HGAME 2022 Week1 writeup by Halo

CRYPTO

English Novel

阅读`encrypt.py`，大致加密方式为：有一个超长的key，对原文的每一个英语字符进行偏移。符号不变化。
给出了很多四百多篇原文和密文，但没有对应。

`type *.txt >>all.txt`

用`cmd`进入文件夹，用以上命令，把文本全部合到同一个txt内。

利用连续字符（例如`!"`）定位到原文对应的密文。

修改一下python脚本，反推出key，并解密flag。得到两组不完整的flag：（*表示未知）

`*game{*0_y0u_kn0w_'Kn0wn-*la1nt*xt_attack'?}`

`hg*me{*0_y0u_k*0*_'K*0w*-pla1ntext_atta*k'?}`

拼合得到`hgame{*0_y0u_kn0w_'Kn0wn-pla1ntext_attack'?}`

括号内第一个字符位置，猜测为d/D。分别尝试，成功解出。

代码如下（没学过Python，凑活看看）

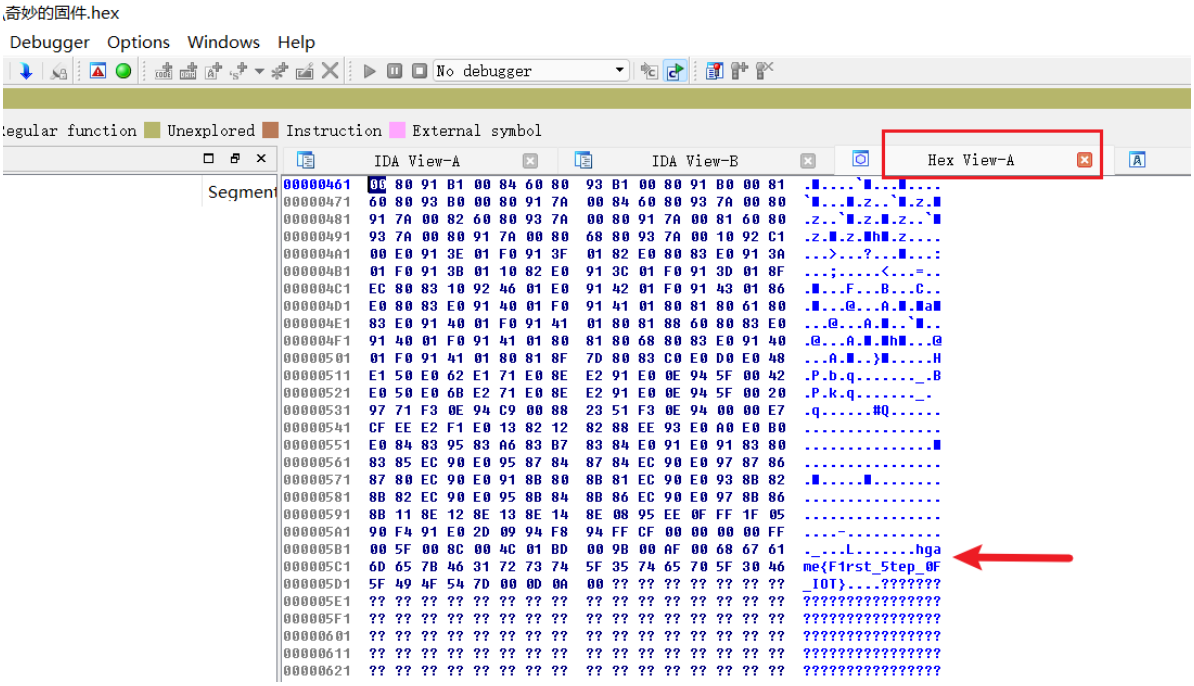
```
data =   "ll did not say.) But he maintained that it could all be done in a
year. And"
result = "oq pjb xxe tiq.) Not ri vmiapdhcez cixy ww vocdj ags wk mkhr mp u
xvqh. Vhx"
```

```
# data =   " read:??'Alfred Simmonds, Horse Slaughterer and Glue Boiler,
Willingdon"
# result = " wwme:??'Lmgzwq Vugmtxht, Hbnvd Shzdheysfhu avv Glpl Wucual,
Akmfcmxtem"
# flag的密文并不长，只需要key前面的部分就足够了
# 符号、空格无法得到key，因此利用两组原文密文，重合可以得到大部分key

##############计算key##############
#assert len(data) <= len(key)
key = {}
for i in range(len(result)):
    if result[i].isupper():
        key[i] = (ord(data[i]) - ord(result[i])) % 26
    elif result[i].islower():
        key[i] = (ord(data[i]) - ord(result[i])) % 26
    else:
        key[i] = 999        #非字母，无法得到key
#print(key)

##############利用计算出的key，得到flag原文##############
data = "klsyf{wO_jOv_caOz_'KsOao-bln1qstxp_juqfqy'?}"
assert len(data) <= len(key)
result = ""
for i in range(len(data)):
    if key[i] < 999:                #对各种情况分别处理
        if data[i].isupper():
            result += chr((ord(data[i]) - ord('A') + key[i]) % 26 + ord('A'))
        elif data[i].islower():
            result += chr((ord(data[i]) - ord('a') + key[i]) % 26 + ord('a'))
        else:
            result += data[i]
    else:
        if not data[i].isalpha():
            result += data[i]
        else:
            result += '*'           #还原失败的字符
print(result)
```

IoT

饭卡的uno

拖入`IDA`，在`Hex`中直接就可找到flag。



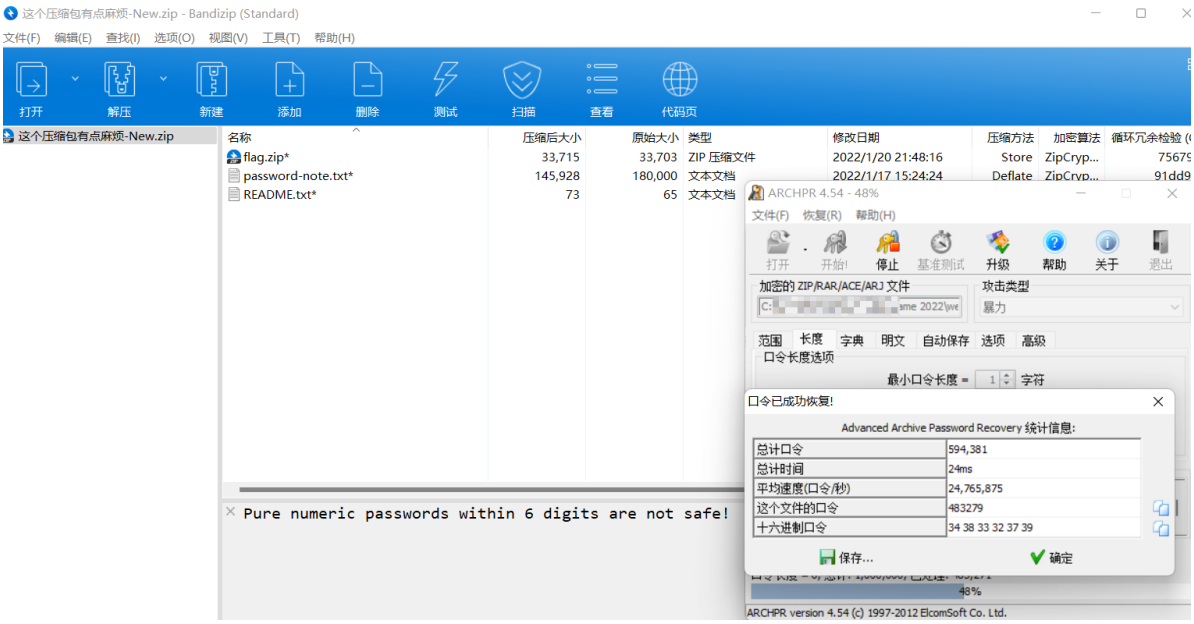
MISC

欢迎欢迎！热烈欢迎！

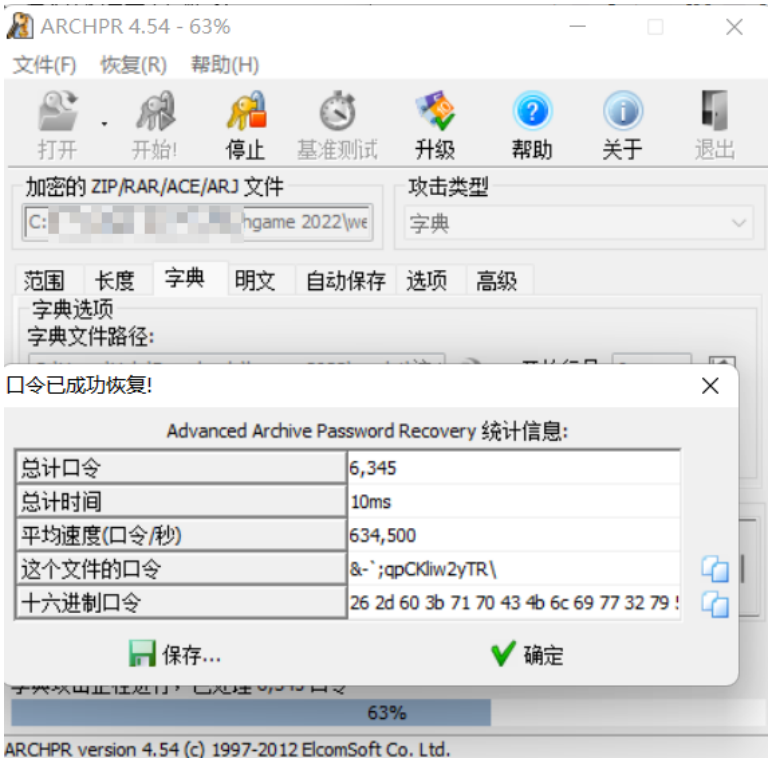
关注“奇安信技术研究院”微信公众号，发送 HelloHGAME2022 获得flag

这个压缩包有点麻烦

第一层：根据提示，6位以内数字，直接 ARCHPR 爆破即可



第二层：有一个字典，于是用 ARCHPR 的字典功能解密

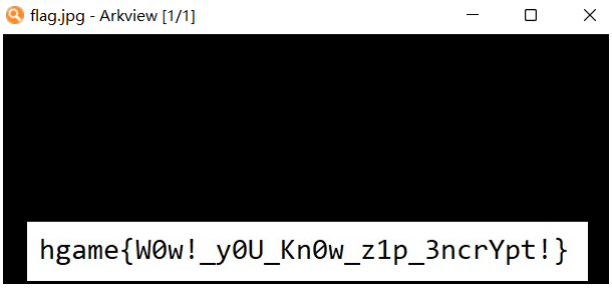


第三层：加密压缩包内外都有一个68字节的`txt`用同样压缩方式打包，尝试明文攻击。明文攻击得到密钥即可获得压缩包内容，无需等待找到口令。

第四层：由上得到`flag.jpg`。`binwalk`发现似乎有个压缩包。分离出来，得到`4FC5.zip`。

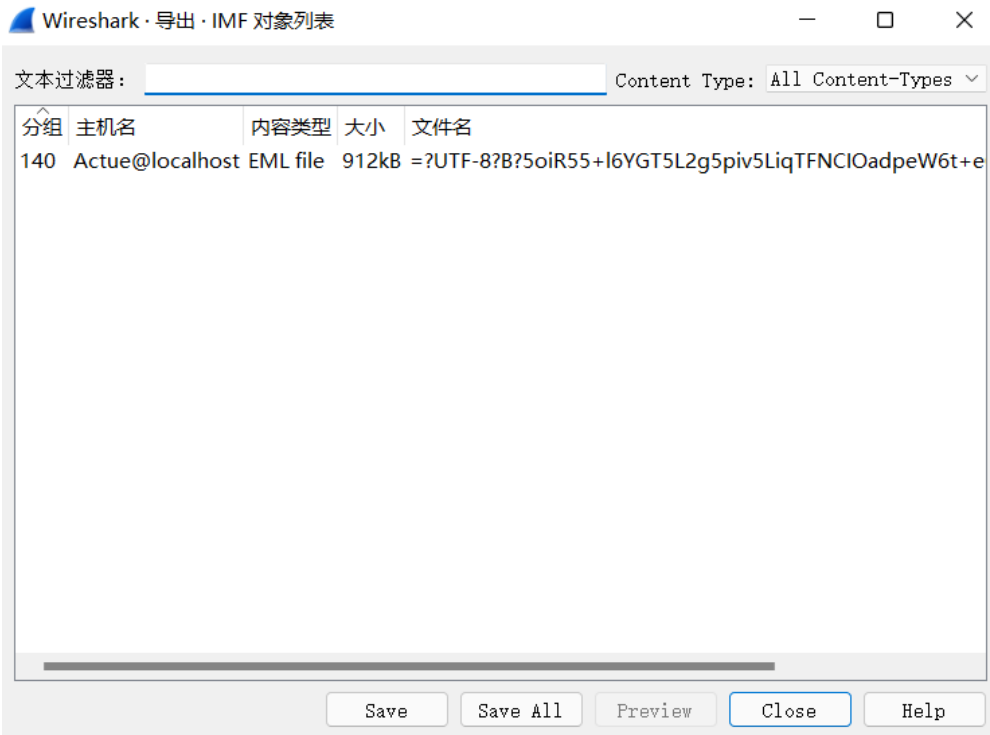
```
PS C:[redacted]ame 2022\week1\这个压缩包有点麻烦-New\flag\flag_decrypted> python .\binwalk .\flag.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
20421         0x4FC5          Zip archive data, encrypted at least v2.0 to extract, compressed size: 12410, uncompressed
 size: 13251, name: flag.jpg
32959         0x80BF          End of Zip archive, footer length: 22
```

第五层：研究了挺久文件名的`4FC5`是什么含义，后来发现只是文件开始的位置。逐个尝试常见解法后发现文件为伪加密。利用`ZipCenOp`工具删除伪加密，得到`flag.jpg`。输入提交flag。



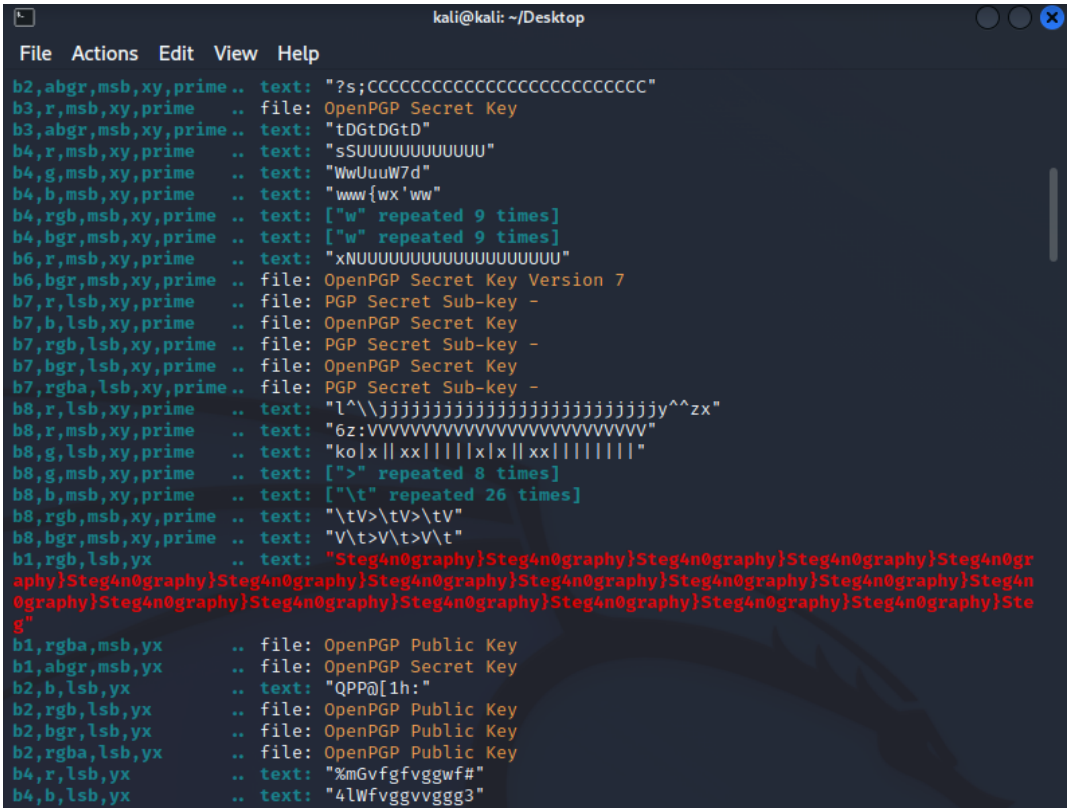
好康的流量

`WireShark`打开，`文件-导出对象`中逐个尝试。在IMF中导出得到`=%3fUTF-8%3fB%3f5oiR55+l6YGT5L2g5piv5LiqTFNCIOadpeW6t+eCuea2qeWbvg==%3f=.eml`。



打开，在邮件附件中下载得到`涩图.png`。仔细端详图片，发现左上角有类似条形码的形状。尝试用ps取色、调色，无果。再用`stegsolve`查看各个通道。在绿色的某个通道看到了条形码，扫出来获得flag前半部分。

接下来尝试了各种方法都没有收获。询问学长后，在邮件标题找到了LSB的提示。另外找了一个`zsteg`工具，把所有通道的LSB全部列出，成功找到flag。

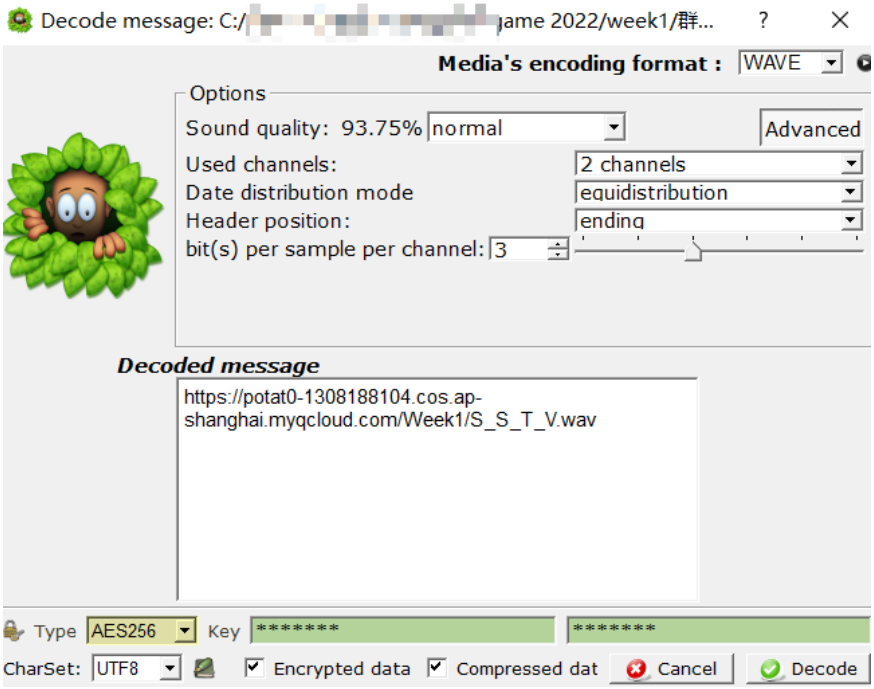


LSB小笔记：LSB隐写会在对应通道一定有非正常的“马赛克”。但不一定会影响通道整图，可以在四边有几像素宽的“马赛克条”。用`zsteg`可以直接暴力列出所有。

群青(其实是幽灵东京)

顺手拖进au，看频谱图。看到`Yoasobi`。右键看文件详细信息。有Why not try try SlientEye。用这个工具提取隐写内容，提取失败。再利用频谱图的`Yoasobi`作为密码，得到一个链接

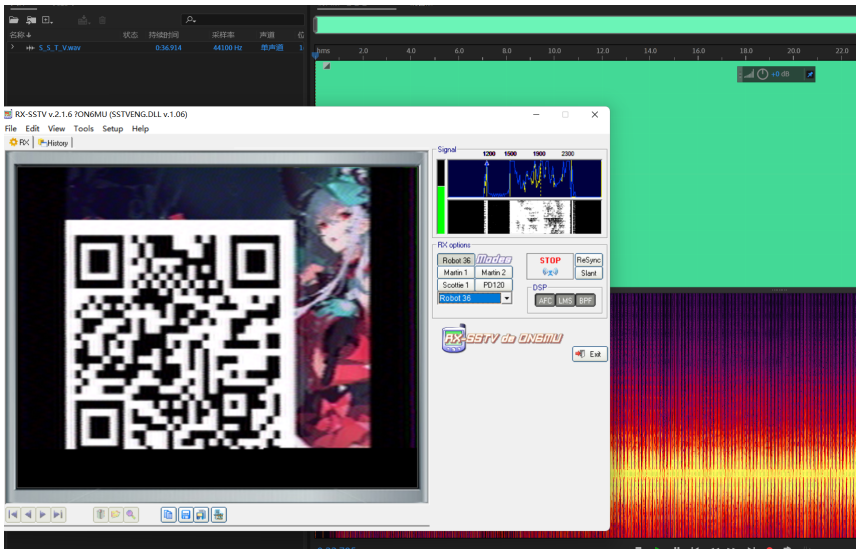
`https://potat0-1308188104.cos.ap-shanghai.myqcloud.com/Week1/S_S_T_V.wav`



查询得知了`SSTV慢扫描电视`。

解1：外放音频，用手机端`Robot36`软件接受解码。得到二维码，扫码得到flag。

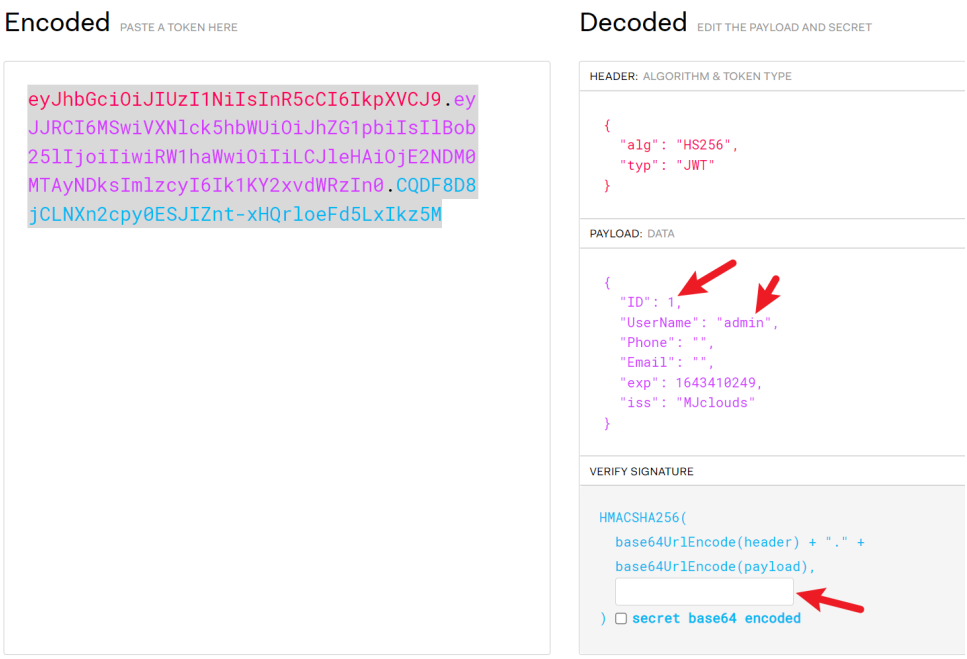
解2：`Virtual Audio Cable`软件将电脑音频输入输出虚拟相连，用`RX-SSTV`软件解码。得到二维码，扫码得到flag。

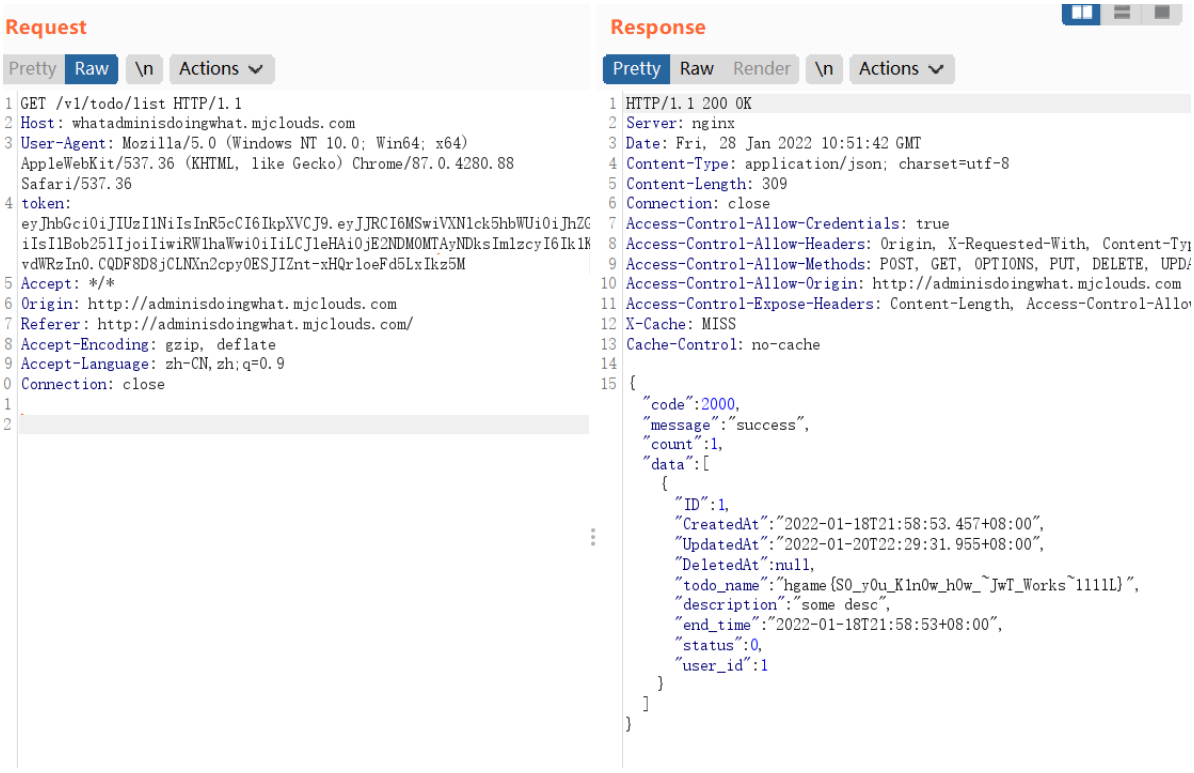


WEB

easy_auth

注册登录，`burpsuite`抓包。看到有token信息。查询得知应该是`jwt`考点。尝试了常见的加密改none、密钥爆破、扫源码等没有结果。询问出题人后，得到提示密钥爆破、简单密钥。于是在`https://jwt.io/`把密钥删了，发现可以成功通过服务器检验。把payload部分改为admin、id改为1，成功看到admin存的flag。



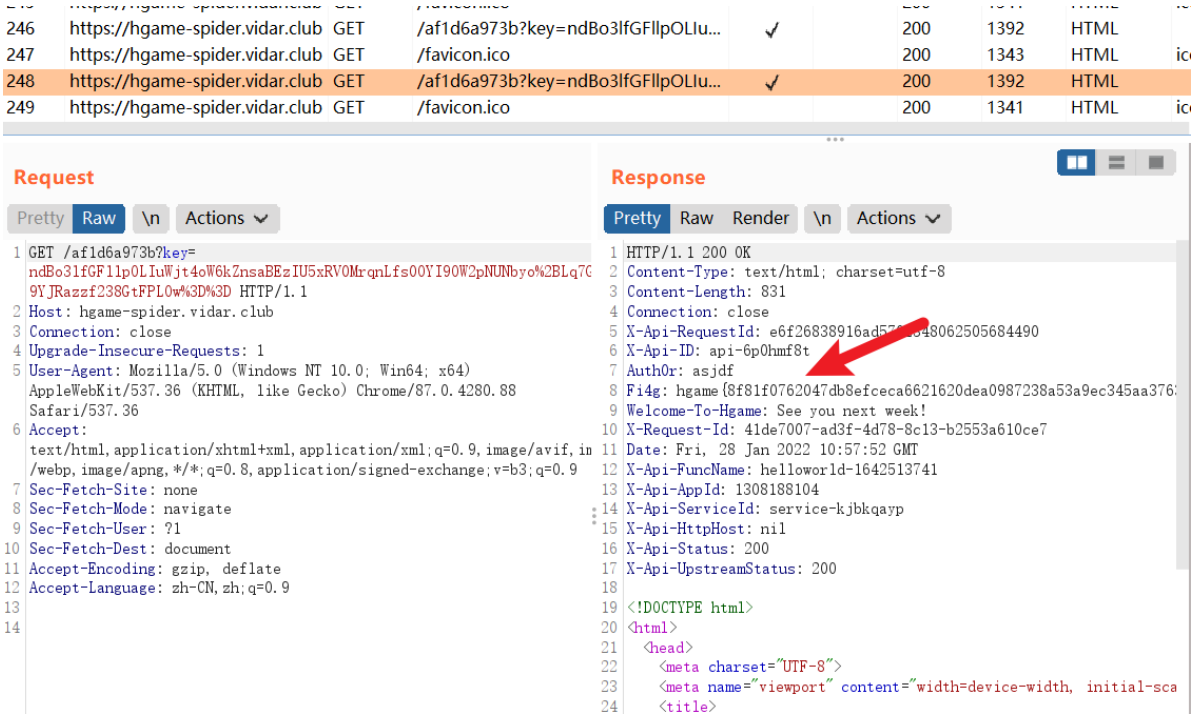


蛛蛛...嘿嘿♥我的蛛蛛

尝试编程自动点击、屏蔽错误按钮、解析链接生成规则等各种方法无果后，最终不得不手动暴力点。在控制台可以看到正确的按钮。

通过第100关后，看到网页上 `我好像在就是把flag落在这里了欸~ 快帮我找找x`

抓包，找到flag。



Tetris plus

一个小游戏，试玩一下。别说，还挺好玩的。玩着玩着，觉得好像3000分很容易就能拿到。于是继续。结果

被骗了 淦。看看源码吧。在`checking.js`最底下发现了上述弹窗的代码。下方注释，看上去是`jsfuck`。于是复制、粘贴到控制台，得到flag。

```
[]+[])[+[]]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+[]+!+[]+!+[]]
[+!+[]]+(![]+[])[!+[]+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([
[]]+(![]+[])[!+[]+!+[]+!+[]]()[+!+[]+[+[]]])()([][(![]+[
[]+[][(![]+[])[+[]]+(![]+[])[!+[]+!+[]]+(![]+[])[+!+[]]+(!
[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+(!
(!![]+[][(![]+[])[+[]]+(![]+[])[!+[]+!+[]]+(![]+[])[+!+[]]
[]]]+(!![]+[])[+[]]+(![]+[])[+!+[]]+(![]+[])[!+[]+!+[]]+([
[]+[])[+[]]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+[]+!+[]+!+[]]
[]+!+[]]+(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([]
(!![]+[])[+[]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]
[]]+(!![]+[][(![]+[])[+[]]+(![]+[])[!+[]+!+[]]+(![]+[])[+!
```

```
'alert("hgame{jsfuck_1s_S0_fUu1n}")'
```

Fujiwara Tofu Shop、

根据页面提示，需要先去一趟秋名山（qiumingshan.net），应该是有关请求头的题。在 BurpSuite 中，把浏览器的请求放到 Repeater。（偷懒不逐一截图了）

1. 需要先去一趟秋名山（qiumingshan.net）

   增加 Referer: qiumingshan.net

2. 只有借助AE86才能拿到车神通行证（Hachi-Roku）

   更改UA User-Agent: Hachi-Roku

3. 86的副驾上应该放一盒树莓（Raspberry）味的曲奇

   参考 Response 中的 Set-Cookie: flavor=Strawberry，增加 Cookie: flavor=Raspberry

4. 汽油都不加，还想去秋名山？请加满至100

   Response 中有响应头 Gasoline: 0。在请求头增加 Gasoline: 100

5. 哪怕成了车神，也得让请求从本地发出来才能拿到 flag！

   参考以前做题经验，这里增加了 X-Forwarded-For 和 client-ip，均失败。其中 XFF 方式服务器有特别的相应。

Request

Pretty | Raw | \n | Actions

```
GET / HTTP/1.1
Host: shop.summ3r.top
Upgrade-Insecure-Requests: 1
User-Agent: Hachi-Roku
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,in
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Referer: qiumingshan.net
Cookie: flavor=Raspberry
Gasoline: 100
X-Forwarded-For: 127.0.0.1
```

Response

Pretty | Raw | Render | \n | Actions

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Gasoline: 0
Server: gin-gonic/gin v1.7.7
Set-Cookie: flavor=Strawberry; Path=/; Domain=loca
 HttpOnly
Date: Fri, 28 Jan 2022 11:39:17 GMT
Content-Length: 27
Connection: close

大黑阔也想当车神?
```

看起来是XFF被ban了。卡了挺久，问了出题人也没有什么进展。搜相关的内容时，看到了这么个东西：

> 这个协议头的格式：
>
> X-Forwarded-For: client, proxy1, proxy2

尝试 X-Forwarded-For: 127.0.0.1, 127.0.0.1，成功得到flag。不过好像是偷鸡拿到的flag。

Request

Pretty | Raw | \n | Actions

```
GET / HTTP/1.1
Host: shop.summ3r.top
Upgrade-Insecure-Requests: 1
User-Agent: Hachi-Roku
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,in
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Referer: qiumingshan.net
Cookie: flavor=Raspberry
Gasoline: 100
X-Forwarded-For: 127.0.0.1, 127.0.0.1
```

Response

Pretty | Raw | Render | \n | Actions

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Gasoline: 0
Server: gin-gonic/gin v1.7.7
Set-Cookie: flavor=Strawberry; Path=/; Domair
 HttpOnly
Date: Fri, 28 Jan 2022 11:40:36 GMT
Content-Length: 31
Connection: close

hgame{I_b0ught_4_S3xy_sw1mSu1t}
```