i春秋web-123(bak备份泄露)

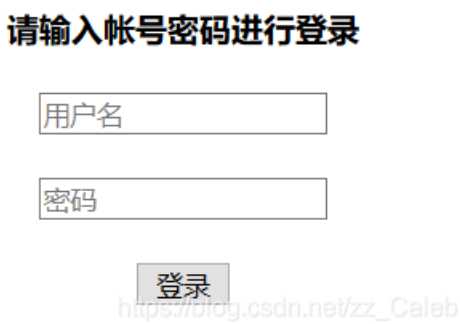
原创

大千SS 于 2019-05-21 23:19:30 发布 538 收藏 1

分类专栏： i春秋 文章标签： i春秋 备份文件泄露

本文链接：https://blog.csdn.net/zz_Caleb/article/details/90417608

进站是一个登陆界面：



查看源码：

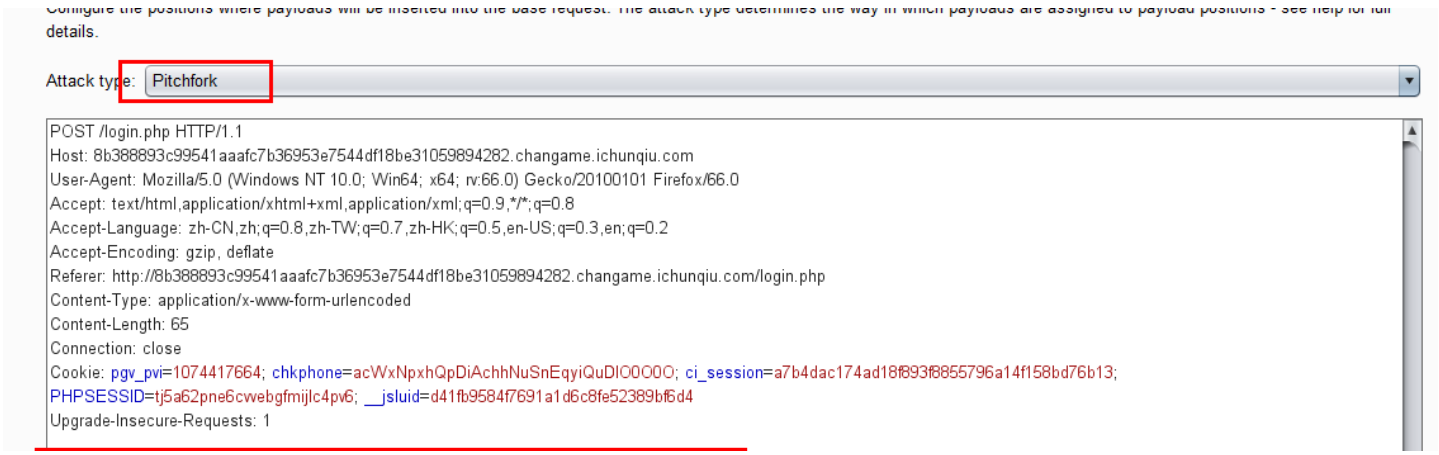
```
    <!-- 用户信息都在user.php里 -->
    <!-- 用户默认默认密码为用户名+出生日期 例如:zhangwei1999 -->
</form>
```

访问了一下user.php，然而页面是空的，试试有没有备份文件，果然是bak备份泄露，下载之后拿到了许多的用户名，但是密码中的日期并不知道，使用bp爆破有两种思路：

1）对一个用户名进行年份的爆破

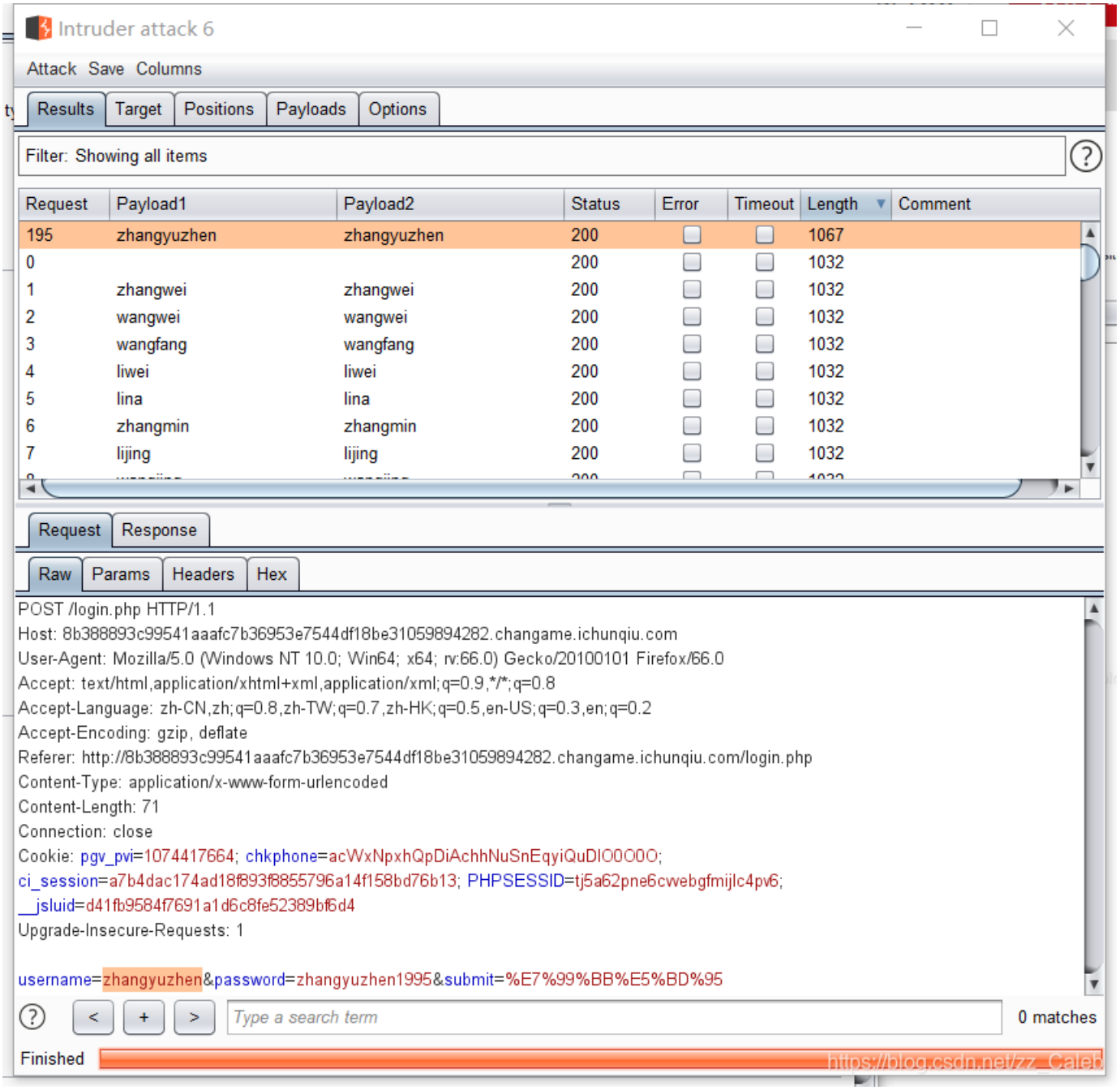
2）对一个年份进行所有用户名的爆破

我选择的是第二个思路：



```
username=§zhangwei§&password=§zhangwei§1995&submit=%E7%99%BB%E5%BD%95
```

payload里面两个地方都是载入的bak备份文件中的用户名，然后开始爆破(这里用的是1995年)：



然后

就可以用这个账号登录了，登录之后页面是空白的，但是源码中有有用的内容：

```
<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> -->
```

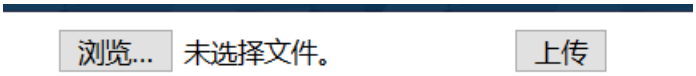
这里有个文件上传的地方，F12把这个地方搞成可用的，我是这样搞的：

1）先在这里吧这几行代码的内容复制下来

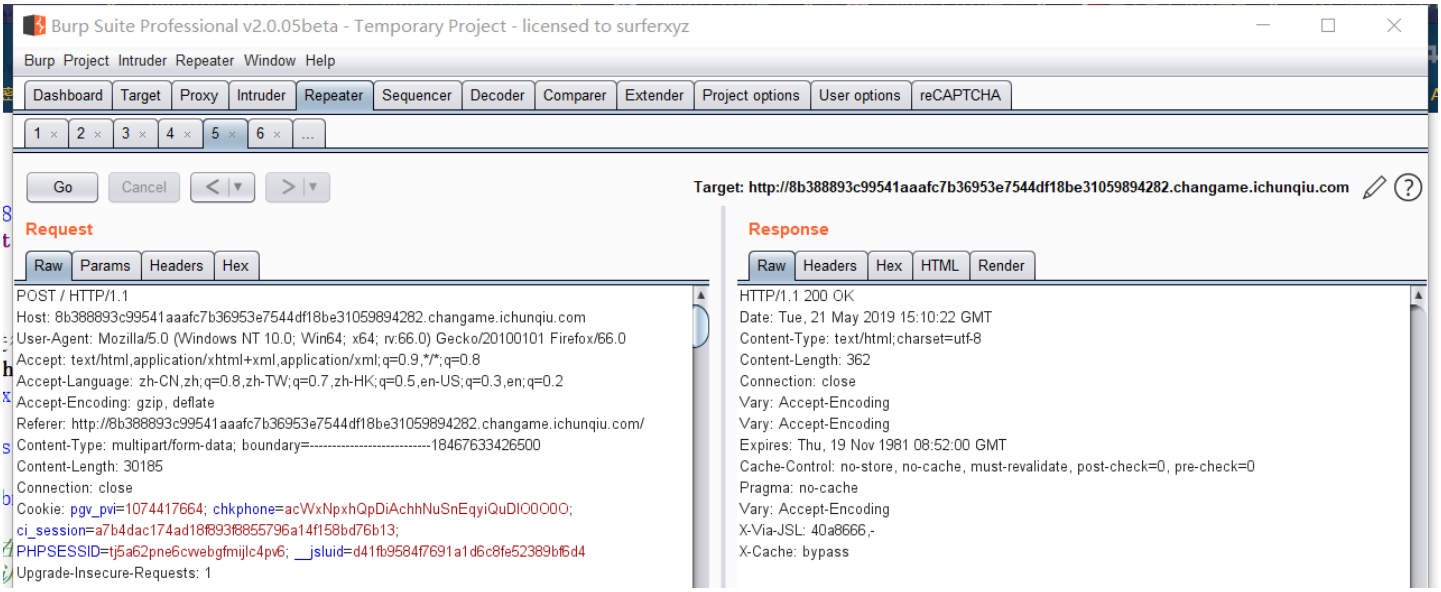
```
<!--
<form action="" method="POST" enctype="multipart/form-data"> <input type="file" name="file" /> <input type="submit" name="submit"
value="上传" /> </form>
-->
```

2）添加代码内容到页面源码
在center这个节点把代码复制上去

然后就出现了文件上传的地方：



随便上传一个文件，这里上传的是个jpg文件，然后抓包：



文件名不合法。。。
改成php上传显示：只允许上传.jpg,.png,.gif,.bmp后缀的文件
然而这四种后缀都是返回文件名不合法。

尝试.jpg.php得到：

```
</html>

文件名不能包含php
```

于是尝试去掉文件名中的php，使用pht或phtml替换即可，经过尝试，这两个后缀都是可以的，上传后得到：

```
<a href="/view.php">view</a>
```

访问view.php：

file?

猜测是让我们以file传递参数，尝试file=flag，得到：filter “flag”
双写一下file=flflagag拿到flag：

```
<?php
echo 'flag is here';
'flag{3da49125-c418-4f81-bb91-b7a3fd766096}-';
?>
```