百度杯CTF比赛 九月场——123

原创

夏日 の blog 于 2020-03-20 14:26:03 发布 904 收藏

分类专栏： CTF-WEB

本文链接：https://blog.csdn.net/zss192/article/details/104988778

目录

题目描述

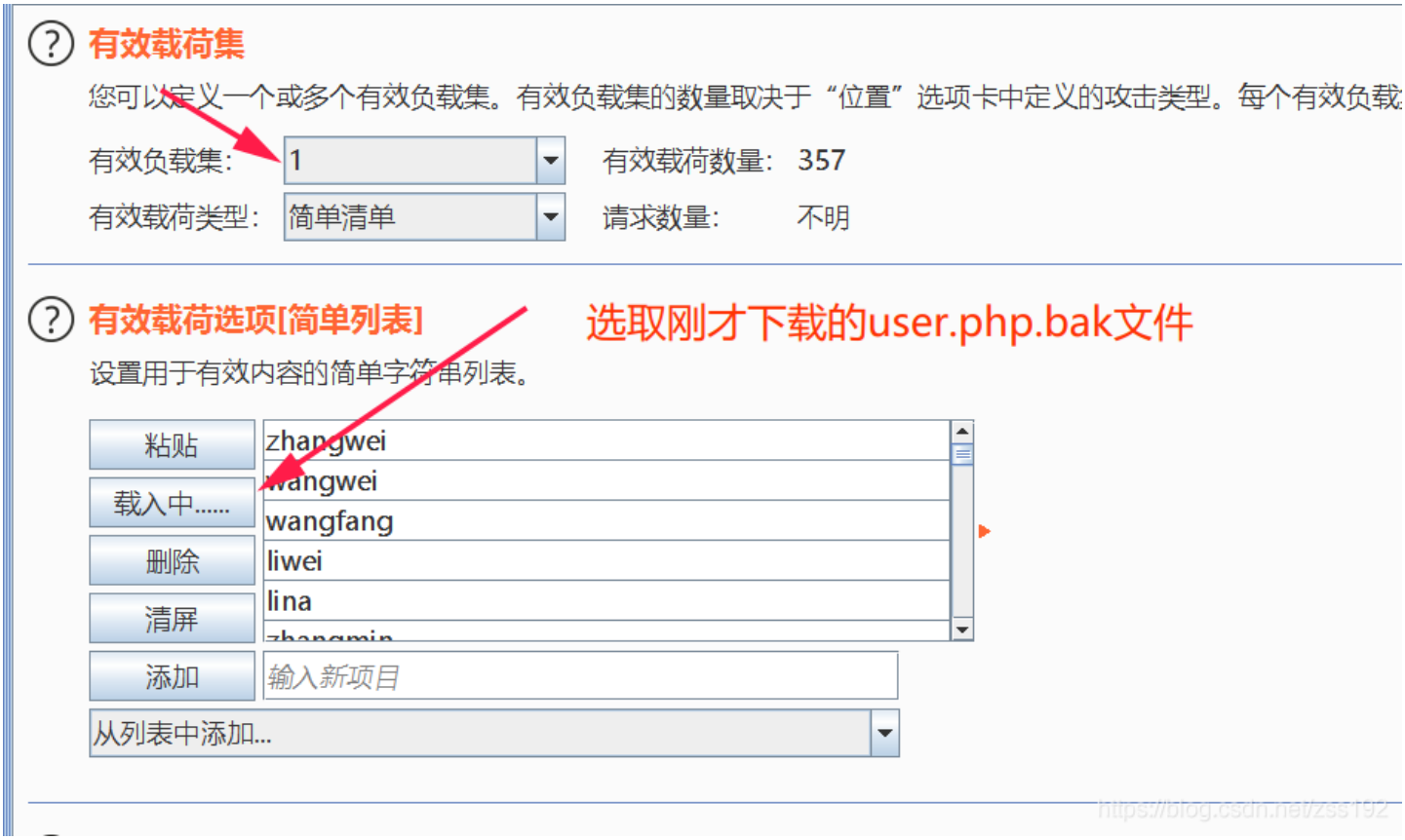
writeup

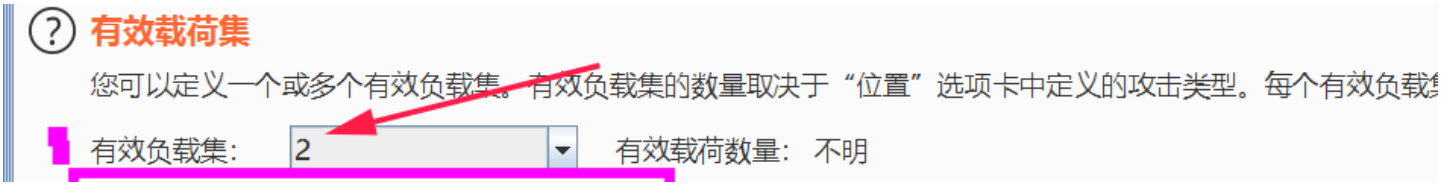
打开页面是一个登录页面，查看源码发现提示语句

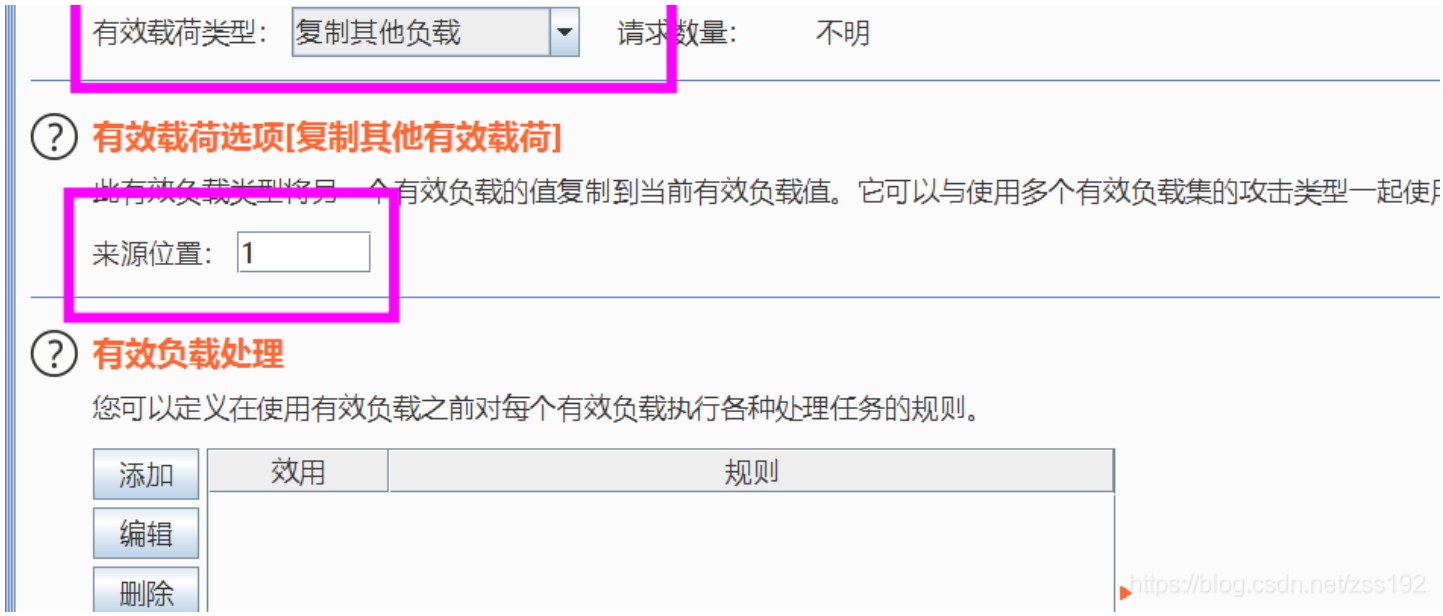
```
<br /> <br />
<input type="submit" name="submit" value="登录" />

<!-- 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user.php发现界面为空，此时尝试打开备份文件，发现user.php.bak，下载后发现用户名，根据上述源码提示采用burpsuite爆破，配置如下，注意**选取Clusterbomb模式**（因为要尝试多个payload，详细见：Burp Suite Intruder4种攻击类型）

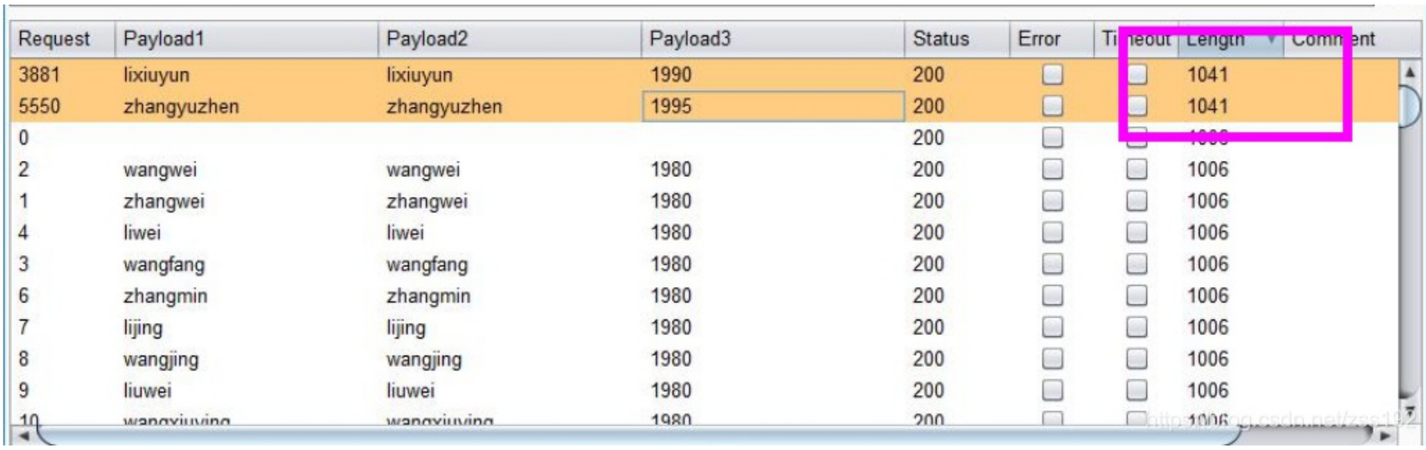
三个payload如下所示





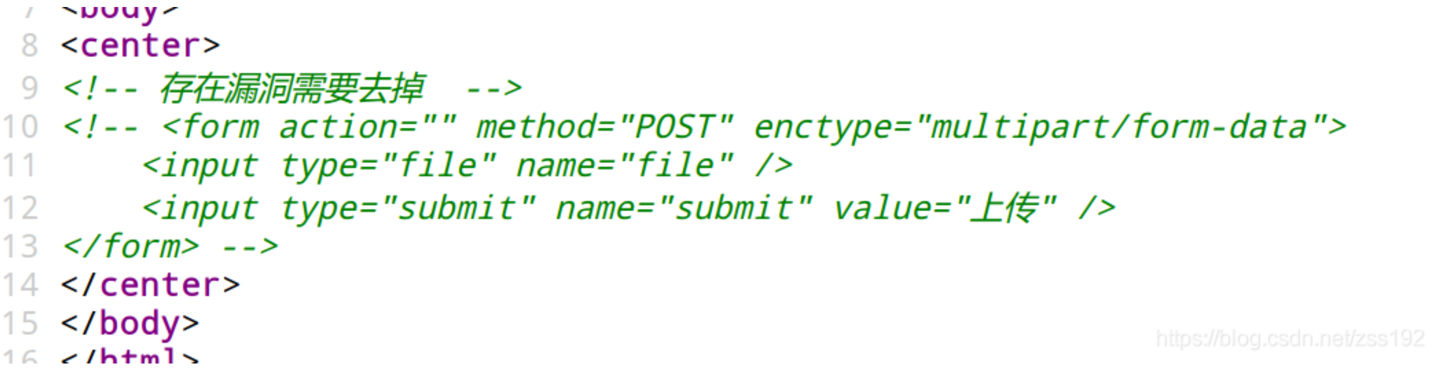


经过一番爆破后发现两个有用的信息



Request	Payload1	Payload2	Payload3	Status	Error	Timeout	Length	Comment
3881	lixiuyun	lixiuyun	1990	200	☐	☐	1041	
5550	zhangyuzhen	zhangyuzhen	1995	200	☐	☐	1041	
0				200	☐	☐	1006	
2	wangwei	wangwei	1980	200	☐	☐	1006	
1	zhangwei	zhangwei	1980	200	☐	☐	1006	
4	liwei	liwei	1980	200	☐	☐	1006	
3	wangfang	wangfang	1980	200	☐	☐	1006	
6	zhangmin	zhangmin	1980	200	☐	☐	1006	
7	lijing	lijing	1980	200	☐	☐	1006	
8	wangjing	wangjing	1980	200	☐	☐	1006	
9	liuwei	liuwei	1980	200	☐	☐	1006	
10	wangxiuying	wangxiuying	1980	200	☐	☐	1006	

选取其中一个登录，发现依然是空白，查看源码发现



```
<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>
```


我们可以看到提示这个表单存在漏洞，所以我们可以按F12然后把表单取消注释（选中<center>右键选择编辑html）

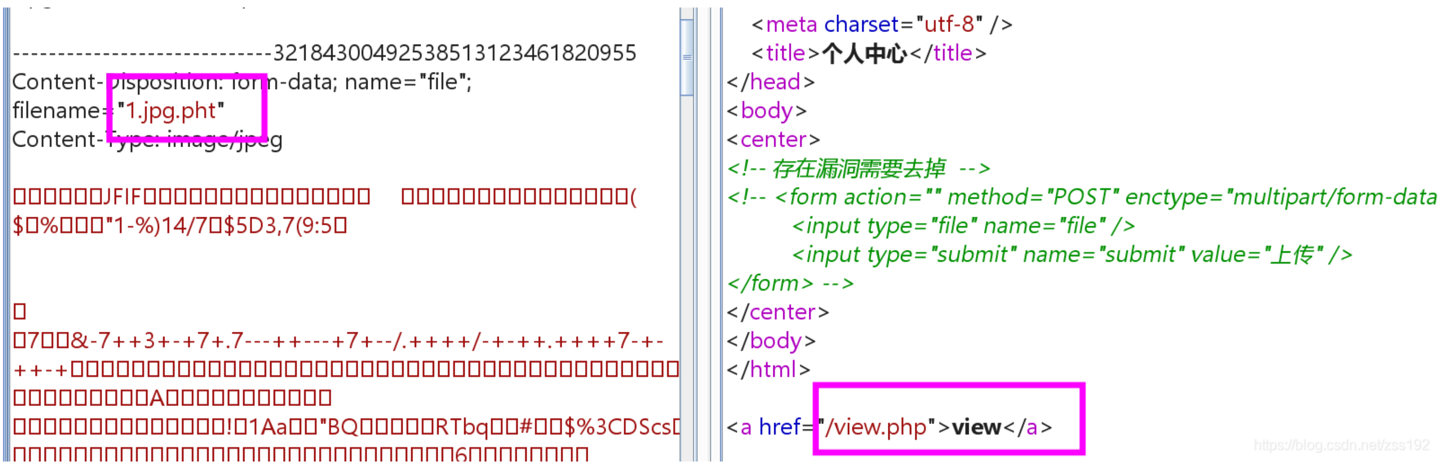
尝试上传一个正常jpg图片提示文件名不合法，猜想这里并不是真的文件上传，并不是用菜刀连上找flag。只是构造文件名，并且上传到服务器成为可执行文件便可通过。

Apache 配置文件中会有

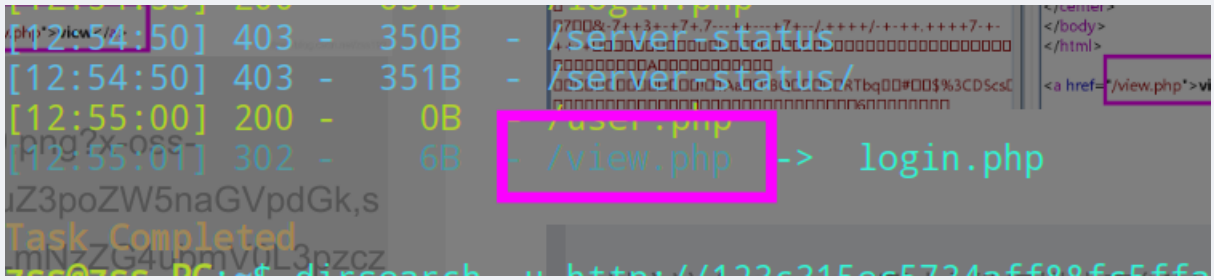
```
.+.ph(p[345]?|t|tml
.+\.phps$
```

文件名满足即可被当做php解析，也就是说php3，php4，php5，pht，phtml,phps都是可以被解析的。

尝试.pht发现返回view.php



其实这个view.php通过文件扫描也可能被找到，我用的dirsearch就发现这个文件



进入view.php,提示file? ,应该是file传参
构造?file=flag.php

---

filter "flag"

提示flag被过滤，尝试双写大小写也不行，最终发现构造

```
?file=flaflagg
```

发现flag

```
<?php
echo 'flag is here';
'flag{2364b0f7-824e-4741-9e89-d6b7964011b1}-';
?>
```

吐槽一句这个file也太迷惑人了，我以为必须是个文件才行。。。

小结

这道题涉及到了文件泄露、爆破、文件上传绕过、关键字绕过。非常好的一道题目，在此特别记录，文中如有错误，请联系我更正。