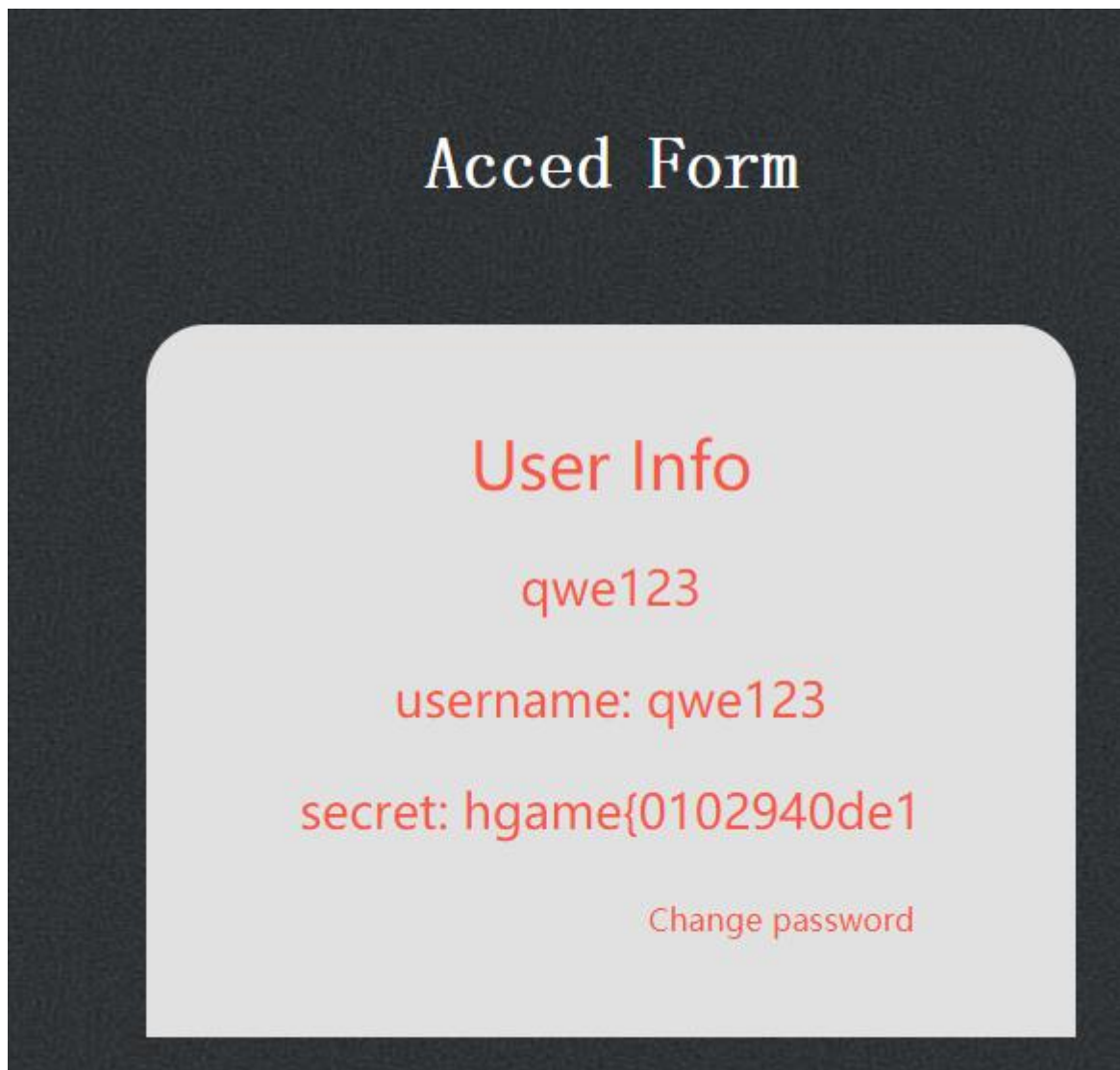


Web

散落的 flag

URL:<http://118.25.18.223:10099/login.php>

一开始，注册一个号，发现没有验证码，之后能在 f12 里发现验证码，填入，发现第一段 flag，



之后有一段时间发现找不到 Flag。。。然后仔细看提示。。。Admin 尝试修改 admin 的密码

请求主体:

`username=admin&password=lkjlkj`

将 username 更改为 admin，成功修改 admin 密码，登录，得到最后一段 Flag。。。

congratulation you get The last flag:`|98924acfce|`(竖线内的内容为最后一段flag)

之后发现找不到第二段。。。。再尝试，再 check\_user.php 里修改 username 成 admin 得到第二段 Flag



最后 Flag:hgame {0102940de110c546b2cf6898924acfce}

Misc

Ngc's wifi

URL:<http://p1kaloi2x.bkt.clouddn.com/hgame/cap/flag2.cap>

下载流量包，根据提示，潍坊，wifi，用 aircrack-ng 破解 wifi，

```
Reading packets, please wait...
Aircrack-ng 1.2 rc4

[00:04:39] 2069504/10421935 keys tested (7366.01 k/s)

Time left: 18 minutes, 53 seconds                                19.86%

KEY FOUND! [ 13375369512 ]

Master Key      : 9B 5C 3B 5B 3F 25 69 62 69 B5 BA 68 33 46 ED 67
                  FA F0 OD 16 9A B4 76 E4 A2 BB 11 B8 ED 68 77 E2

Transient Key   : 70 91 68 49 97 2C 1B 3D A9 FE 1C CF CC 6C 35 E8
                  FB 81 40 A0 10 5D 17 E7 D8 FC AF 21 B7 43 76 78
                  2C 3A D5 CB B4 27 81 C0 C8 61 D3 18 40 A7 D4 96
                  D5 85 76 05 F0 32 31 51 DD 3B 9D A6 2E 96 35 06

EAPOL HMAC     : B1 83 7E F7 06 7B 37 98 34 B6 3B 45 FC F2 D8 9D

C:\Users\77699\Desktop\aircrack-ng-1.2-rc4-win\bin\64bit>
```

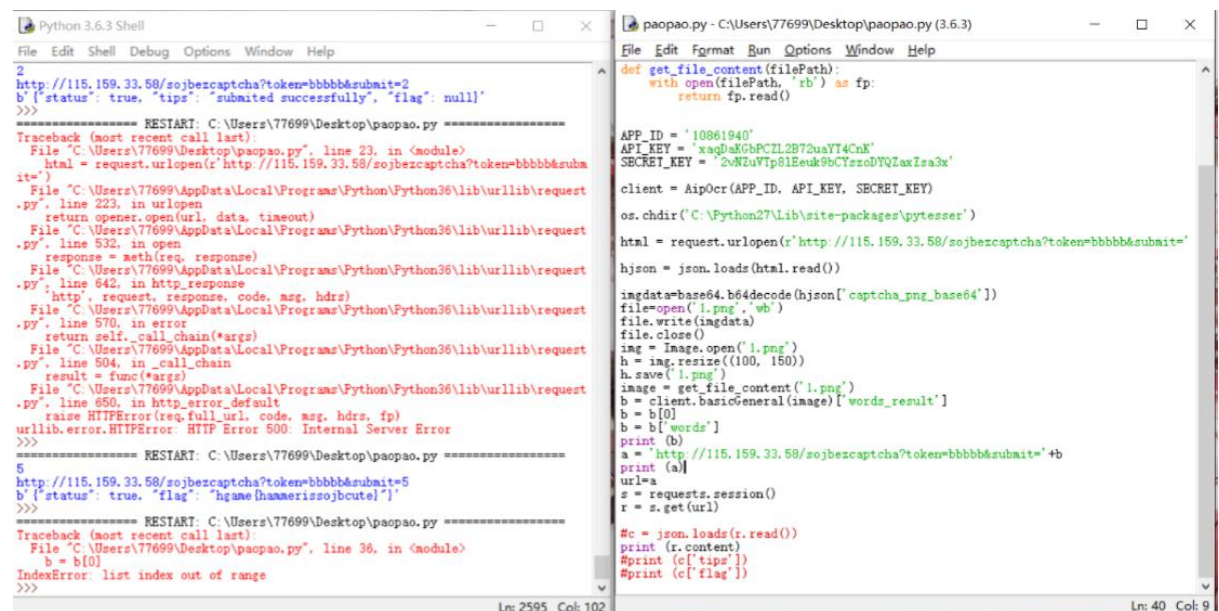
确认 flag

Flag:hgame{13375369512}

So jb ez captcha

URL:<http://115.159.33.58/sojbezcaptcha>

按照提示一步一步来。。。 (为什么我的 tesseract 怎么执着。。。只识别成英文，最后换成百度的文字识别。。。。)



```
Python 3.6.3 Shell
File Edit Shell Debug Options Window Help
2
http://115.159.33.58/sojbezcaptcha?token=bbbb&submit=2
b'{"status": true, "tips": "submitted successfully", "flag": null}'
>>>
===== RESTART: C:\Users\77699\Desktop\paopao.py =====
Traceback (most recent call last):
  File "C:\Users\77699\Desktop\paopao.py", line 23, in <module>
    html = request.urlopen(r'http://115.159.33.58/sojbezcaptcha?token=bbbb&submit=2')
  File "C:\Users\77699\AppData\Local\Programs\Python\Python36\lib\urllib\request.py", line 223, in urlopen
    return opener.open(url, data, timeout)
  File "C:\Users\77699\AppData\Local\Programs\Python\Python36\lib\urllib\request.py", line 532, in open
    response = meth(req, response)
  File "C:\Users\77699\AppData\Local\Programs\Python\Python36\lib\urllib\request.py", line 642, in http_response
    http.request, response, code, msg, hdrs)
  File "C:\Users\77699\AppData\Local\Programs\Python\Python36\lib\urllib\request.py", line 570, in error
    return self._call_chain(*args)
  File "C:\Users\77699\AppData\Local\Programs\Python\Python36\lib\urllib\request.py", line 504, in _call_chain
    result = func(*args)
  File "C:\Users\77699\AppData\Local\Programs\Python\Python36\lib\urllib\request.py", line 650, in http_error_default
    raise HTTPError(req.full_url, code, msg, hdrs, fp)
urllib.error.HTTPError: HTTP Error 500: Internal Server Error
>>>
===== RESTART: C:\Users\77699\Desktop\paopao.py =====
5
http://115.159.33.58/sojbezcaptcha?token=bbbb&submit=5
b'{"status": true, "flag": "hgame{hammerissojbcute}"}'
>>>
===== RESTART: C:\Users\77699\Desktop\paopao.py =====
Traceback (most recent call last):
  File "C:\Users\77699\Desktop\paopao.py", line 36, in <module>
    b = b[0]
IndexError: list index out of range
>>>
```

```
paopao.py - C:\Users\77699\Desktop\paopao.py (3.6.3)
File Edit Format Run Options Window Help
def get_file_content(filePath):
    with open(filePath, 'rb') as fp:
        return fp.read()

APP_ID = '10861940'
API_KEY = 'xagDaGhPCIL2872uaYT4CnK'
SECRET_KEY = '2vNzuVtp81Eeuk9bCYzso0YQZaxIa3x'
client = AipOcr(APP_ID, API_KEY, SECRET_KEY)
os.chdir('C:\Python27\Lib\site-packages\pytesseract')

html = request.urlopen(r'http://115.159.33.58/sojbezcaptcha?token=bbbb&submit=')
hjson = json.loads(html.read())

imgdata=base64.b64decode(hjson['captcha_png_base64'])
file=open('1.png','wb')
file.write(imgdata)
file.close()
img = Image.open('1.png')
h = img.resize((100, 150))
h.save('1.png')
image = get_file_content('1.png')
b = client.basicGeneral(image)['words_result']
b = b[0]
b = b['words']
print(b)
a = 'http://115.159.33.58/sojbezcaptcha?token=bbbb&submit='+b
print(a)
url=a
s = requests.session()
r = s.get(url)

#c = json.loads(r.read())
print(r.content)
#print(c['tips'])
#print(c['flag'])
```

Flag:hgame{hammerissojbcute}

猿宵快乐:娱乐猜灯谜送分

会长的名称

Flag:hgame{processor}

Crypto

ezECC

URL:<http://p3xlhyup6.bkt.clouddn.com/ecc>

没搞清算法。。。但找到了工具。。。 Ecctool

Rx[Pub]	513848964032483
Ry[Pub]	886359250407321

然后得到 Flag:hgame{1400208214439804}