

## Web

### 1. easy\_php (没学完 php, 时间不够)

打开源代码, 发现提示,  
应该和 robots.txt 有关,  
根目录下输入 robots.txt,  
发现 img/index.php, 输入,  
出现 php, “./” 被 “” 替换, 应该  
在根目录有文件, 用御剑扫描根目录, 发现  
flag.php, 但提示  
maybe\_you\_should\_think\_think。查资料后  
感觉是 lfi 的问题, 需要截断, emmm, 到  
8 点了……

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=
  <meta http-equiv="X-UA-Compatible" co
  <title>where is my robots</title>
</head>
<body>
  come on ! second wait you
</body>
</html>
```

## Misc

### 1. Are You Familiar with DNS Records?

关于 dns 记录, cmd 指令 nslookup 来查看记录, 最后在 txt 记录里发现 flag。

```
> set type=txt
> project-all.club
服务器: UnKnown
Address: 192.168.1.1

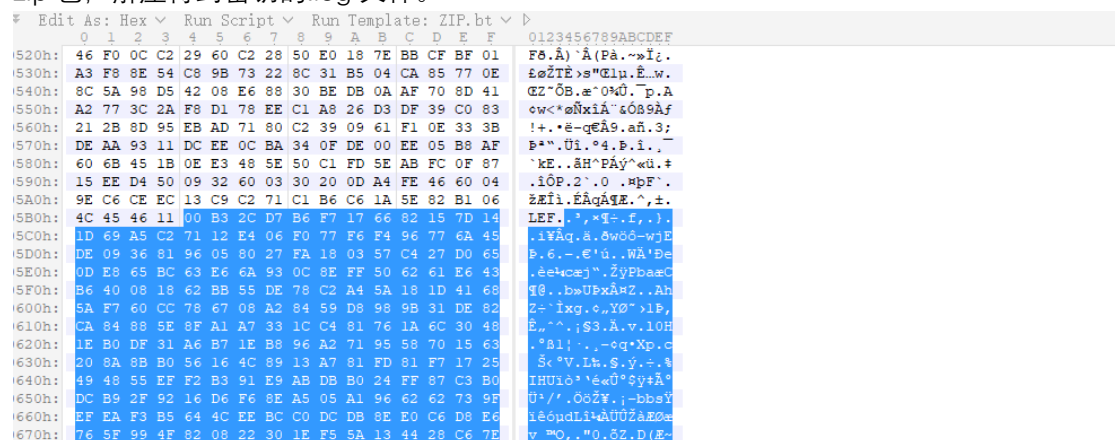
非权威应答:
project-all.club      text =
    "flag=hgame{seems_like_you_are_familiar_with_dns}"
project-all.club      text =
    "v=spf1 include:spf.mail.qq.com ~all"
>
```

### 3. 找得到我嘛? 小火汁

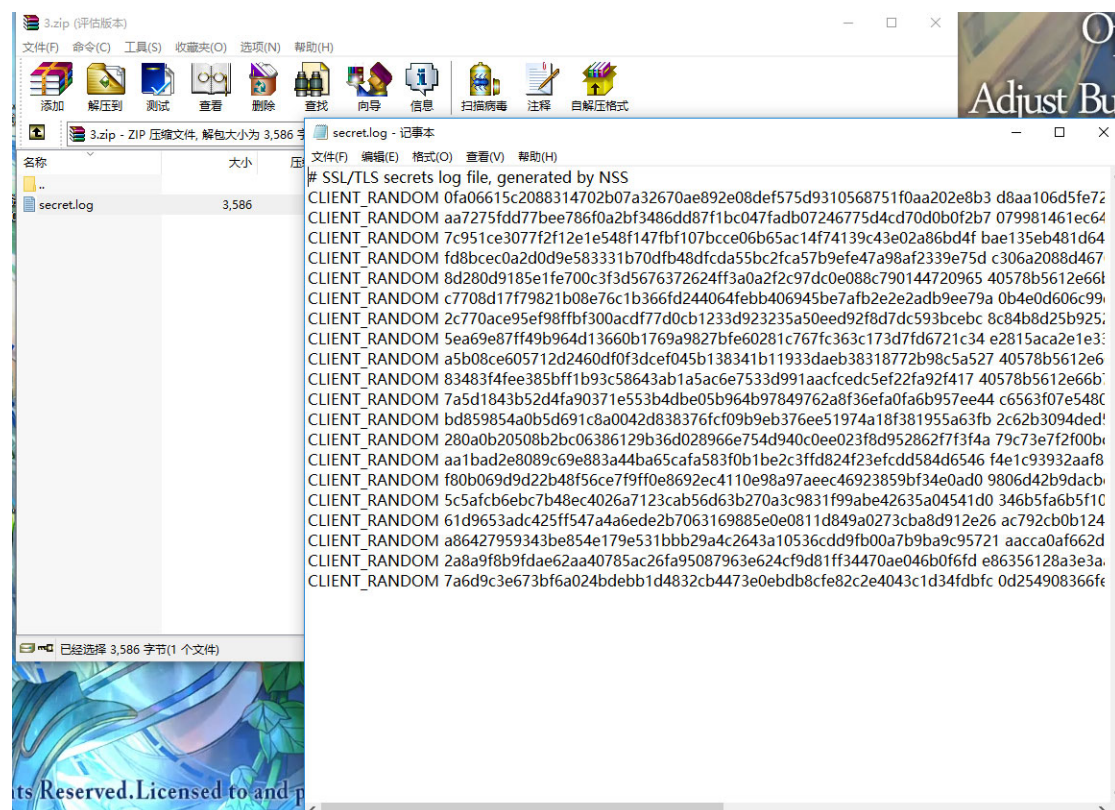
下载文件为流量包, hng 提示 https, 应该是与 ssl 解码有关。解码需要密钥, 用 binwalk 分析流量包, 发现有密钥文件的压缩包。

```
58638      0x26BAE      XML document, version: "1.0"
59526      0x26F26      XML document, version: "1.0"
60246      0x271F6      XML document, version: "1.0"
60946      0x274B2      XML document, version: "1.0"
61666      0x27782      XML document, version: "1.0"
63246      0x27DAE      XML document, version: "1.0"
80878      0x2C28E      Zip archive data, at least v2.0 to extract, compressed size: 1862, uncompressed size: 3586
name: secret.log
82960      0x2CAB0      End of Zip archive, footer length: 22
84966      0x2D286      XML document, version: "1.0"
85666      0x2D542      XML document, version: "1.0"
86510      0x2D88E      XML document, version: "1.0"
87210      0x2DB4A      XML document, version: "1.0"
```

用 Wireshark 打开流量包, 查找 zip 字符, 无结果, 查找 zip 头文件 16 进制代码, 发现 ftpdata, 且有两个, 发现一个没有头文件, 一个没有尾文件, 感觉是压缩包被拆成了两个, 选中两组数据到处有分组字节流, 用 010editor 将尾文件数据复制到头文件数据下, 另存, 得到完整 zip 包, 解压得到密钥的 .log 文件。



Template Results - ZIP.bt					
Name	Value	Start	Size	Color	Comment
struct ZIPFILERECORD record		0h	0h	Fg: Bg:	



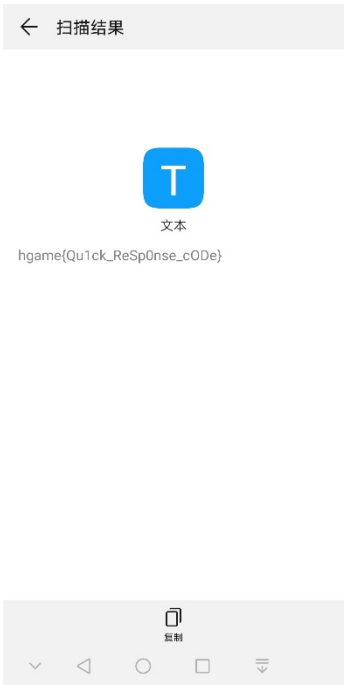
Wireshark 首选项中 ssl 导入 .log, 发现数据得到解码, 找了半小时, 发现导出 http 对象有新文件, 其中有 zip 包, 导出后解压用 010editor 打开发现 flag



下载解压，将文本复制到网页得到不完整的二维码，看了下和二维码有关的东西，应该是少了定位用图案的 QR code，ps 手动绘制 8\*8 的定位用图案（加白框）修补，在 25\*25 试了半天行不通后开始尝试各种尺寸，发现 33\*33 可用



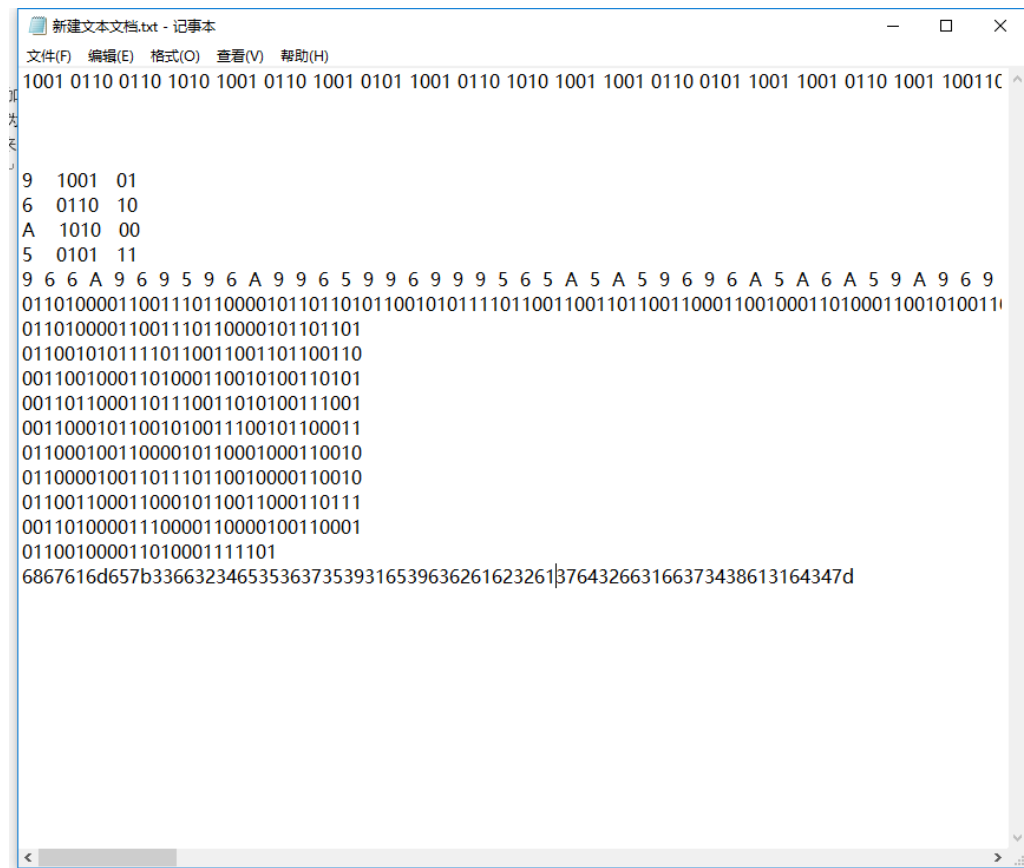
扫描得 flag



## CRYPTO

### 1. 浪漫的足球圣地

以为和足球有关，百度加常用密码查询发现原来是曼彻斯特密码，和计算机有关的编码和解码应该是 IEEE 802，应为只表示为 0 和 1，所以将原文转为二进制（真的长，长到没法在线转换只能手动操作，后来发现根本不用转二进制……），再根据规则转换，得到新二进制代码，转为字符串得到 flag。

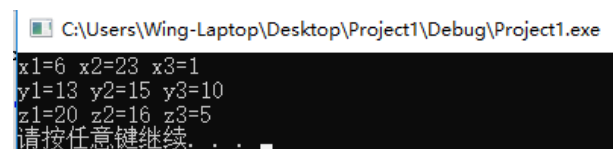


```
新建文本文档.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
1001 0110 0110 1010 1001 0110 1001 0101 1001 0110 1010 1001 1001 0110 0101 1001 1001 0110 1001 10011C
9 1001 01
6 0110 10
A 1010 00
5 0101 11
9 6 6 A 9 6 9 5 9 6 A 9 9 6 5 9 9 6 9 9 5 6 5 A 5 A 5 9 6 9 6 A 5 A 6 A 5 9 A 9 6 9
01101000011001110110000101101101011001010111101100110011011001100011001000110100011001010011
01101000011001110110000101101101
01100101011110110011001101100110
00110010001101000110010100110101
00110110001101110011010100111001
00110001011001010011100101100011
01100010011000010110001000110010
01100001001101110110010000110010
01100110001100010110011000110111
00110100001110000110000100110001
011001000011010001111101
6867616d657b33663234653536373539316539636261623261b376432663166373438613164347d
```

### 2. hill

希尔密码，现代问题，将字母转为矩阵。  
密钥为 3\*3 矩阵，与下方矩阵相乘模 26  
为上方矩阵的一个 3\*3 子矩阵，用 c 语言  
(一个一个试过去) 得到密钥矩阵为

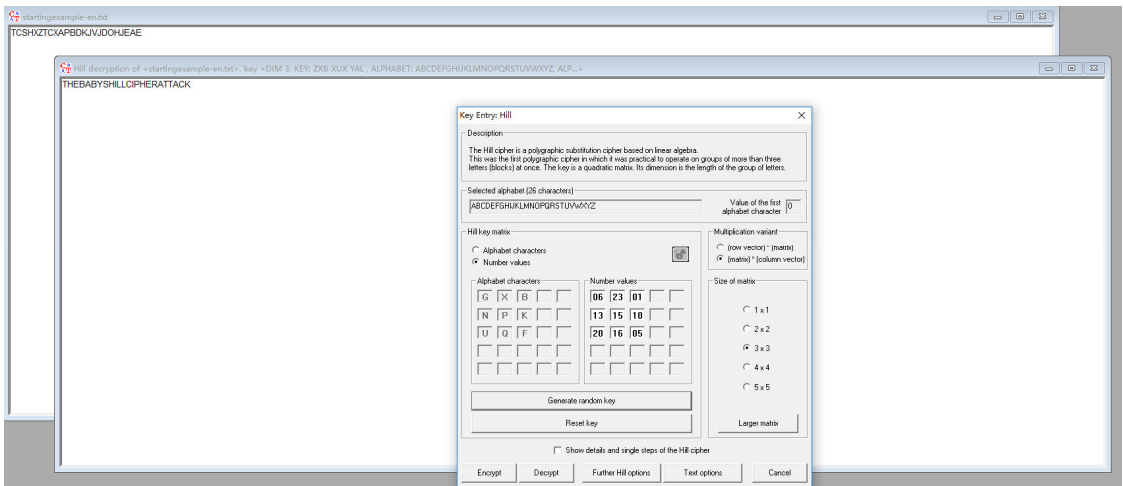
```
| 19 7 19 0 3 21 14 4
2 23 2 15 10 9 7 0
18 25 23 1 9 3 9 4
```



```
C:\Users\Wing-Laptop\Desktop\Project1\Debug\Project1.exe
x1=6 x2=23 x3=1
y1=13 y2=15 y3=10
z1=20 z2=16 z3=5
请按任意键继续. . .
```

```
1 24 8
0 18 11
1 7 11
```

用 cryp tool 解密得 flag。



3. Vigenere

维多利亚密码，上解密网站直接得 flag。

Result

Clear text [hide]

Clear text using key "guess":

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 gfyuytukxariyydfjlpwxsdbzwwqt