i春秋123

转载

weixin_30652271 于 2019-08-05 18:51:00 发布 137 收藏
原文链接：http://www.cnblogs.com/wosun/p/11304876.html

打开是个普普通通的登录窗口，下尝试根据提示12341234进行输入，发现不正确。。。可能1234是指步骤，然后查看源码

```
<!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>
```

发现了绿色的提示信息，我们就根据提示试试打开user.php

打开是白板网页，源码也是白板，那就抓包试试

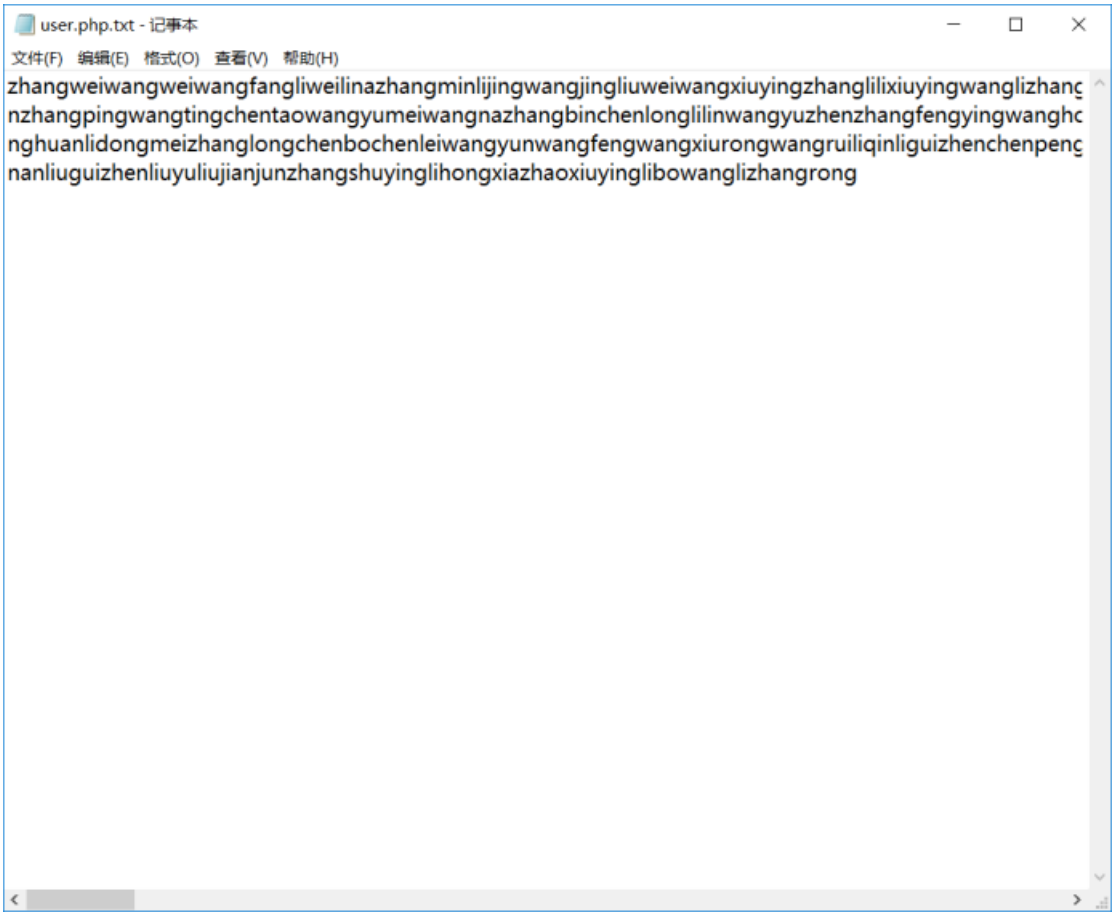
抓包也没找到什么关键信息。。。。那就试试注入吧

没反应。。。。

去看了看wp，发现这是个**文件读取漏洞、备份文件**的题

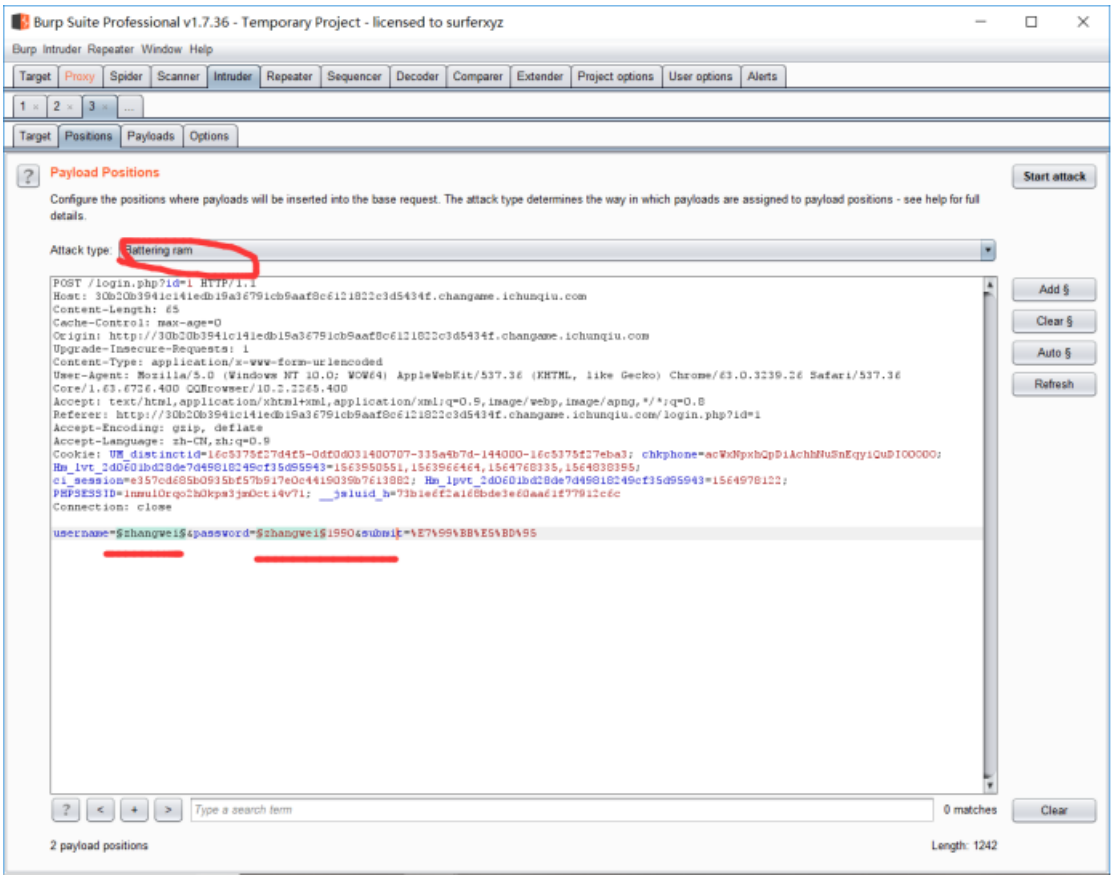
根据步骤，直接访问user.php.bak，提示我们下载备份文件

下载后直接将bak格式改为txt格式，然后就可以看见一堆所谓的用户名了

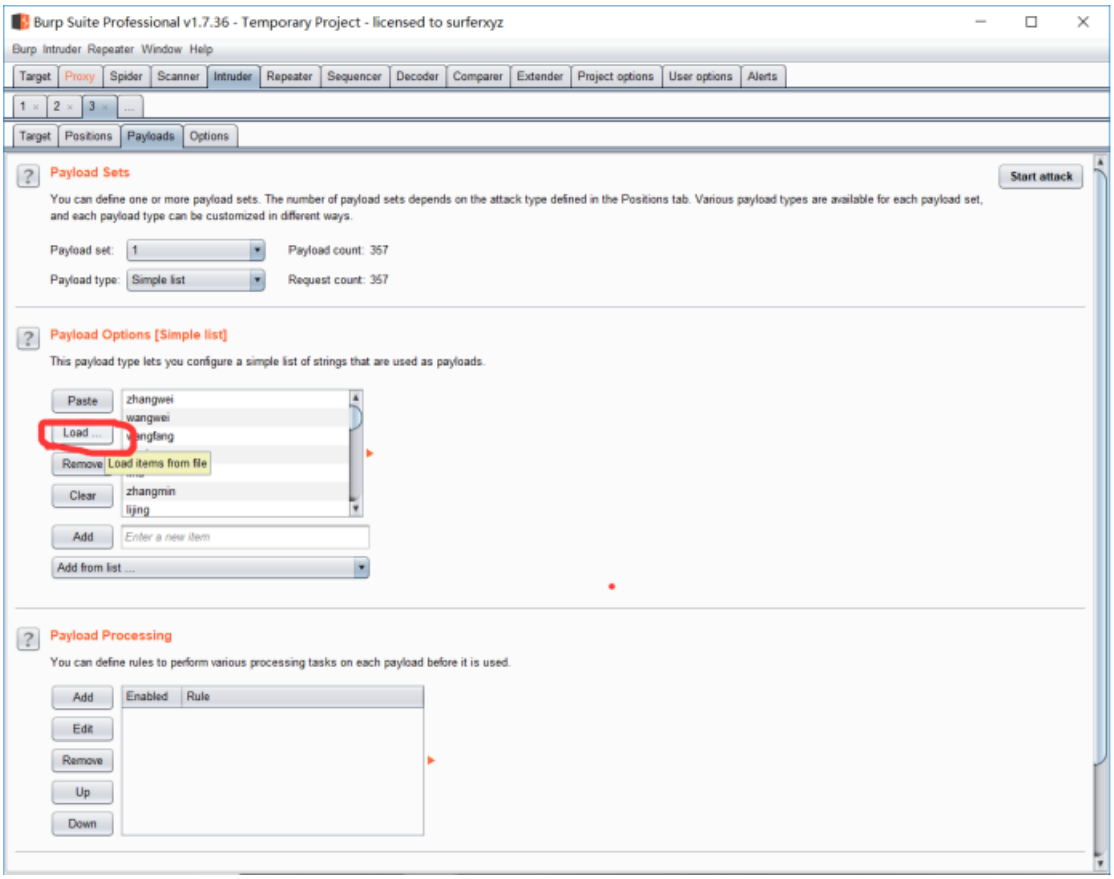


然后使用爆破，先进行login.php界面的抓包

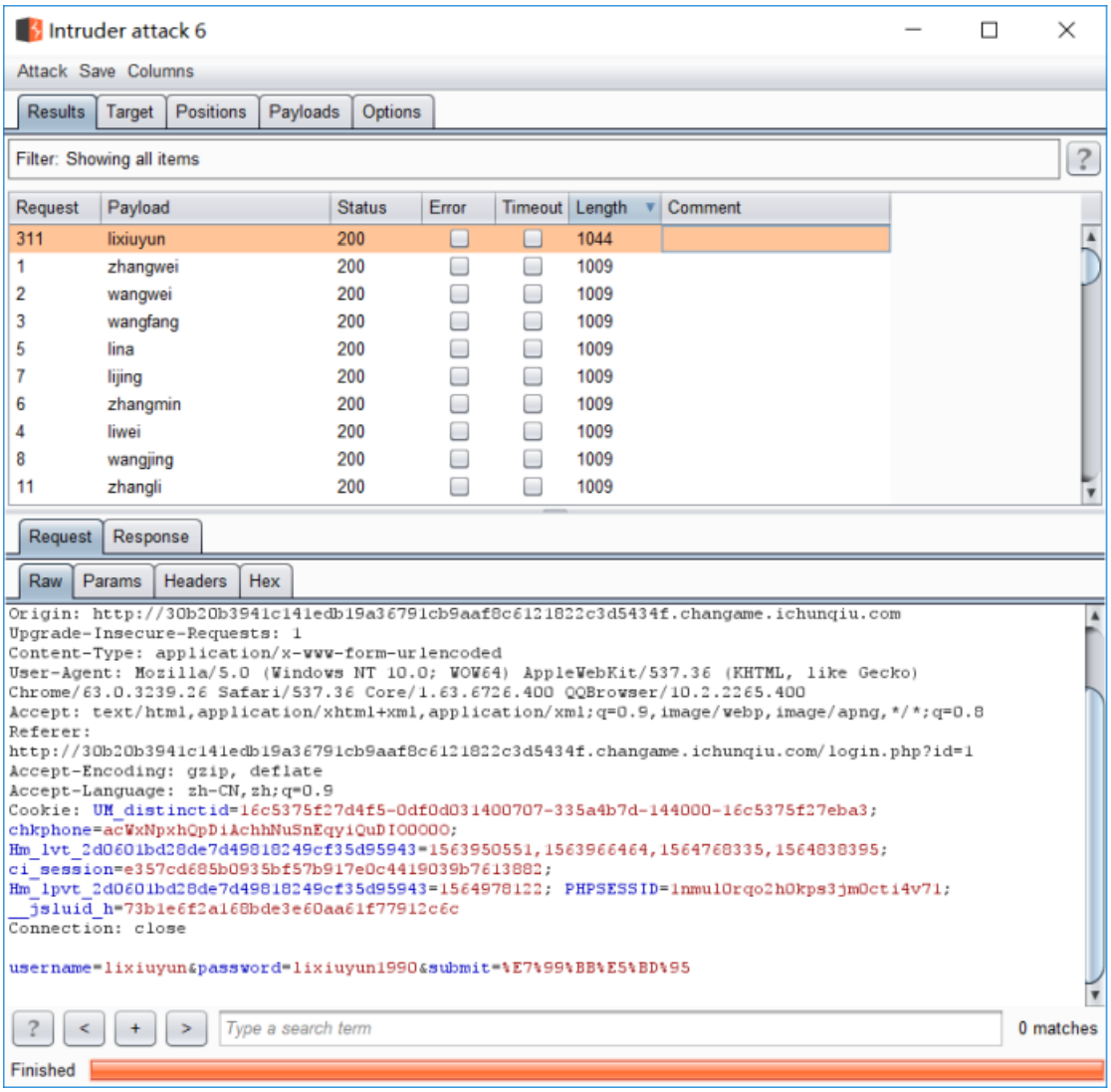
然后去掉不需要改变的变量，切换成攻城锤模式

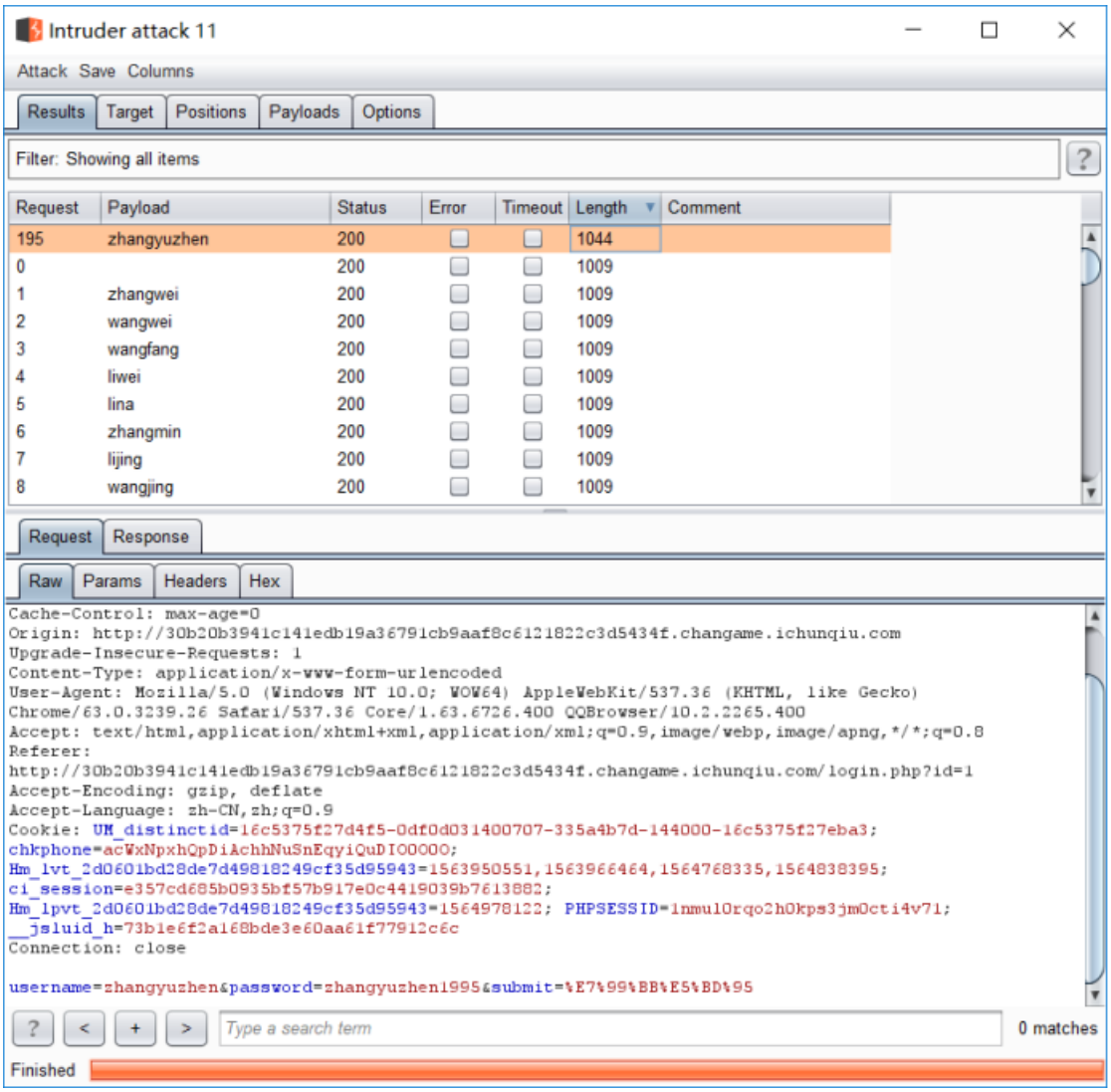


然后导入刚刚的user.php.txt

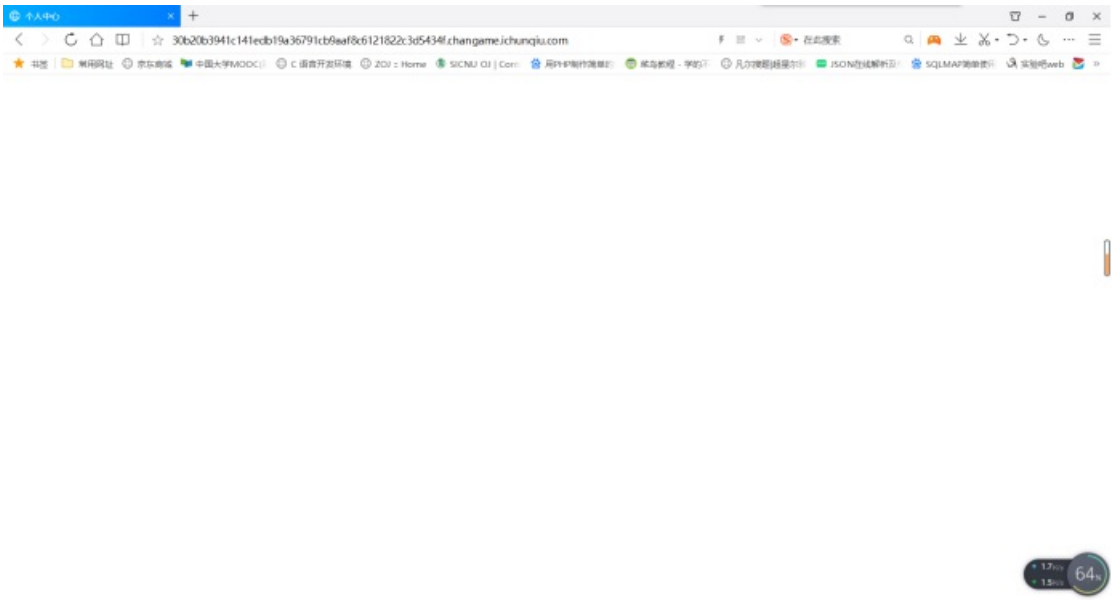


然后开始attack，每次attack结束后根据提示更改密码后面的年份


Intruder attack 6
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
311 lixiuyun 200 1044
1 zhangwei 200 1009
2 wangwei 200 1009
3 wangfang 200 1009
5 lina 200 1009
7 lijing 200 1009
6 zhangmin 200 1009
4 liwei 200 1009
8 wangjing 200 1009
11 zhangli 200 1009
Request Response
Raw Params Headers Hex
Origin: http://30b20b3941c141edb19a36791cb9aaf8c6121822c3d5434f.changame.ichunqiu.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400 QQBrowser/10.2.2265.400
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer:
http://30b20b3941c141edb19a36791cb9aaf8c6121822c3d5434f.changame.ichunqiu.com/login.php?id=1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba3;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1563950551,1563966464,1564768335,1564838395;
ci_session=e357cd685b0935bf57b917e0c4419039b7613882;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1564978122; PHPSESSID=1nmul0rqo2h0kps3jm0cti4v71;
__jsluid_h=73b1e6f2a168bde3e60aa61f77912c6c
Connection: close
username=lixiuyun&password=lixiuyun1990&submit=%E7%99%BB%E5%BD%95
Type a search term
0 matches
Finished



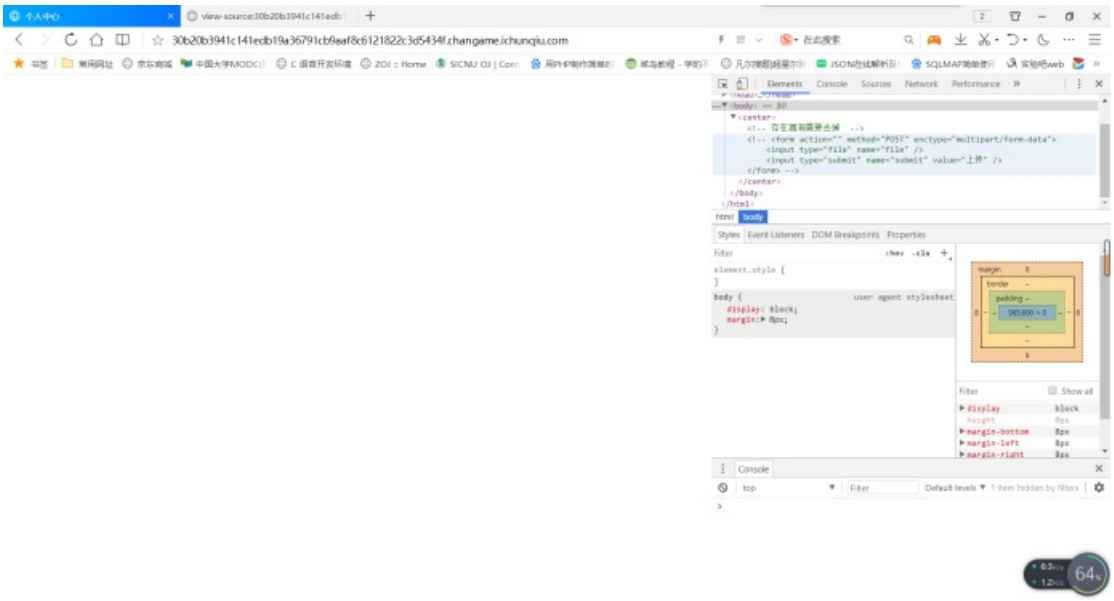
随机安排一个就可以登录进去了



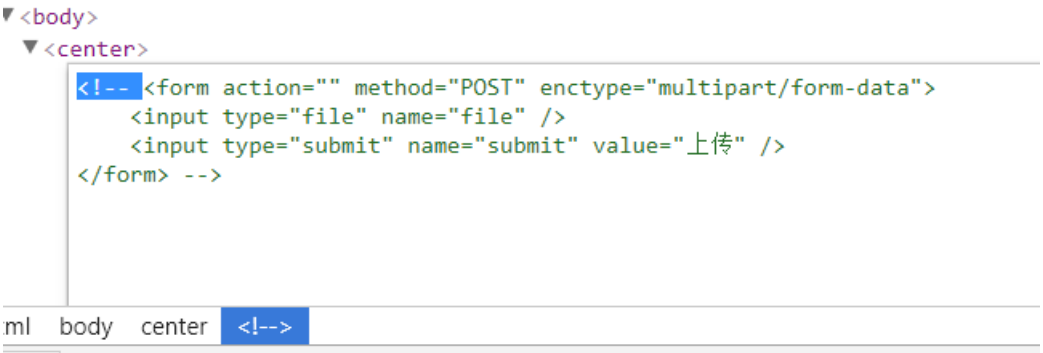
进去也是白板，右键源码

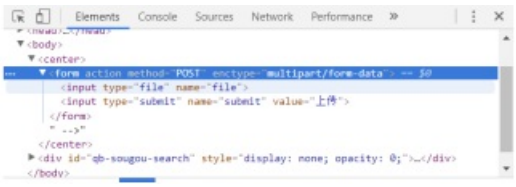
```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>个人中心</title>
</head>
<body>
<center>
<!-- 存在漏洞需要去掉  -->
<!-- <form action="" method="POST" enctype="multipart/form-data">
    <input type="file" name="file" />
    <input type="submit" name="submit" value="上传" />
</form> -->
</center>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

看到提示，然后这里我们可以按F12去修改网页源码



然后删除掉注释





弹出文件上传框，但是这里上传木马是被屏蔽了的

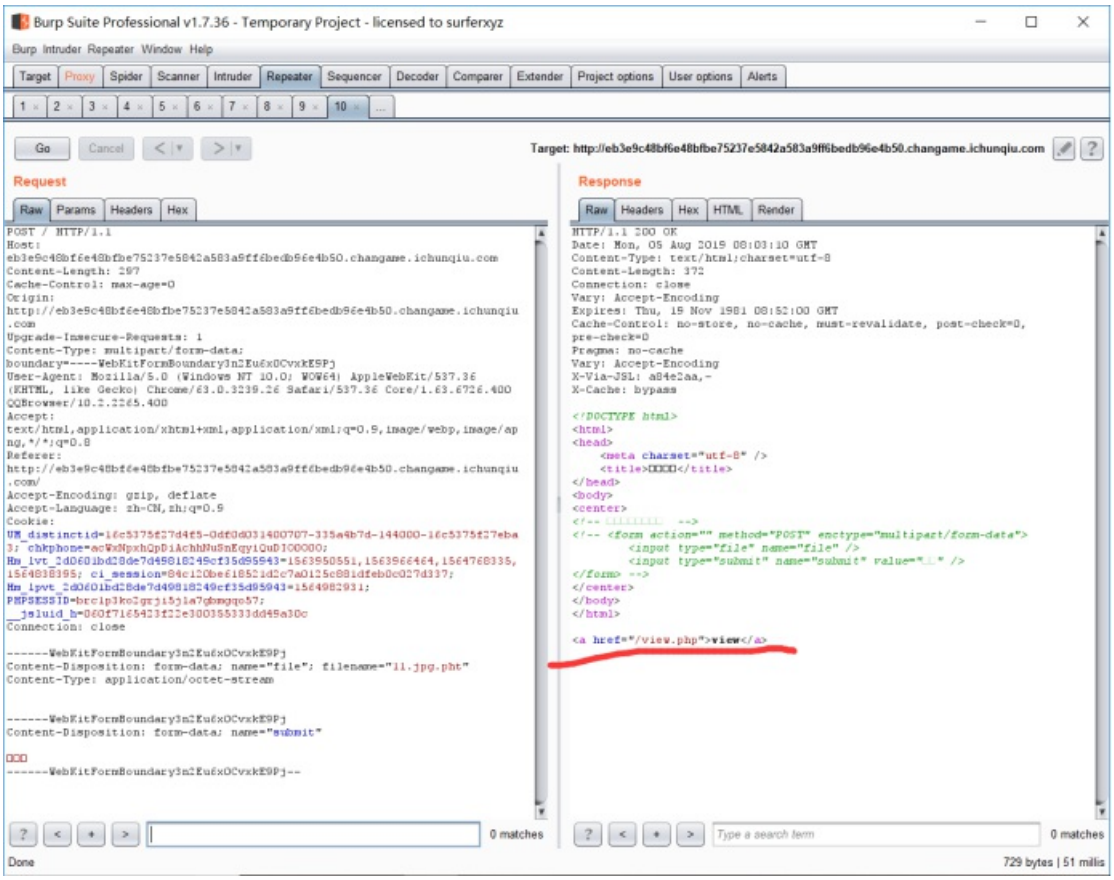
只允许上传.jpg,.png,.gif,.bmp后缀的文件

文件名不合法

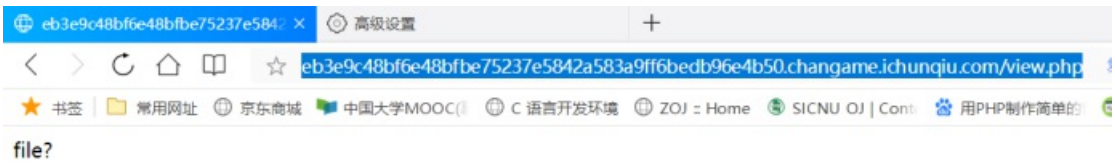
再直接上传jpg试试

。。。。。有点鸡貌了，又去看了看wp才知道这里是修改pht后缀，原因是Apache 配置文件中会有.+.ph(p[345]?|t|tml)此类的正则表达式，文件名满足即可被当做php解析

直接上传任意文件，其后缀满足是.pht就行了，如我随意将123.jpg重命名为123.jpg.pht



然后这里就直接访问view.php试试



file？应该是文件读取类型，问我们file的量是什么，查看源码没什么信息就直接在url中试试?file=1

弹出提示过滤flag，我们试试file=flag，果然被过滤了

既然有过滤我们就绕过试试

最开始我用大小写混写的方法结果绕过不了，再尝试双写就可以了

?file=flflagag

提交flag{巴拉巴拉}就行了

转载于:https://www.cnblogs.com/wosun/p/11304876.html