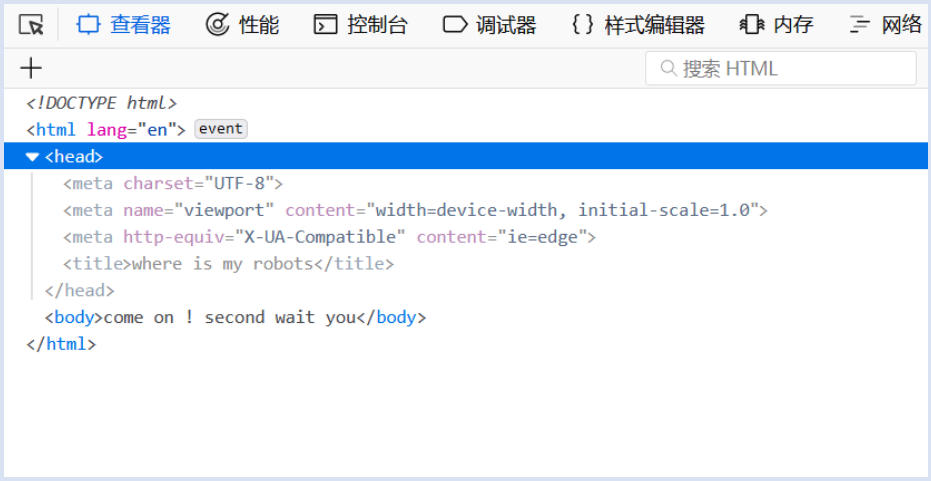
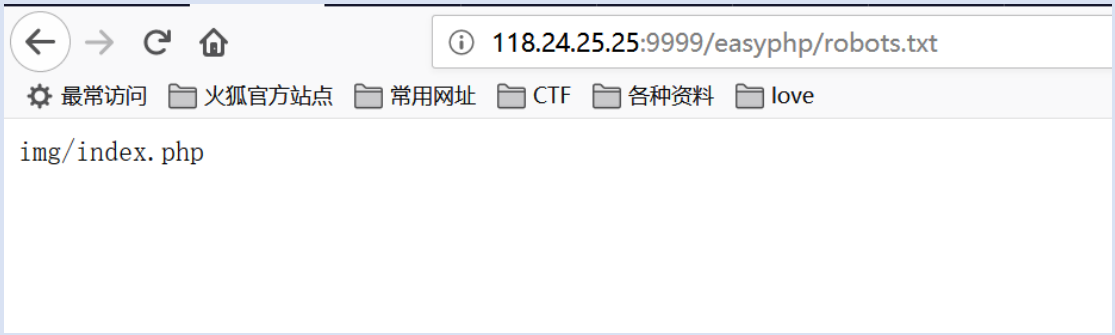
Web

easy_php

url: http://118.24.25.25:9999/easyphp/index.html



进去之后看源码，注意到标题是 where is my robots，于是去查看 robots.txt 文件。(这是一个协议文件，里面一般标明了重要的页面路径，表示这些页面是不能被爬虫抓取的。这也为我们的做题提供了一些线索)



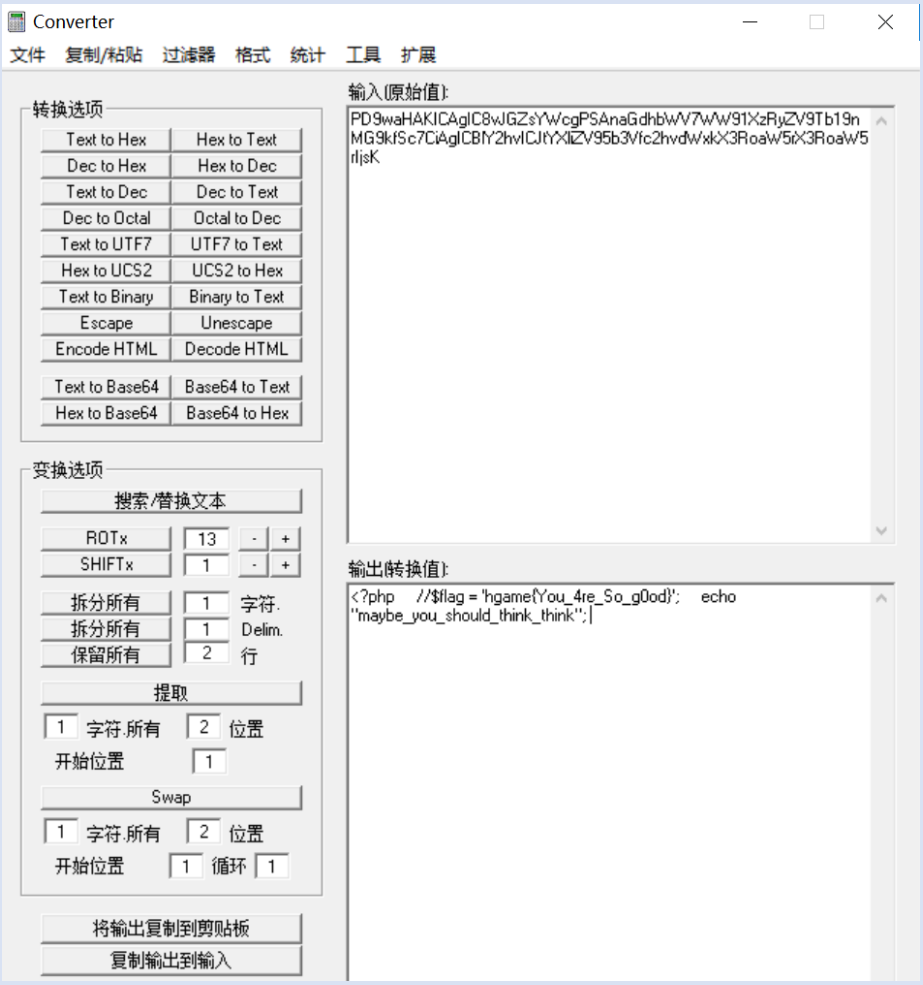
于是去查看 img/index.php (进来就是 xx 社区，滑稽)

代码审计时间：str_replace('../', ' ', $img)会把变量 img 里的../替换成空格，所以可以构造..././绕开这一判定。首先我发现在 easyphp 目录下有一个 flag.php 文件。我一开始尝试

了?img=..././flag 发现不行

然后思路断了，去问了 hint 之后才意识到这里的 include_once 可能存在文件包含漏洞。尝试如下构造（可以得到 flag.php 的源码并且以 base64 编码方式显示）

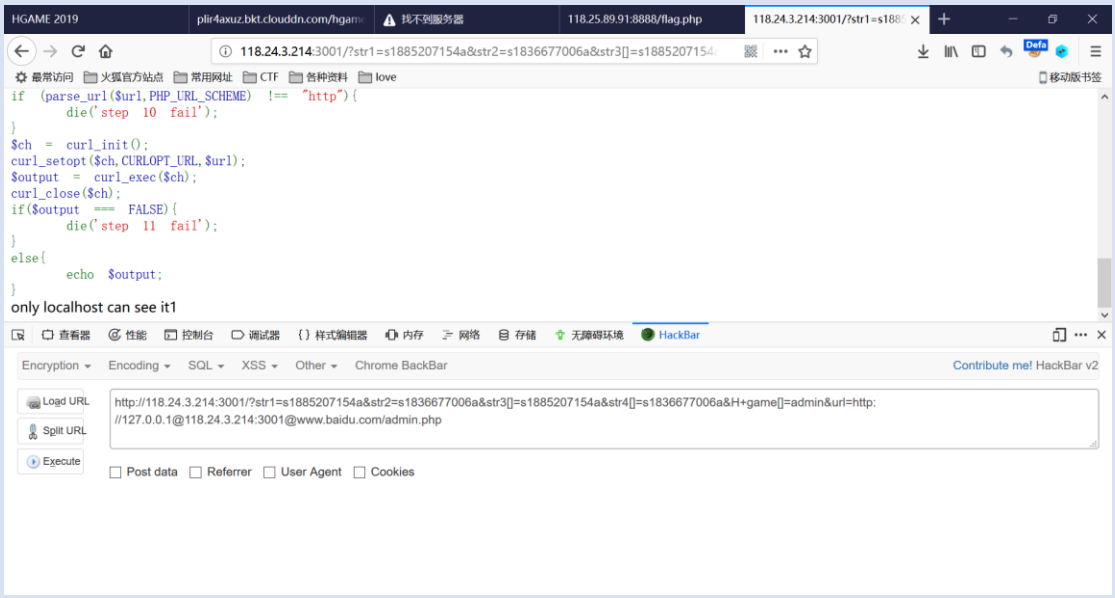
解码后得到 flag



php trick

url：http://118.24.3.214:3001/

这题没做出来……但还是想保存一下解题进度。构造如下，前面 11 步都绕过了，也成功在页面返回了 admin.php 的内容，但是还是在 localhost 这卡住了。等官方 wp 出来后看看到底应该怎么做吧。



Misc

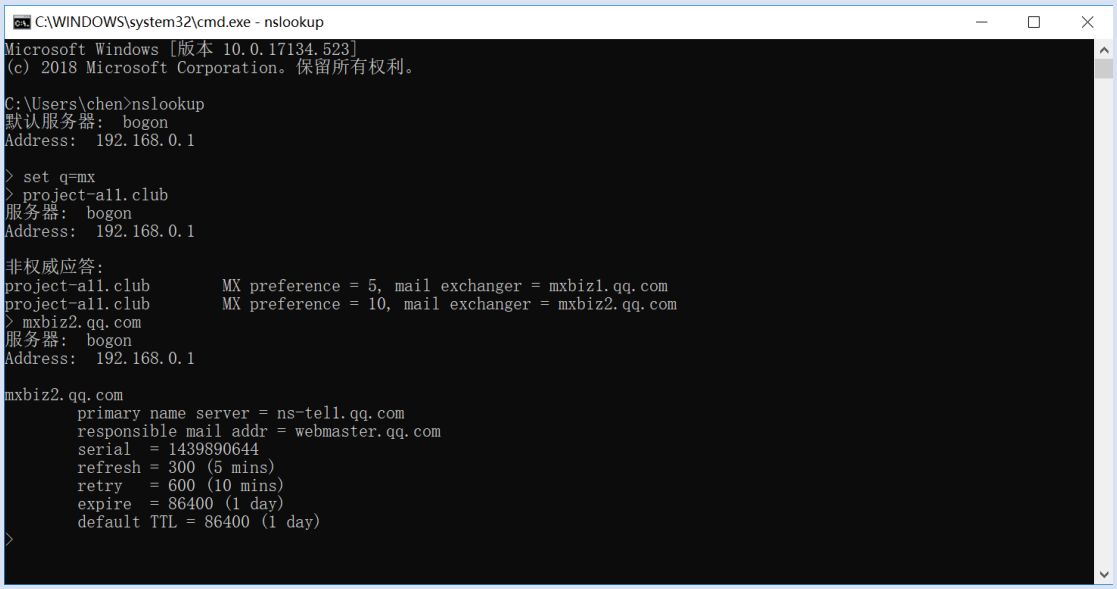
Are You Familiar with DNS Records?

url： http://project-a11.club/

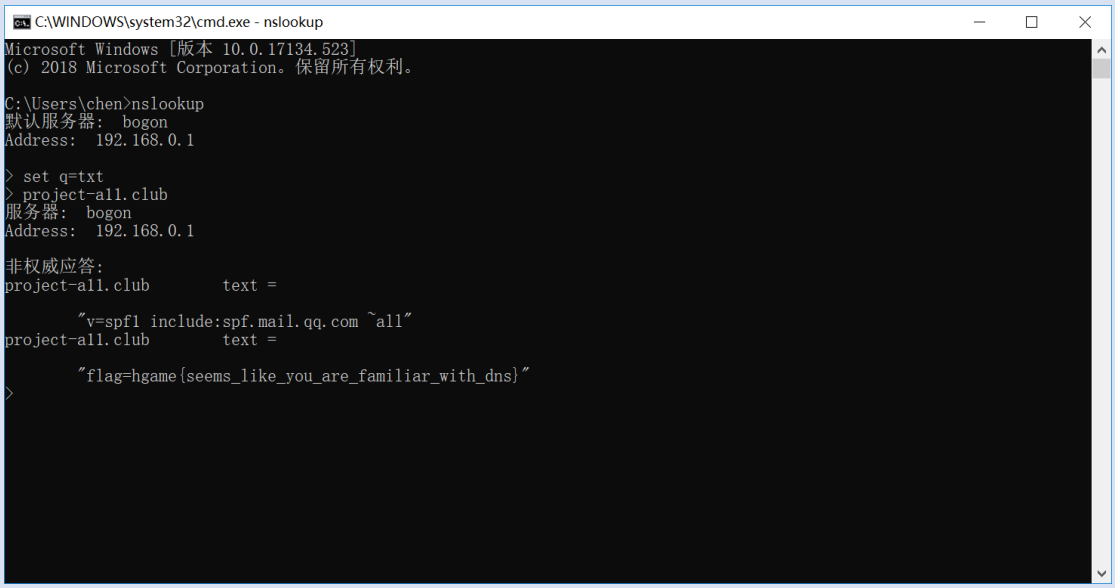
一开始尝试用 wireshark 抓包，但是抓到的 dns 包里什么都没有。
hint 放出来之后：

然并卵的hint: DNS 有很多种不一样的记录类型，其中一种类型如果没有正确设置就可能被其他邮件服务器拒收，flag 就在此域名的第二条此类型记录里

查资料了解了下 dns 的各个记录类型，好像是 mx 记录如果把值设置成 IP 地址（本来应该设成主机名），邮件就会被拒收。
于是查了下怎么看 mx 记录，用命令行里的 nslookup 操作了一番，但是什么都没有。【什么，难道不是 mx 记录吗？】



想到另一个和邮件接收有关的 dns 记录类型是 txt 记录，所以我就试着查了下 txt 记录，找到了 flag:



初识二维码

url:

http://plqfgjy5a.bkt.clouddn.com/%E5%88%9D%E8%AF%86%E4%BA%8C%E7%BB%B4%E7%A0%81.zip

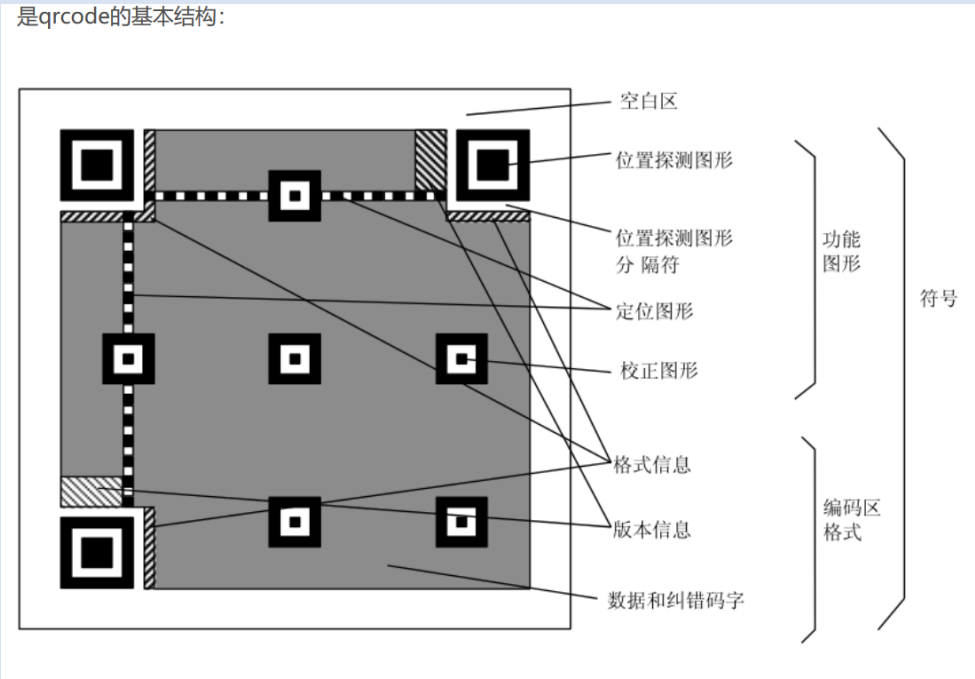
下载下来，解压，打开 txt：可以看出来是图片转 base64。

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

+AAAACXBIWXMAAAsTAAALEwEAmpwYAAAKTWlDQ1BQaG90b3Nob3AgSUNDIHByb2ZpbGUA
AHjanVN3WJP3Fj7f92UPVkLY8LGXbIEAIiOsCMgQWaIQkgBhhBASQMWFiApWFBURnEhVxILVCkidi
OKgKLhnQYqIWotVXDjuH9yntX167+3t
+9f7vOec5/zOec8PgBESJpHmomoAOVKFPDrYH49PSMTJvYACFUjgBCAQ5svCZwXFAADwA3l4fnS
wP/wBr28AAgBw1S4kEsfh/4O6UCZXACCRAOAiEucLAZBSAMguVMgUAMgYALBTs2QKAJQAAGx5
fEliAKoNAOz0ST4FANipk9wXANiiHKkIAI0BAJkoRyQCQLsAYFWBUiwCwMIAoKxAIi4EwK4BgFm2M
kcCgL0FAHaOWJAPQGAAgJlCLMwAIDgCAEMeE80DIEwDoDDSv
+CpX3CFuEgBAMDLlc2XS9IzFLiV0Bp38vDg4iHiwmyxQmEXKRBmCeQinJebIxNI5wNMzgwAABr50c
H+OD+Q5+bk4eZm52zv9MWi/mvwbyI
+IfHf/ryMAgQAEE7P79pf5eXWA3DHAbB1v2upWwDaVgBo3/ldM9sJoFoK0Hr5i3k4/EAenqFQyDw
dHAoLC
+0lYqG9MOOLPv8z4W/gi372/EAe/tt68ABxmkCZrcCjg/1xYW52rlKO58sEQjFu9+cj/seFf/2OKdHiNL
FcLBWK8ViJuFAiTcd5uVKRRCHJleIS6X8y8R+W/QmTdw0ArIZPwE62B7XLbMB
+7gECiw5Y0nYAQH7zLYwaC5EAEGc0Mnn3AACTv/mPQCsBAM2XpOMAALzoGFyolBdMxggAAESg
gSqwQQcMwRSswA6cwR28wBcCYQZEQAwkwDwQQgbkgBwKoRiWQRlUwDrYBLWwAxqgEZrhEL
TBMTgN5+ASXIHrcBcGYBiewhi8hgkEQcgIE2EhOogRYo7YIs4IF5mOBCJhSDSSgKQg6YgUUSLFyHK
kAqlCapFdSCPyLXIUOY1cQPqQ28ggMor8irxHMZSBslED1AJ1QLmoHxqKxqBz0XQ0D12AlqJr0Rq0
Hj2AtqKn0UvodXQAfYqOY4DRMQ5mjNlhXIyHRWCJWBomxxZj5Vg1Vo81Yx1YN3YVG8CeYe8IJAK
LgBPsCF6EEMJsgpCQR1hMWEOoJewjtBK6CFcJg4Qxwicik6hPtCV6EvnEeGI6sZBYRqwm7iEeIZ4lXic

用在线工具重新转成图片后得到一张图片，是二维码的一部分。

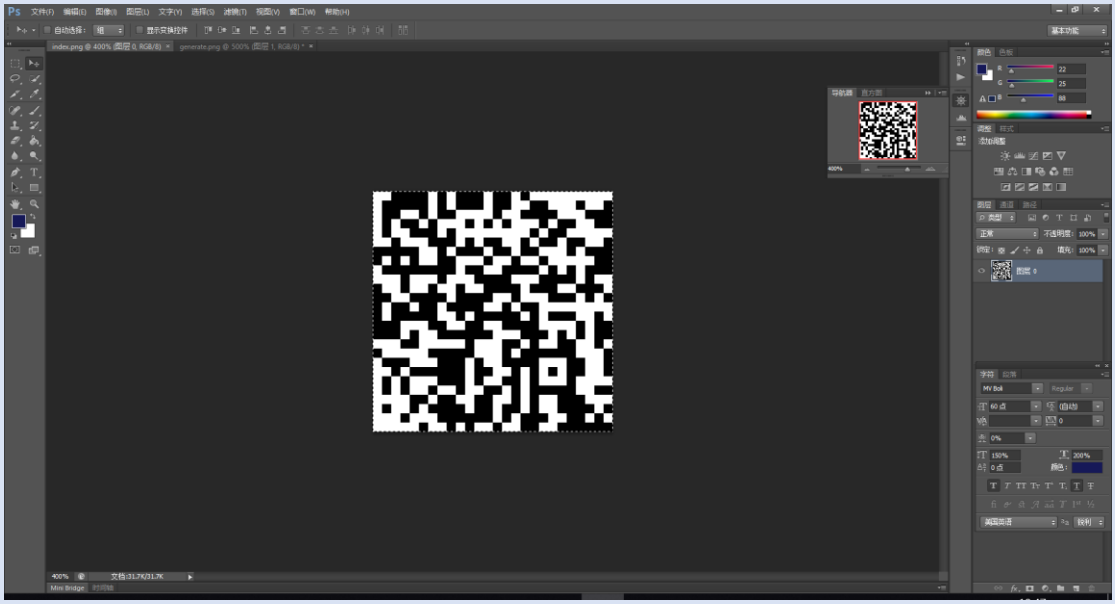
上网了解一下二维码的基本结构就知道二维码的原始数据信息是储存在右下角区域的（就是在我们得到的这张图片里的区域），但是二维码没有位置探测图形和定位图形是识别不出来的。



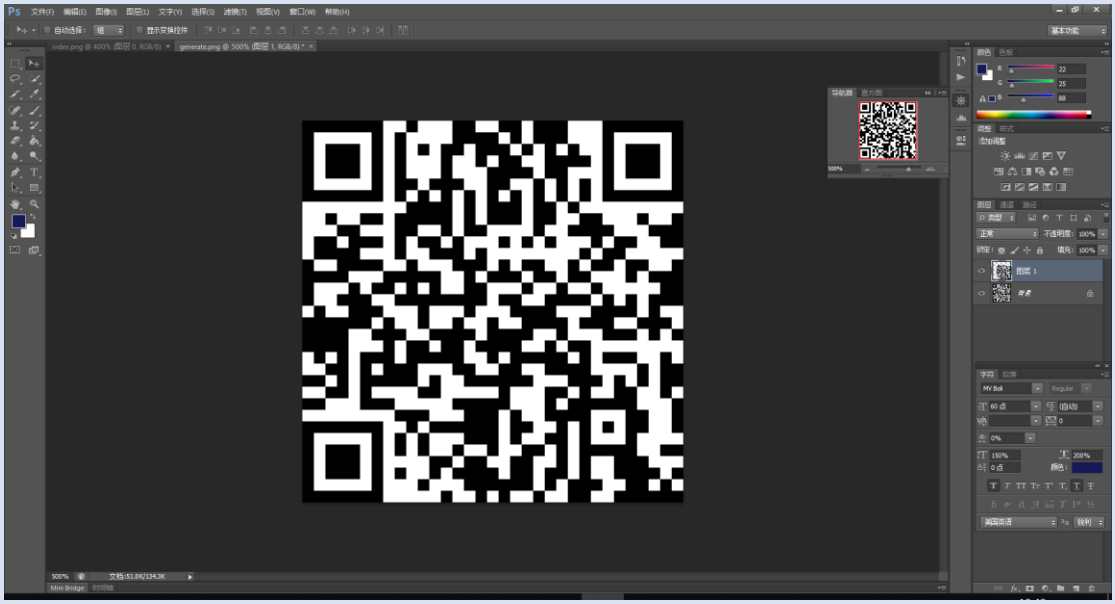
于是我就想随便找个完整的二维码，然后把 base64 解出来的图片覆盖完整二维码

的一部分，这样大概就能识别出原始数据了。

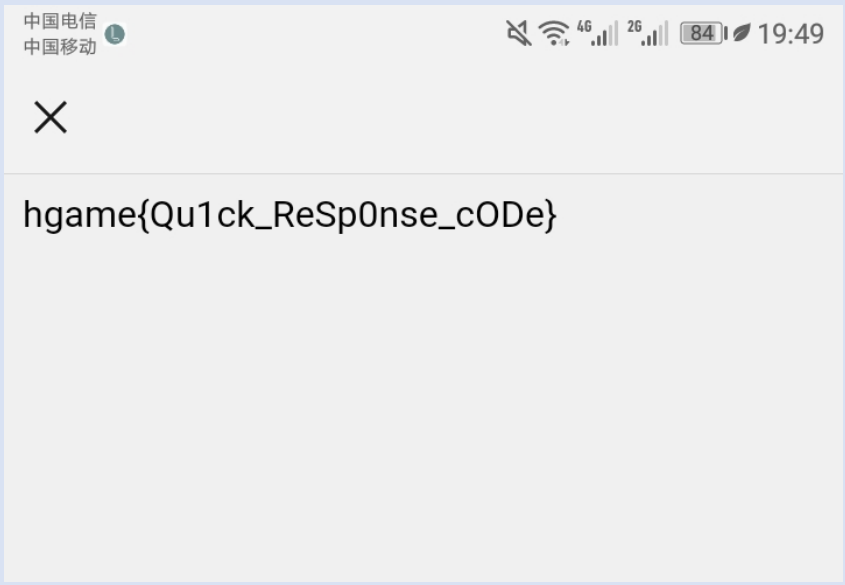
拖进 ps，切掉图片白边，ctrl+c 复制图片：



打开一个我刚在网上随便生成的二维码【记得要保证两张二维码的大小相匹配（我一格格数过来的……）】，ctrl+v 粘贴，然后鼠标拖动，直到完美重合：



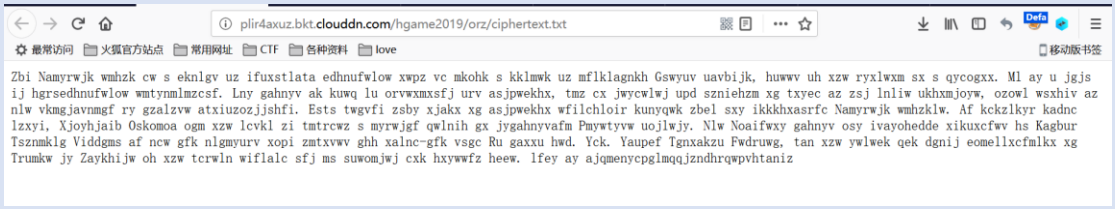
打开手机微信扫描，得到 flag：



Crypto

Vigener~

url：http://plir4axuz.bkt.clouddn.com/hgame2019/orz/ciphertext.txt



把得到的密文放进在线解密工具里直接解密就得到 flag 了