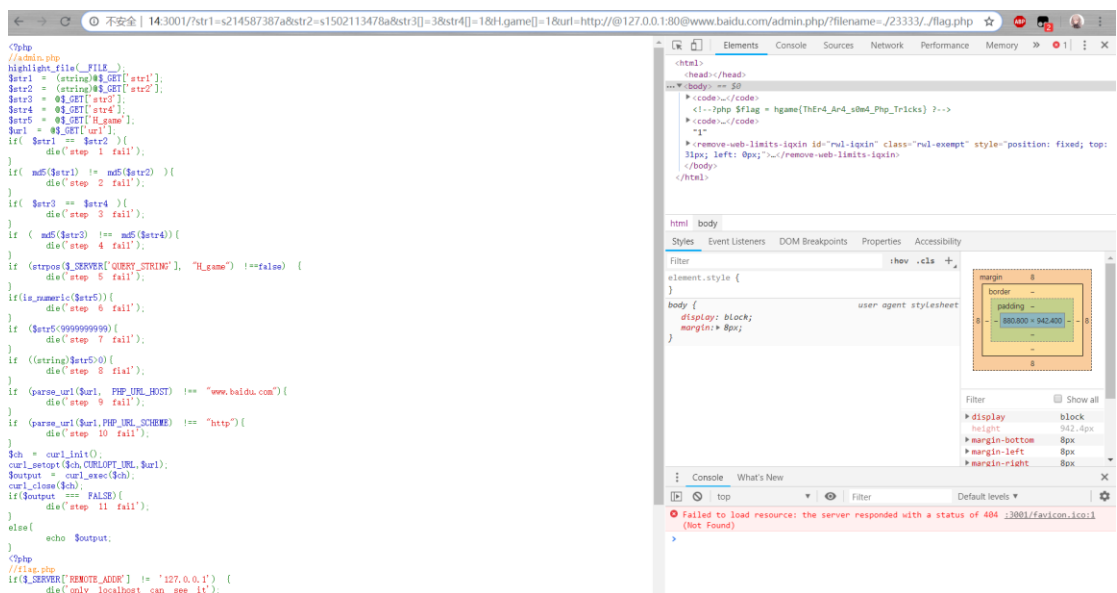
```
118.24.25.25:9999/easyphp/img/index.php?img=php://filter/convert.base64-encode/resource=.../flag

PD9waHAKICAgIC8vJGZsYWcgPSAnaGdhbWV7WW91XzRyZV9Tb19nMG9kfcSc7CiAgICBIY2hviCjtYXliZV95b3Vfc2hvdWxkX3RoaW5rX3RoaW5rIjsK <?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

```
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  
  
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']);  
?>
```



```

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

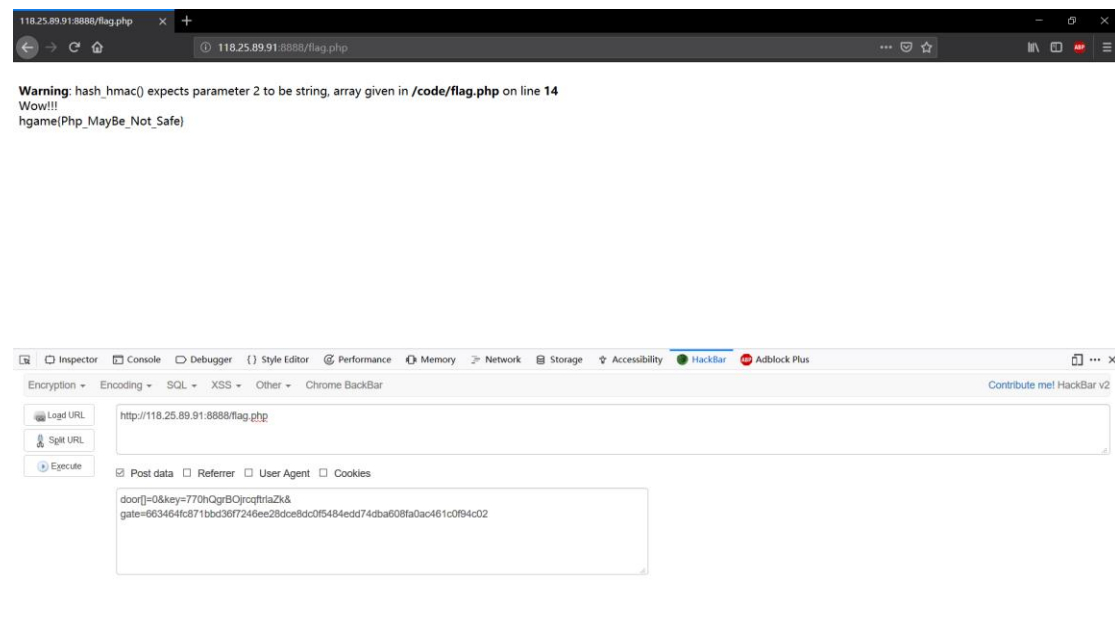
if (isset($_POST['door'])) {
    $secret = hash_hmac('sha256', $_POST['door'], $secret);
}

$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。



找个搞 pyc 的网站放一下

请选择pyc文件进行解密。支持所有Python版本

选择文件

未选择任何文件

```
print 'Plz Input Your Flag:\n'
enc = raw_input()
len = len(enc)
enc1 = []
enc2 = ''
aaa = 'io0avquaDb}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

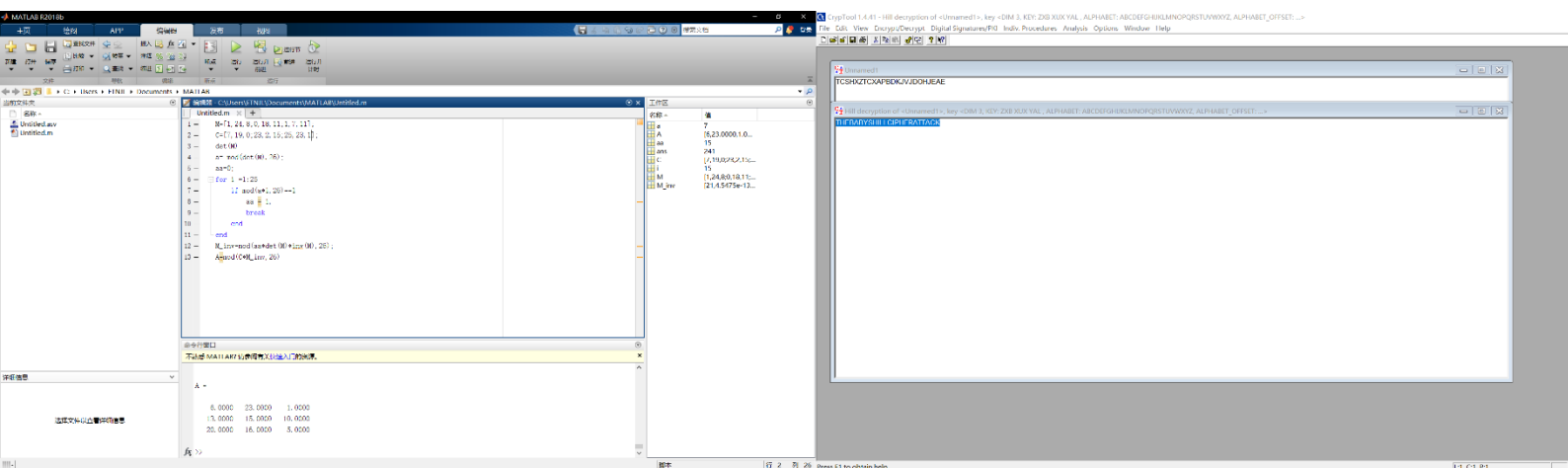
enc2 = enc2.join(s1)
if enc2 in aaa:
    print "You 're Right!"
else:
    print "You're Wrong!"
```

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？）