i春秋“百度杯”九月场 | 123

原创

g1ut_t0ny 于 2020-07-04 10:53:10 发布 97 收藏

文章标签： CTF 夺旗赛

本文链接：https://blog.csdn.net/g1ut_t0ny/article/details/107120937

123题目

分值：50分　　类型：Web　　题目名称：123

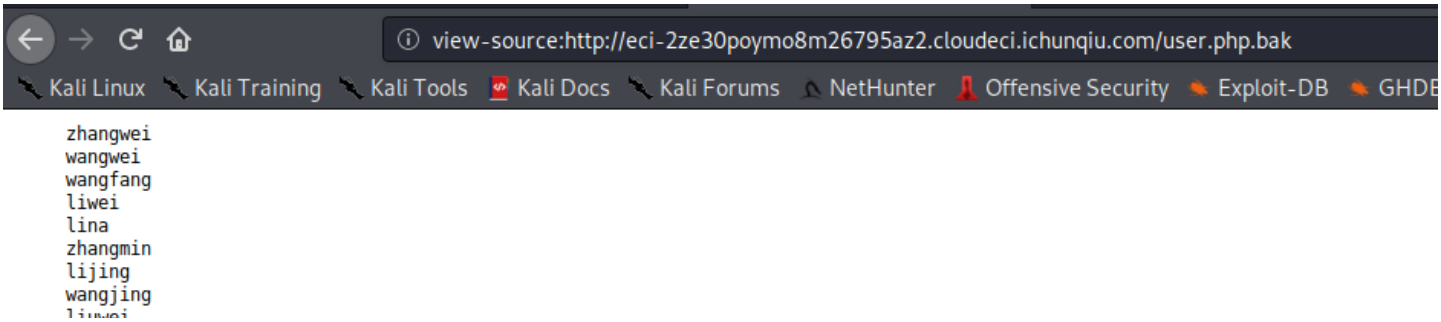
题目内　12341234，然后就解开了

步骤

1、查看源代码

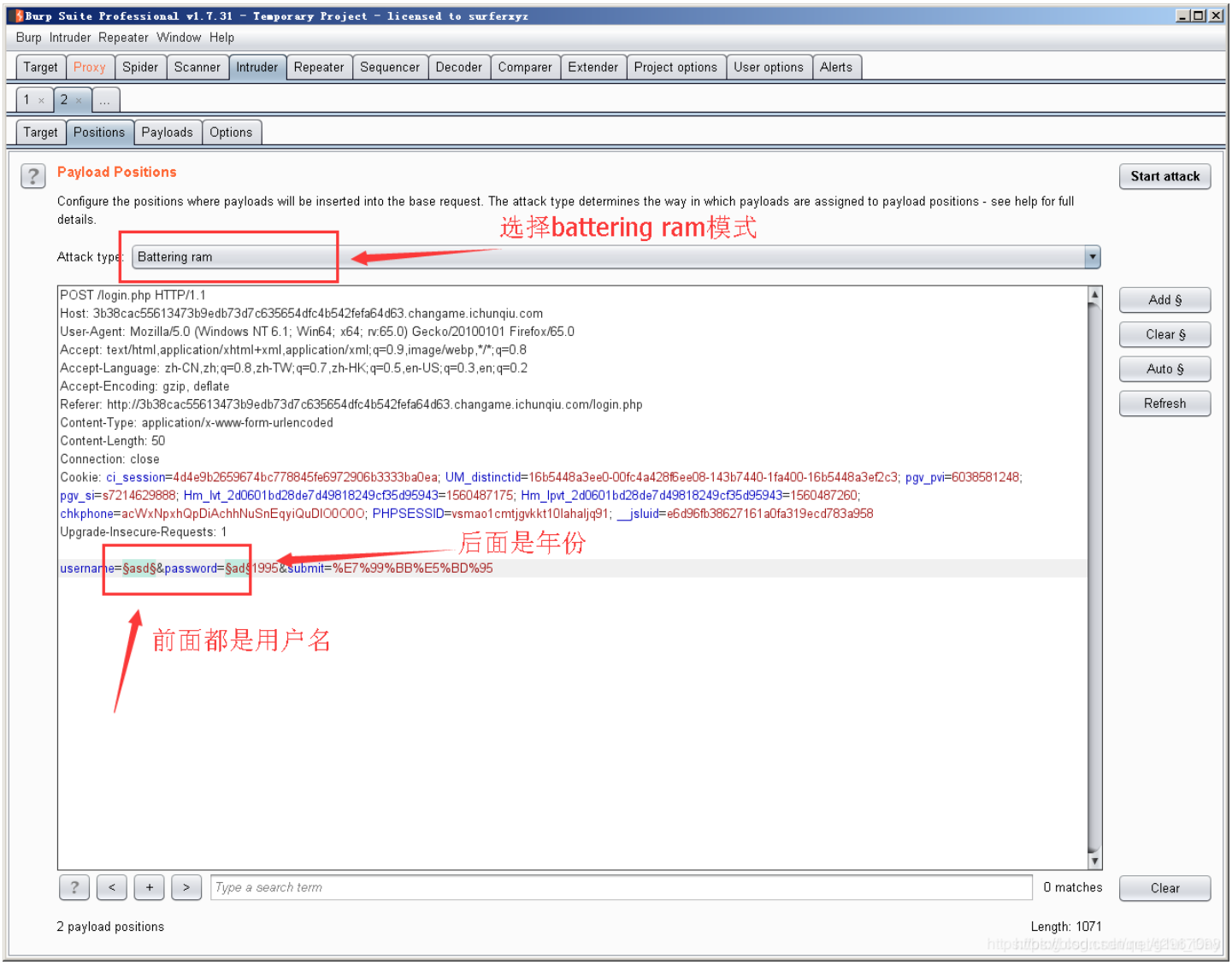
```
<body>
<center>
  <h4>请输入帐号密码进行登录</h4>
  <form action="" method="POST">
    <input type="text" name="username" placeholder='用户名' />
    <br /><br />
    <input type="password" name="password" placeholder='密码' />
    <br /><br />
    <input type="submit" name="submit" value="登录" />

    <!-- 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>
```


2、我必须要给自己颁一个瞎猫碰上死耗子奖项，顺手访问的user.php啥也没有，我就好奇输了一个.bak文件，寻思万一有备份呢，这不是巧了。

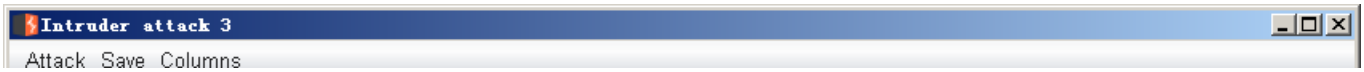


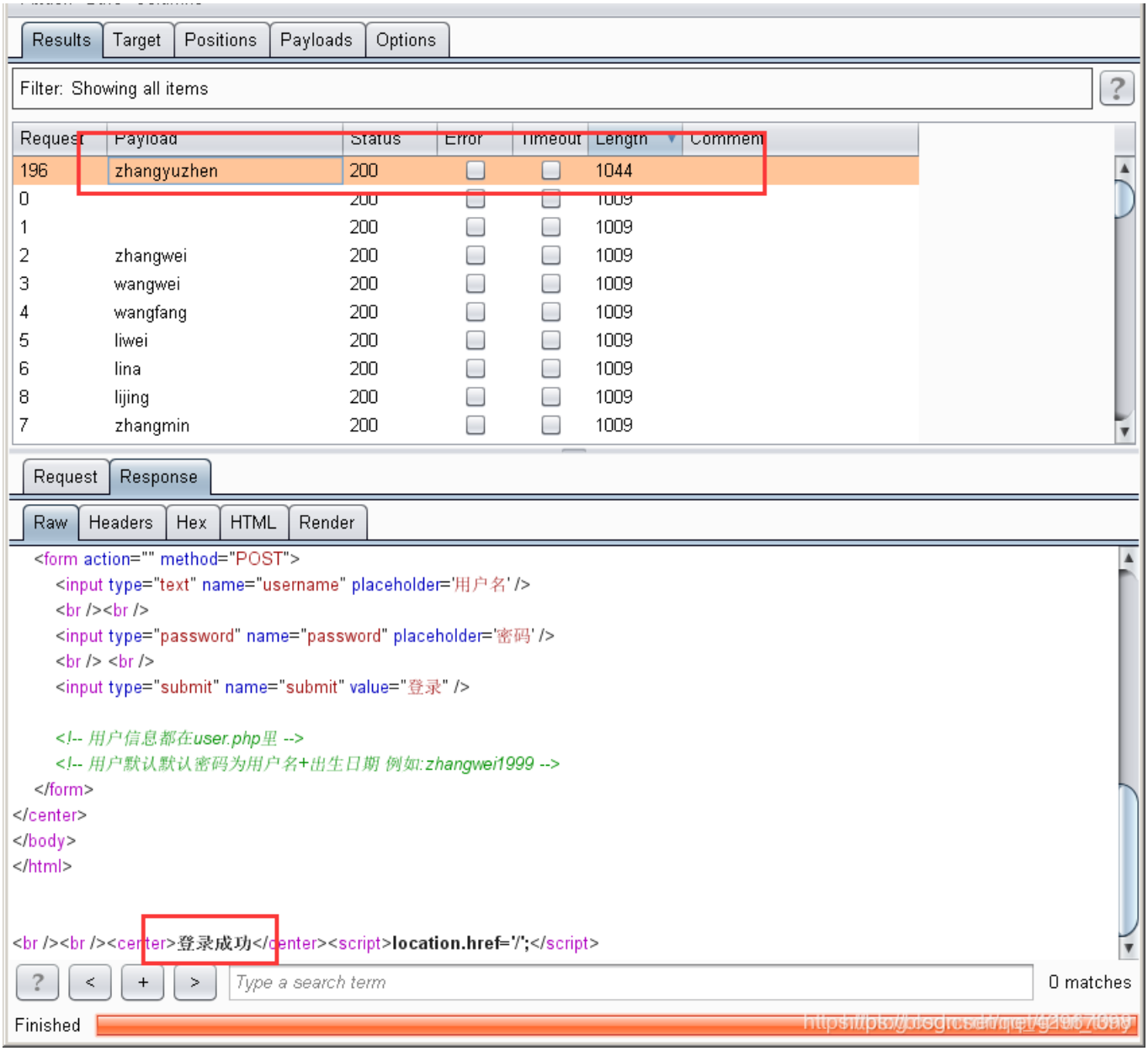
```
tiuwei
wangxiuying
zhangli
lixiuying
wangli
zhangjing
zhangxiuying
liqiang
wangmin
limin
wanglei
liuyang
wangyan
wangyong
lijun
zhangyong
lijie
zhangjie
zhanglei
wangqiang
lijuan
wangjun
zhangyan
zhangtao
wangtao
liyan
wangchao
```


3、用burpsuite爆破，将用户名保存在本地当作密码，同时设置为battering ram(对变量同时进行破解。多个标记同时进行。多参数同时爆破，但用的是同一个字典。）



4、爆出密码lixiuyun1990(至于为什么1990，别问，问就是wp说的)

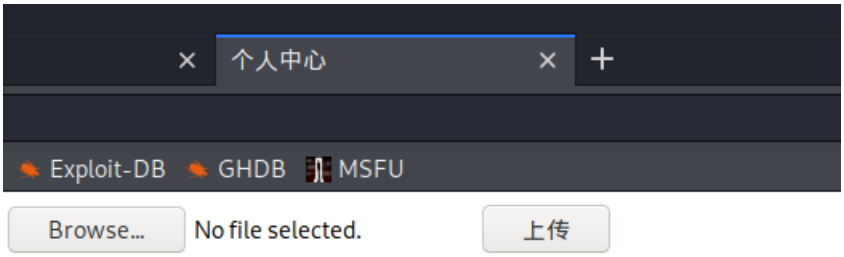




5、登陆进去也是啥也没有，试图修改审查元素，但发现改不动，于是**本地创建html**进行访问

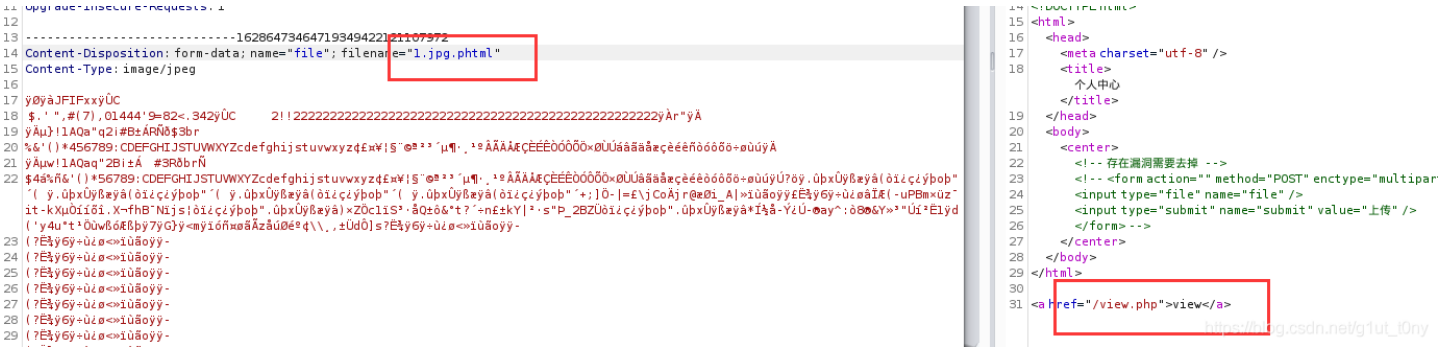
```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>个人中心</title>
</head>
<body>
<center>
<!-- 存在漏洞需要去掉  -->
<form action="http://eci-2ze4kxu6bgamo2zs10te.cloudeci.ichunqiu.com/" method="POST" enctype="multipart/form-data
">
 <input type="file" name="file" />
 <input type="submit" name="submit" value="上传" />
</form>
</center>
</body>
</html>
```

6、访问到的是一个文件上传页面

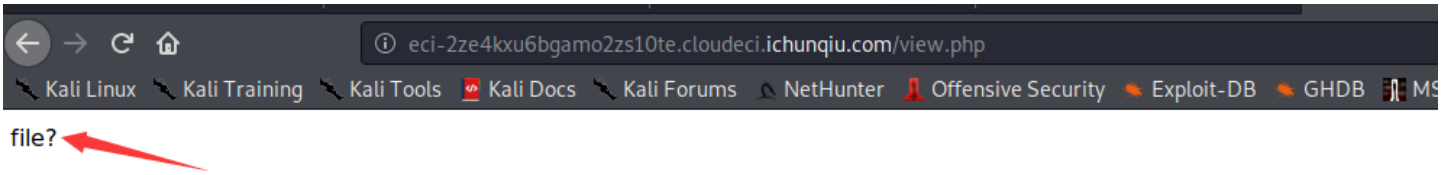


7、随便上传几种文件试试(jpg/php等)，发现提示“文件名不合格”“文件内容不合适”等提示信息

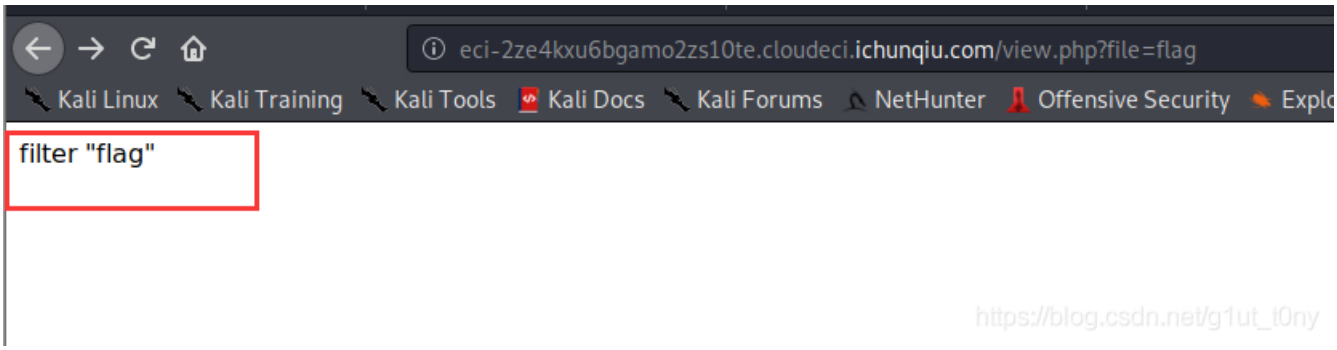
8、考虑用其他文件名绕过(php2, php3, php4, php5, phps, pht, phtm, phtml.htaccess …),但我发现.jpg的后缀不能删，只能在后面添加后缀，具体原因我也不清楚。。。



9、得到一个新的文件/view.php，对他进行访问，发现页面有一个file，考虑文件包含？



10、于是尝试直接查询file=flag



11、既然过滤一个，那考虑双写绕过一下file=flaflagg