

i春秋 12341234, 然后就解开了

原创

[抬头、展望45°天空](#) 于 2021-05-21 16:48:32 发布 88 收藏

分类专栏: [ctf](#) 文章标签: [php web](#)

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/engineers/article/details/117127041>

版权

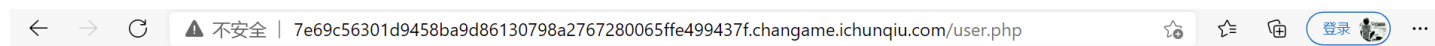


[ctf 专栏收录该内容](#)

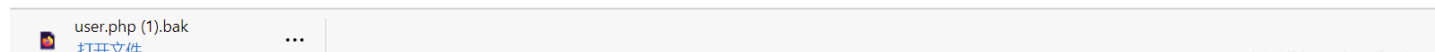
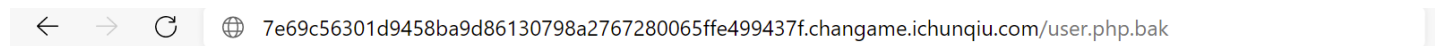
4 篇文章 0 订阅

订阅专栏

查看源码, 点击进去, 发现是空白的



则有可能是文件泄露

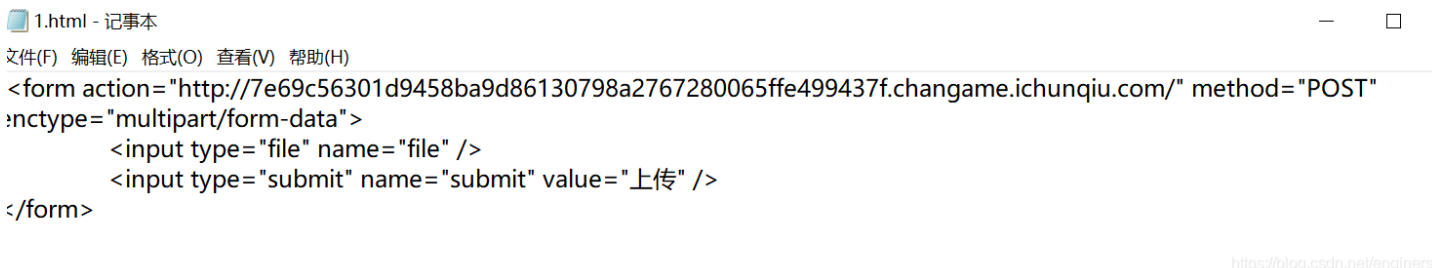


这里进行爆破，知道其中一个正确密码，登录进去



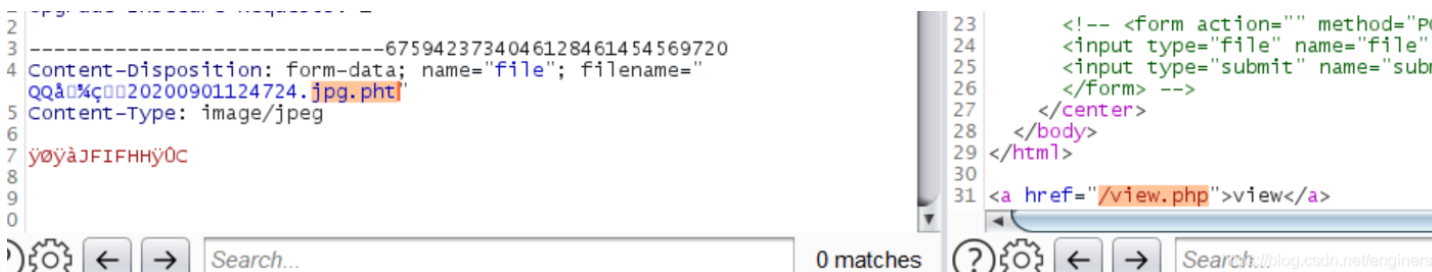
```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <meta charset="utf-8" />
5   <title>个人中心</title>
6 </head>
7 <body>
8 <center>
9 <!-- 存在漏洞需要去掉 -->
10 <!-- <form action="" method="POST" enctype="multipart/form-data">
11   <input type="file" name="file" />
12   <input type="submit" name="submit" value="上传" />
13 </form> -->
14 </center>
15 </body>
16 </html>
17
18
```

属于文件上传题型了，可以在本地写一个html文件，指向该地址



```
1.html - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<form action="http://7e69c56301d9458ba9d86130798a2767280065ffe499437f.changame.ichunqiu.com/" method="POST"
enctype="multipart/form-data">
  <input type="file" name="file" />
  <input type="submit" name="submit" value="上传" />
</form>
```

接下来用brup修改文件名，这里我打算连接蚁剑，试了php文件和jpg文件结合也不行，单个jpg文件也不行，看了网上的答案是
通过改文件后缀，不理解原因



```
2 -----
3 -----6759423734046128461454569720
4 Content-Disposition: form-data; name="file"; filename="
  QQ&0%ç0020200901124724.jpg.pht"
5 Content-Type: image/jpeg
6
7 yøÿàJFIFHHÿ0C
8
9
0
```

```
23 <!-- <form action="" method="PO
24 <input type="file" name="file"
25 <input type="submit" name="subm
26 </form> -->
27 </center>
28 </body>
29 </html>
30
31 <a href="/view.php">view</a>
```

php的可替代形式有php3, php4, php5, pht, phtml



最后是这个，file是变量，有过滤

