2022---hgame第一周WriteUp

原创

3tefanie丶zhou 已于 2022-02-02 16:22:35 修改 819 收藏 1
分类专栏： CTF 文章标签： 安全
于 2022-02-02 14:08:04 首次发布

文章目录

Misc

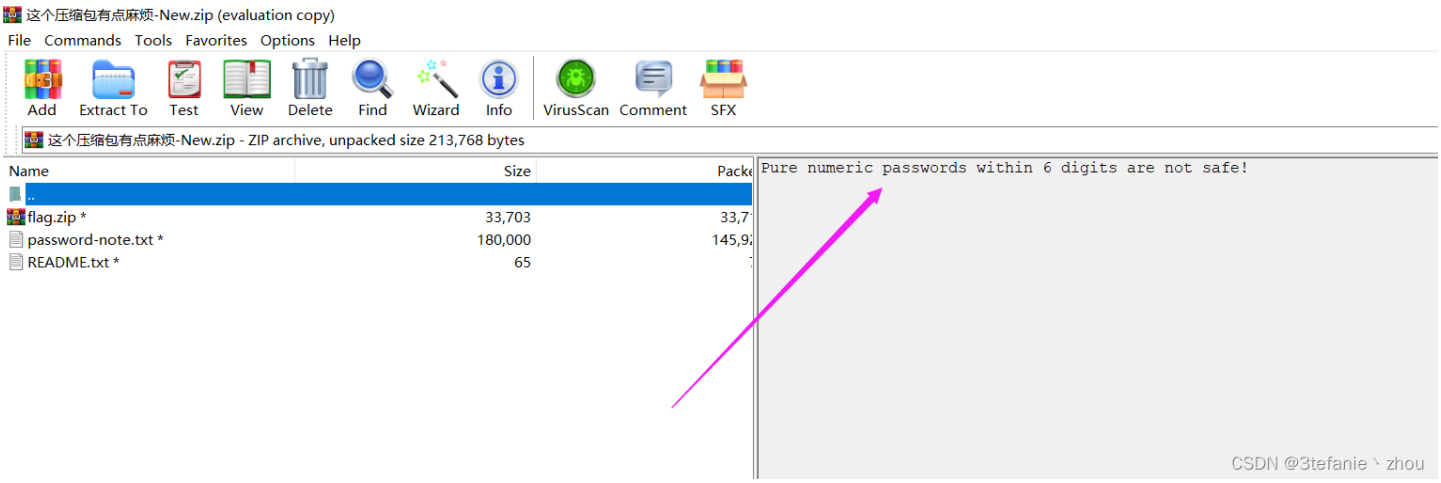
欢迎欢迎！热烈欢迎！

签到题，关注题目给的公众号，发送指定字符串即可获取flag


```
hgame{We1com3_t0_HG@ME_2O22}
```

这个压缩包有点麻烦

第一层，注释写明密码是六位数字，直接上工具暴力破解，得到密码




```
password:483279
```

第二层，从readme.txt中得知另一个txt是它的密码本。欧克，跑字典就完事了

`readme.txt`

```
I don't know if it's a good idea to write down all the passwords.
```

跑出密码为：

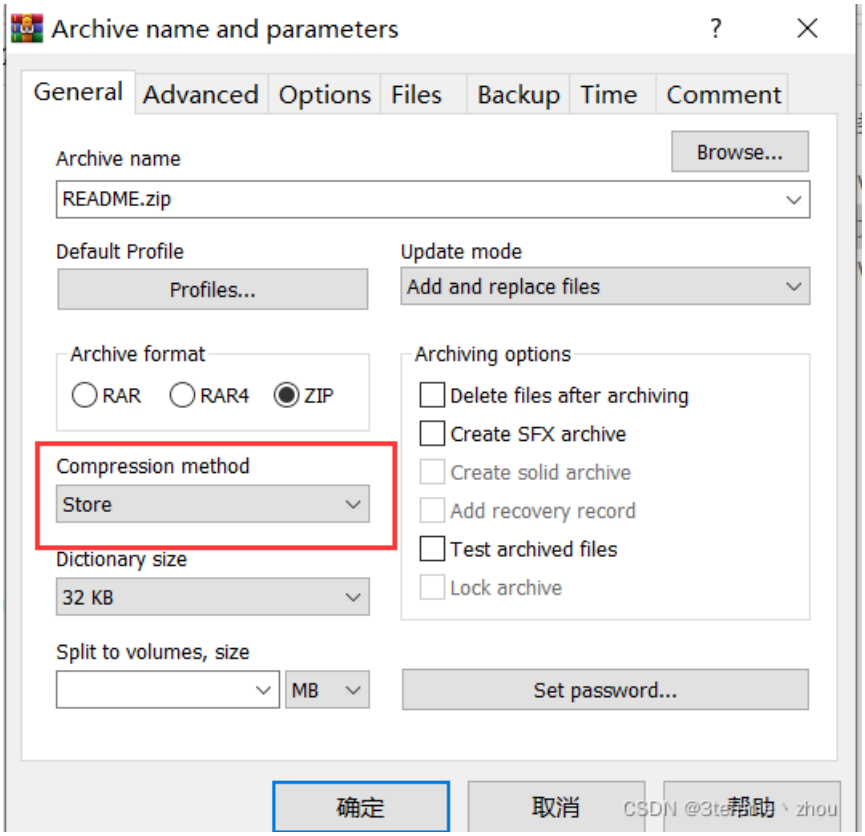
```
password:&-`;qpCKliw2yTR\
```

第三层

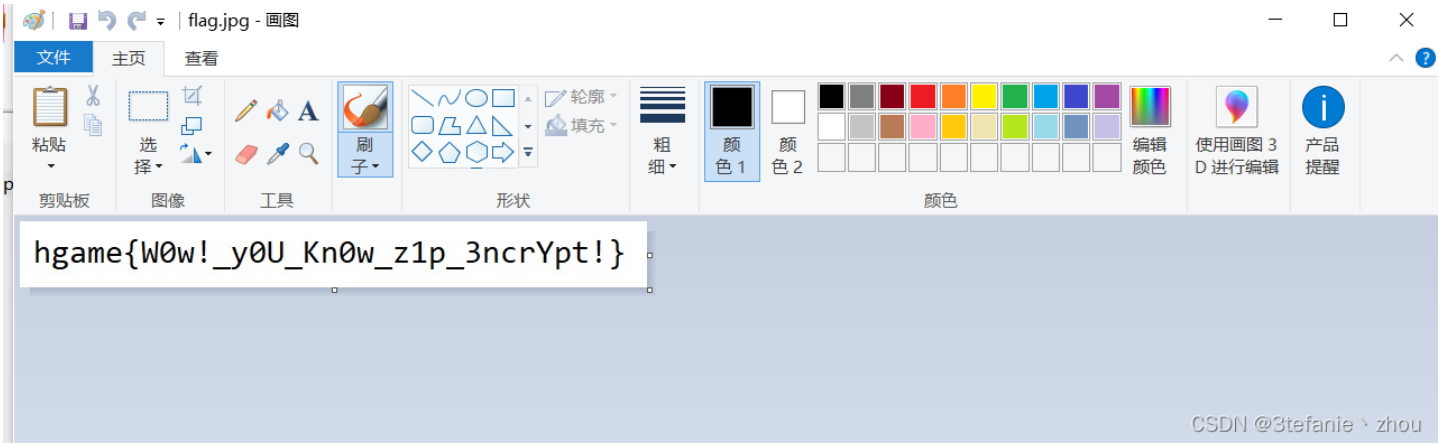
`readme.txt`

```
If you don't like to spend time compressing files, just stores them.
```

得知这一个压缩包是由store方式压缩的，所以我们采用该压缩方式压缩明文



之后进行明文攻击即可
第四层，是一个伪加密，但是和平时不一样
这次需要修改`压缩源文件数据区`和`压缩源文件目录区`的全局方式位标记
将两个全局方式位标记修改伪00 00即可




```
hgame{WOw!_y0U_KnOw_z1p_3ncrYpt!}
```

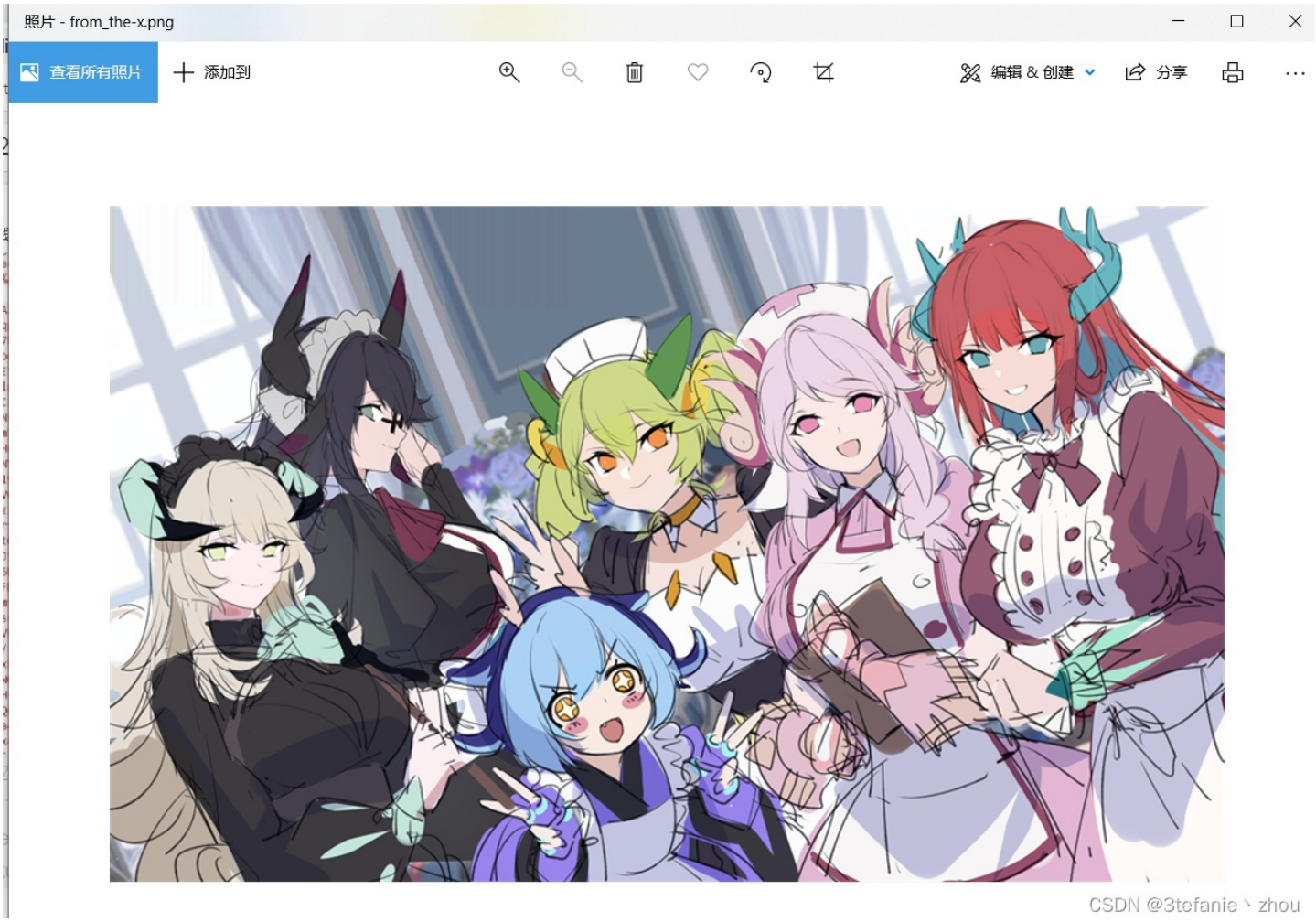
好康的流量

追踪TCP流发现一张base64编码的图片

```
--------------C749C3423D3952356F67A368
Content-Type: image/png;
 name="=?UTF-8?B?5rap5Zu+LnBuZw==?="
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename*=UTF-8''%E6%B6%A9%E5%9B%BE%2E%70%6E%67
```

```
iVBORw0KGgoAAAANSUhEUgAAA2MAAAIPCAYAAAD+cAacAAEAAElEQVR4nOz9eZBlWX7XCX7O
du99vseSkftamZVZWaWSVJtUqpJKIIEaAU0bIGiaMZuxXgzNYNPMwHTb9Fib0TYDA3RrpmEG
EKIQaGGQUCPQioS2kkpb7VVS7bkvkREZkRHh4dt7dzvnzB+/c++7z/25h7tHRGZkdvzSPCPC
33t3e/eec36/7/f3apP/cGnoooAEDkDVv5uoma5KDh99xJLizkmanmhlT+69+0b+72v3fXv
o27nqNud8/4QIuOm5vL6NhvrE5roaXcC46pkc2tCXTeAosgdC4s5AONxRVU2xBZMYSjyDJc5
sNA0LdVOTdu0xBgPPi5AKYV1lnwxw40sSiloFEppDJYszyiKAlc4iIE61NQ7Jc2kIZpINBAb
iIByCuUVIQZ8CIQ6AlHOtzuUCLTpH1ahFMQY8crTli1eeUIIhDpACzrTWCwmNyilCDHSVp5W
tXjtiY28T6GwuWF1NOLMvStYNFtbE8aTmth0++uuw/TfMULrW8qyptqpCTrS1tuU5SWUuvZ9
FoG2e6GFrckOG5slW+MKlaXrmT4fQ2Bnc4MQG2KM8lrargoGZwuKxSUW11blu0vHt+Q9d65a
sKrfT6gDSydWufdtjxNjmP/9Hng/K0LtOfvC16gmY1SmUUBbK65u1WxWY6JXrCwWmFyxOa7Z
aRt8I2cdQ8C3DU1V4ictQSuCNYDGtoa15RGn1hZZKDKUgjK2bG5WjMuGVu9zvLuP+yY8b3Pj
evdzvdvdb/u7Y/d2rnUcx72+19rumzSs0SwWGUtFhlGwMy5Z39hke1zivZ95bzcPoTTGWVyW
Y5yF9MwqBbkzrC0WZNawNa4YVw1FnrO2ssIoz9M+DasrK6ytrJI5d8gjlX3EGCmrkvWrV9na
3sbHSIiB8WTCzqTEWc1i4agbz1bZ0viI0hoVI01TU453qKuSGEK/Za0U1mW40QiXFyhjUUQU
kdwZlkcZ1ihGBJYWRjz42JNorffOJQdFlOM3RrG4kHNidQljNJeubHHx0hZNG9DaQgQfIt57
fNviQ4AYUQqsteR5TjHKyTKHtQatNUoplFL9MXnv8V7mDKXox9S29bRtIMaIMRqtNcZonLMs
LeasLucsjBxGp/c3nq3tkitXJ5RlSzjk+TpnOLk64szpRfLcsrlVcfHSNpvbFSHs3YZKnykK
S4xQlg1NG/ZueJ/QWrG8lHPn6UWWF3N88EyqhnHlGVee1gemk+3gc0pROMvKUsHyosNZjUr3
2XWF6v93C0Y88J9v1jjoWezXFNcRSileeO0yL7xyjjvvugv/2nkee/wJ8iw72jgwZ7sfe/lV
/vnnvsKfevuD/MV3vO26tjeMmfXUIcOHyPZOzeX1MVs7dXp2jh4KcJlhdSlnaSGtd2rPeNIw
njQ0recGneahQmuF0YrMGYrcsriQsbSQkWcGrQ93jbSKEGVEnXkhhkgTPXWTBuy3UCilsGjy
zGJTwqEU6KgxuUY5BURJbqqAVkp+n6UJO0RCiH3CoYNMPPK5a0eMkagDMYRp0qIgEokxElTA
q5T0OIXRBh1kYgRQXt4//MpU/1/6d5QbVg3eMfMvpeS4M40OacJ10wVJjNPzU8jEopWe2QdE
QoxUoaWsGnlAlMGYg6+DUqC9xkSZrCFiFxYw5BzmCVKAJvTnkeHICoM1ZpokpdC5wWXZ3Lkr
ak9QnibUeN9OL6iCCYq6CjPXWGeKcbVFVY5RQV/zOOfsEWMsi6O1fkCMgMkieWFw0RBNpMHL
tTQ6PcgxZd6SsGuV7tm0oAO5H+umpW48wci2rda4wmBytfvxvh2343UJrWSSMlphjaHIHUWe
YY3ec0+mMhJSeIiEIAv74VgXQqRpJYmzVp6DtvW0TbeYV4QQaJqGtp1THLtGKKWwxpK5DGPM
9HfWYowmpLHfGo3RaSyMEZRCa4M2ZlpQSicVI4Tgib4lxpDW0vL0tgEaH4ko6qioJhPG25uz
2zhUpCsXoW0DTdOilBQUM2emx4nqkysZQ+g/F9I1765797P7+nQ//SZnXpO5qPt9jLJN7wPe
```

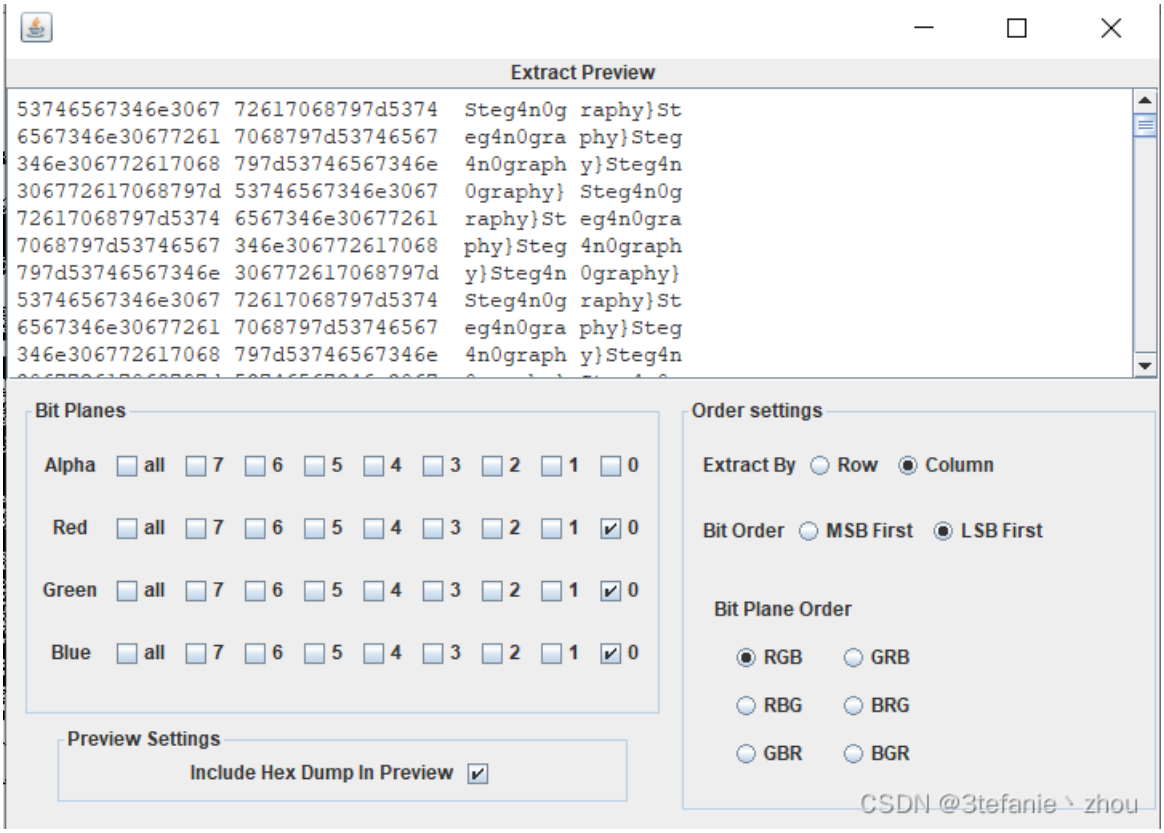

解码，保存位新的图片



使用stegSolve查看，在green 2通道发现条形码，使用工具扫描获得部分flag


```
hgame{ez_1mg_
```

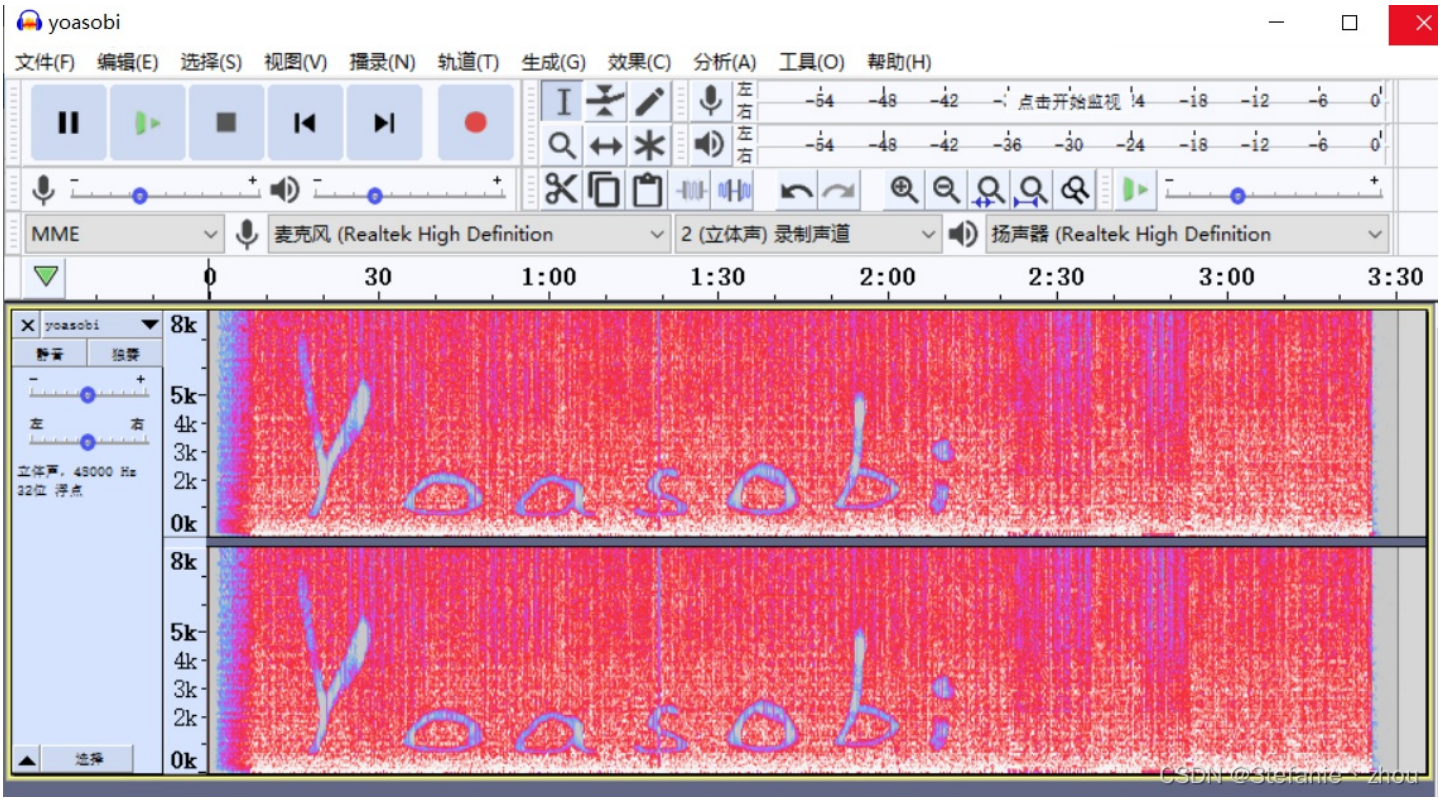
查看LSB,发现另一半flag




```
hgame{ez_1mg_Steg4n0graphy}
```

群青(其实是幽灵东京)

在频谱区发现一串字符串



```
Yoasobi
```

使用silenteye解密,得到一个下载链接

```
https://potat0-1308188104.cos.ap-shanghai.myqcloud.com/Week1/S_S_T_V.wav
```

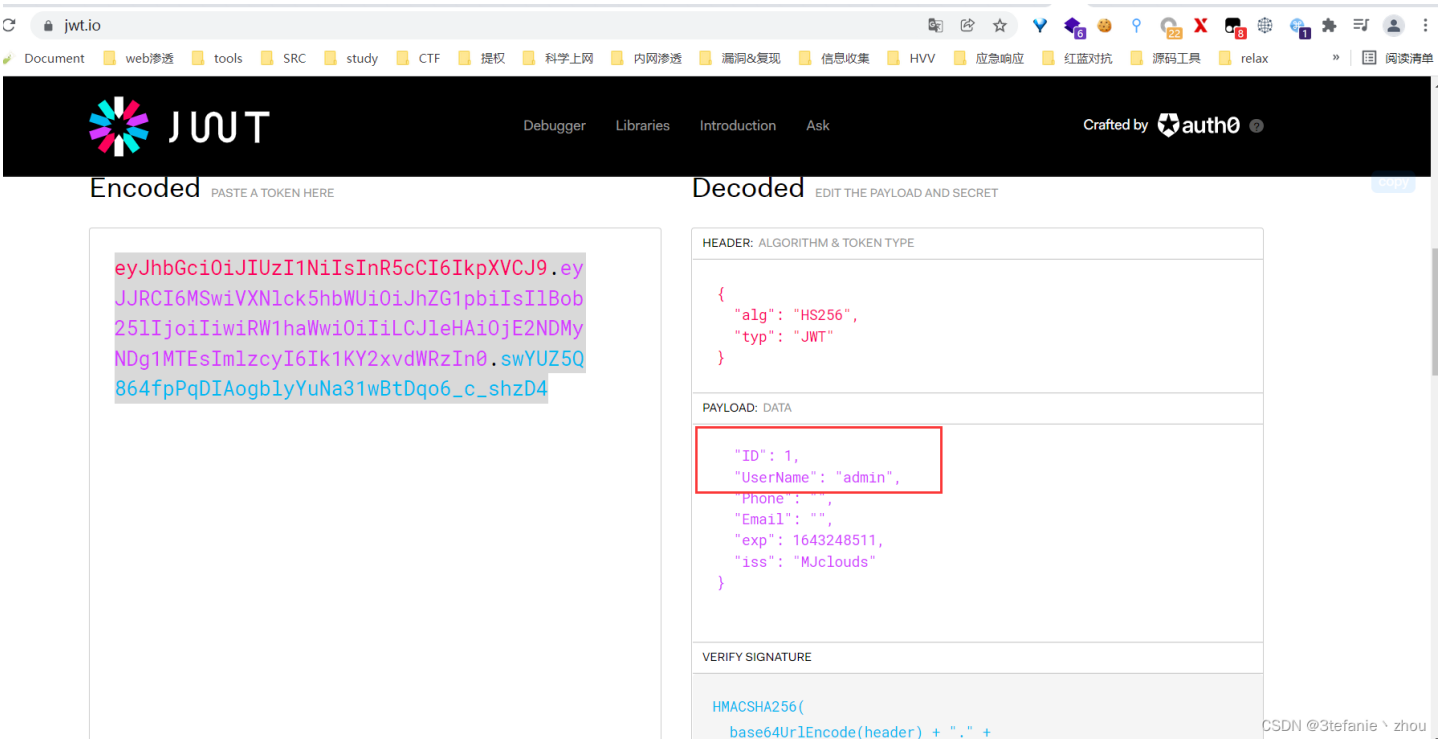
根据提示SSTV，应该是一个无线电解码
直接使用RX-SSTV解码，得到一个二维码，扫描得到flag

```
hgame{1_c4n_5ee_the_wav}
```

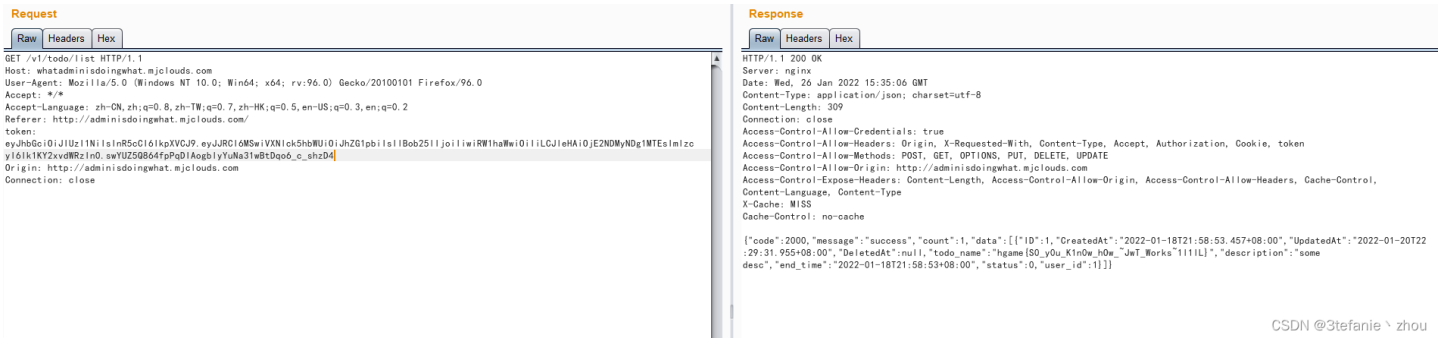
Web

easy_auth

抓包发现token是明显的jwt格式，于是想到jwt伪造token



将ID修改为1，username修改为admin
抓包替换token，得到flag



蜘蛛...嘿嘿❤我的蜘蛛

过关型题目，写个脚本一直发送请求直到结束即可

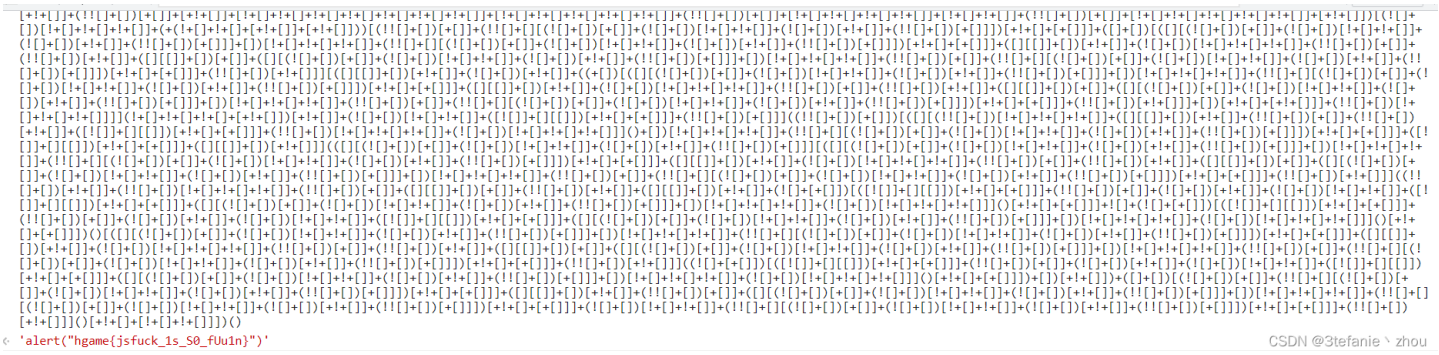
```python
import requests
import re
url = 'https://hgame-spider.vidar.club/425b3ac1d1'
response = requests.get(url)
get_key = re.findall(r'href="\?key=(.*?)">',response.text)
while True:
    if get_key:
        response = requests.get(url+'?key='+get_key[0])
        get_key = re.findall(r'href="\?key=(.*?)">',response.text)
        continue
    else:
        break
print(response.headers['Fi4g'])
```

flag:

```
hgame{eaeca5a65c1400a1aea2d7fcfb3abe5199c61c1105f65ccf81afe18bfd03e5a7}
```

Tetris plus

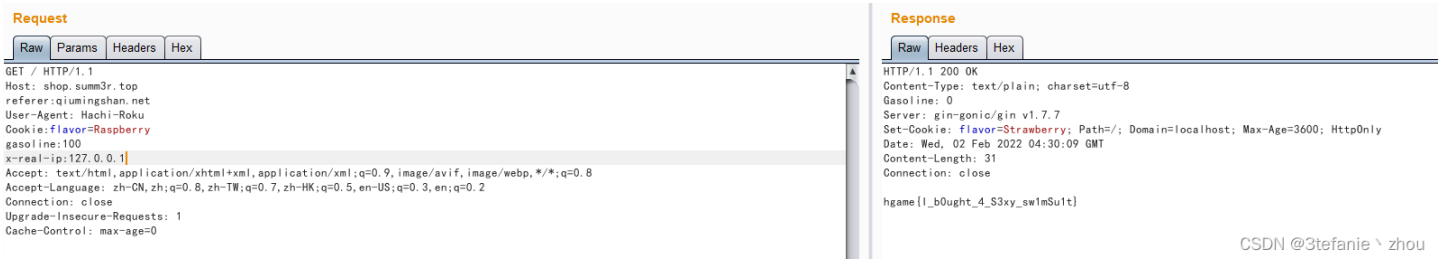
在js源码中找到jsfuck编码的字符串，直接在控制台输出即可




```
hgame{jsfuck_1s_S0_fUu1n}
```

Fujiwara Tofu Shop

根据题目提示添加到对应头部字段即可




```
hgame{I_b0ught_4_S3xy_sw1mSu1t}
```

Crypto

Dance Line

记录移动轨迹，向X和Y轴移动分别记为0和1，将得到二进制转为字符串即可

```
from PIL import Image

pic = Image.open(r'C:\Users\82093\Desktop\hgame\crypto\danceline.bmp')
width,height = pic.size
x_list = []
y_list = []
for x in range(width):
    for y in range(height):
        num = pic.getpixel((x,y))
        if num == (84, 150, 206) or num ==(0, 0, 0):
            x_list.append(x)
            y_list.append(y)
flag_bin = ''
for i in range(len(x_list)-1):
    flag_bin += '0'*(x_list[i+1]-x_list[i])+'1'*(y_list[i+1]-y_list[i])
flag = ''
for j in range(0,len(flag_bin),8):
    k = flag_bin[j:j+8]
    ascii_k = int(str(k),2)%128
    flag += chr(ascii_k)
print(flag)
```

```
hgame{Danc1ng_L1ne_15_fun,_15n't_1t?}
```

EASY RSA

```
#coding:utf-8
import gmpy2
from Crypto.Util.number import *
c_list = [(12433, 149, 197, 104), (8147, 131, 167, 6633), (10687, 211, 197, 35594), (19681, 131, 211, 15710), (3
3577, 251, 211, 38798), (30241, 157, 251, 35973), (293, 211, 157, 31548), (26459, 179, 149, 4778), (27479, 149,
223, 32728), (9029, 223, 137, 20696), (4649, 149, 151, 13418), (11783, 223, 251, 14239), (13537, 179, 137, 11702
), (3835, 167, 139, 20051), (30983, 149, 227, 23928), (17581, 157, 131, 5855), (35381, 223, 179, 37774), (2357,
151, 223, 1849), (22649, 211, 229, 7348), (1151, 179, 223, 17982), (8431, 251, 163, 30226), (38501, 193, 211, 30
559), (14549, 211, 151, 21143), (24781, 239, 241, 45604), (8051, 179, 131, 7994), (863, 181, 131, 11493), (1117,
 239, 157, 12579), (7561, 149, 199, 8960), (19813, 239, 229, 53463), (4943, 131, 157, 14606), (29077, 191, 181,
33446), (18583, 211, 163, 31800), (30643, 173, 191, 27293), (11617, 223, 251, 13448), (19051, 191, 151, 21676),
(18367, 179, 157, 14139), (18861, 149, 191, 5139), (9581, 211, 193, 25595)]
flag = ''
for i in c_list:
    e = i[0]
    p = i[1]
    q = i[2]
    c = i[3]
    n = p*q
    phi = (p-1)*(q-1)
    d = gmpy2.invert(e,phi)
    m = pow(c,d,n)
    flag +=str(long_to_bytes(m)).replace('b','').replace("'",'')
print(flag)
```

```
hgame{L00ks_l1ke_y0u""ve_mastered_RS4!}
```

Matryoshka

将摩斯逆序，再解码，得到16进制字符串

```
466642756645466E6D4C73364433736959744C3658327034694E306364536C796B6D3972514E396F4D53316A6B7339724B3252366B4C3868
6F72303D
```

转成字符串

```
FfBufEFnmLs6D3siYtL6X2p4iN0cdSlykm9rQN9oMS1jks9rK2R6kL8hor0=
```

维吉尼亚解密，key:hgame

```
YzBibXZnaHl6X3swUmF6X2d4eG0wdGhrem9fMG9iMG1fdm9rY2N6dF8hcn0=
```

base64解密

```
c0bmvghyz_{0Raz_gxxm0thkzo_0ob0m_vokcczt_!r}
```

栅栏

```
cbvhz{Rzgx0hz_o0_ocz_r0mgy_0a_xmtko0bmvkct!}
```

凯撒（位移21）

```
hgame{Welc0me_t0_the_w0rld_0f_crypt0graphy!}
```

English Novel

分别在密文目录和明文目录大小排序，找到题目提示的两个txt

```
ori="e appeared to be that Napoleon and Mr. Pilkington had each played an ace of spades simultaneously"
enc="h sbqctbno uw ox fbay Rbyalrkq pnz Vs. Dwonbnolun chk kuld cteafx ze qbb iz bhktox cismkalhnqxprn"
key=[]
for i in range(len(ori)):
    key.append(ord(enc[i])-ord(ori[i]))
encrpt="klsyf{W0_j0v_ca0z_'Ks0ao-bln1qstxp_juqfqy'?}"
result=""
for i in range(len(encrpt)):
        if encrpt[i].isupper():
            result += chr((ord(encrpt[i]) - ord('A') -key[i]) % 26 + ord('A'))
        elif encrpt[i].islower():
            result += chr((ord(encrpt[i]) - ord('a') - key[i]) % 26 + ord('a'))
        else:
            result += encrpt[i]
print (result)
```

由于选取的片段存在空格，所以得到的flag在空格位的字符会存在部分偏差，手工修改即可

```
hgame{D0_y0u_kn0z_'Kn0wn-pla1nsext_attack'?}
```

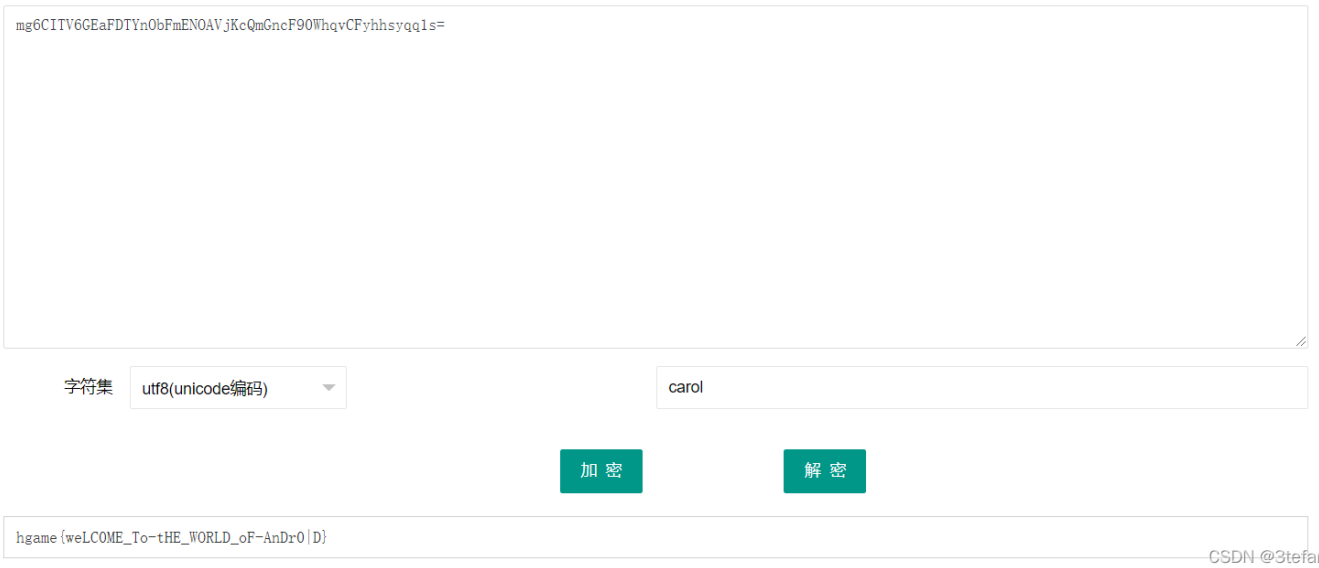
Reverse

flagchecker

```
import javax.crypto.spec.SecretKeySpec;

public class MainActivity extends AppCompatActivity {
    /* access modifiers changed from: protected */
    @Override // android.support.p003v7.app.AppCompatActivity, android.support.p000v4.app.ComponentActivity, android.support.p000v4.app.FragmentActivity
    public void onCreate(Bundle bundle) {
        super.onCreate(bundle);
        setContentView(C0273R.layout.activity_main);
        ((Button) findViewById(C0273R.C0275id.button)).setOnClickListener(new View.OnClickListener() {
            /* class com.example.flagchecker.MainActivity.View$OnClickListenerC02721 */

            public void onClick(View view) {
                byte[] bArr = new byte[0];
                try {
                    bArr = MainActivity.encrypt(((EditText) MainActivity.this.findViewById(C0273R.C0275id.editTextTextPersonName)).getText().toString(), "ca
                } catch (Exception e) {
                    e.printStackTrace();
                }
                if (Base64.encodeToString(bArr, 0).replace("\n", "").equals("mg6CITV6GEaFDTYnObFmENOAVjKcQmGncF90WhqvCFyhhsyqq1s=")) {
                    Toast.makeText(MainActivity.this, "Congratulations!!!", 1).show();
                } else {
                    Toast.makeText(MainActivity.this, "Fail,try again.", 1).show();
                }
            }
        });
    }

    public static byte[] encrypt(String str, String str2) throws Exception {
        SecretKeySpec secretKeySpec = new SecretKeySpec(str2.getBytes(), 0, str2.length(), "RC4");
        Cipher instance = Cipher.getInstance("RC4");
        instance.init(1, secretKeySpec);
        return instance.doFinal(str.getBytes());
    }
}
```


cipher:mg6CITV6GEaFDTYnObFmENOAVjKcQmGncF90WhqvCFyhhsyqq1s=
key:carol

在线RC4即可得到flag



hgame{weLC0ME_To-tHE_WORLD_oF-AnDr0|D}

easyasm

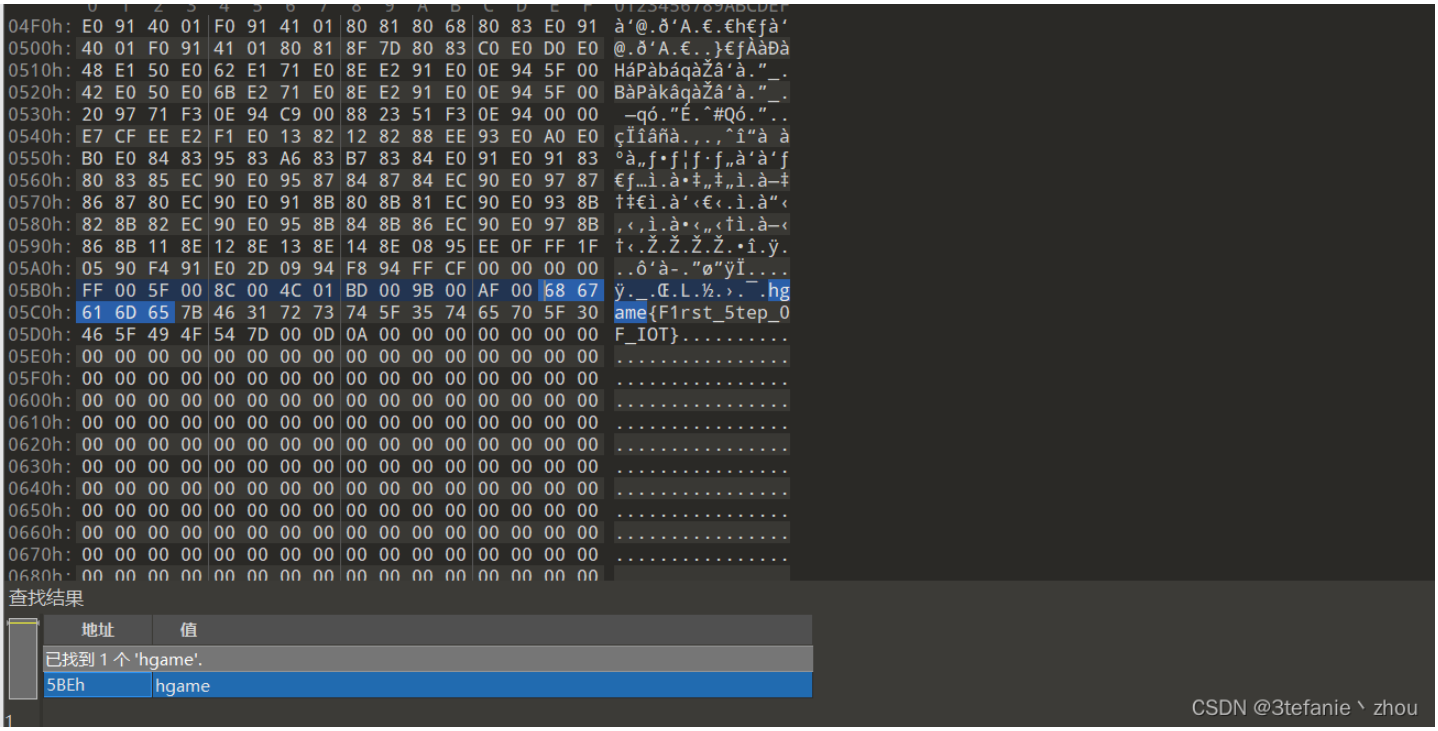
```python
#coding:utf-8
import string
es=[0x91, 0x61, 0x01, 0xC1, 0x41, 0xA0, 0x60, 0x41, 0xD1, 0x21, 0x14, 0xC1, 0x41, 0xE2, 0x50, 0xE1, 0xE2, 0x54,
0x20, 0xC1, 0xE2, 0x60, 0x14, 0x30, 0xD1, 0x51, 0xC0, 0x17]
ds = 'hgame{Fill_in_your_flag}'
si = 0x1c
dict = string.printable
flag = ''
es_re_1 = []
for i in es:
    es_re_1.append(i^0x17)
k = 0
for i in range(si):
    for j in range(len(dict)):
        ax = (ord(dict[j])<<4)&0xffff
        bx = (ord(dict[j])>>4)&0xffff
        if (ax+bx)&0xffff&0xff == es_re_1[i]:
            flag +=dict[j]
print(flag)
```

```
hgame{welc0me_to_4sm_w0rld}
```

Lot

饭卡的uno

丢到16进制文本编辑器直接搜索hgame



【请不要把陌生人的些许善意，视为珍稀的瑰宝，却把身边亲近人的全部付出，当做天经地义的事情，对其视而不见。】