攻防世界-web-bug-从0到1的解题历程writeup

原创

CTF小白 于 2020-04-15 14:25:33 发布 1984 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_41429081/article/details/105534291

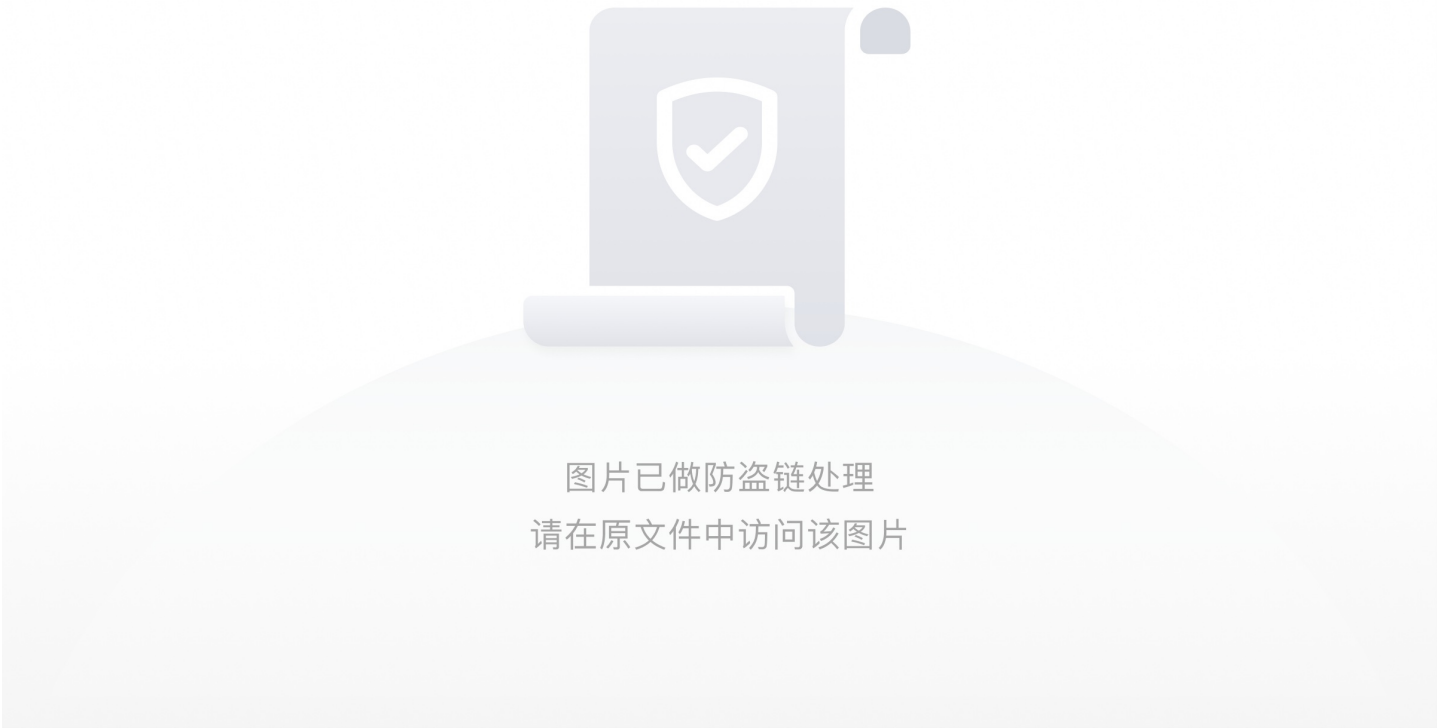
题目分析

拿到题目首先注册了一下admin账号发现账号存在。然后后登陆后发现Manage需要admin权限，那么大概就是要获取到admin账号或者admin权限了。

尝试了一下发现

先输入自己注册的正确账号令其跳转到修改密码界面，然后修改username直接找回admin的密码即可

成功登陆admin账号



发现进入admin模块提示IP NOT allowed。

尝试修改IP添加请求头X-Forwarded-For: 127.0.0.1

得到提示 `<!-- index.php?module=filemanage&do=???-->`

u1s1这个do后面猜一个我是真的没有猜到，找了一下wp才知道，原来是do=upload，根据前面的filemanege猜出的。。。。。

发现是一个上传页面，估计就是上传图片马了。

随意上传了一下发现并不会给上传后的路径。。看了下wp才知道。。咋都是脑洞，只要成功上传了一个php文件似乎就给flag了。。

找了以前的一个图片马，修改后缀为php4或者php5都可以得到flag

图片已做防盗链处理
请在原文件中访问该图片