Web

散落的 flag

先注册，点获取验证码后

```
POST /get_phone_num.php HTTP/1.1
Host: 118.25.18.223:10099
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://118.25.18.223:10099/register.php
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 17
Cookie: PHPSESSID=efd278a1a5d5152299bf7f4ddf8cfac9
Connection: close

phone=13318451598
```

在 response 里得到验证码

```
POST /check_user.php HTTP/1.1
Host: 118.25.18.223:10099
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://118.25.18.223:10099/user_info.php
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 14
Cookie: PHPSESSID=efd278a1a5d5152299bf7f4ddf8cfac9
Connection: close

username=adooo
```

```
HTTP/1.1 200 OK
```

Server: nginx/1.7.7
Date: Mon, 26 Feb 2018 13:13:23 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.0.0
Content-Length: 28

["adooo","hgame{0102940de1"]

把 username 改成 admin 得到中间那段 flag

再修改密码的时候再把 username 改成 admin，然后登陆 admin 用户得到最后一段 flag

hgame{0102940de110c546b2cf6898924acfce}

密码学

ezECC

网上脚本拿来改一点点

```
a = 499590297305427
b = 30115568120981
M = 1026347883361447

def add(A,B):
    if A==(0,0): return B
    if B==(0,0): return A
    x1,y1 = A
    x2,y2 = B
    if A!=B:
```

```
            p = (y2-y1)*pow(x2-x1,M-2,M)
        else:
            p = (3*x1*x1+a)*pow(2*y1,M-2,M)
        x3 = p*p-x1-x2
        y3 = p*(x1-x3)-y1
        return (x3%M,y3%M)


base = (817367249716330, 483834901818242)

X = (0,0)

for i in range(M):
        if i==622849:
            break
        X = add(X, base)
print(X)
```