# HGAME 2022 Week1 writeup by X1aoba1

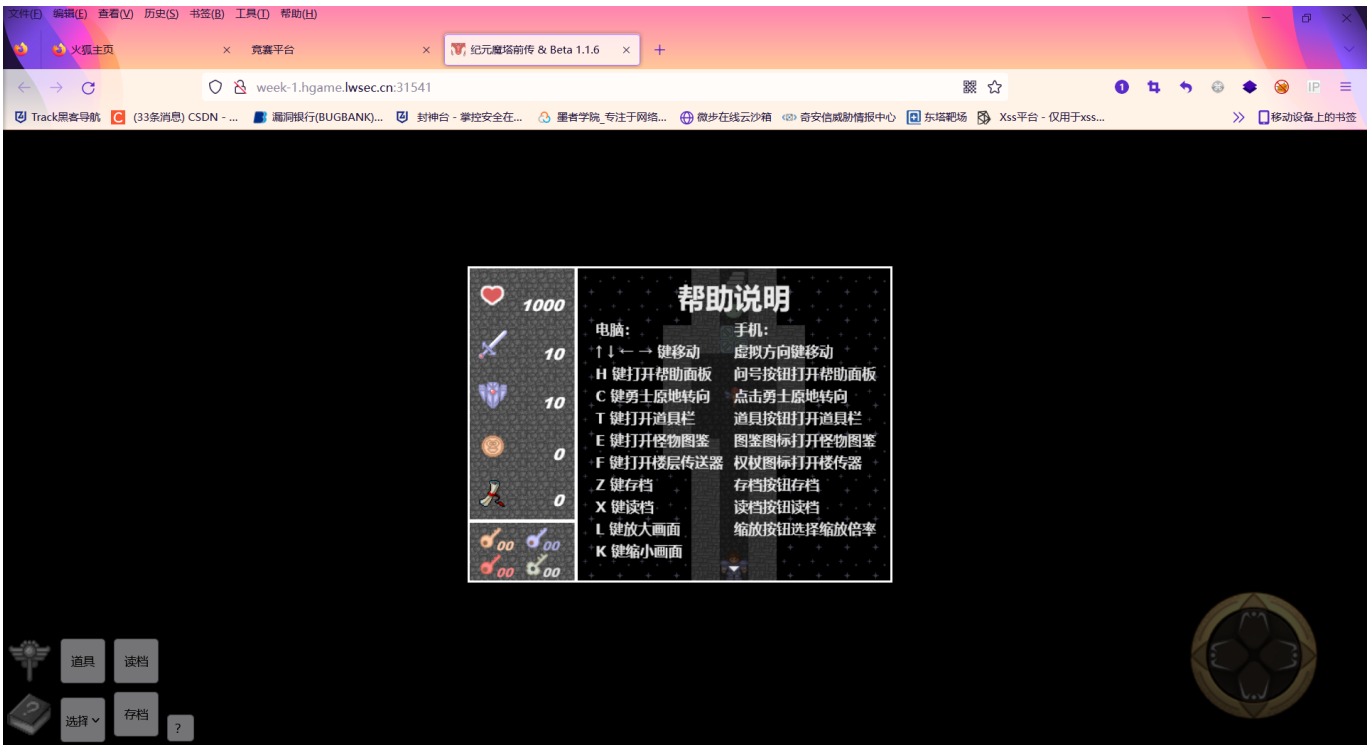
## Table of Contents



## WEB

### Classic Childhood Game

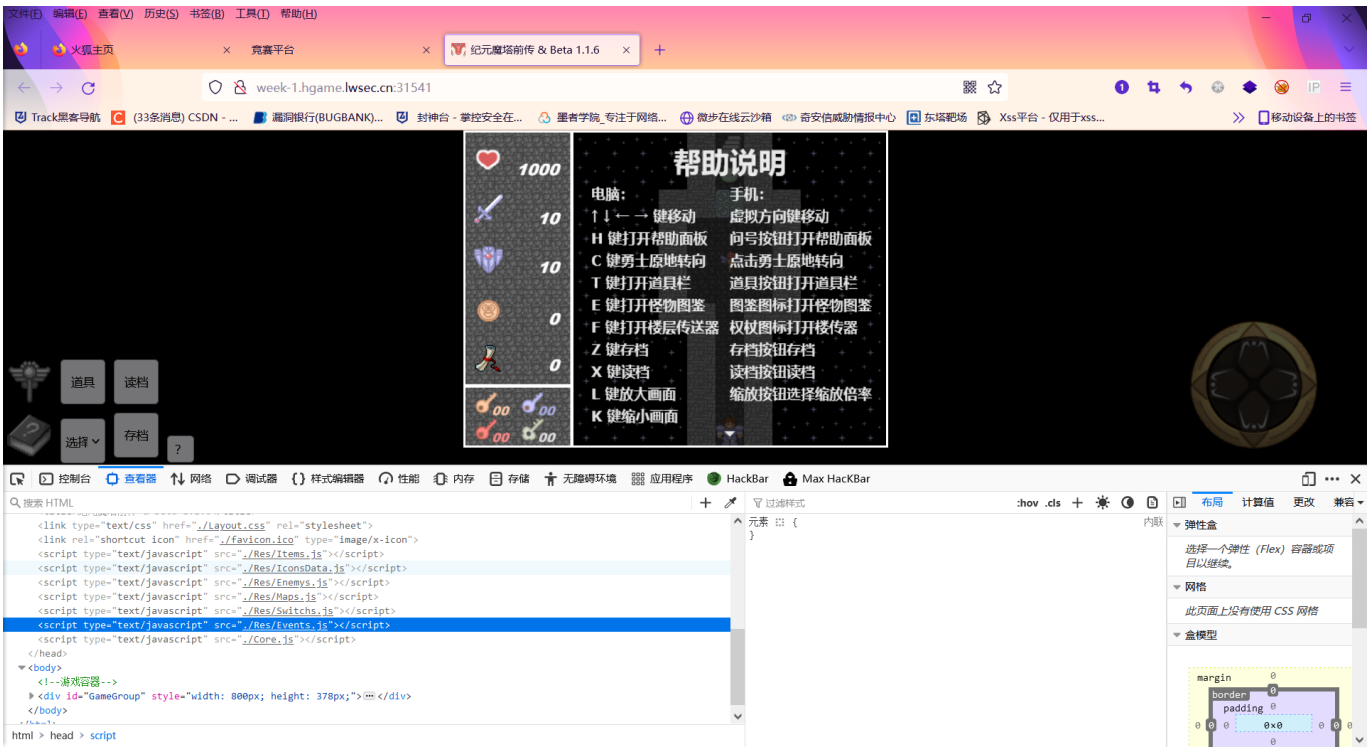
打开赛题，是一个游戏




一般这种题是在游戏通关后给flag，但是肯定不是要我们打通关

flag通常以某种形式藏在js的某个函数里,通关后触发事件

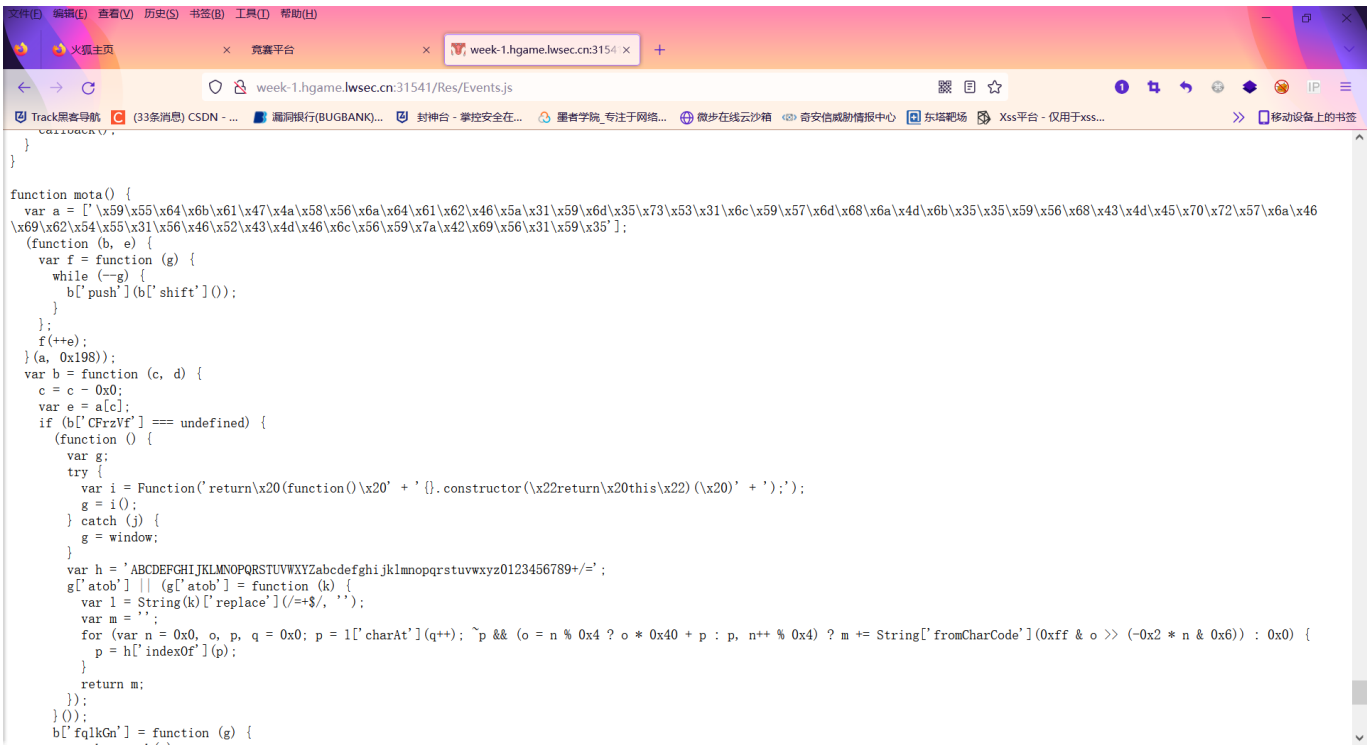
F12打开控制台




盲猜Flag藏在Events.js里，直觉（不是

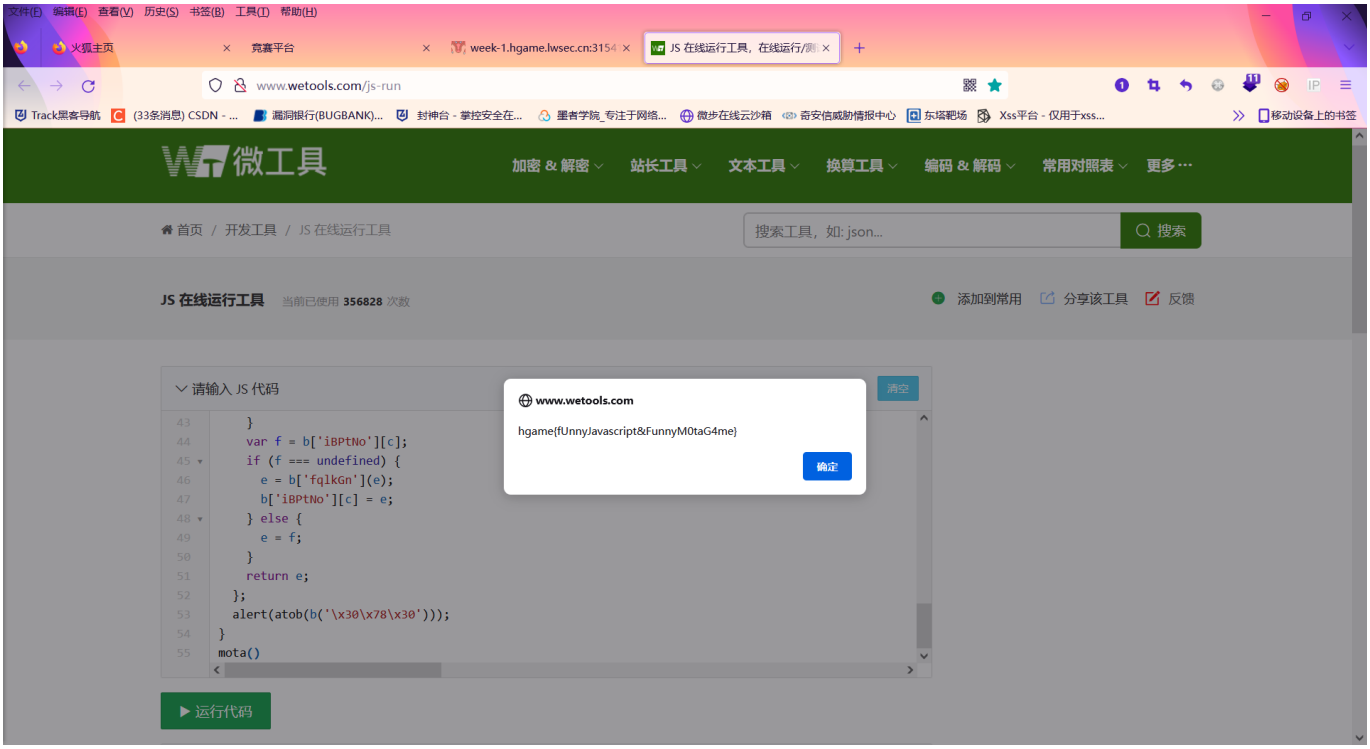
打开文件，直接去寻找通关后发生的事件

发现可疑函数mota()




```
function mota() {
  var a = ['\x59\x55\x64\x6b\x61\x47\x4a\x58\x56\x6a\x64\x61\x62\x46\x5a\x31\x59\x6d\x35\x73\x53\x31\x6c\x59\x57\x6d\x68\x6a\x4d\x6b\x35\x35\x59\x56\x68\x43\x4d\x45\x70\x72\x57\x6a\x46
\x69\x62\x54\x55\x31\x56\x46\x52\x43\x4d\x46\x6c\x56\x59\x7a\x42\x69\x56\x31\x59\x35'];
  (function (b, e) {
    var f = function (g) {
      while (--g) {
        b['push'](b['shift']());
      }
    };
    f(++e);
  }(a, 0x198));
  var b = function (c, d) {
    c = c - 0x0;
    var e = a[c];
    if (b['CFrzVf'] === undefined) {
      (function () {
        var g;
        try {
          var i = Function('return\x20(function()\x20' + '{}.constructor(\x22return\x20this\x22)(\x20)' + ');');
          g = i();
        } catch (j) {
          g = window;
        }
        var h = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=';
        g['atob'] || (g['atob'] = function (k) {
          var l = String(k)['replace'](/=+$/, '');
          var m = '';
          for (var n = 0x0, o, p, q = 0x0; p = l['charAt'](q++); ~p && (o = n % 0x4 ? o * 0x40 + p : p, n++ % 0x4) ? m += String['fromCharCode'](0xff & o >> (-0x2 * n & 0x6)) : 0x0) {
            p = h['indexOf'](p);
          }
          return m;
        });
      }());
      b['fqlkGn'] = function (g) {
```

在线js环境运行一下

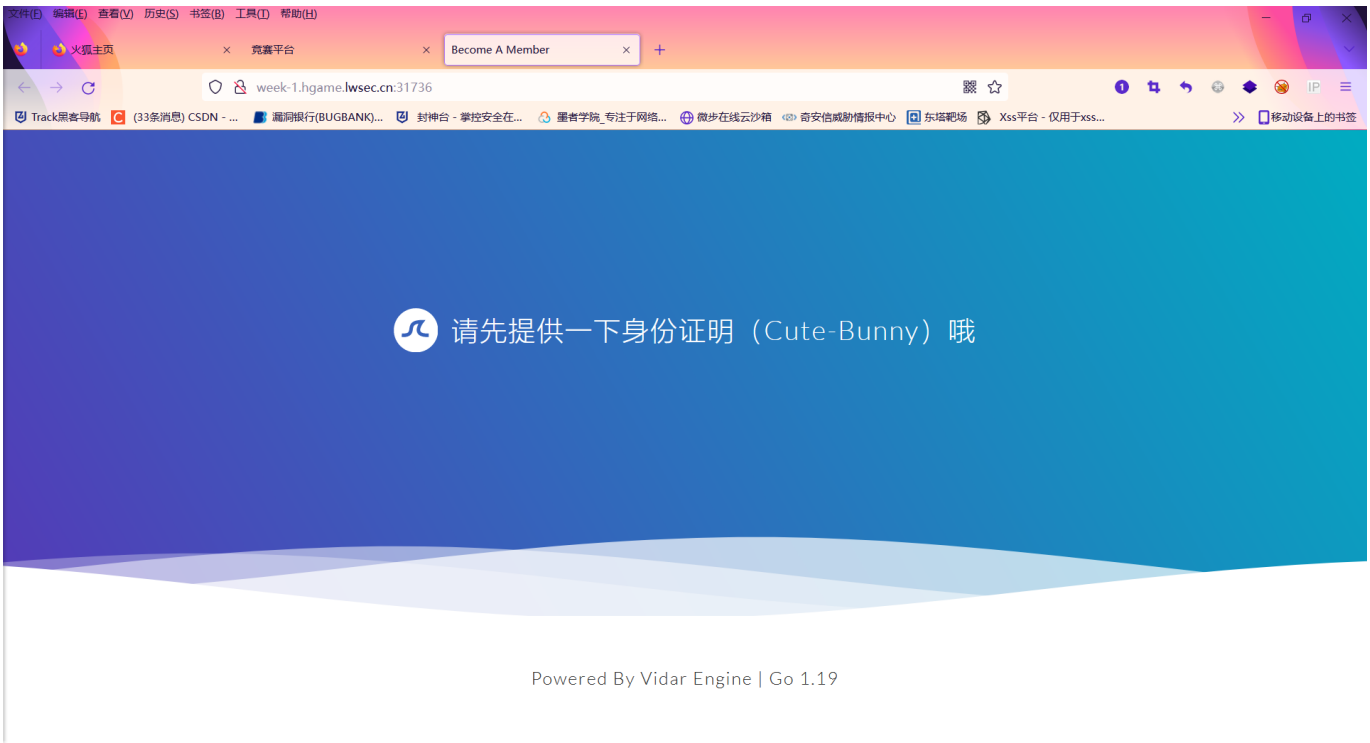



拿到Flag，结束

## Become A Member

题目里面说是HTTP知识，应该是信息头伪造

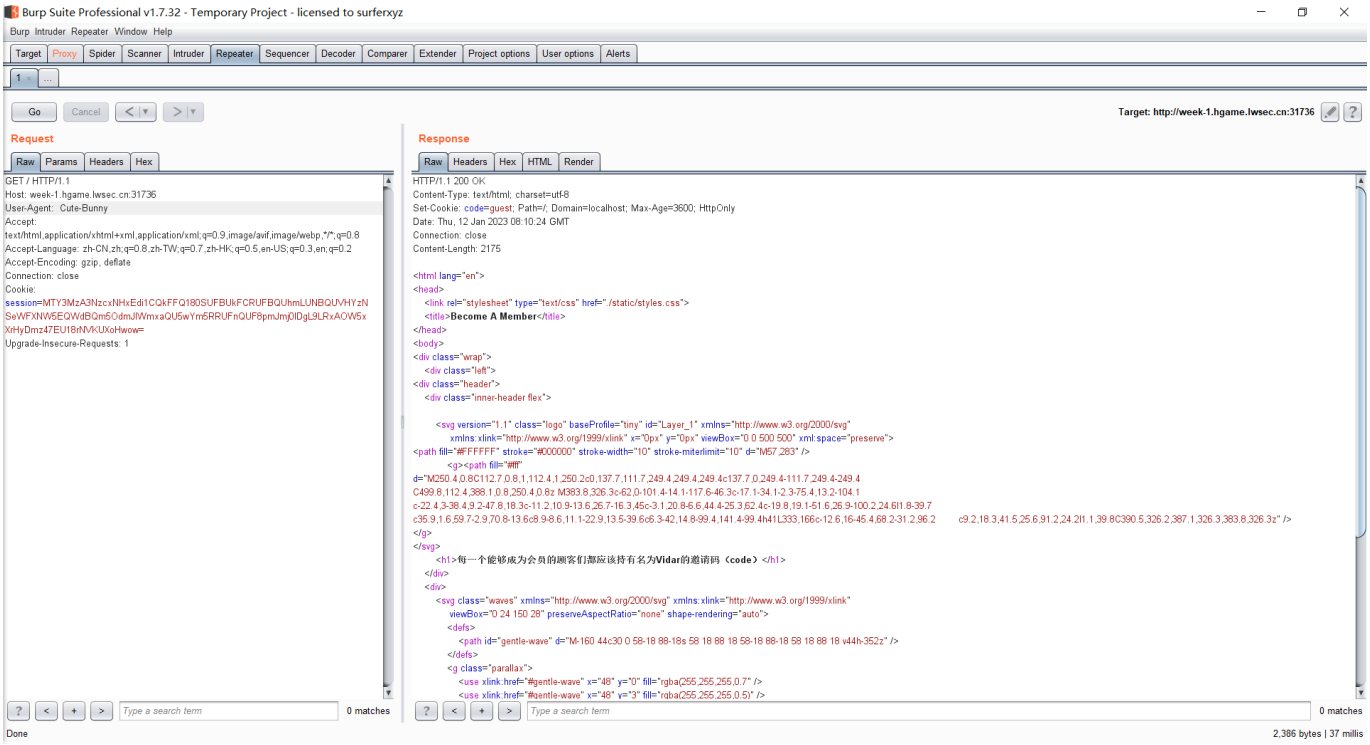
打开题目环境



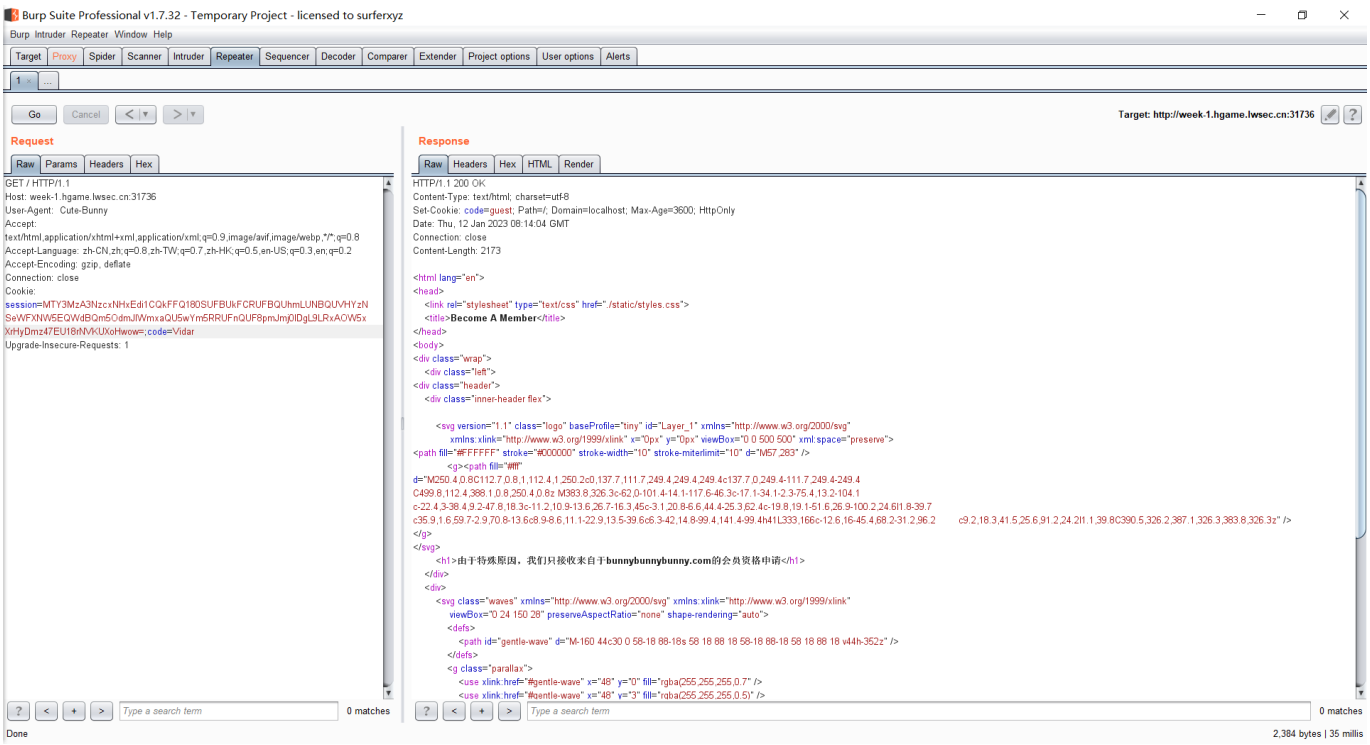
这里让提供身份证明，一开始一直想用cookie，后来咨询从出题人，才知道忽略了一个重要且常用的东西 User-Agent 用户代理

直接抓包发送到Repeater

修改UA为Cute-Bunny

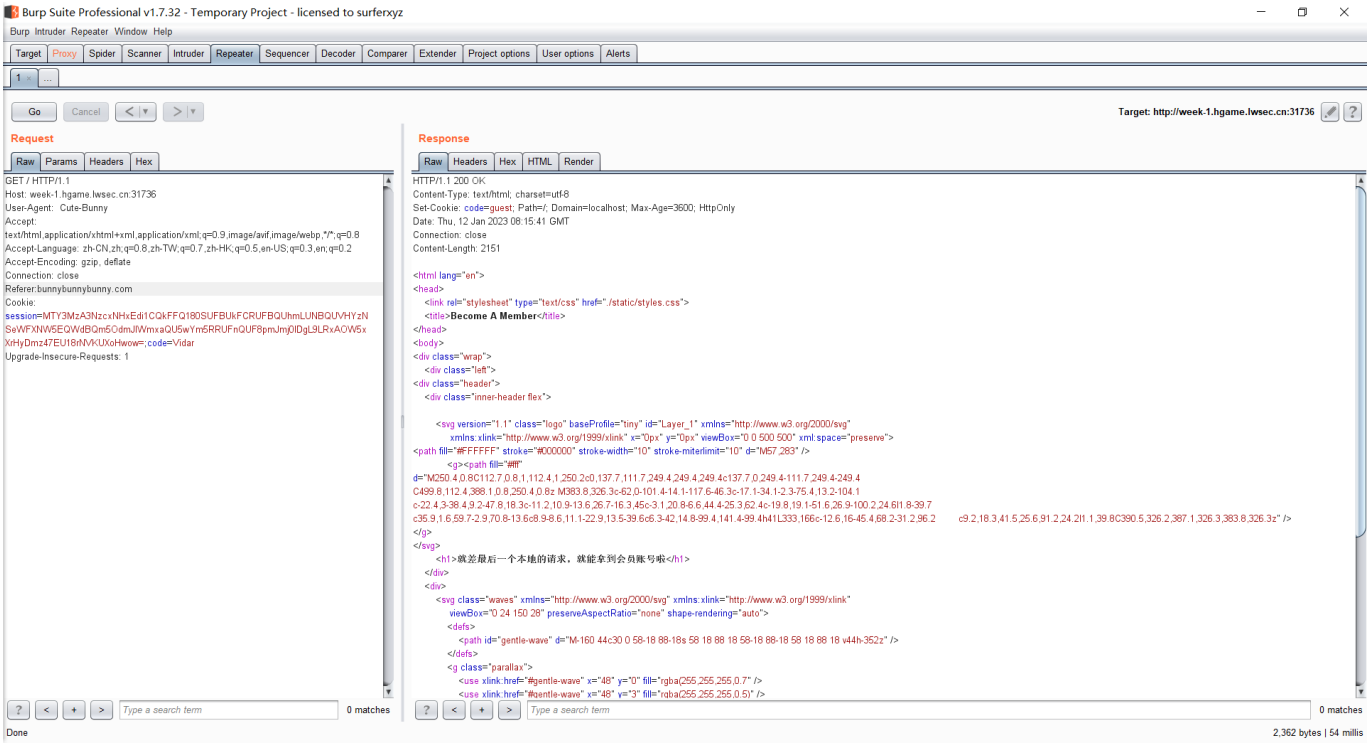



再次修改Cookie中的code=Vidar



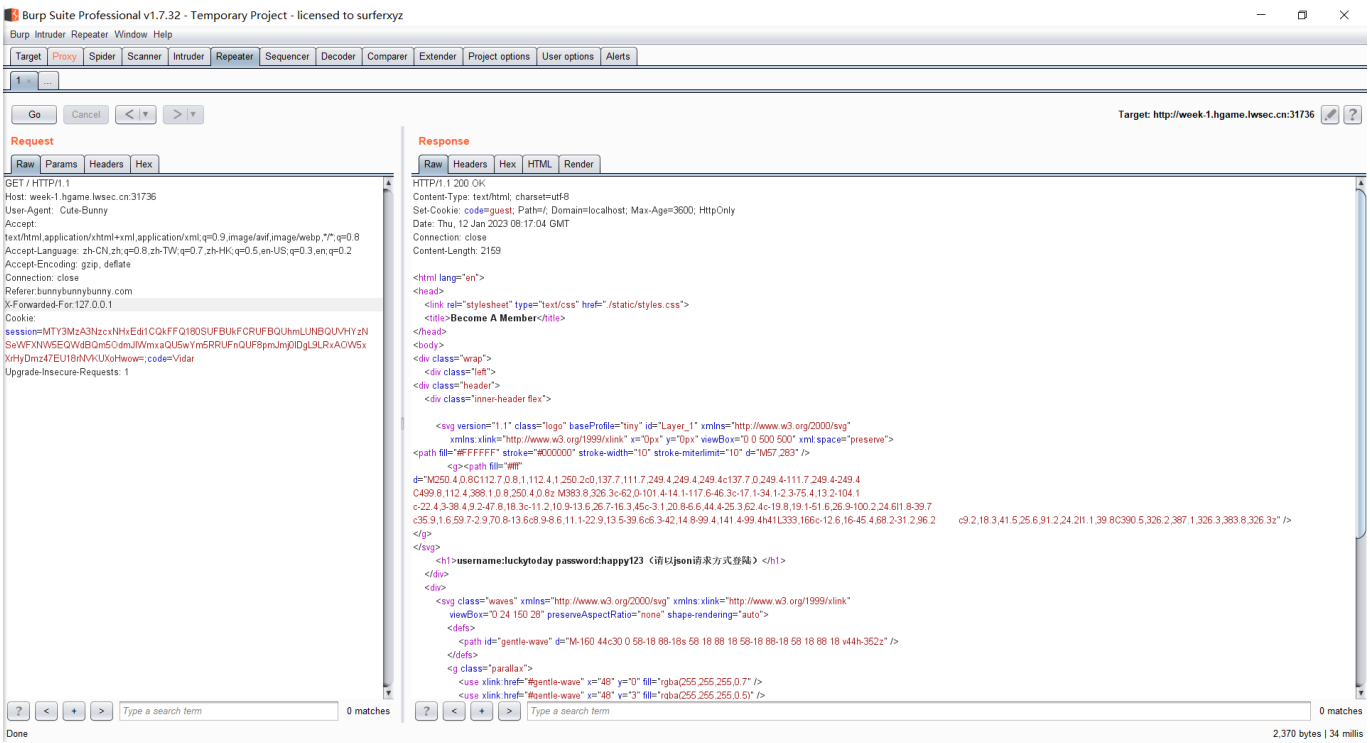
这边应该是Referer头伪造（因为试过Host不行）

添加Referer=bunnybunnybunny.com



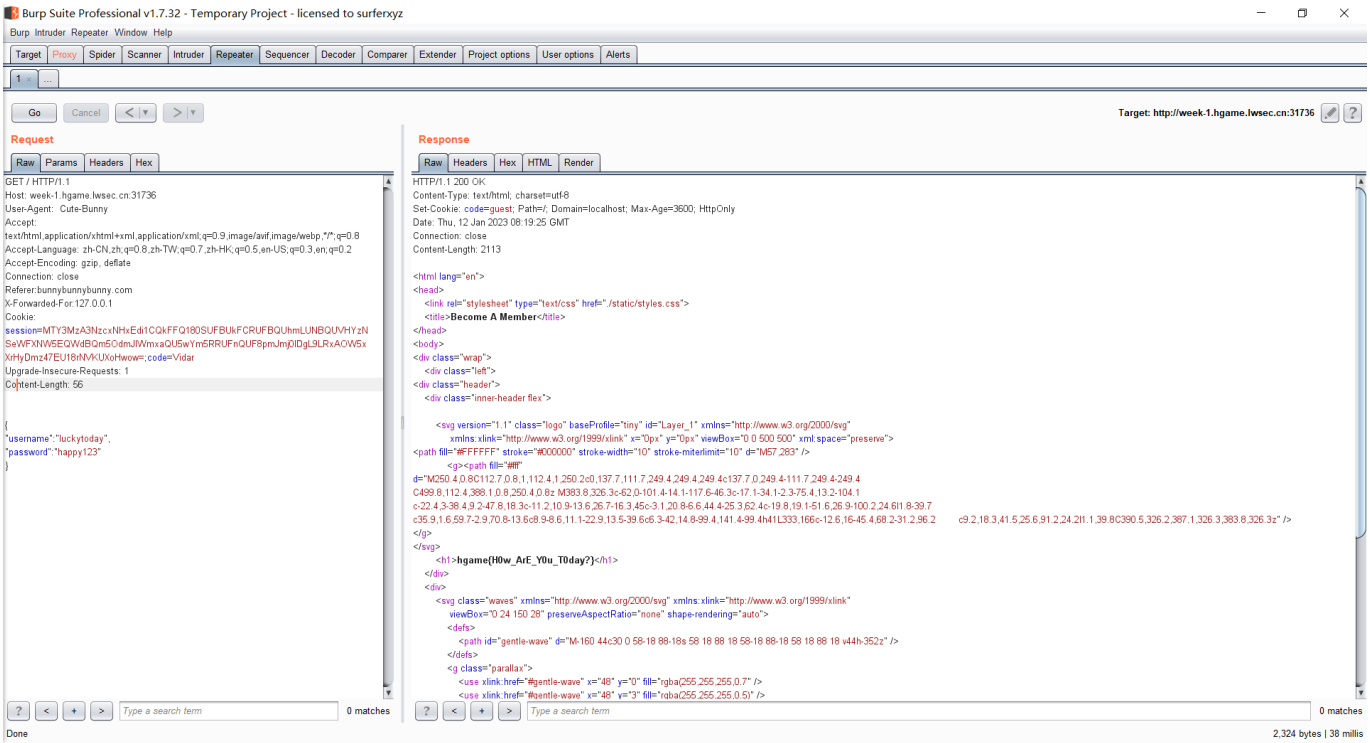

这个就很熟悉了XFF伪造

添加X-Forwarded-For=127.0.0.1




直接在请求体中添加json格式的账号密码即可

注：这里仍然使用GET请求，不使用POST，因为出题人懒得改代码啦（不是

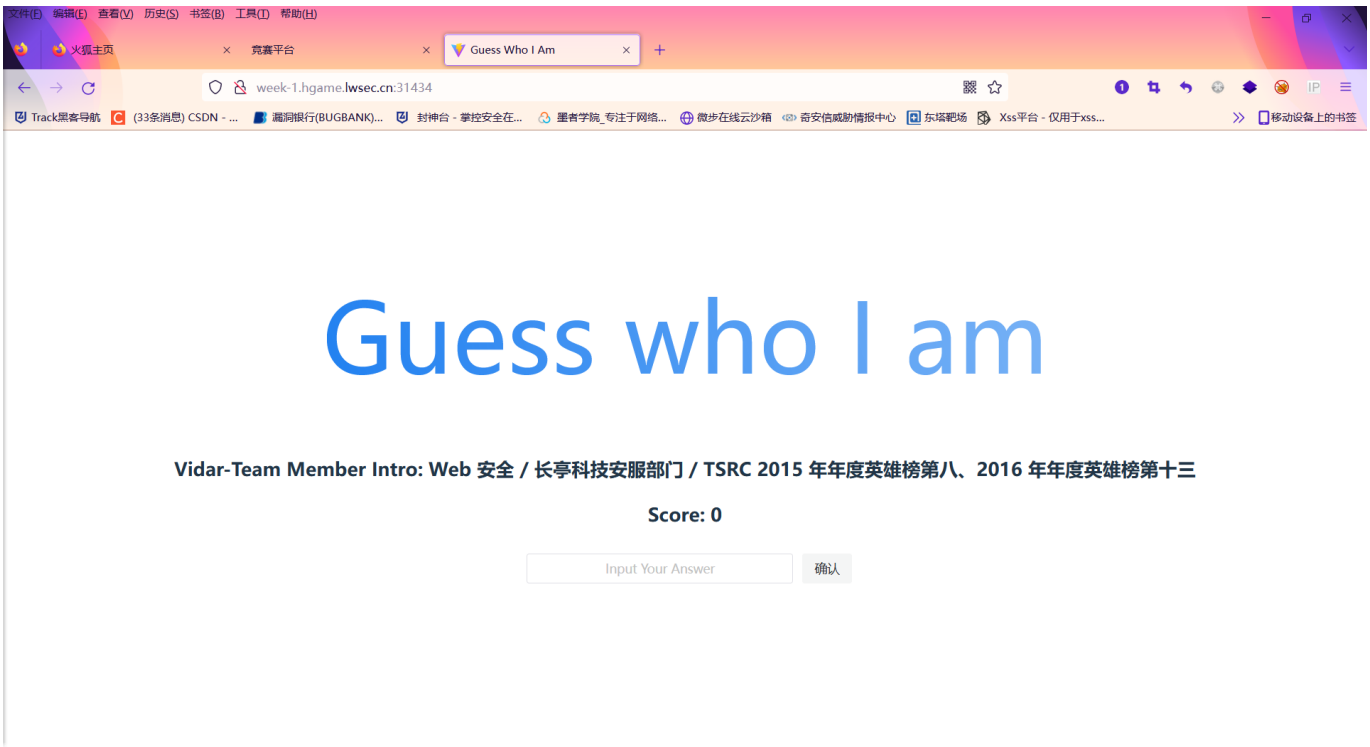



拿到Flag，结束

## Guess Who I Am

题目里面说要写脚本

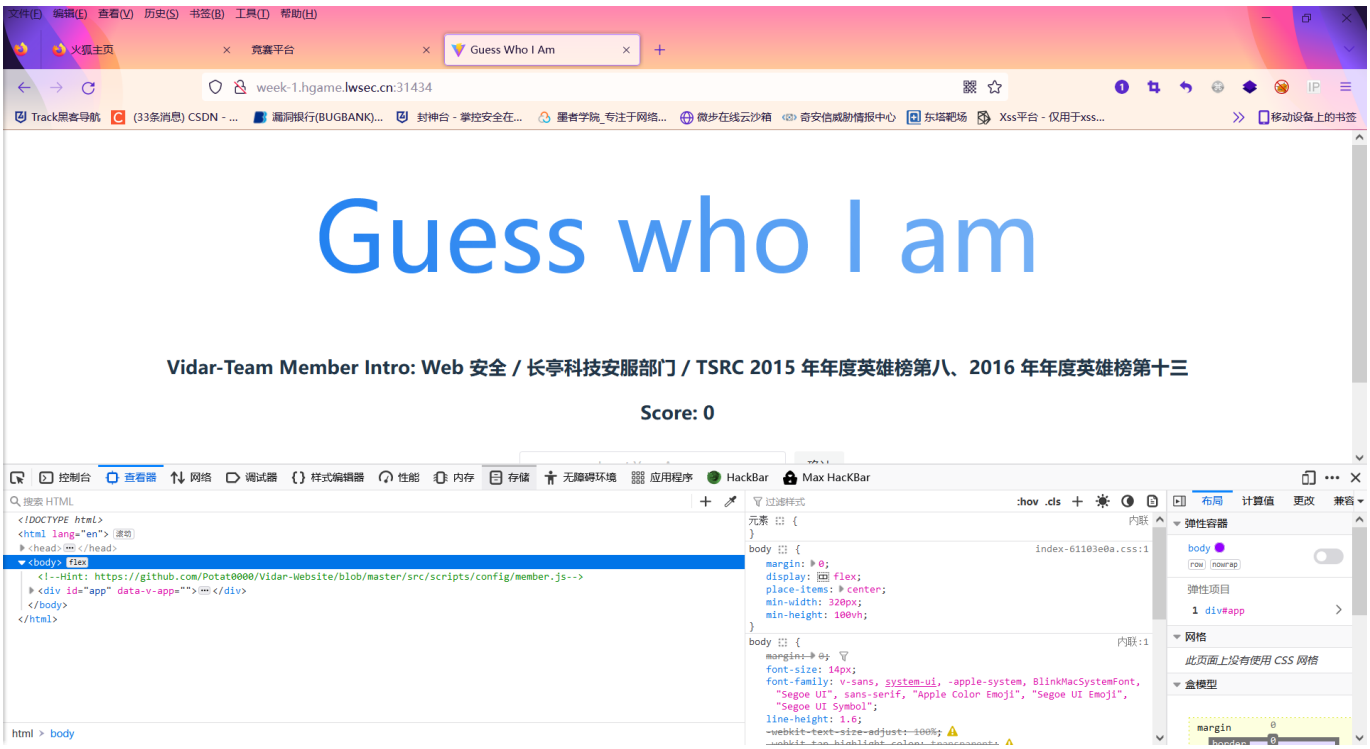
打开环境



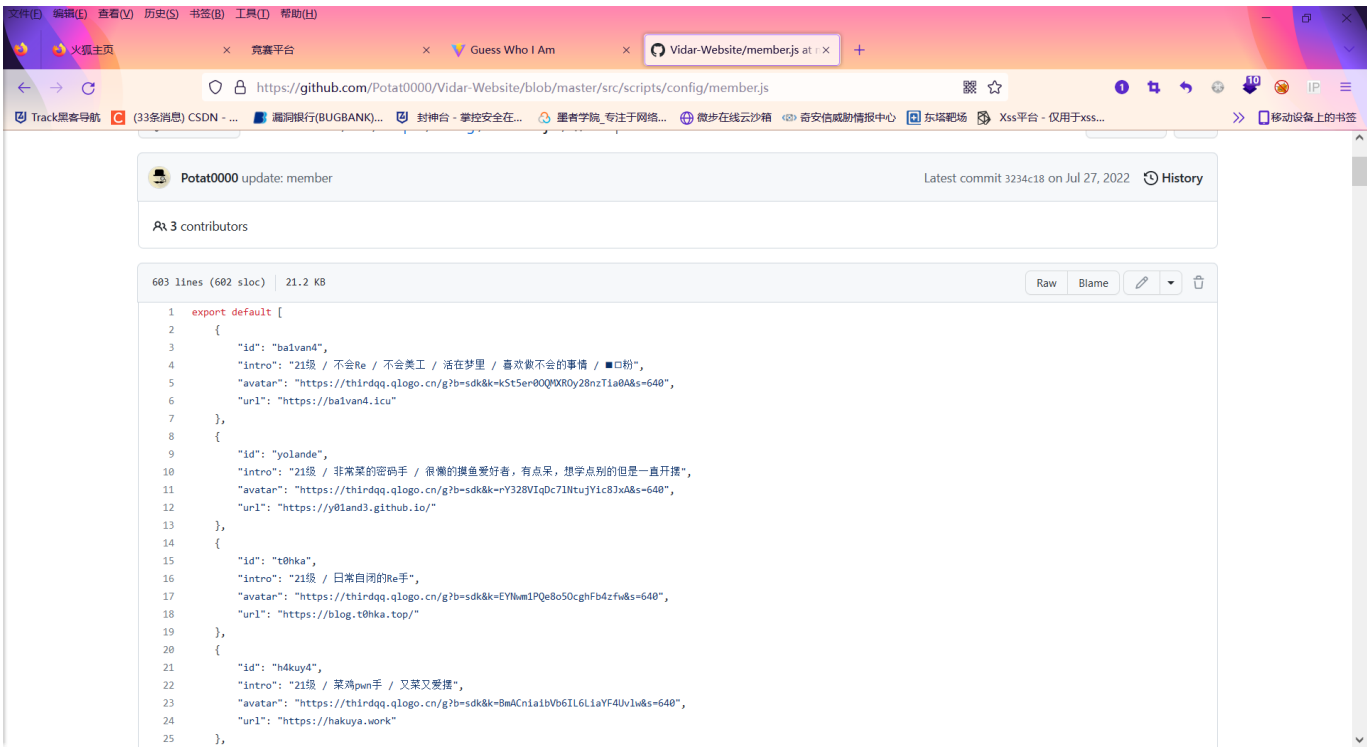

是要写脚本自动答题嘞

找答案吧，打开F12

发现Hint




打开，发现js文件里有答案




尝试写Python脚本（现学）

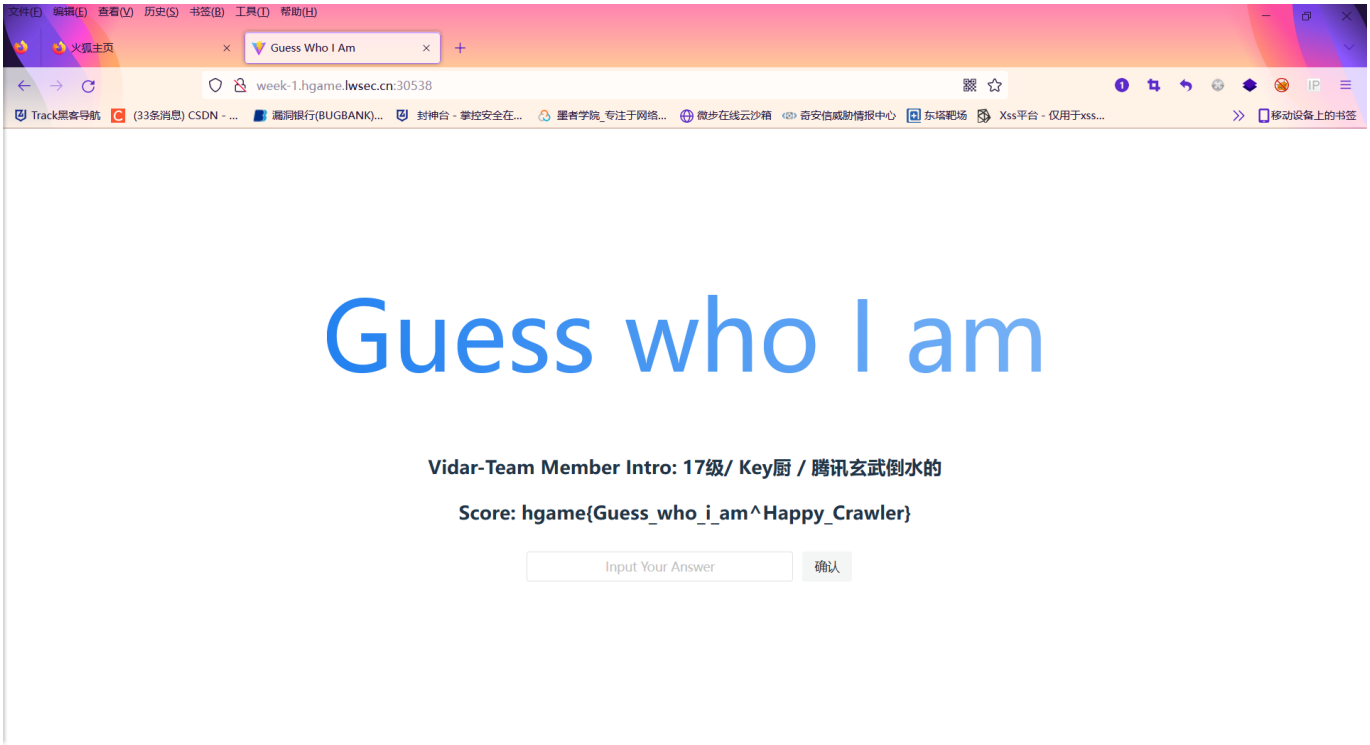
学习request.....

写出来的脚本报错...

结束，果断使用人工脚本

一个一个人工搜索

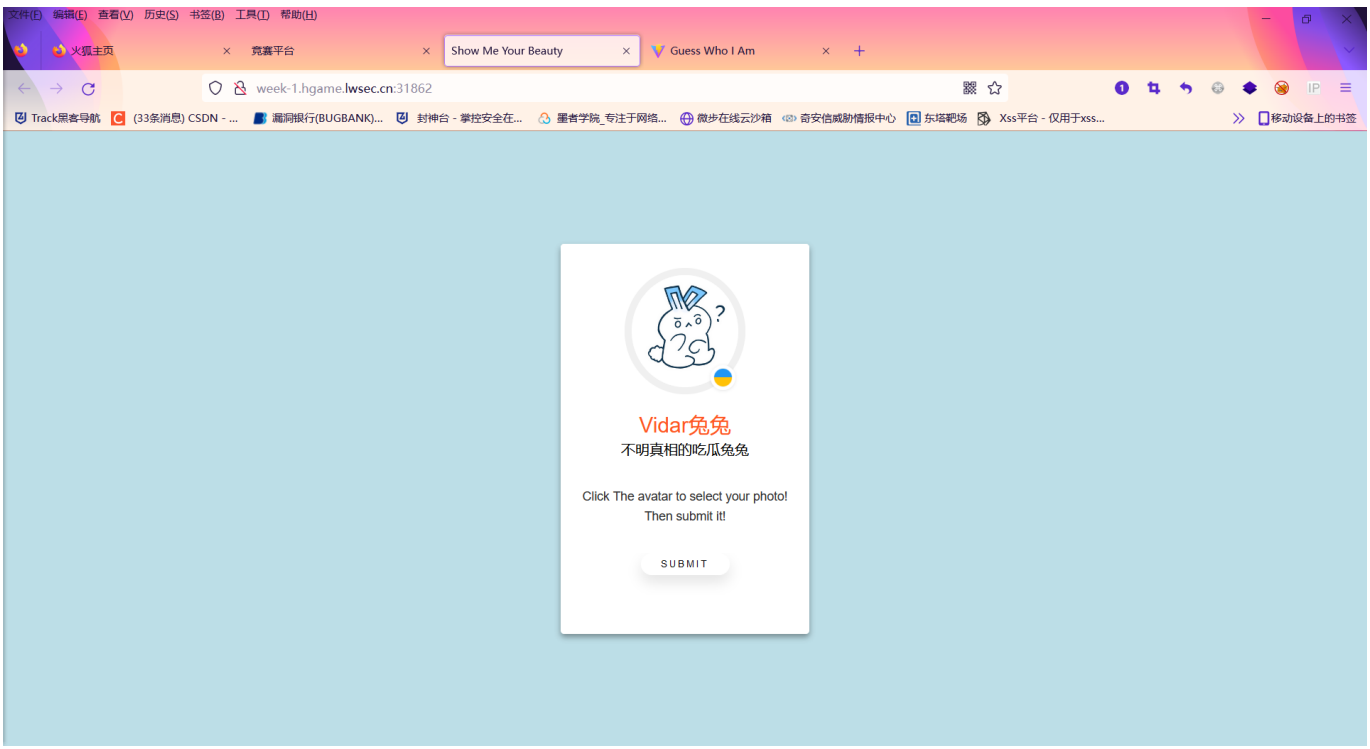
最终拿到Flag，手断了




## Show Me Your Beauty

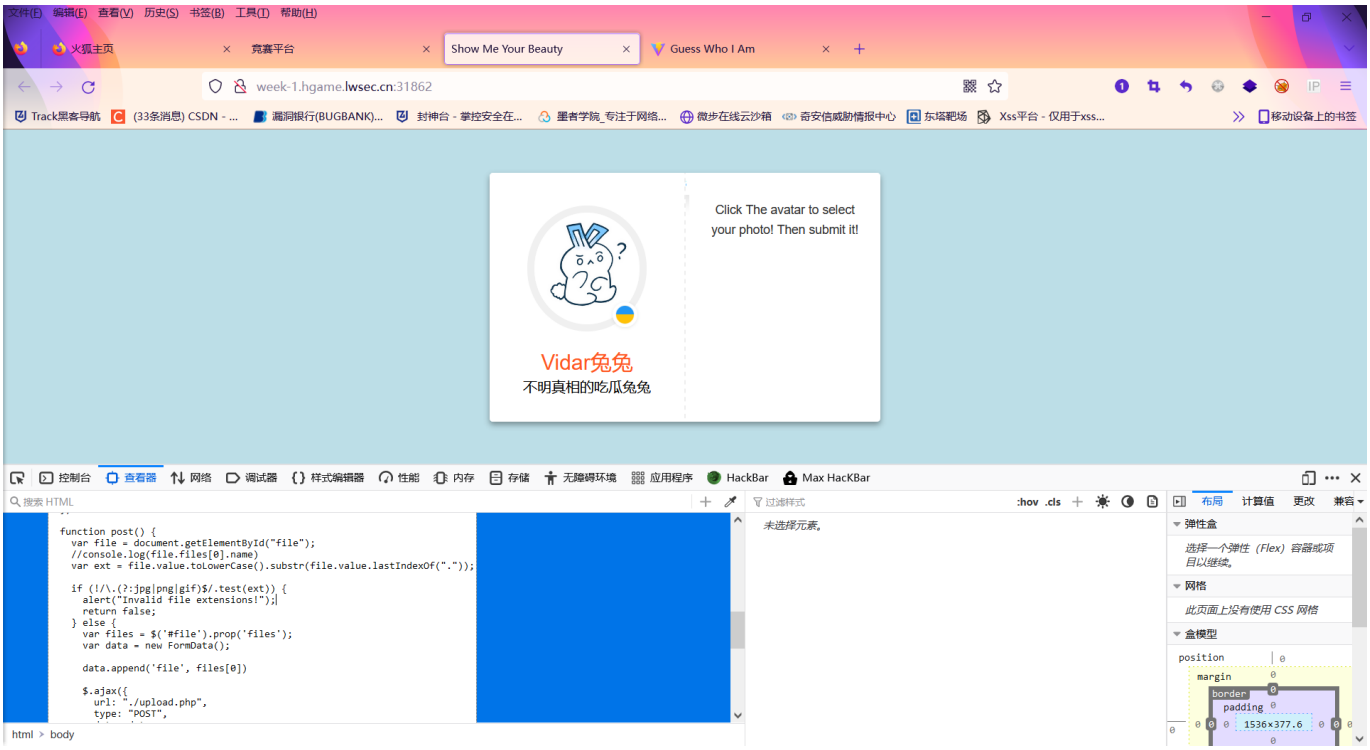
看题目描述，是文件上传题

打开环境




可以通过上传头像来上传shell

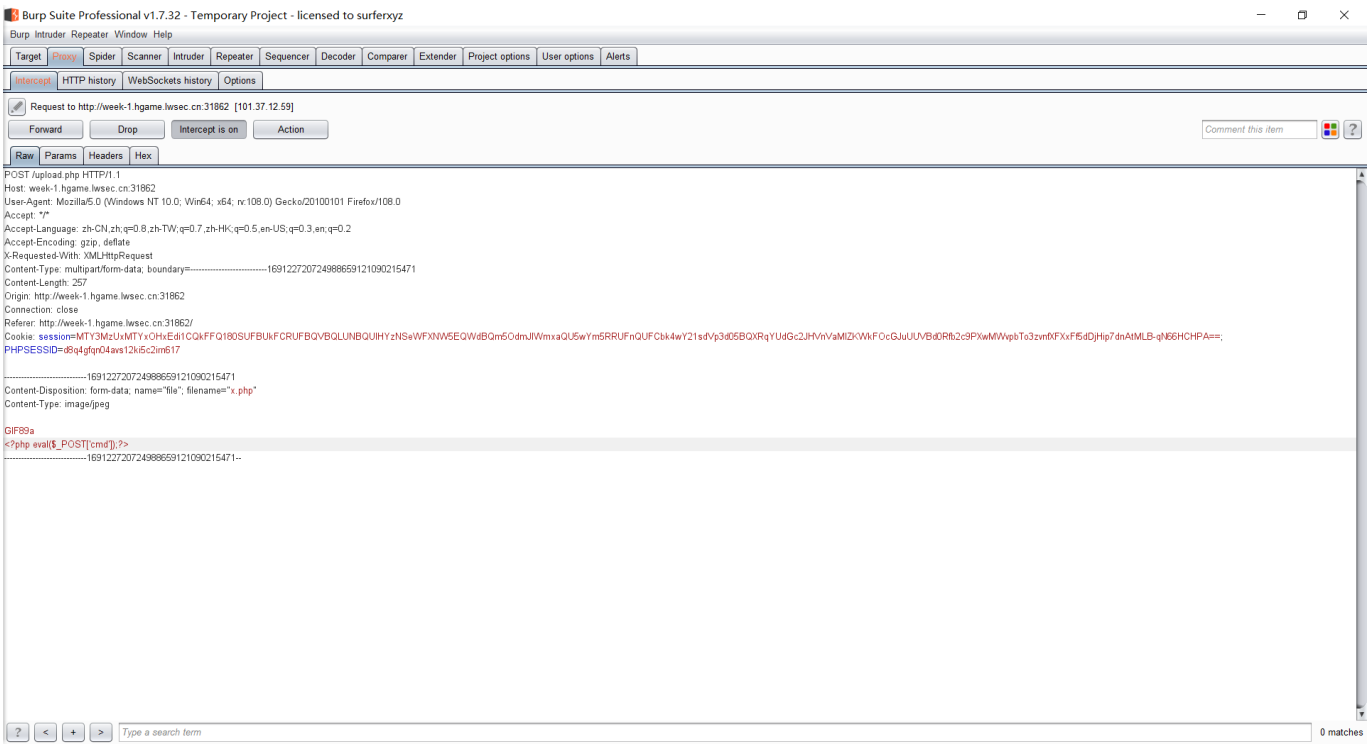
先看看前端有没有验证



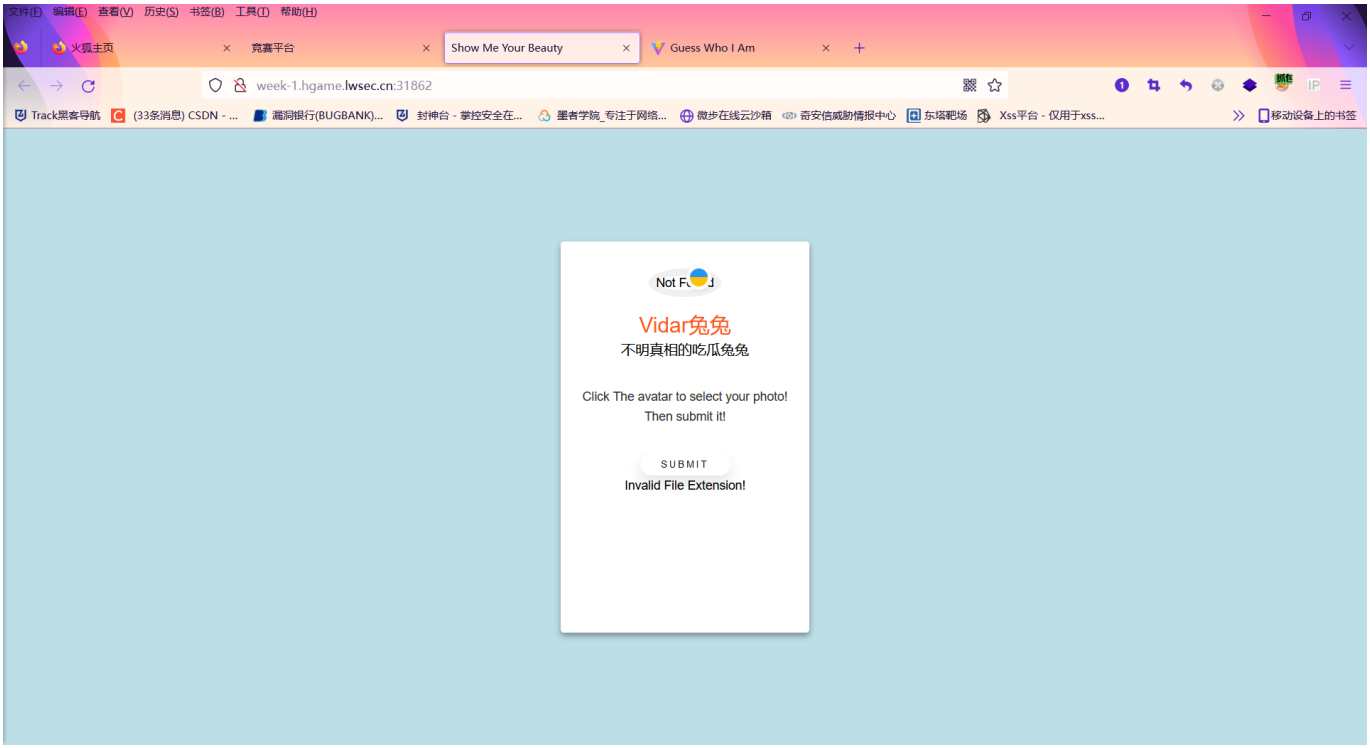

发现前端有白名单验证

上bp，抓包改后缀名就可以绕过前端

改后缀名为.php



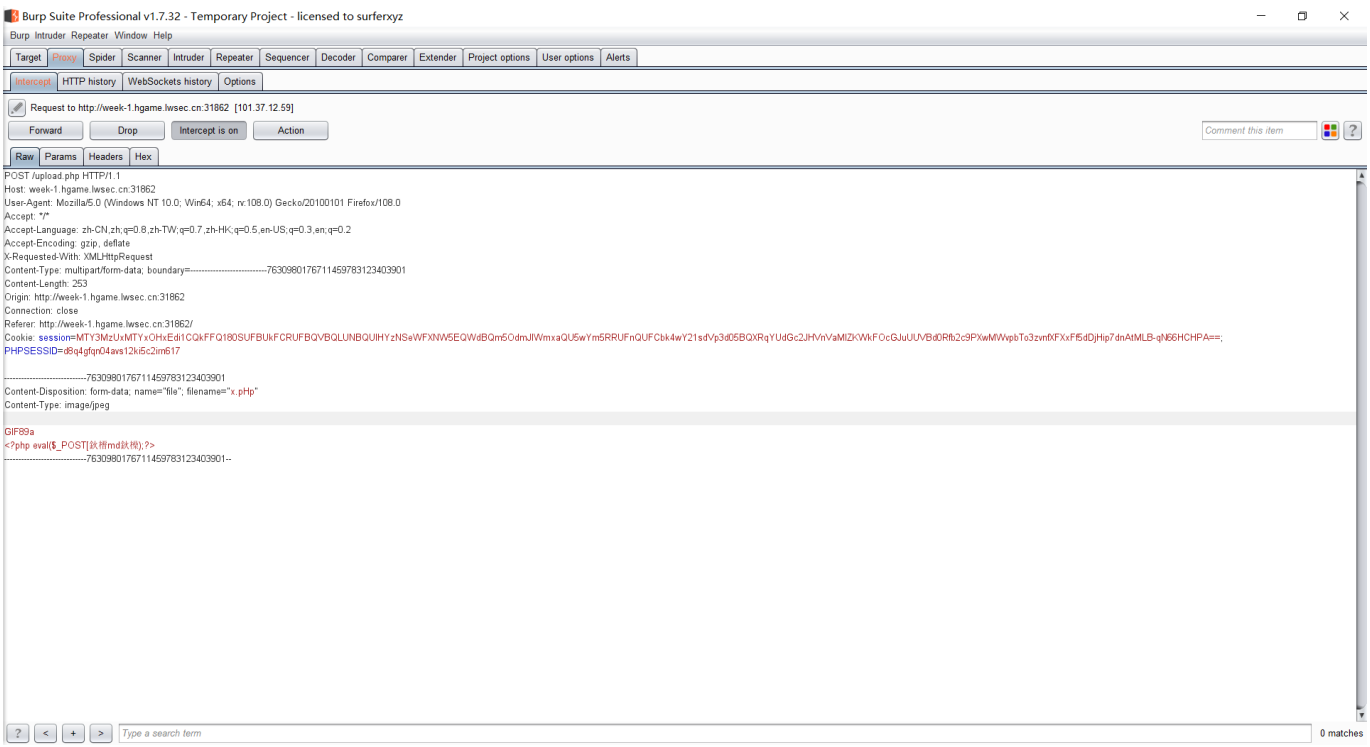

发现不行，后端也有验证



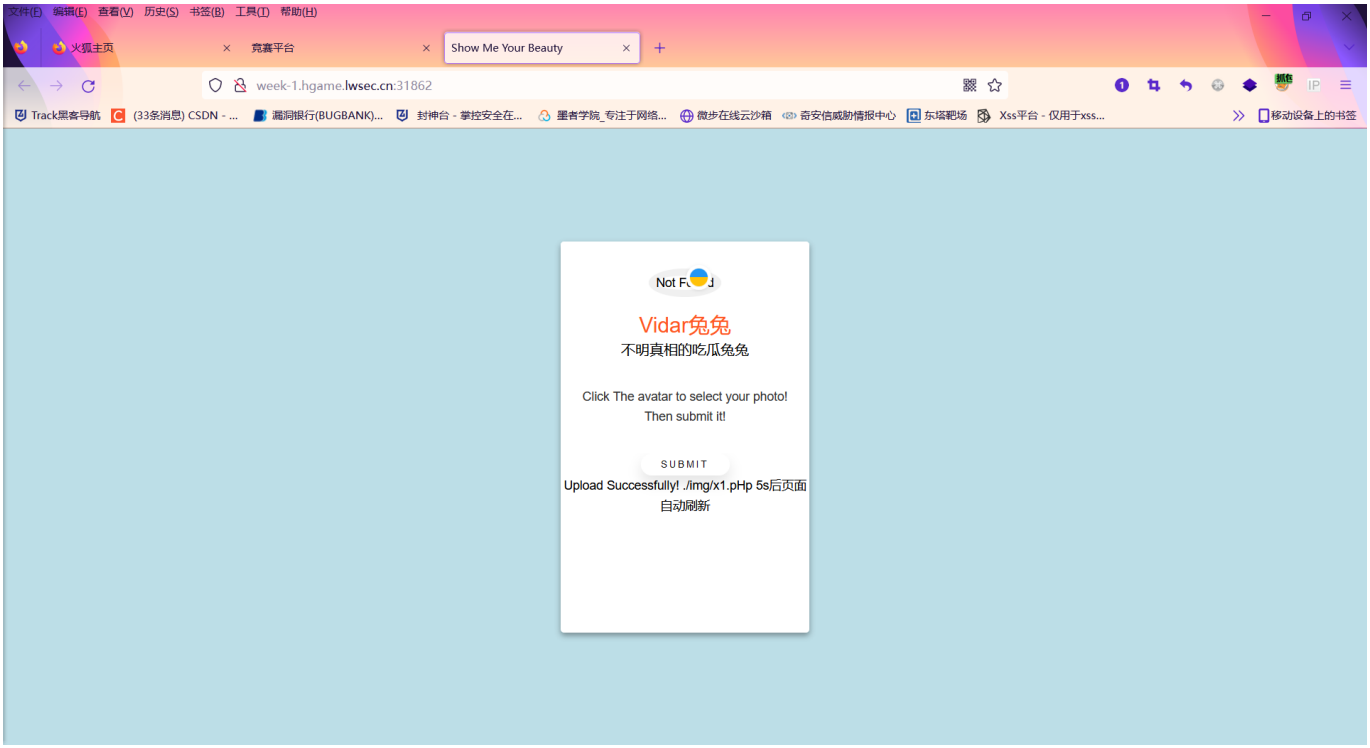

一开始想到修改.htaccess文件，然后发现被过滤了,pht,phtml,php3等等都被过滤掉了

再后来尝试最简单的大小写绕过，竟然成功了

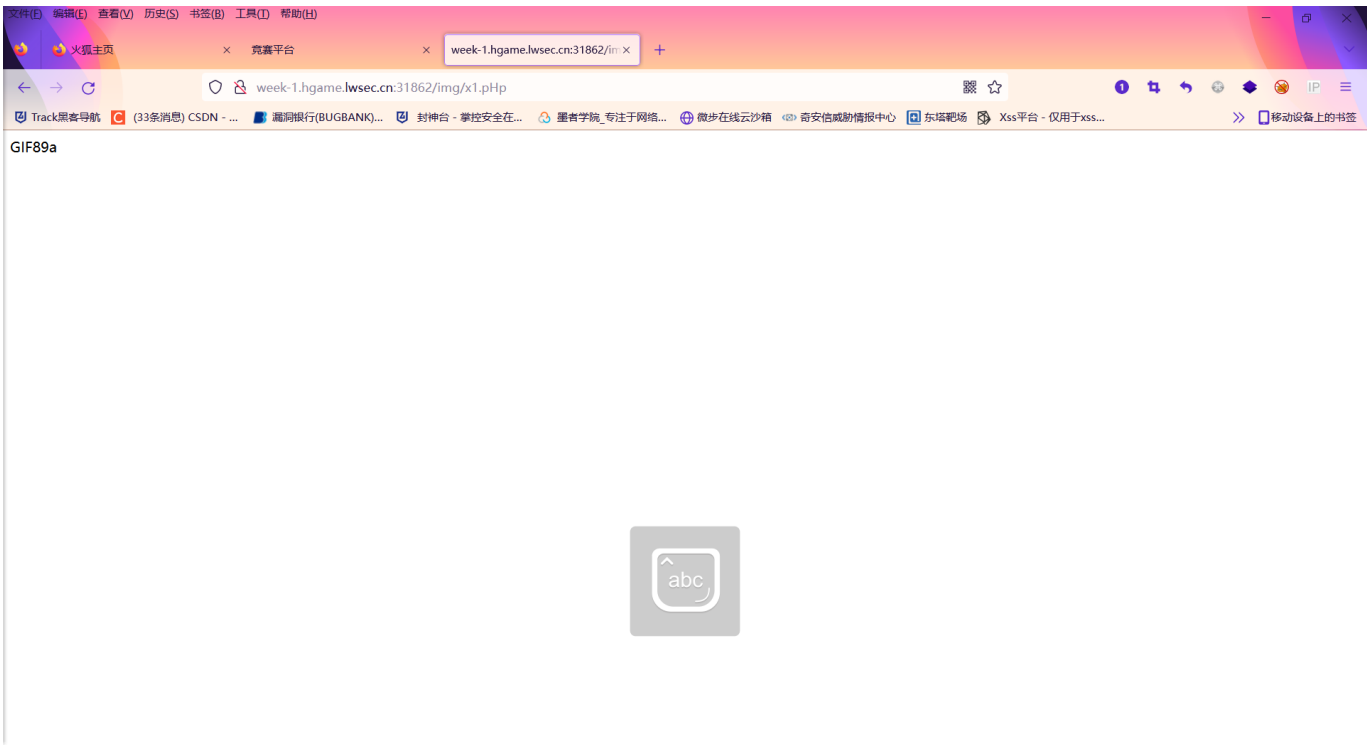
修改后缀为.pHp




上传成功，给了文件储存位置



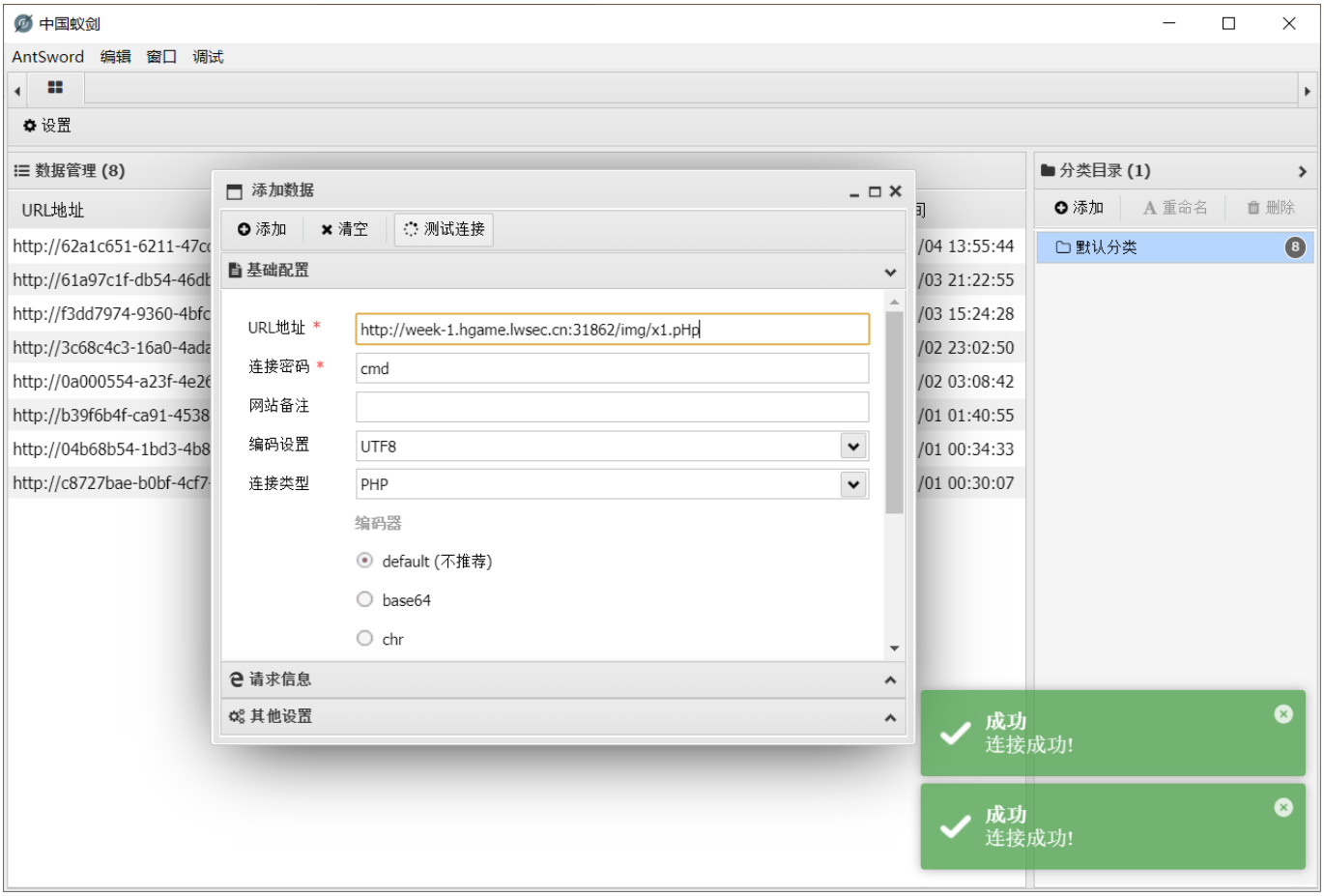

在浏览器中尝试能否打开，能打开，说明我们的shell上传成功



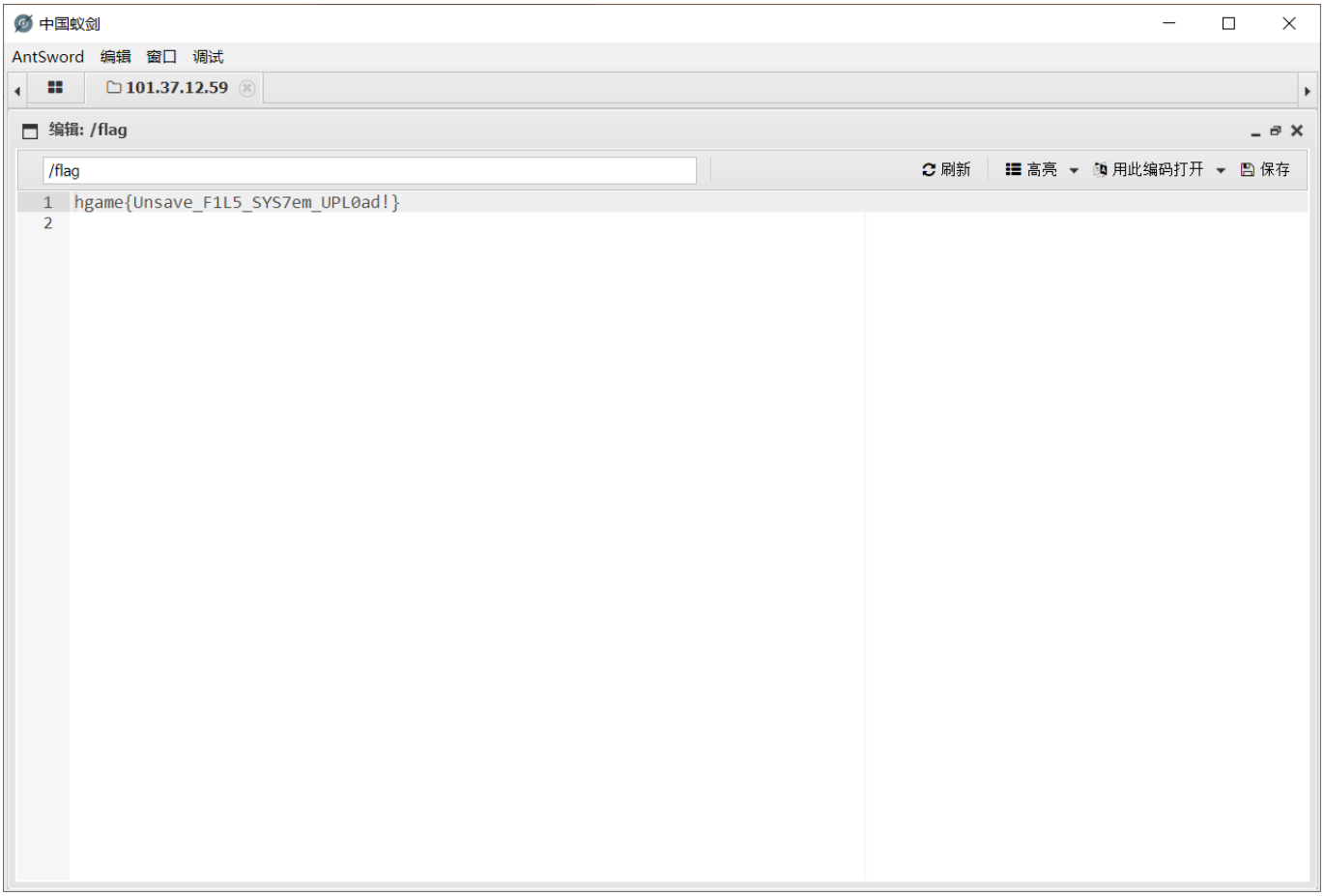

发现可以,现在有两种做法

1. 直接上菜刀，或者蚁剑连接
2. 用POST传参cmd,执行命令

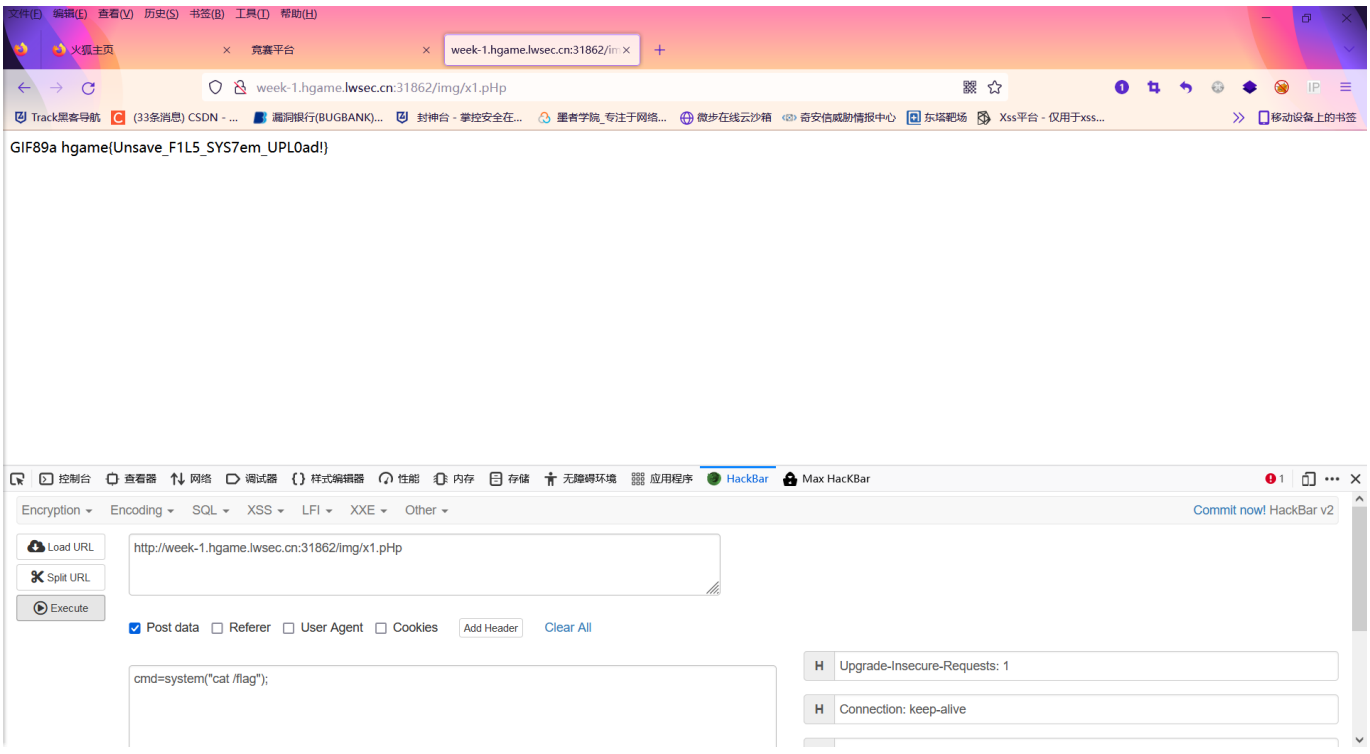
我是用蚁剑连接的




Flag一般在根目录下面




还可以直接用HackBar传参

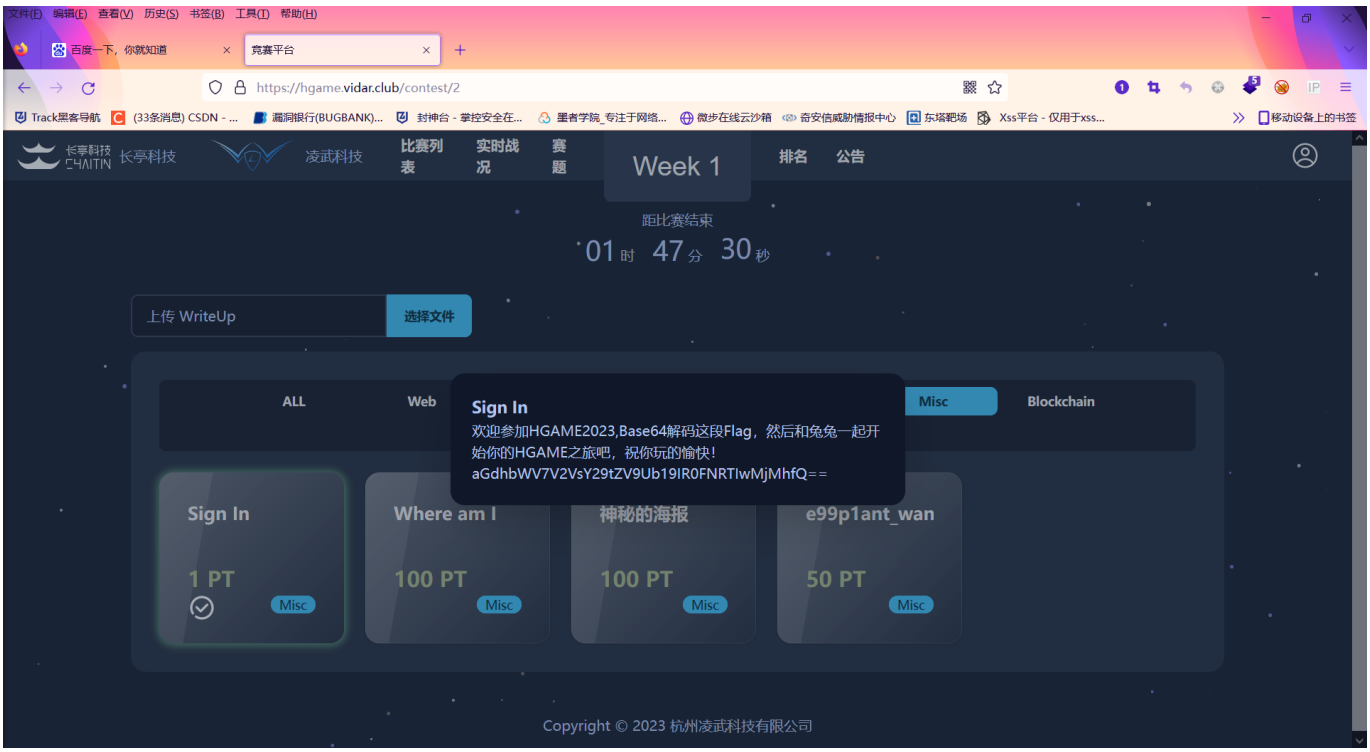



拿到Flag，结束

# Misc

## Sign In

打开题目




复制，base64解码即可