




# 攻防世界 web 进阶 bug

原创

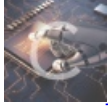
[\\_Christo](#)  于 2019-08-08 00:31:40 发布  1898  收藏 2

分类专栏: [ctf](#) 文章标签: [xctf web 攻防世界 bug](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_42499640/article/details/98793342](https://blog.csdn.net/weixin_42499640/article/details/98793342)

版权



[ctf 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

打开题目

注册一个账号

登陆上去

点击 manage 选项卡

提示不是 admin 进不去

那就不用 admin 进

点击找回密码

输入刚刚注册的账号信息

进入修改密码页面

设置代理

打开 burpsuite

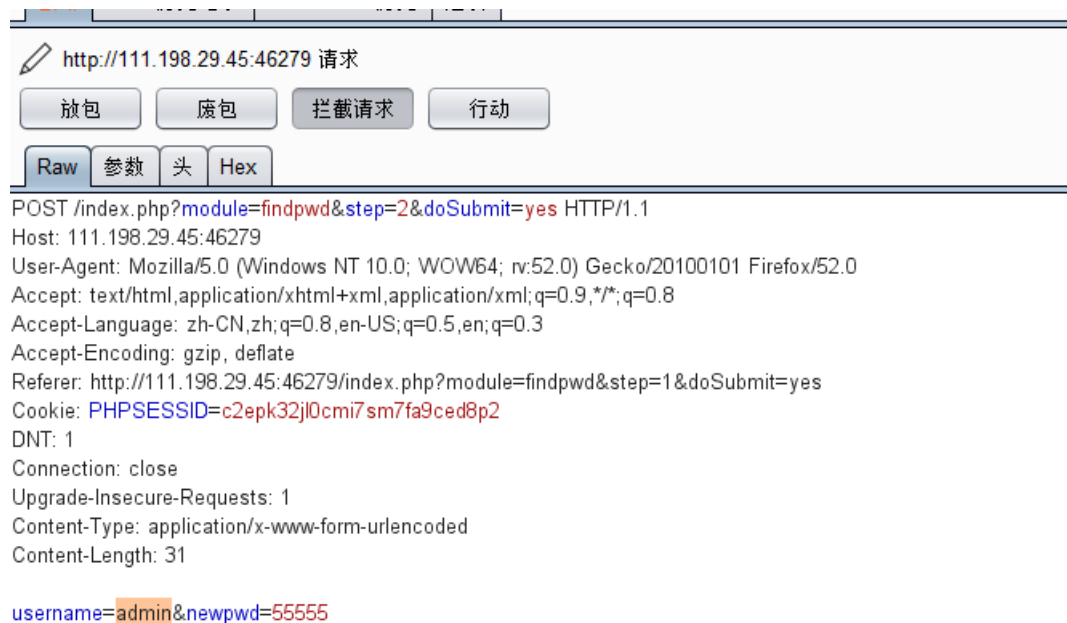
点击拦截

页面里设置新密码

提交

bp拦截到包

username参数修改成admin



http://111.198.29.45:46279 请求

发包 废包 拦截请求 行动

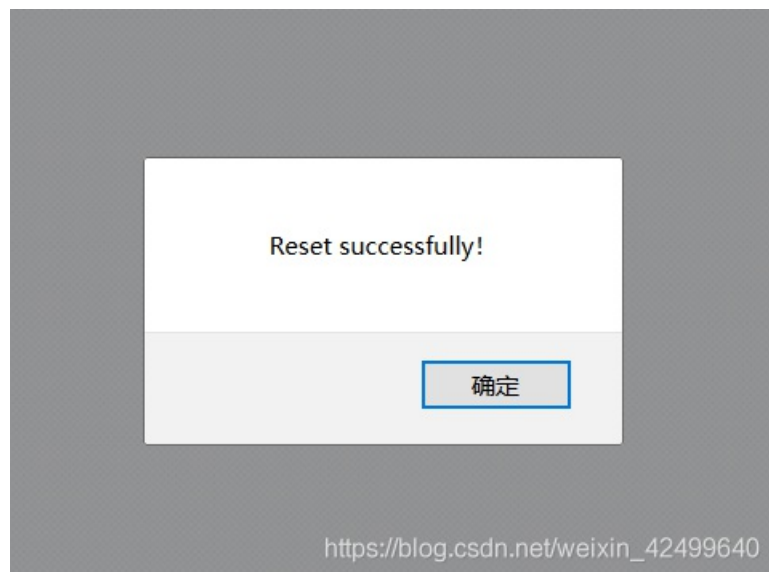
Raw 参数 头 Hex

```
POST /index.php?module=findpwd&step=2&doSubmit=yes HTTP/1.1
Host: 111.198.29.45:46279
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://111.198.29.45:46279/index.php?module=findpwd&step=1&doSubmit=yes
Cookie: PHPSESSID=c2epk32jl0cmi7sm7fa9ced8p2
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 31

username=admin&newpwd=55555
```

[https://blog.csdn.net/weixin\\_42499640](https://blog.csdn.net/weixin_42499640)

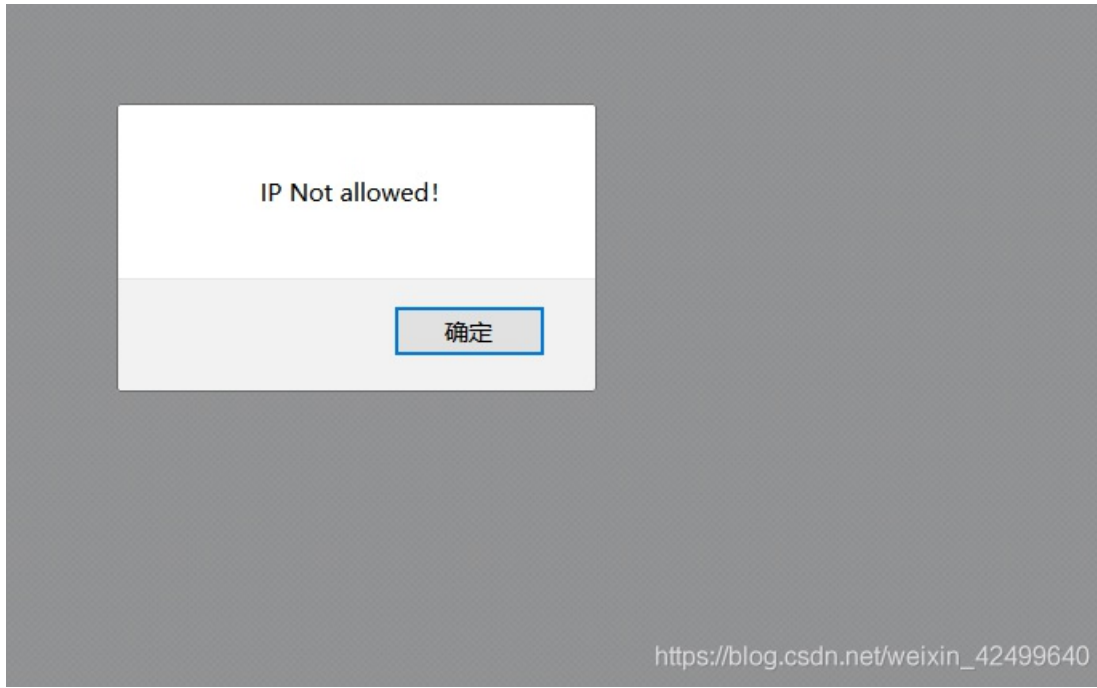
发包



修改成功

现在admin账户的密码被修改为我们自己设置的密码

使用admin帐户登陆



但ip不对

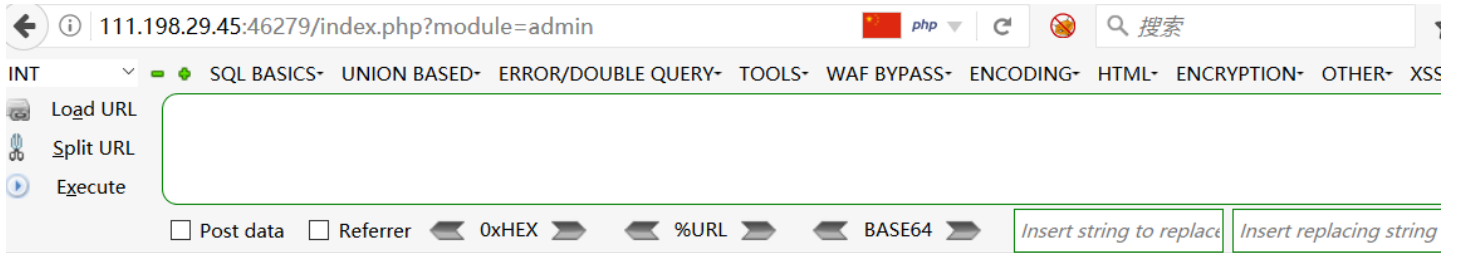
简单

那就变成本机访问

设置本机的ip 127.0.0.1

接着用bp抓包

头部加入参数X-Forwarded-For: 127.0.0.1



Where Is The Flag?

⋮ )

[https://blog.csdn.net/weixin\\_42499640](https://blog.csdn.net/weixin_42499640)

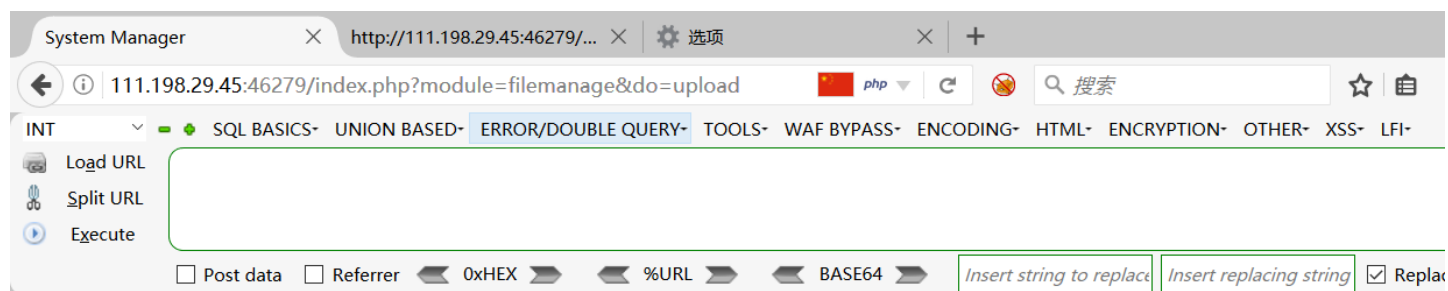
ok进来了

查看网页源码

可以看到有个提示

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

看到filemanage, 怕不是个文件上传  
do理所当然的猜测upload  
试试看



Just image?



浏览... 未选择文件。

upload

[https://blog.csdn.net/weixin\\_42499640](https://blog.csdn.net/weixin_42499640)

Orz

尝试上传php文件



[https://blog.csdn.net/weixin\\_42499640](https://blog.csdn.net/weixin_42499640)

就知道肯定没这么简单  
但试试又不掉块肉

试了很多次发现文件名和MIME类型都进行了过滤

看wp发现是  
文件内容绕过  
自建txt文本写入

```
<script language='php'>随便</script>
```

改成图片格式上传

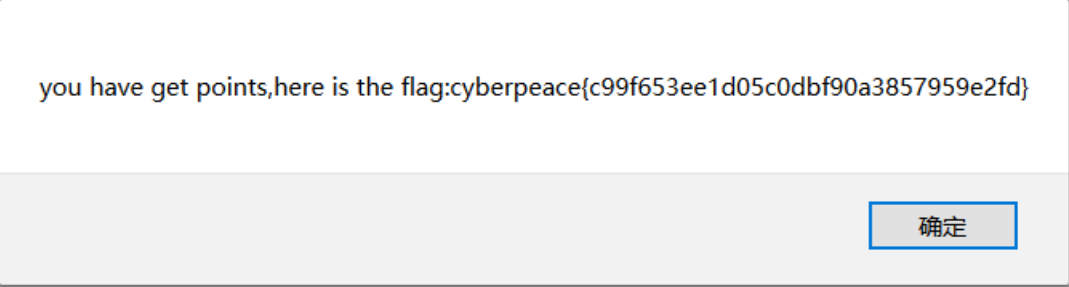
把包抓下来

修改文件后缀名为.php4或.php5

(这里表示不懂为什么是这俩其他的就不行，求师傅们教一下 Orz)

放包

得到flag



you have get points,here is the flag:cyberpeace{c99f653ee1d05c0dbf90a3857959e2fd}

确定

[https://blog.csdn.net/weixin\\_42499640](https://blog.csdn.net/weixin_42499640)