Hgame Week4 Write Up

——Li4n0

1.Web部分：

1.散落的flag：

先注册，发现需要接受手机验证码，F12，在响应里发现验证码，注册成功后，在自己的主页发现第一段 flag 。

然后推测第二段、第三段验证码应该跟其余的功能有关系，于是尝试修改密码，将表单里的 User Id 改成 admin 试一试，成功修改了 admin 的密码，登录后发现了最后一段flag。

那么第二段 flag 在哪里呢。。ლ('◉◗◉ ` ლ)....于是再次登录自己的账号，发现登陆后还有一个 check id 的操作，那么将自己的 id 也改成 admin ，重新发送。在响应里面拿到第二段 flag 。

2.Misc部分：

1.ngc‘s wifi：

找了个工具，生成潍坊的手机号字典，把握手包拿去 aircrack-ng 就能跑出来了

2.sojbeasycaptcha：

emm之前一直没明白这个迷之 timeout 是咋回事（其实现在也不明白

感谢豪神不厌其烦的跟我解释。。。。

按照题目要求 Get 一个 token 过去，发现 base64 编码后的图片验证码（ps：最开始只有10种base64，只需要自己人工分辨，然后做成字典，就能轻松的识别了。。。不过在我弄懂timeout之前这个被修复了。。）

那么尝试其他方法，大致的思路是，因为这个验证码只有黑白两种颜色，而且没有任何干扰，所以可以尝试通过rgb值来区分不同数字。上脚本:

1. 获取不同图片的 rgb 特征并生成字典（需要先集齐 0-9 的图片并且人工识别好）

```
def get_feature():
    dic = {}
    for root, dir, files in os.walk('code/'):
        for filename in files:
            img = PIL.Image.open('code/%s' % filename)
            black = 0
            for x in range(img.size[0]):
                for y in range(img.size[1]):
                    for i in img.getpixel((x, y)):
                        if i < 255:
                            black += 1
            dic[black] = filename[:-4]      #filename形如 1.jpg
```

```
    print(dic)
```

于是得到了一个这样的字典：

```
dic = {180: '0', 90: '1', 150: '2', 162: '3', 153: '4', 156: '5', 198: '6', 105: '7', 204: '8',
195: '9'}
```

2. get flag：

```
def get_image():
    status_code = 500

    while status_code != 200:
        c = request.get(url)
        status_code = c.status_code
        try:
            code = json.loads(str(c.content)[2:-1])["captcha_png_base64"]
            with open('code.png', 'wb')as file:
                file.write(base64.b64decode(code))
        except:
            print(status_code)
            pass


def get_flag():
    dic = {180: '0', 90: '1', 150: '2', 162: '3', 153: '4', 156: '5', 198: '6', 105: '7',
204: '8', 195: '9'}
    img = PIL.Image.open('code.png')
    black = 0
    for x in range(img.size[0]):
        for y in range(img.size[1]):
            for i in img.getpixel((x, y)):
                if i < 255:
                    black += 1

    status_code = 500           #解决随机 500 的影响...
    while status_code != 200:
        try:
            print(dic[black])
            b = request.get(url+'&submit=%s'%dic[black])
            status_code = b.status_code
        except:
            b = request.get(url + '&submit=1')
            status_code = b.status_code
    print(b.content.decode('utf-8'))




 while i < 20:      #这里设置多少都没关系，看到flag就手动停止就好
```

```
    get_image()
    get_flag()
    i += 1
```

然后就能get flag了

Ps：

训练赛结束了，感谢学长们在这个寒假给我们提供这么好的学习的机会！回顾一下这四周，学到了很多新知识（虽然自己还是这么菜……），接下来就是继续学习。。希望正式赛能多做出几道题吧。。