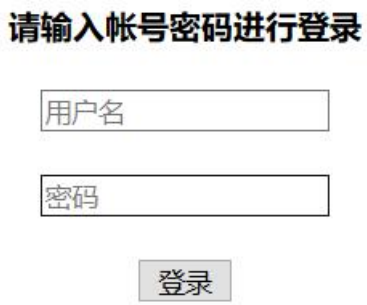
百度杯”CTF比赛 九月场123 ---------i春秋

转载

weixin_30359021 于 2019-07-08 00:15:00 发布 142 收藏
文章标签： php
原文链接：http://www.cnblogs.com/zhangyukui/p/11146414.html

题目地址：https://www.ichunqiu.com/battalion

进入题目



咦，这是让我输题目上的12341234？

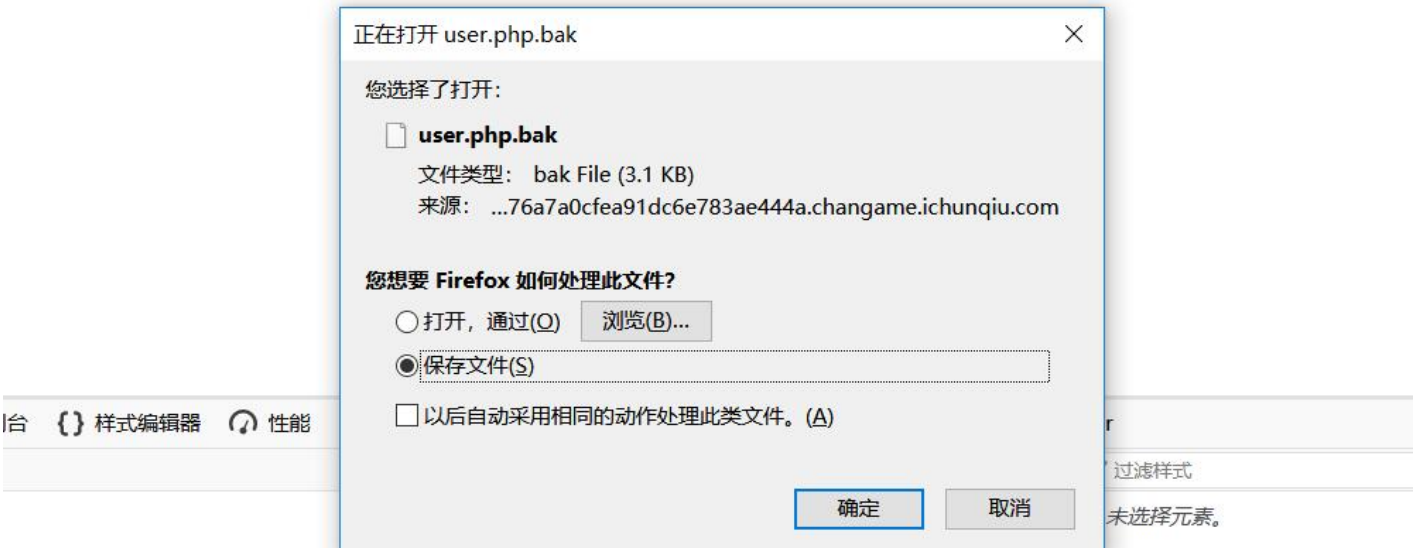
然后然后，被骗了。。

看一下源码

```
  <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>
```

有东西,访问一下user.php,什么都没有。。

但是可以访问，应该是隐藏了什么东西，百度搜一下隐藏文件的类型，找到一个.bak的，数据备份文件,访问



user.php.bak - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
zhangweiwangweiwangfangliweilinazhangminlijingwangjingliuweiwangxiuyingzhanglilixiuying
wanglizhangjingzhangxiuyingliqiangwangminliminwangleiliuyangwangyanwangyonglijunzhangyong
.ijiezhangjiezhangleiwangqianglijuanwangjunzhangyanzhangtaowangtaoliyanwangchaolimingliyong
wangjuanliujieliuminlixialilizhangjunwangjiezhangqiangwangxiulanwanggangwangpingliufang
zhangyanliuyanliujunlipingwanghuiwangyanchenjingliuyonglilingliguiyingwangdanliganglidan
wangbinlipengzhangpingzhanglizhanghuizhangyuliujuanlibinwanghaochenjiewangkaichenlichenmin
wangxiuzhenliyulanliuxiuyingwangpingwangpingzhangboliuguiyingyangxiuyingzhangyingyangli
zhangjianlijun4liliwangbozhanghongliudanlixinwangliyangjingliuchaozhangjuanyangfanliuyan
.iuyinglixuelixiuzhenzhangxinwangjianliuyulanliuhuiliubozhanghaozhangmingchenyanzhangxia
zhenyanyangjiewangshuailihuiwangxueyangjunzhangxuliugangwanghuayangminwangninglilningwangjun
.iuguilanliubinzhangpingwangtingchentaowangyumeiwangnazhangbinchenlonglilinwangyuzhen
zhangfengyingwanghonglifengyingyangyanglitingzhangjunwanglinchenyingchenjunliuxiachenhao
zhangkaiwangjingchenfangzhangtingyangtaoyangbochenhongliuhuanwangyuyingchenjuanchengang
wanghuizhangyingzhanglinzhangnazhangyumeiwangfengyingzhangyuyinglihongmeiliujialiulei
zhangqianliupengwangxuzhangxueliyangzhangxiuzhenwangmeiwangjianhualiyumeiwangyingliuping
wangmeilifeiwanglianglileilijianhuawangyuchenlingzhangjianhualiuxinwangqianzhangshuailijian
zhenlinliyangchenqiangzhaojingwangchengzhangyuzhenchenchaochenliangliunawangqinzhanglanying
zhanghuiliuchangliqianyangyanzhangliangzhangjianliyunzhangqinwanglanyingliyuzhenliuping
zhenguiyingliuyingyangchaozhangmeichenpingwangjianliuhongzhaoweizhangyunzhangningyanglin
zhangjiegaofengwangjianguoyangyangchenhuayanghuawangjianjunyangliuliuyangwangshuzhenyangfang
.ichunmeiliujunwanghaiyanliulingchenchenwanghuanlidongmeizhanglongchenbochenleiwangyun
wangfengwangxiurongwangruiliqinliguizhenchenpengwangyingliufeiwangxiuyunchenmingwangguirong
.ihaowangzhiqiangzhangdanlifengzhanghongmeiliufengyingliyuyingwangxiumeilijiawanglijuan
zhenhuizhangtingtingzhangfangwangtingtingwangyuhuazhangjianguolilanyingwangguizhenlixiumei
zhenyulanchenxialiukaizhangyuhualiuyumeiliuhualibingzhangleiwangdonglijianjunliuyuzhen
wanglinlijianguoliyingyangweiliguirongwanglongliutingchenxiulanzhangjianjunlixiurongliuming
zhouminzhangxiumeilixuemeihuangweizhanghaiyanwangshulanlizhiqiangliulilikaizhangyuzhangfeng
.iuxiulanzhangzhiqianglilonglixiuyunlixiufanglishuailixinliuyunzhanglililijiezhangxiuyun
wangshuyingwangchunmeiwangxinwangguizhizhaolizhangxiuhuazhanglinhuangminyangjuanwangjinfeng
zhoujiewangleichenjianhualiumeiyangguiyinglishuyingchenyuyingyangxiuzhensunxiuyingzhaojun
zhaoyongliubingyangbinliwenchenlinchenpingsunweizhanglichenjunzhangnanliuguizhenliuyu
.iujianjunzhangshuyinglihongxiazhaoxiuyinglibowanglizhangrong
```

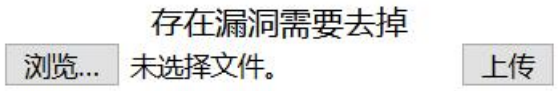
头皮有点发麻，文件内的像是用户名,把这些用户名和刚才的密码格式丢到burp里面去爆破

Request	Payload	Status	Error	Timeout	Length	Comment
195	zhangyuzhen	200	☐	☐	1044	
0		200	☐	☐	1009	
1	zhangwei	200	☐	☐	1009	
2	wangwei	200	☐	☐	1009	
3	wangfang	200	☐	☐	1009	
4	liwei	200	☐	☐	1009	
5	lina	200	☐	☐	1009	
6	zhangmin	200	☐	☐	1009	
7	lijing	200	☐	☐	1009	
8	wangjing	200	☐	☐	1009	
9	liuwei	200	☐	☐	1009	

根据爆出的用户名密码进行登录

```
<!--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>
-->
```

隐藏部分感觉像是上传的东西，用火狐开发者工具把注释给去了，显示出一个上传界面



上传一个php文件

只允许上传.jpg,.png,.gif,.bmp后缀的文件

不能上传，那就修改一下后缀名，用burp进行拦截修改

好像进行了双重的过滤，更改后缀名（php的别名：php2, php3, php4, php5, phps, pht, phtm, phtml），分别进行测试，得到一条信息

```
<!-- 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>

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

存在view.php,进行访问

file?

尝试使用file进行查询flag，view.php?file=flag

filter "flag"

过滤了flag，更改一下，view.php?file=flflagag

```
<?php
echo 'flag is here';
'flag{5827d89c-2671-4dcf-83ef-0099859f65e0}-';
?>
```

出现flag

转载于:https://www.cnblogs.com/zhangyukui/p/11146414.html