i春秋 “百度杯”CTF比赛 九月场 123

原创

「已注销」 于 2018-09-15 17:51:04 发布 1099 收藏

分类专栏： i春秋

友链：https://cutt.ly/7777aaaa

本文链接：https://blog.csdn.net/include_heqile/article/details/82716225

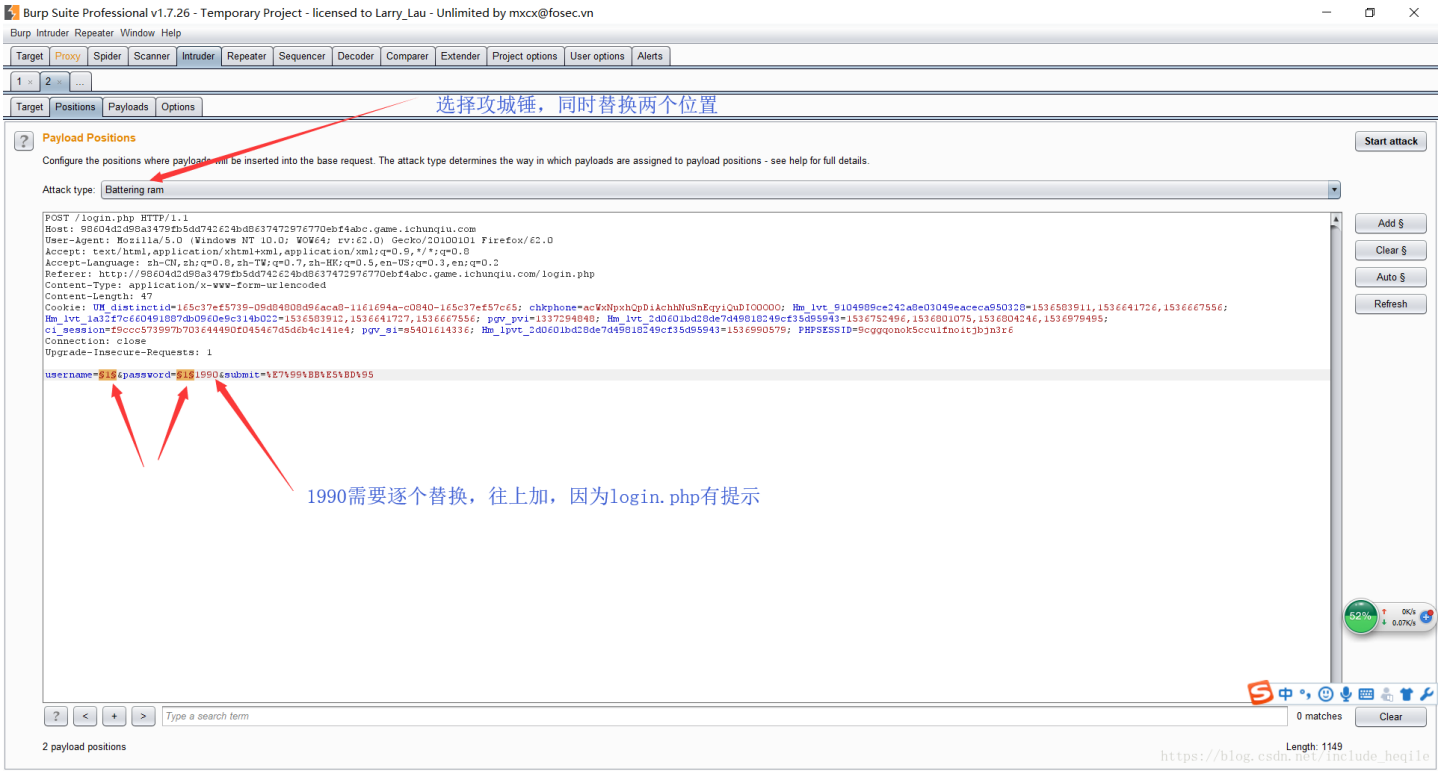
https://www.ichunqiu.com/battalion?t=1&r=0

首先查看源代码，得到提示说用户信息在`user.php`中，但是我们访问`user.php`是得不到任何信息的，得不到任何线索，看`writeup`得到提示，关键词**文件读取漏洞、备份文件**

于是我就试着访问了`user.php.bak`，得到了用户名信息，然后根据`login.php`注释部分的提示，用户密码为**用户名+出生年份**

明显需要使用爆破，得到的用户名文件作为`payload`，具体是这样的：

BurpSuite Intrude使用

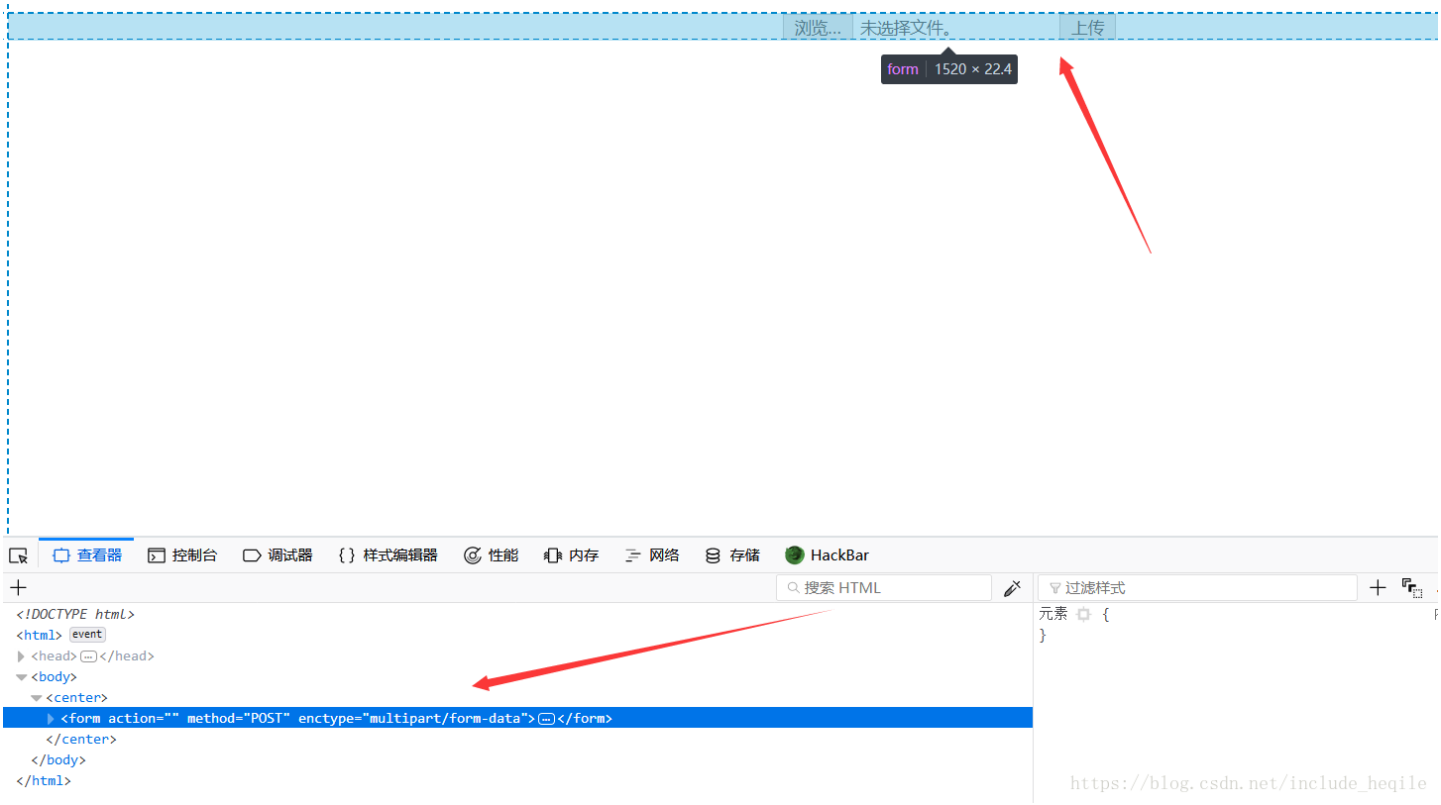


把我们得到的`user.php.bak`文件作为`payload`，即可得到用户名和密码

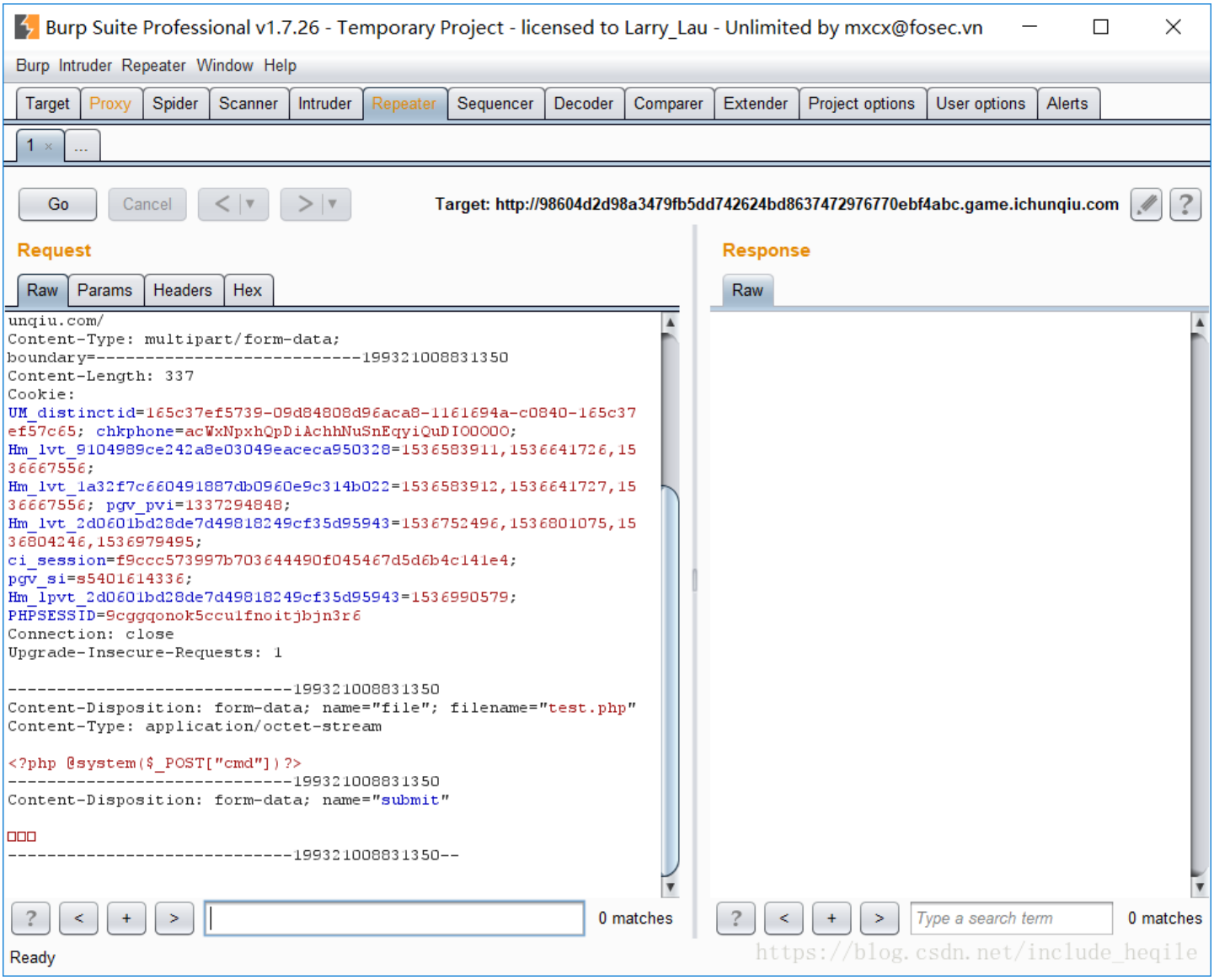
进入页面后查看源代码：


```
<!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>
```

直接使用`firefox`的开发者工具更改页面



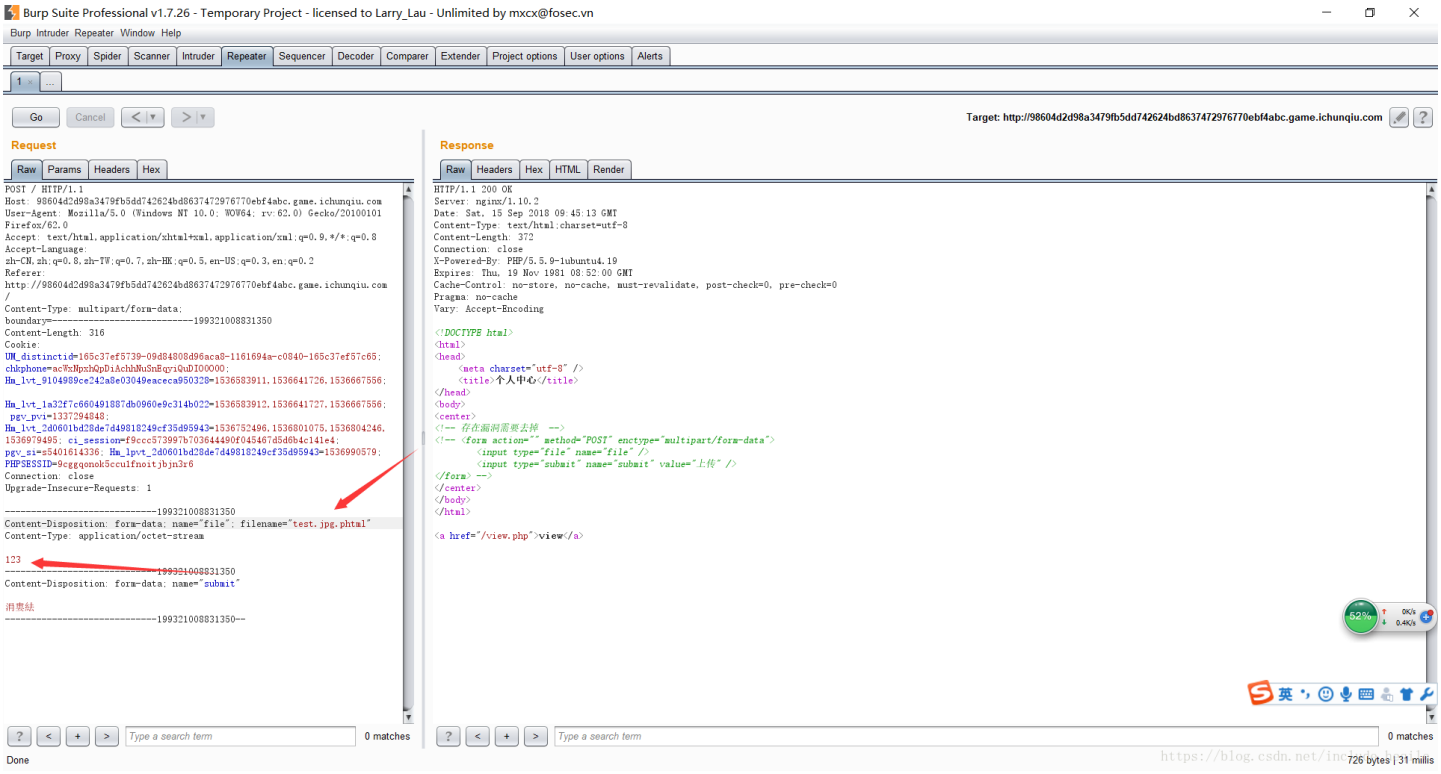
写个一句话木马，上传抓包：



传不上去，有过滤，更改各种后缀：

```
php2, php3, php4, php5, phps, pht, phtm, phtml
```

文件名和文件内容的双重过滤，经过各种尝试之后，得到如下页面：



访问`view.php`

file?

直接`view.php?file=flag.php`，结果为`filter "flag"`

因为前面做题一直都是`flag.php`存放`flag`，所以试了半天`flaflagg.php`，最后把`.php`去掉就得到`flag`了，只是一个简单的字符过滤绕过，假如不是把`flag`替换成空而是替换成`_`，就没那么容易了


```
<?php
echo  'flag  is  here';
'flag{425bb7fb-c20d-406c-b83d-adffd7737566}-';
?>
```