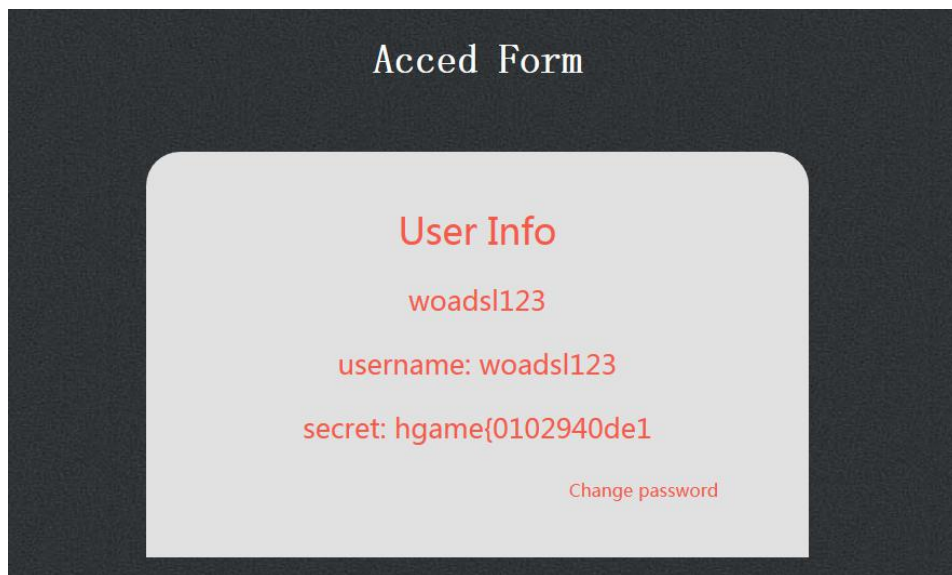


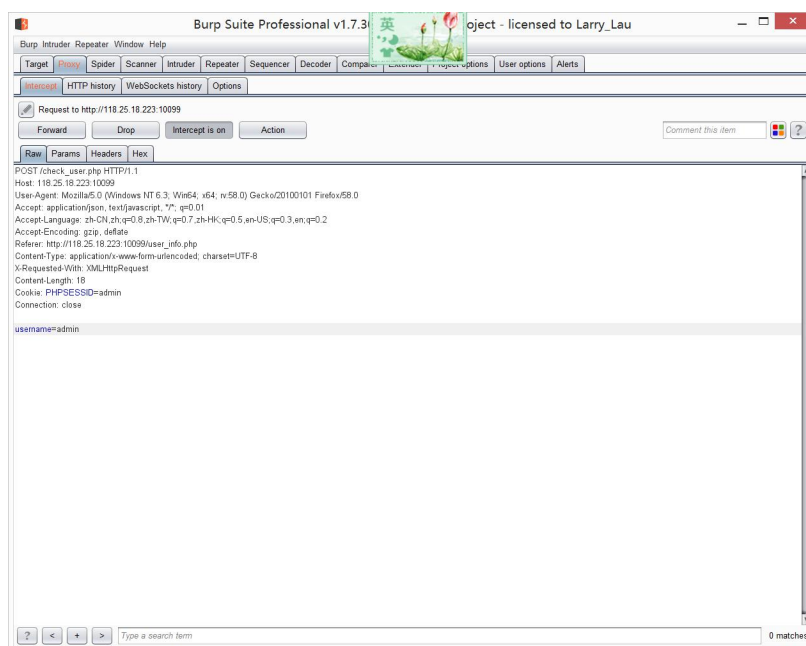
## Web

### 散落的 flag

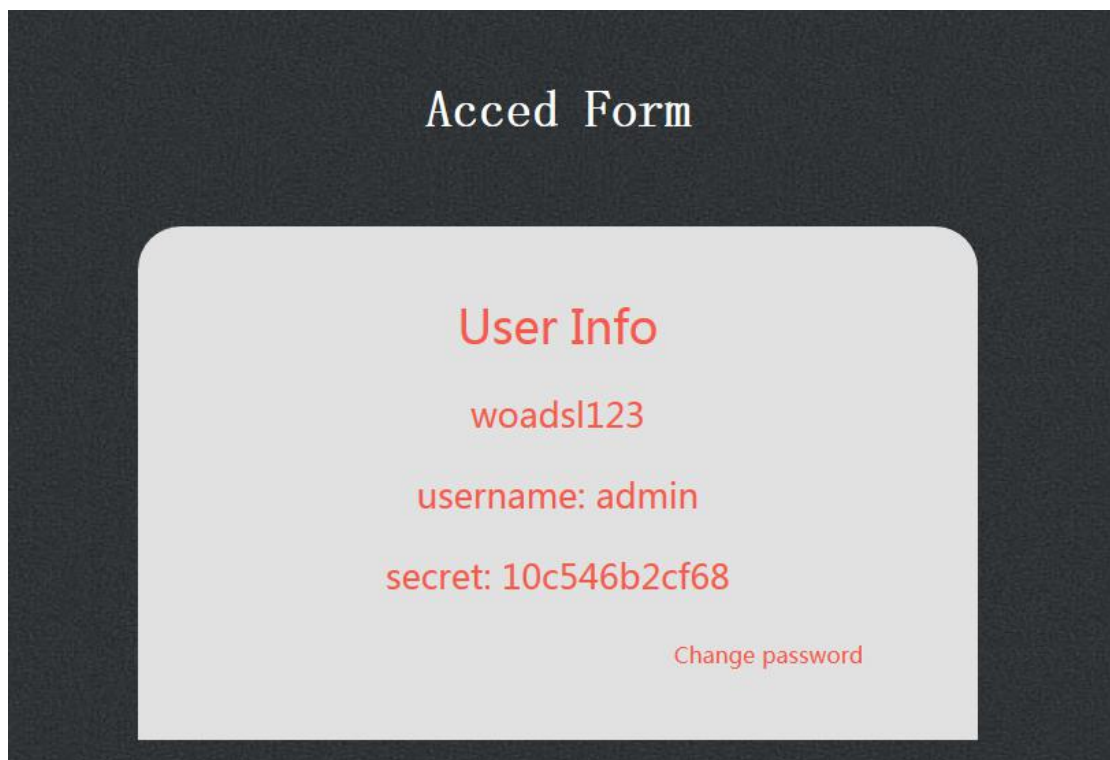
一开始做的时候真的没头脑=。=只能做出第一个三分之一部分



后来给了 hint 说有两个在 admin 下面，我打开 burpsuite 发现有个 cookie 字样就改了一下在这里将



post 请求的名字换成 admin 就可以看到 admin 的了，



那么最后一个呢我觉得应该是登录 admin 的账号密码，既然有 change password 就应是将 admin 的账号密码改了之后再登录了，我发现了主要是要用 burpsuite 把所有不是 admin 都改成 admin。。。。



## Misc

### Ngc's wifi

这道题一开始的 url 真的是坑了我=。=

使命分析发现就一个 ngc's wifi 然鹅没有握手包，这怎么破密码真的找不到。然后我想看有几个人过得时候发现又多了一个新的打开来之后，原谅我的 iso 文件被我删了，kali 坏掉了，用了木头字典，山东潍坊的电话号码，直接生成字典。然后用 aircrack-ng 就可以破解密码了，大概是 aircrack-ng -e [字典] [流量文件] 直接这样会让你选一个，找到一个 ngc's wifi 就可以了，我大概跑到 13% 就破解了 =。= 我记得是 133 开头的 =。=



So jbecaptcha

一开始我真的找不到哪里有验证码，他需要用 get 还要加上 token，那么就只要将网址加上 token=几就行了，然后会出来 base64 加密的一段文字，解密之后会发现 IHDR，然后用 python 写个脚本发现是

个数字，就是需要 token=1&submit=那个数字，我就直接使用百度的 api 来解决这道题了，之前我使用 tesseract-ocr 的时候一直显示没有图片我也不知道是因为图片太小了还是什么的，就想起那时候用文字识别的时候看到过百度的 api 接口，就用上了，大概是要连续三次成功吧=。=一脸懵逼，然后就拿到了 flag

```
{
  "flag": null,
  "tips": "wrong answer",
  "status": false
},
{
  "log_id": 2874516979225630092,
  "words_result_num": 1,
  "words_result": [{"words": "2"}]
},
http://115.159.33.58/soibezcaptcha?token=1&submit=2
{
  "status": true,
  "tips": "submitted successfully",
  "flag": null
},
{
  "log_id": 2844081169414740900,
  "words_result_num": 1,
  "words_result": [{"words": "7"}]
},
http://115.159.33.58/soibezcaptcha?token=1&submit=7
{
  "status": true,
  "tips": "submitted successfully",
  "flag": null
},
{
  "log_id": 608442330131903497,
  "words_result_num": 1,
  "words_result": [{"words": "5"}]
},
http://115.159.33.58/soibezcaptcha?token=1&submit=5
{
  "status": true,
  "flag": "hgame(hammerissojbcute)"
},
{
  "log_id": 5100476040270729102,
  "words_result_num": 1,
  "words_result": [{"words": "5"}]
}
```

Crypto

ezECC

Ecc 椭圆加密

这道题我看了网上的教程真的是似懂非懂，然后去翻了一下看雪的密码学的软件有两个 <https://tools.pediy.com/windows/cryptography.htm>

DSAToolV13		DSA算法辅助工具
ECC算法		
ECCTool v1.04	readyu	椭圆曲线密码学工具 ECCTool v1.04 [update 20080901]
Elliptic Curve Builder	Marcel Martin	椭圆曲线算法生成器
IDA的加密特征库		

下载了一个下来，主要是第一个 ECCTool v1.04

打开来

ECCTOOL v1.04

**General Settings**

CurveBits: 64 ThreadPriority: Normal/8 ecm\_n: 50 Cost: 0s 203ms  
 NumberBase: 10 Seed Padding: Type any chars here ecm\_k: 101 CPU: 02773:736f9280  
 RNG Salt: Pau Type: CE361D0667E597A8B6AAC14221DDF65EB5882C2C3C4CDDFB51B1D18D6312DCA4B

CurveType: GF(P)

Curve over GF(P)  $Y^2 = X^3 + A \cdot X + B \pmod{P}$  CLEAR ECC

<input type="checkbox"/> S160/L	1338103827070457522061368408972759476317570084916	160
<input type="checkbox"/> Hash/H	4236684983161257254	62
NP	18210200700161031311	64
A/a2	499590297305427	49
B/a6	30115568120981	45
<input type="checkbox"/> p	1026347883361447	50

GENERATE GET NP GET ORD GET AB FACTOR NP

Kangaroo k\*G=R SAVE CFG LOAD CFG CLEAR KEY

KeyPairs

Q[Order]	0	0
k[Priv]	622849	20
Gx[Base]	817367249716330	50
Gy[Base]	483834901818242	49
Rx[Pub]	513848964032483	49
Ry[Pub]	886359250407321	50

CHK ORDER TEST RAND G NEW K NEW G CALC R L\*G+H\*R CHK Gy CHK Ry PAUSE STOP

Done Pub:  $R(x,y) = k * G(x,y)$ . ABOUT EXIT

把所有的数据输进去按一下 **CALC R** 就有公钥出来了，加起来的值就是 flag: hgame{Rx+Ry}