HGAME 2022 Week1 writeup by pankas

web

easy_auth

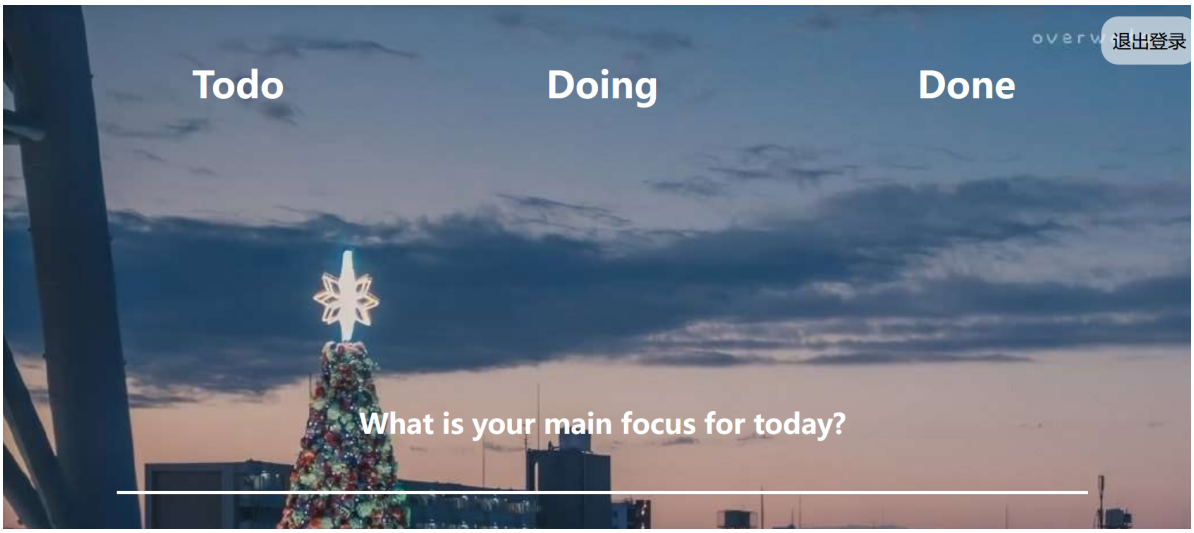
先看一下题目，有提示

> 尊贵的admin写了个todo帮助自己管理日常，但他好像没调试完就部署了....一个月后，当他再一次打开他的小网站，似乎忘记了密码...他的todo之前记录了很重要的东西，快帮帮他
> 不要爆破!

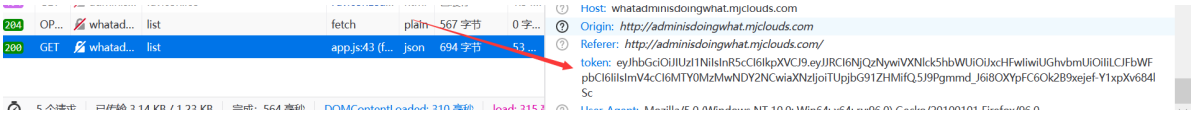
这里目标网站时在开发中的，flag应该在admin用户里。

打开发现输入admin密码随便写一个，结果不对，那注册一个看看

注册号登录进去



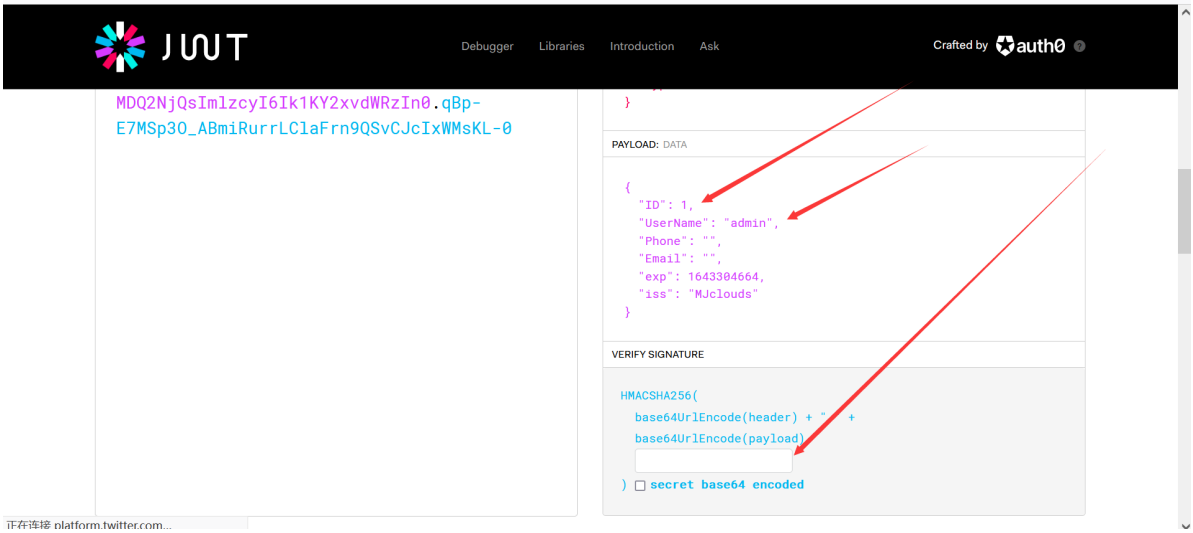
看了下这个页面也没什么，抓一下包发现token



这个token是**JWT**，网上搜索一下进能知道只要找到了JWT的secret就可以伪造token发送到服务器通过验证了

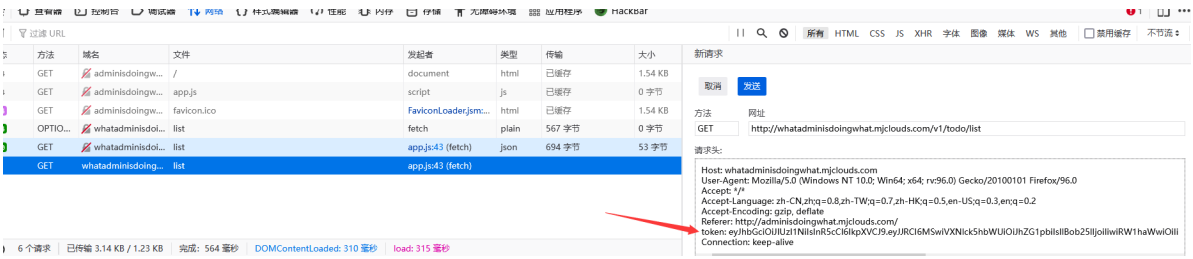
由于题目说是还在调试当中， 猜测secret为空，试一试。

到**jwt.io**这个网站里

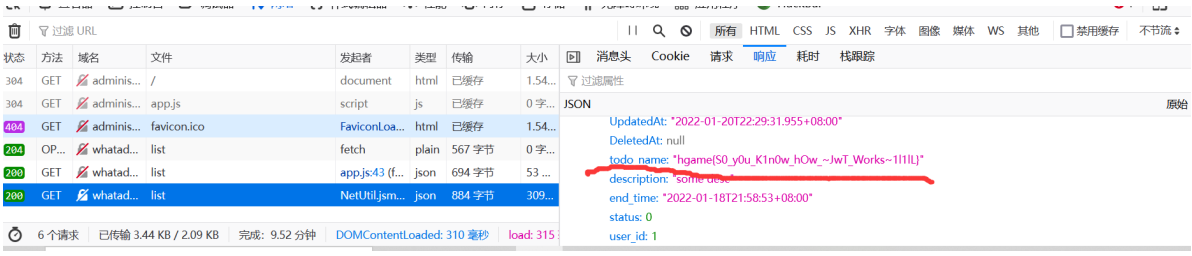


将UserName改为admin，ID改为1(最贵的admin开发者肯定是网站注册的第一个人)，下面的secret为空，

将修改后的token发送



拿到flag



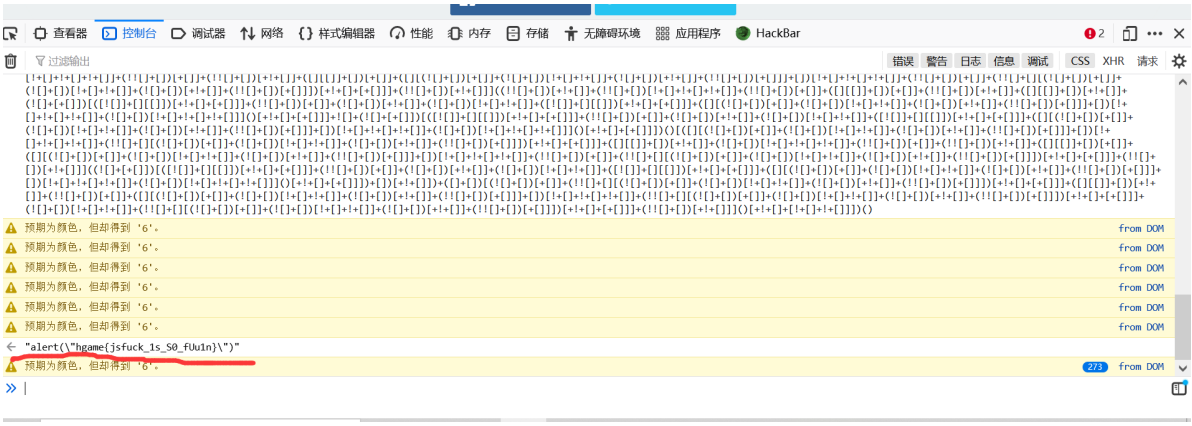
这里简单说一下原理

> 验证方法：首先服务端会产生一个`secret`，然后以这个`secret`作为密钥，使用第一部分选择的加密方式（这里就是`HS256`），对第一部分和第二部分拼接的结果进行加密，然后把加密结果放到第三部分。
> 因为加密算法我们已经知道了，如果我们只要再得到加密的`secret`，我们就能伪造数据，并且通过服务器的检查。

Tetris plus

提示说要玩够3000分，不可能的。像这类浏览器小游戏那肯定是先查看js源码。

结果在这个checking.js文件里发现了jsfuck代码，jsfuck可以直接放到控制台运行，试试看。



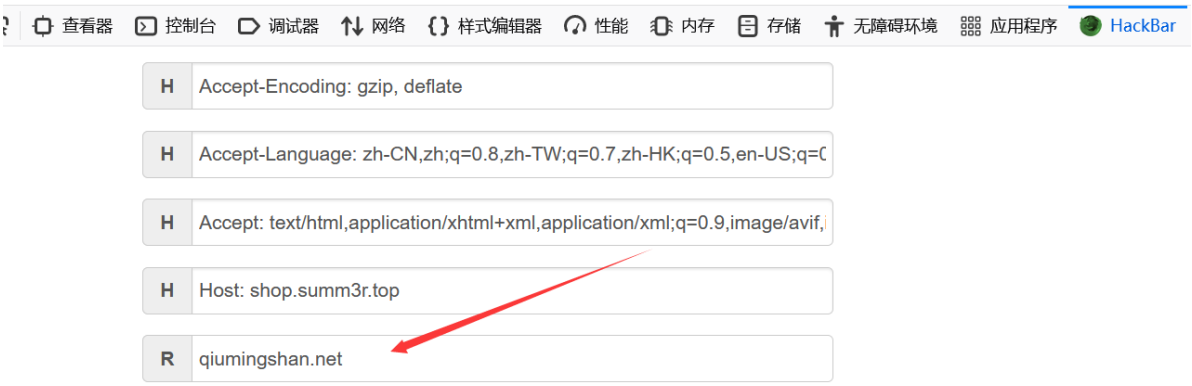
放到控制台运行拿到flag。

Fujiwara Tofu Shop

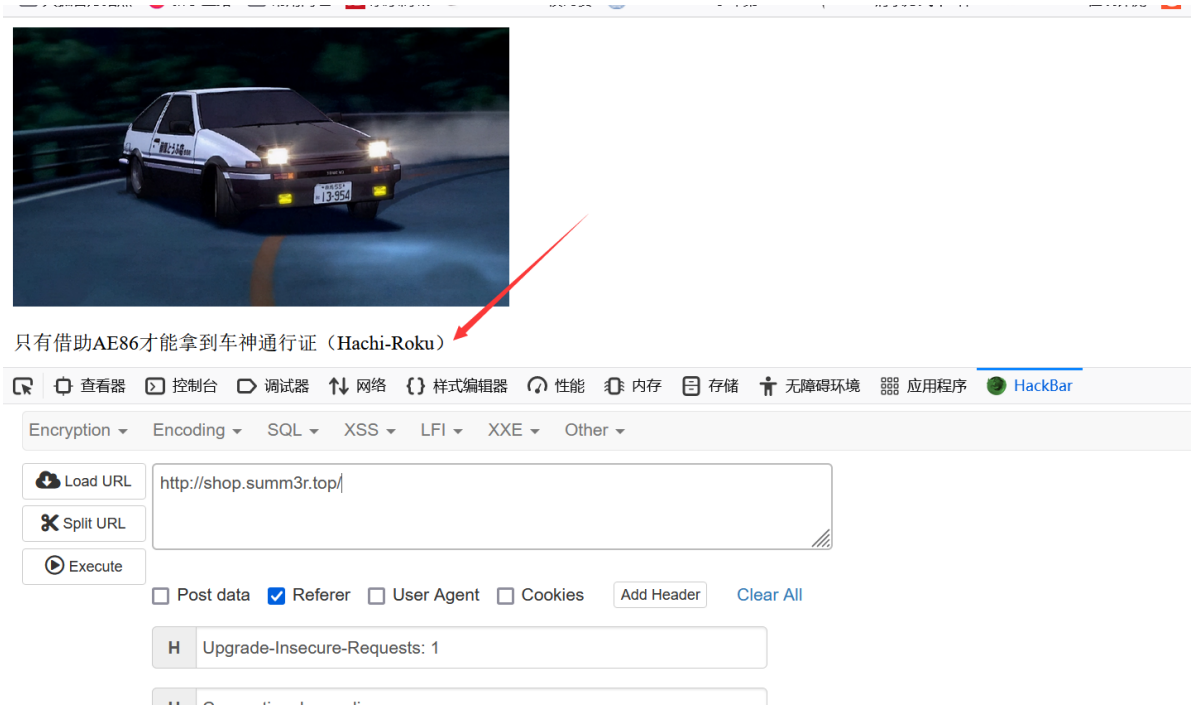
秋名山飙车啊，进去看一看。

提示说首先要到`qiumingshan.net`这个地方去，那么在web中的意思就是要让你的referer为`qiumingshan.net`

用HackBar添加请求头referer

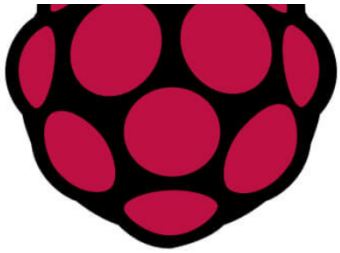


Execute后又出现

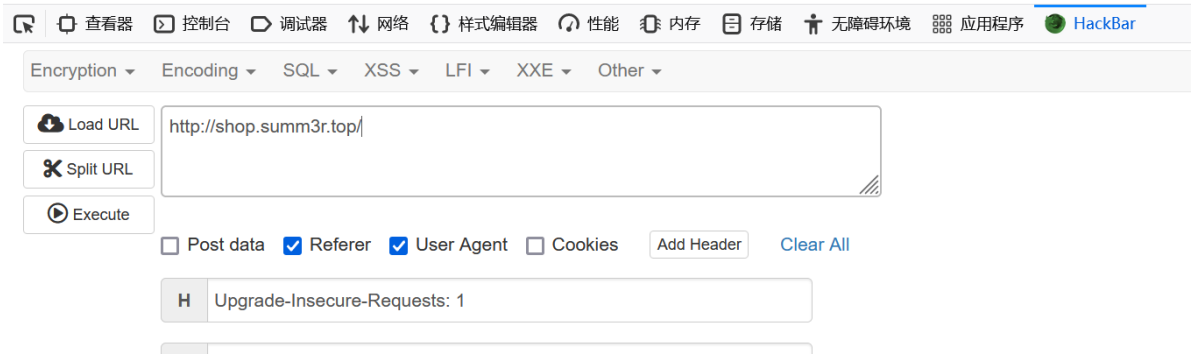


通行证啊，那么修改一下User-Agent为`Hachi-Roku`即可

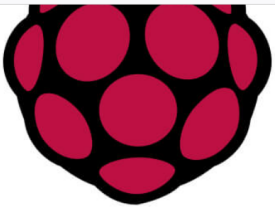
继续得到



86的副驾上应该放一盒树莓（Raspberry）味的曲奇



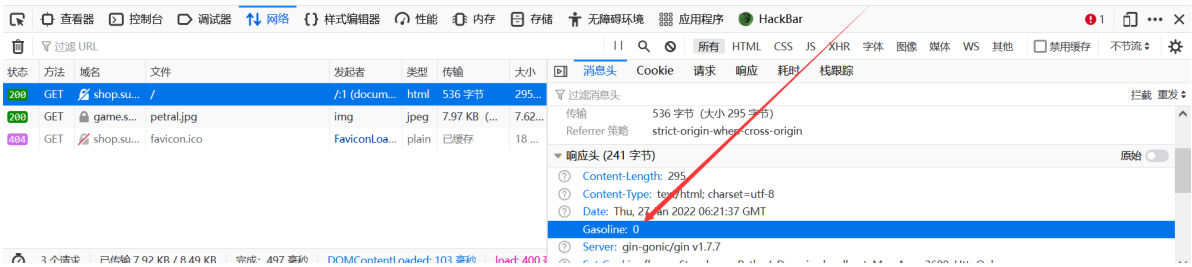
要求其cookie的**味道**是`Raspberry`，那么在Cookies上添加上`flavor=Raspberry`



86的副驾上应该放一盒树莓（Raspberry）味的曲奇

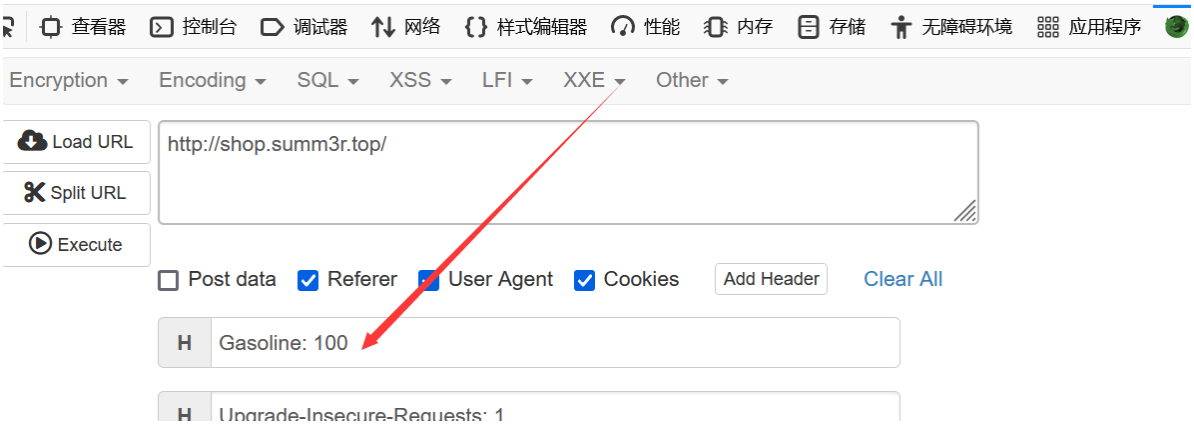
之后.....还有，要求加油到100，查看请求头可以看到当前`Gasoline`为0

汽油都不加，还想去秋名山？请加满至100



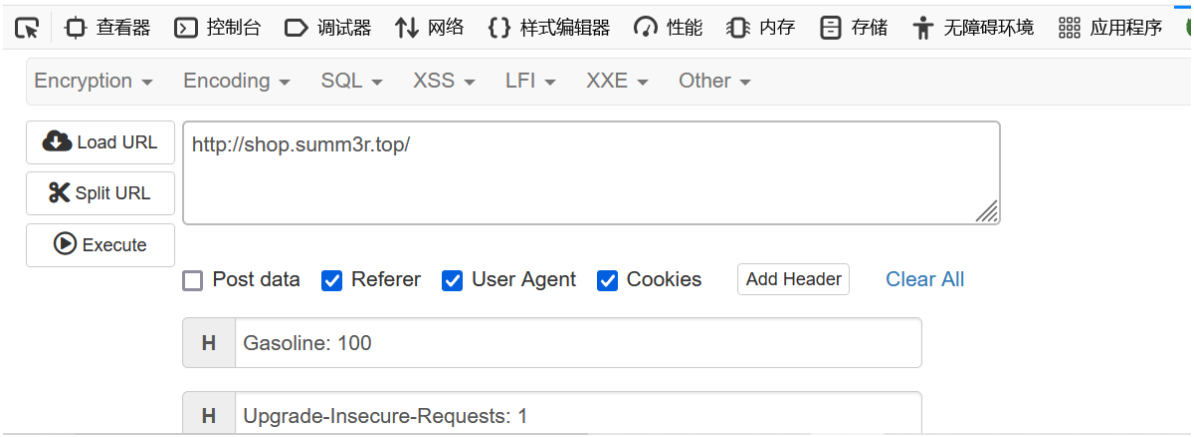
那么在请求头里添加上`Gasoline: 100`即可

弋油都不加，还想去秋名山？请加满至100



之后又要求其请求从本地发出来

哪怕成了车神，也得让请求从本地发出来才能拿到 flag！

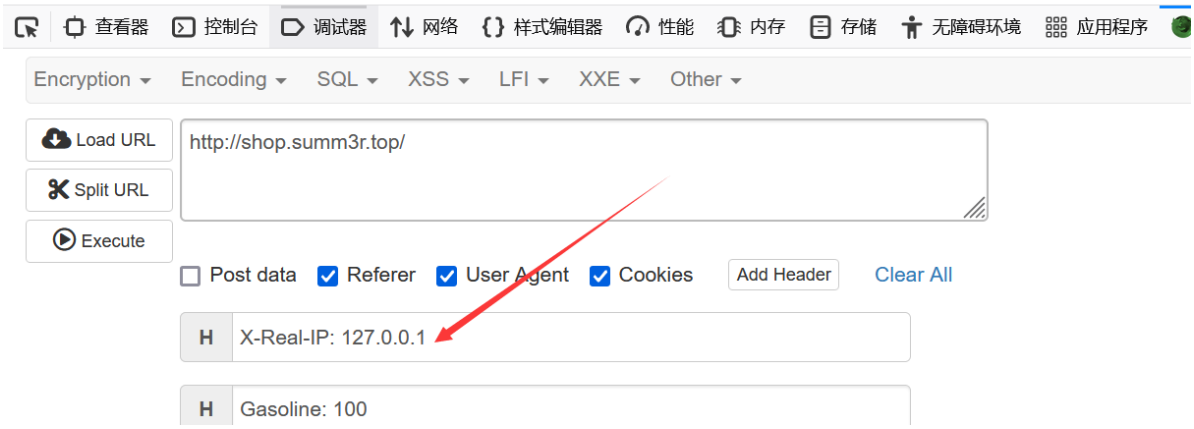


那可以使用伪造请求IP的方法，又如下几种

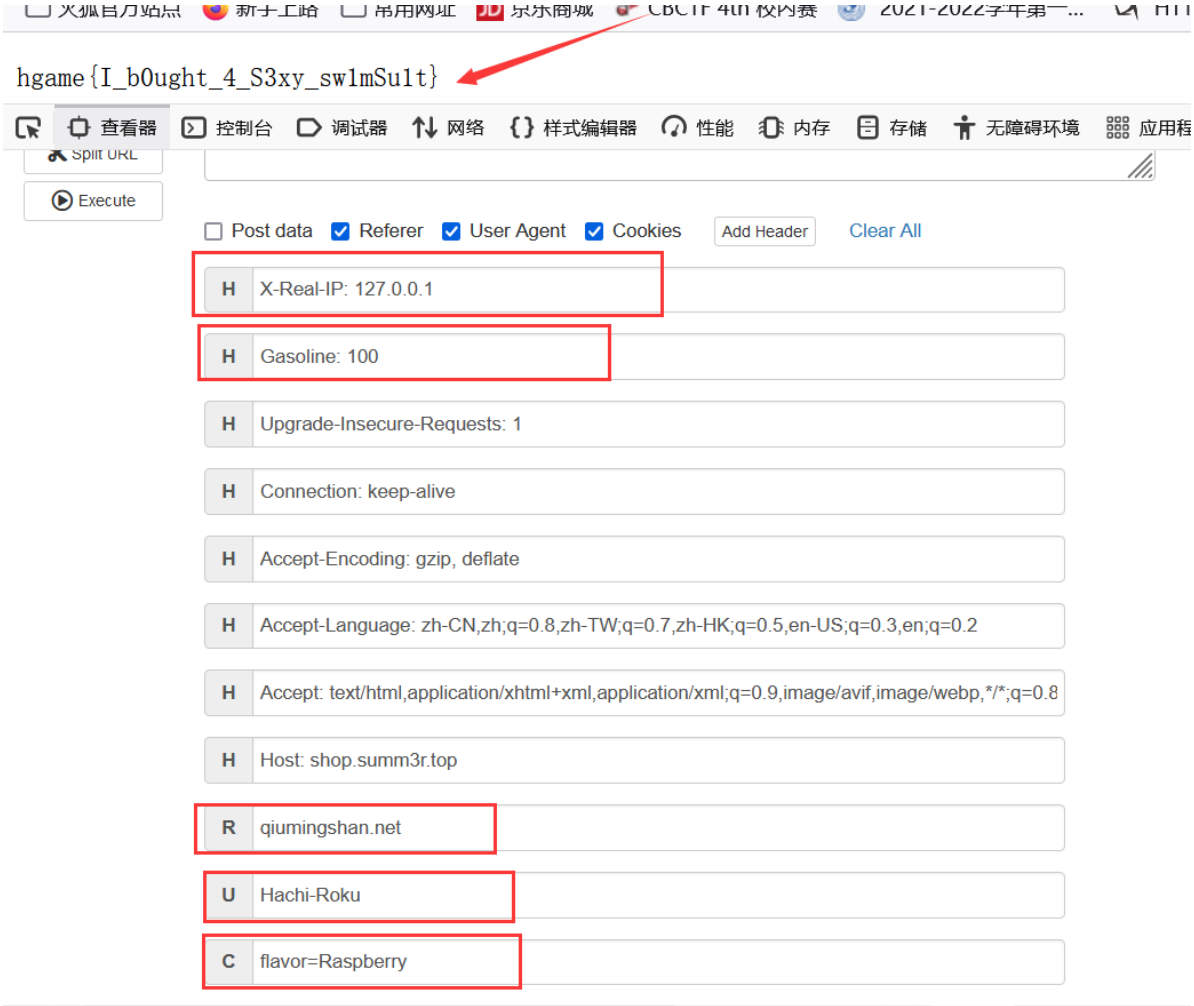
```
X-Forwarded-For:
X-Forwarded-Host:
X-Client-IP:
X-remote-IP:
X-remote-addr:
True-Client-IP:
Client-IP:
X-Real-IP:
```

全都试一遍发现只有`X-Real-IP`没有被ban，伪造IP为本地127.0.0.1

哪怕成了车神，也得让请求从本地发出来才能拿到 flag！



执行后成功拿到flag



蛛蛛...嘿嘿♥我的蛛蛛

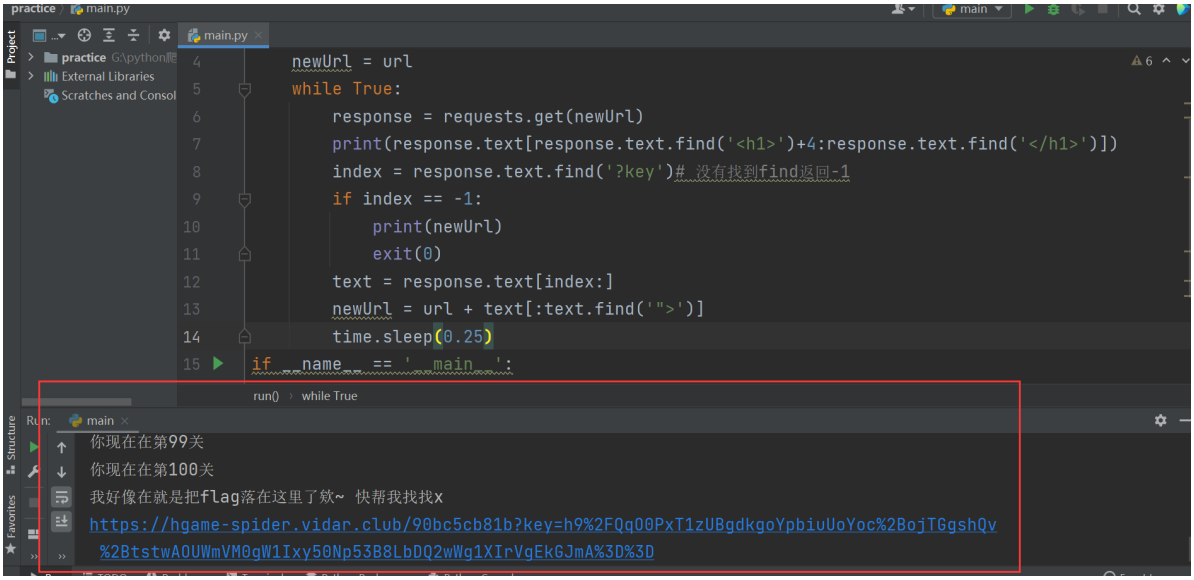
这题也是个小游戏，这个按钮也是越点越多，而且只有一个是真的。先玩几关看一下它响应的内容，很有规律。

每次都会在原url基础上拼接一个`?key=##########`。那直接交给爬虫。

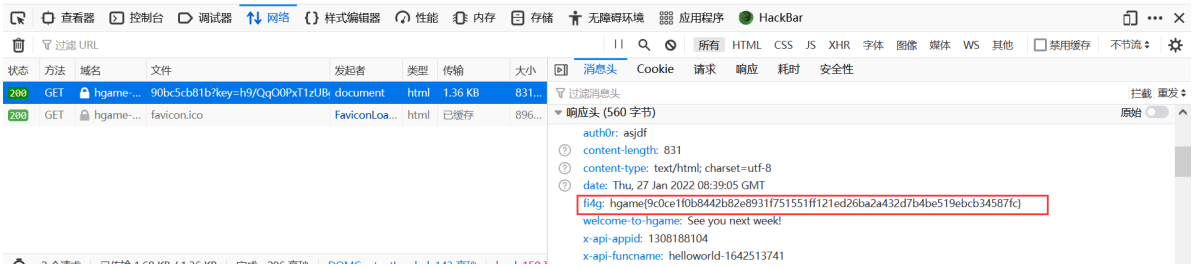
不废话，上代码。

```
import requests
import time
def run(url):
    newUrl = url
    while True:
        response = requests.get(newUrl)

 print(response.text[response.text.find('<h1>')+4:response.text.find('</h1>')])
        index = response.text.find('?key')# 没有找到find返回-1
        if index == -1:
            print(newUrl)
            exit(0)
        text = response.text[index:]
        newUrl = url + text[:text.find('">')]
        time.sleep(0.5)
if __name__ == '__main__':
    run('https://hgame-spider.vidar.club/90bc5cb81b')
```



发现在100关后面，点开爬到的url



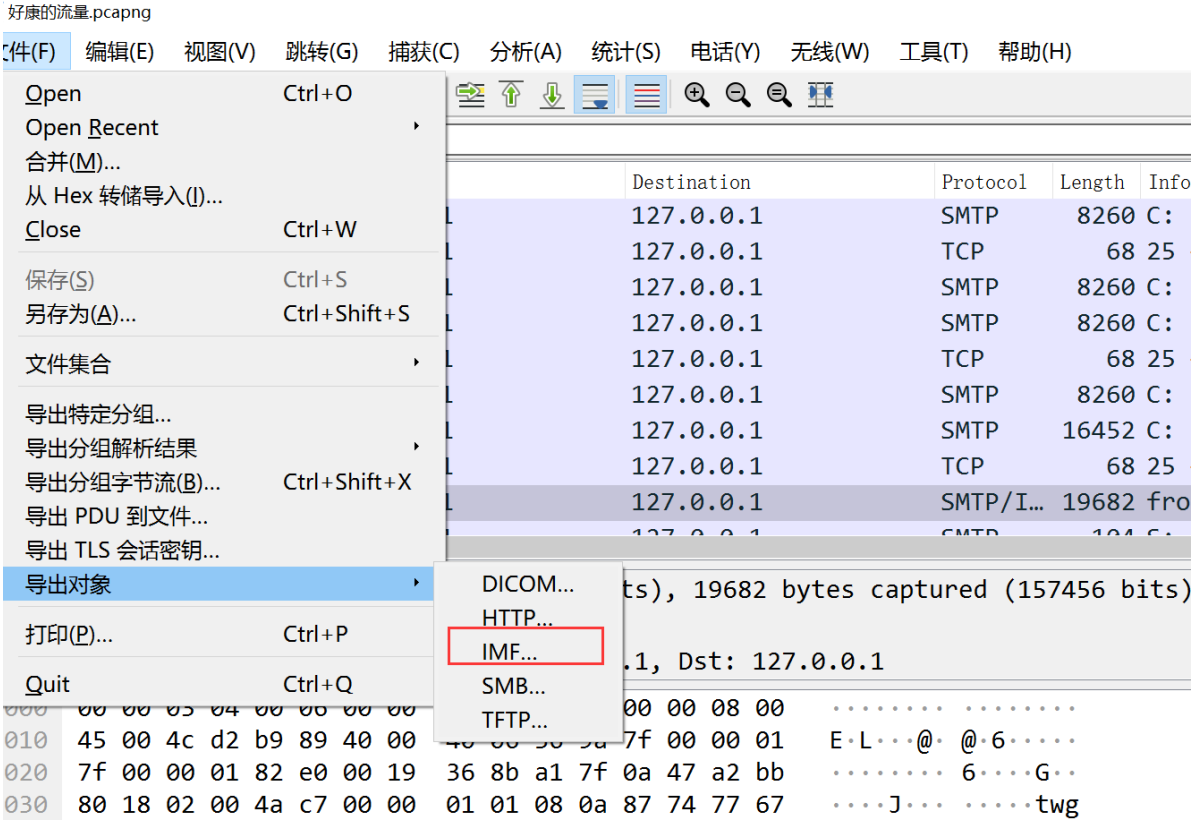
在请求头里发现flag

Misc

好康的流量

下载附件拿到一份截获的流量，用wireshark打开用导出为邮件

好康的流量.pcapng

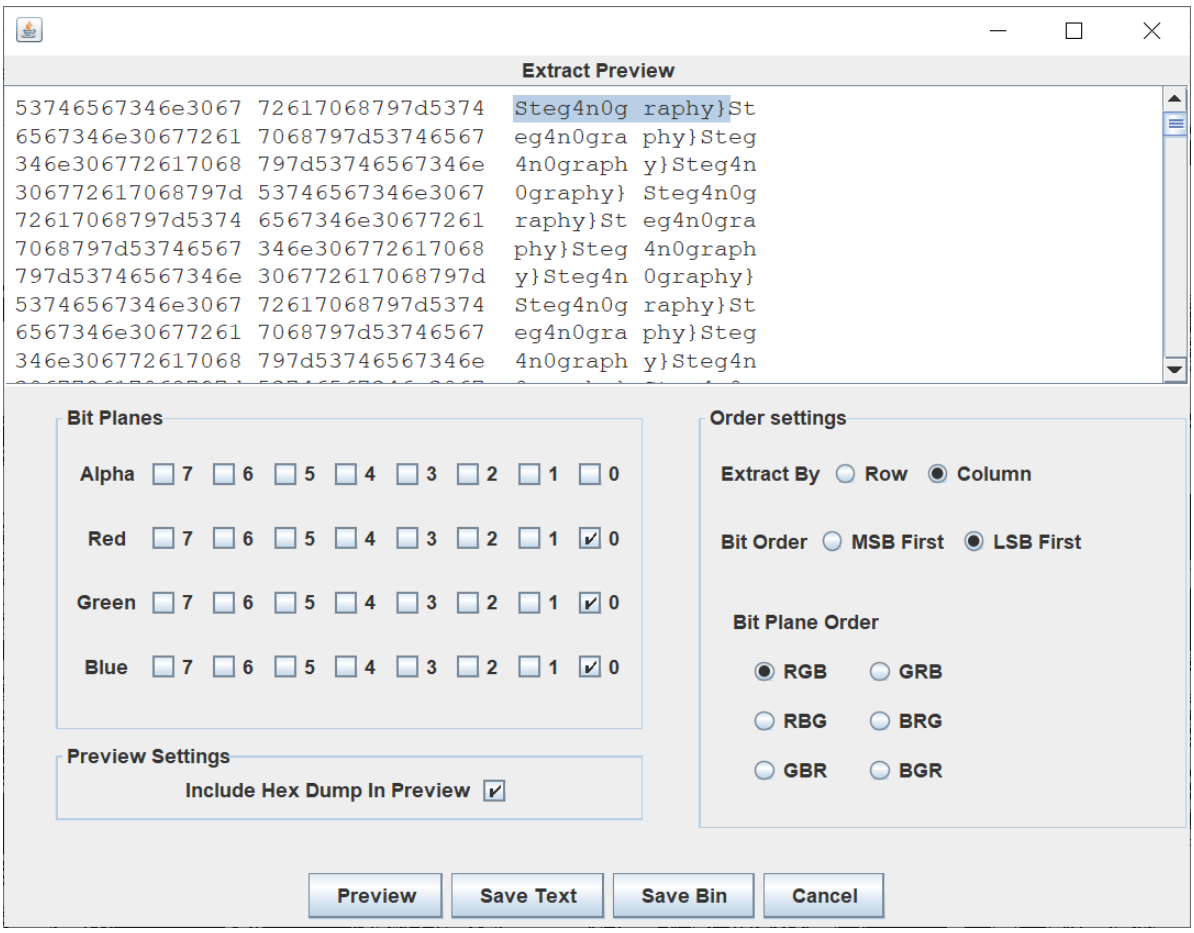


拿到**涩图**

这个图片试了很多方法，最后发现使用stegsolver打开发现一个条形码。

扫码拿到一半的flag。

还有一半应该是lsb隐藏的。



使用工具拿到另一半。（这里其实是试出来的）

饭卡的uno

下载附件使用 **010editor**打开就是flag