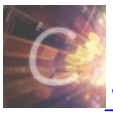
flag就在flag.php中

原创

Peithon 于 2018-05-13 19:20:26 发布 33530 收藏 19

分类专栏： Web 文章标签： CTF writeup flag在flag.php中 远程图片上传

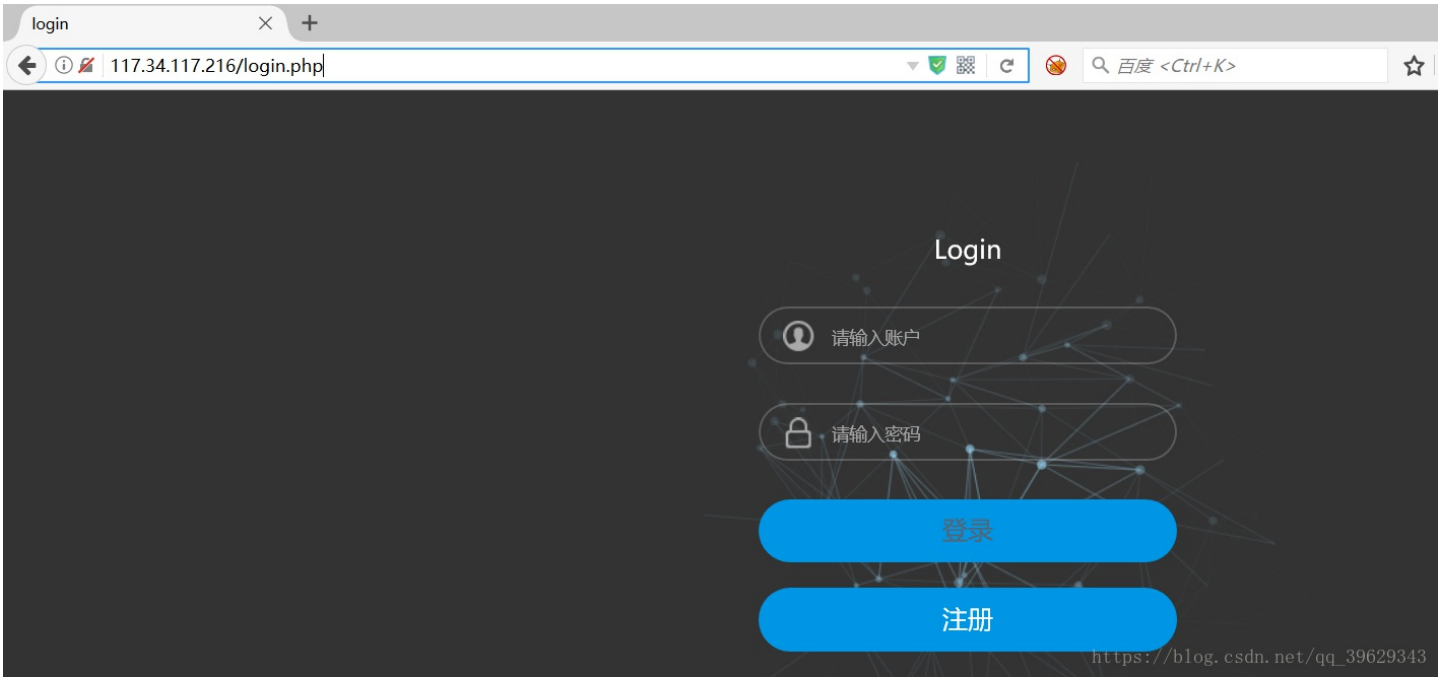
本文链接：https://blog.csdn.net/qq_39629343/article/details/80301831



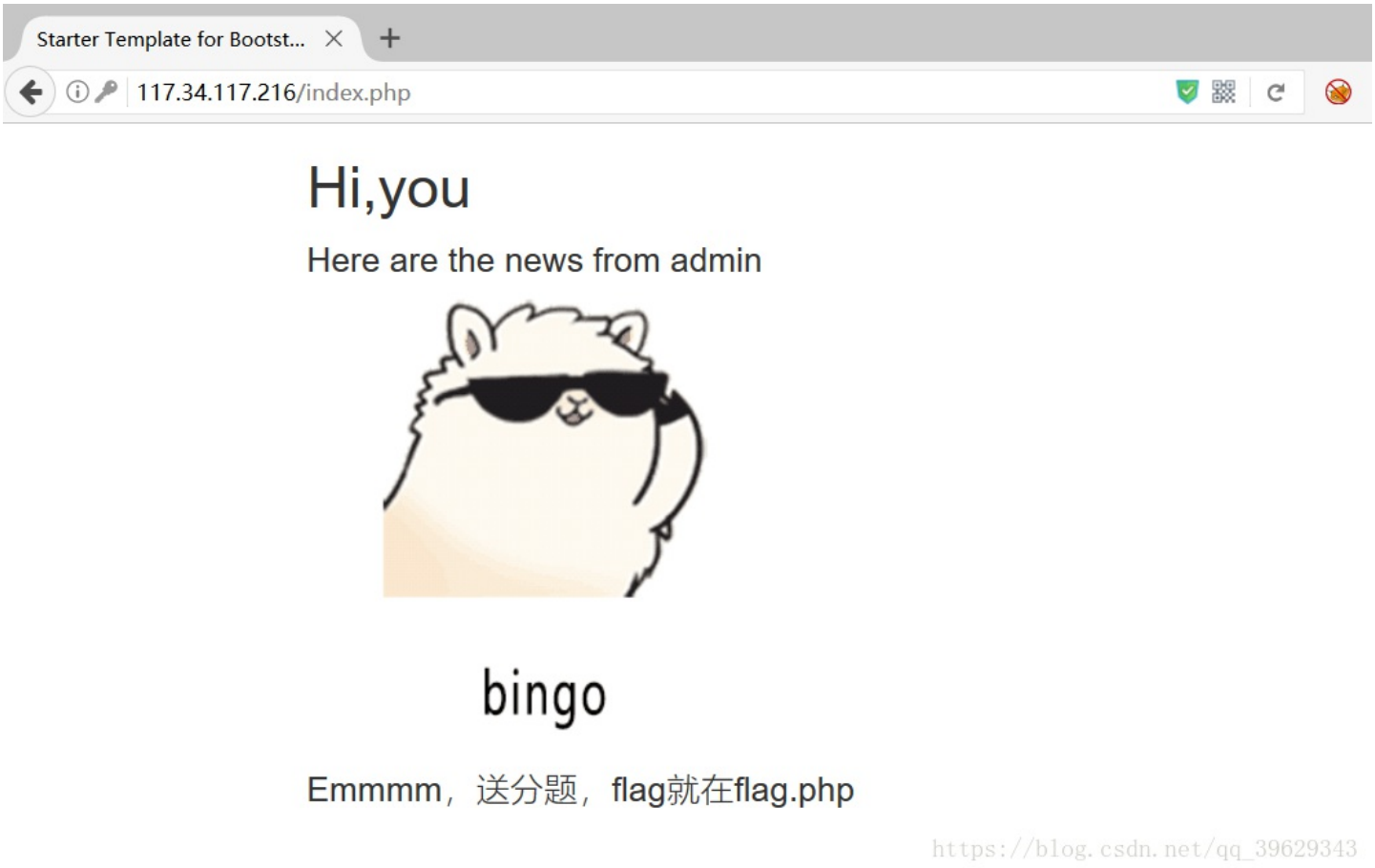
Web1

题目地址

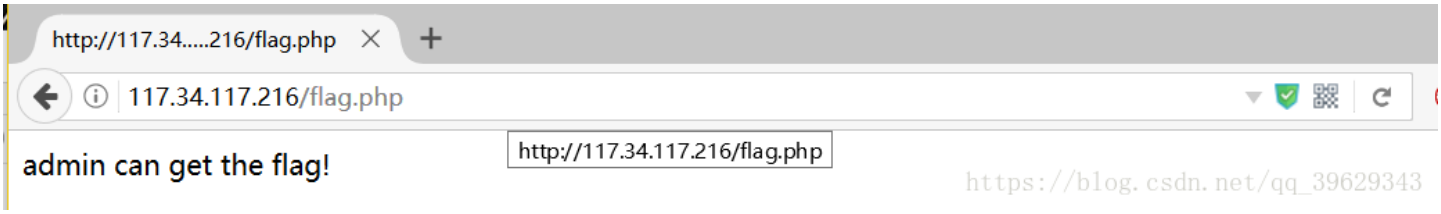
1.访问题目存在一个登录界面



2.注册一个用户登录，然后会跳转到另一个界面，会给出一些提示

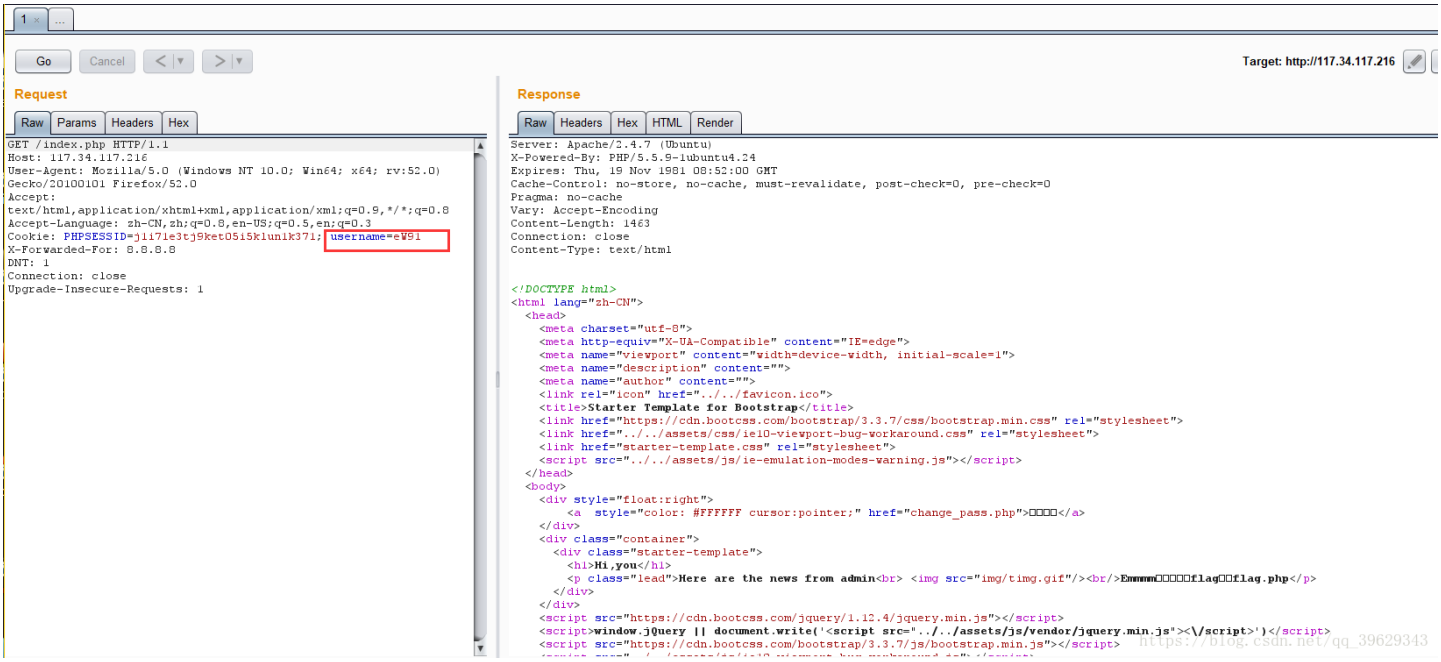


3.访问flag.php,试试可不可以得到flag

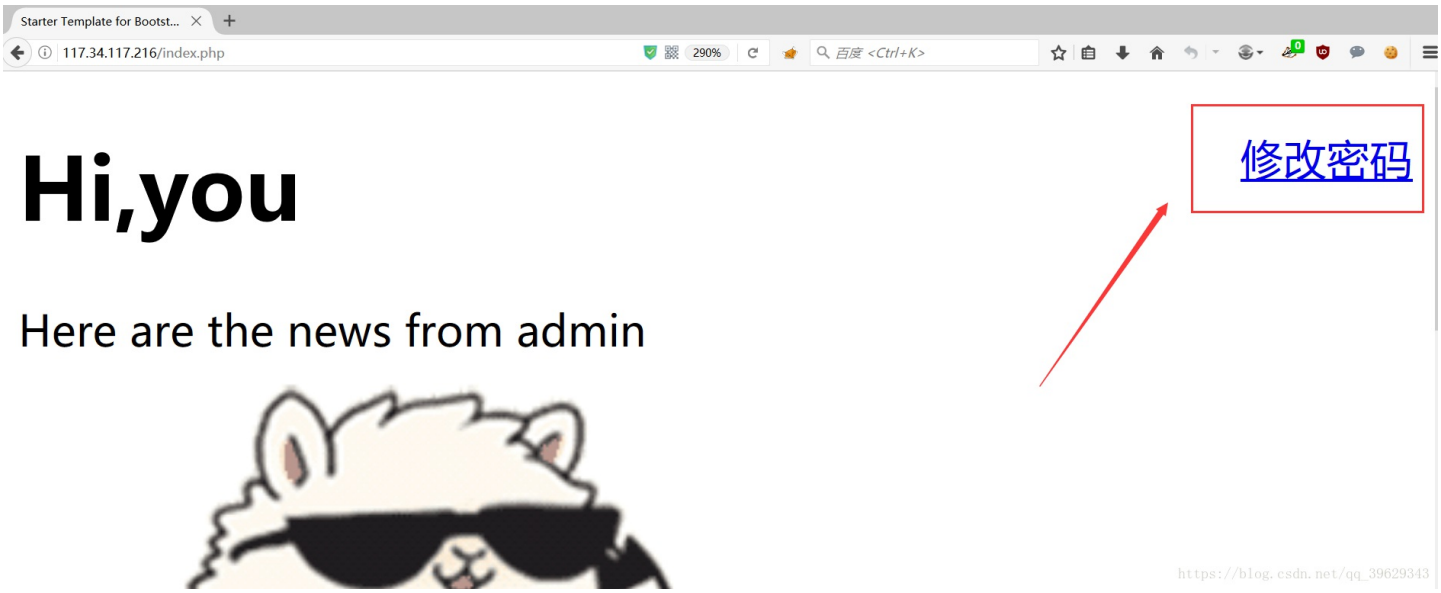


提示admin可以得到flag,然后跳转回登录界面,猜测这和Cookie是有关的

4.抓包



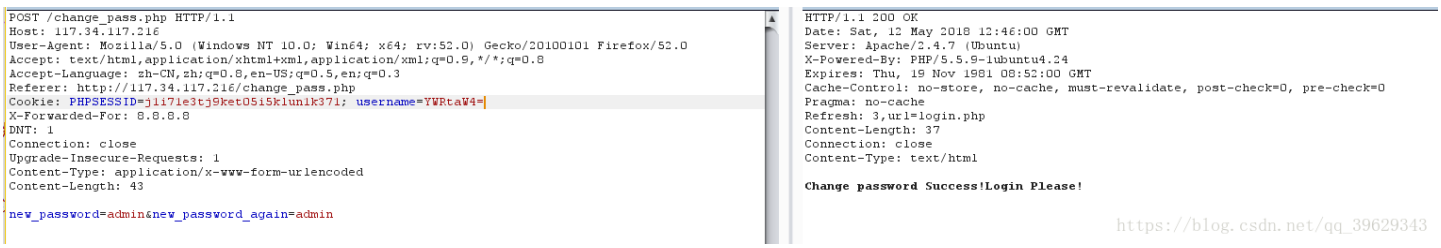
发现在`Cookie`里有`username`，而且每一个用户的username是不一样的，后面的值是base64加密之后的



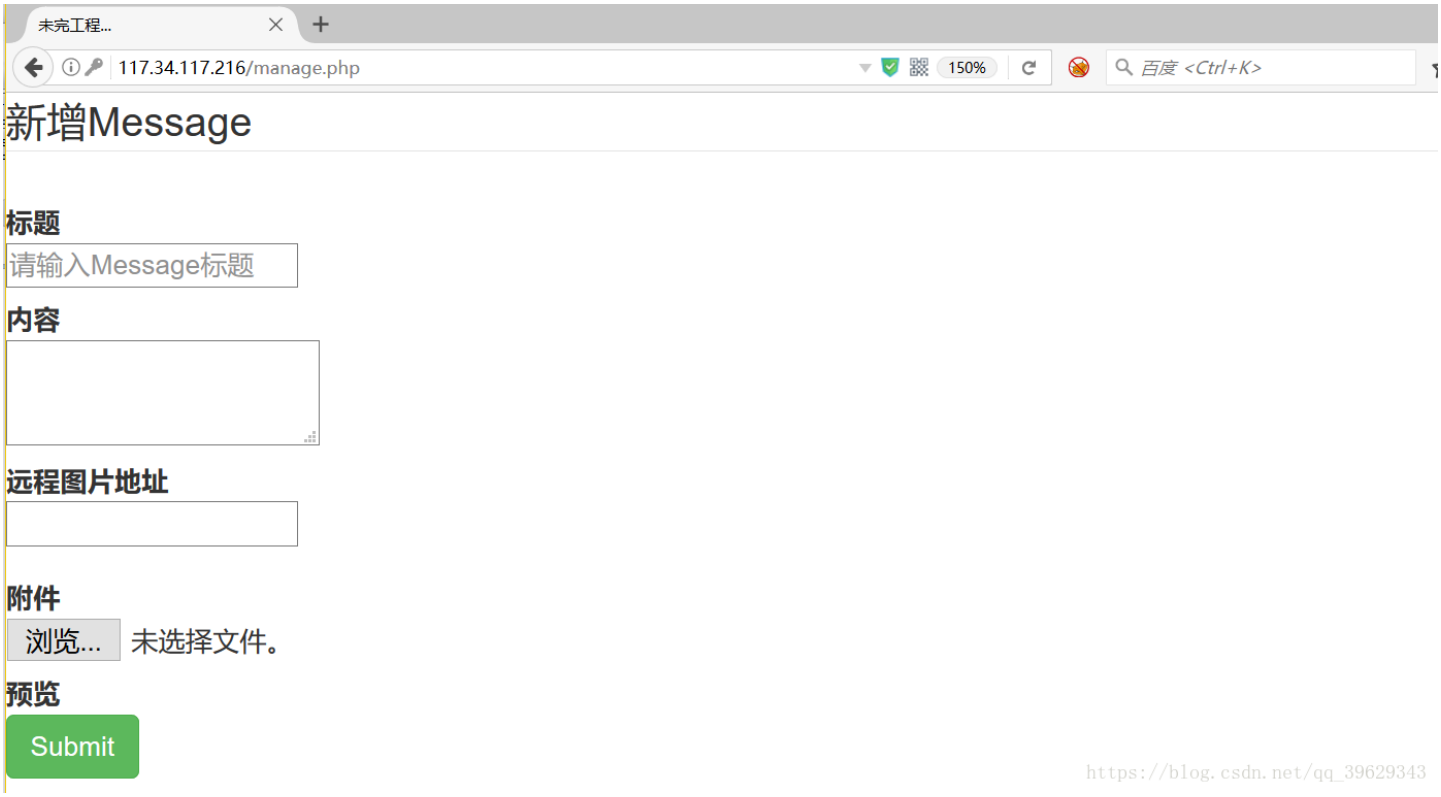
在登录成功跳转的那个页面还有一个修改密码的功能，就是说我们可以把amdin的密码修改了，然后以admin的身份进行登录

5.改包

首先得到`admin`经过base64加密的值`YWRtaW4=`,然后在burpsuite上进行改包



修改成功之后以amdin的身份登陆

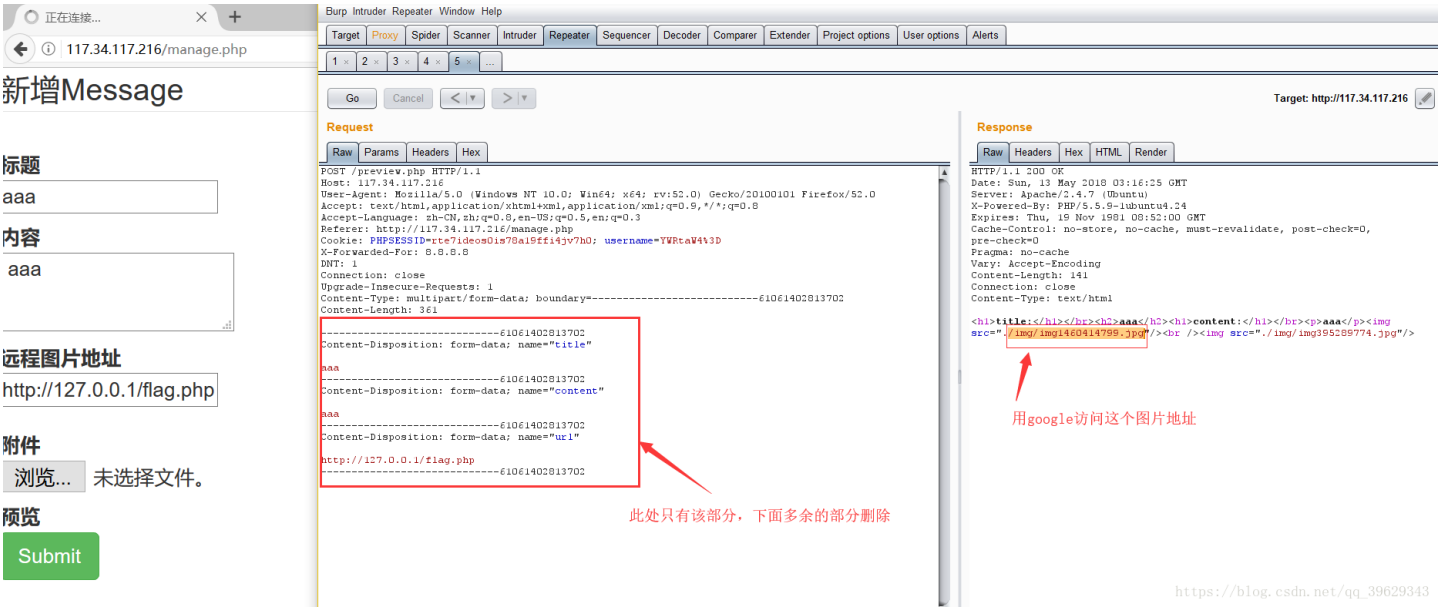


在这一步刚开始以为是使用%00截断,然后用菜刀连接得到flag，结果发现不是这样

经过多种尝试，得到正确的get flag的姿势

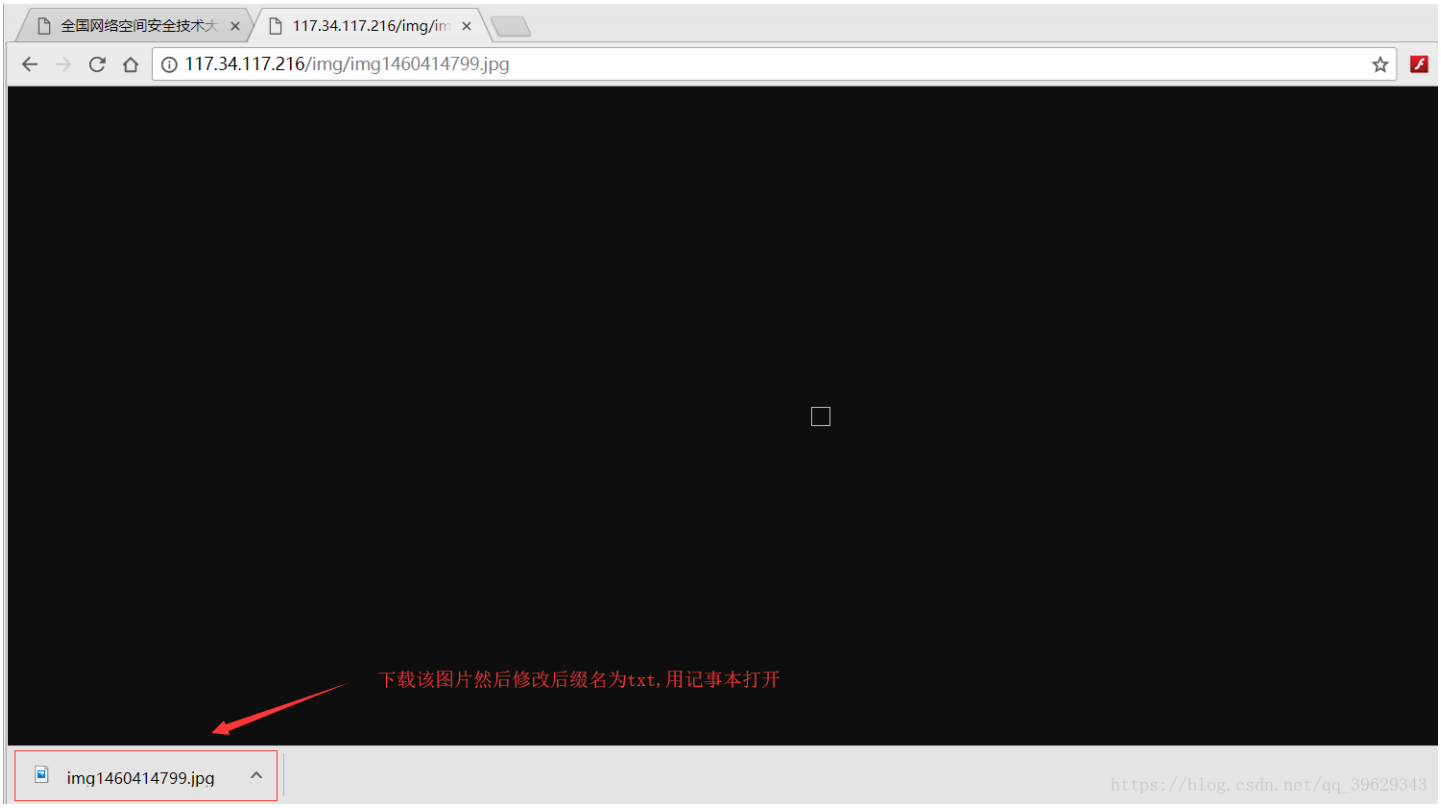
6.本地包含flag.php文件

之前提示说flag在flag.php，现在是使用admin身份登陆，而且这里有远程图片地址，那么这里就应该是要在本地包含flag.php



原本抓包会有附件这一行的信息，删除掉,点击 go 就会出现两个图片地址。访问第一个

7.使用google访问图片地址



在这里是看不到flag的，先把图片下载到本地

8.修改后缀得到flag

因为使用图片格式打不开，所以修改后缀为txt试试，就得到了flag