攻防世界-web-ics-07-从0到1的解题历程writeup

原创

CTF小白 于 2020-04-17 15:20:14 发布

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_41429081/article/details/105581272

题目分析

首先拿到题目描述：工控云管理系统项目管理页面解析漏洞

找到题目入口

点击view-source对源码进行审计

```
if (isset($_GET[page]) && $_GET[page] != 'index.php') {      include('flag.php');    }else {      header('Location: ?page=flag.php');    }
```

就是page参数不传index.php就会包含上flag.php，如果page参数为index.php就会跳转到page=flag.php

```
<?php     if ($_SESSION['admin']) {       $con = $_POST['con'];       $file = $_POST['file'];       $filename = "backup/".$file;       if(preg_match('/.+\.ph(p[3457]?|t|tml)$/i', $filename)){           die("Bad file extension");       }else{           chdir('uploaded');           $f = fopen($filename, 'w');           fwrite($f, $con);           fclose($f);       }     }     ?>
```

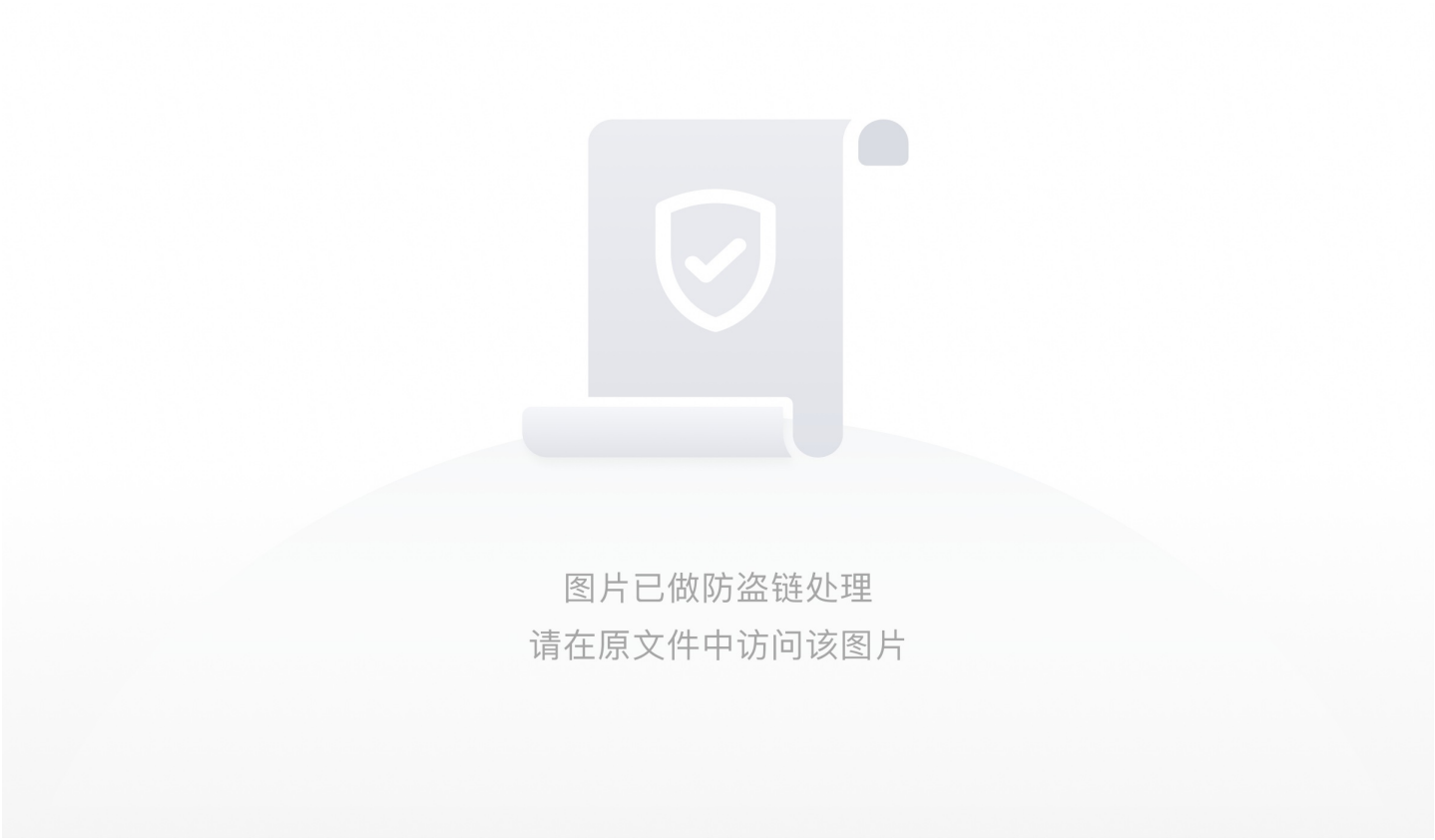
存在session admin为true，则可通过这边上传木马，但是可以发现的是，对文件名有一个正则，这个等会再看。首先看如何将session的admin设为true。

```
<?php      if (isset($_GET[id]) && floatval($_GET[id]) !== '1' && substr($_GET[id], -1) === '9') {        include 'config.php';        $id = mysql_real_escape_string($_GET[id]);        $sql="select * from cetc007.user where id='$id'";        $result = mysql_query($sql);        $result = mysql_fetch_object($result);      } else {        $result = False;        die();      }      if(!$result)die("<br >something wae wrong ! <br>");      if($result){        echo "id: ".$result->id."</br>";        echo "name:".$result->user."</br>";        $_SESSION['admin'] = True;      }      ?>
```

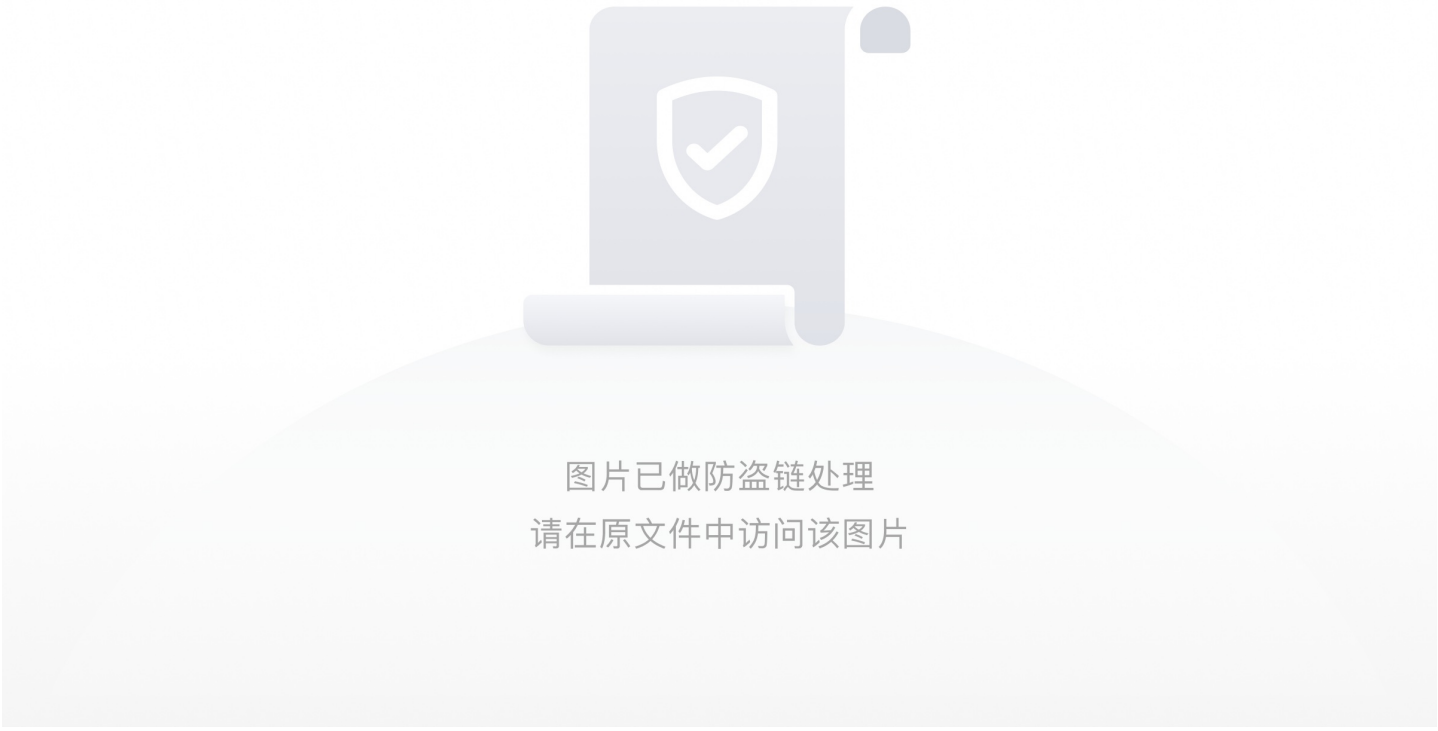
存在参数id，且参数不为1且最后一位为9。会去执行查找项目功能。

解题流程

随意输入id为9查看反馈为

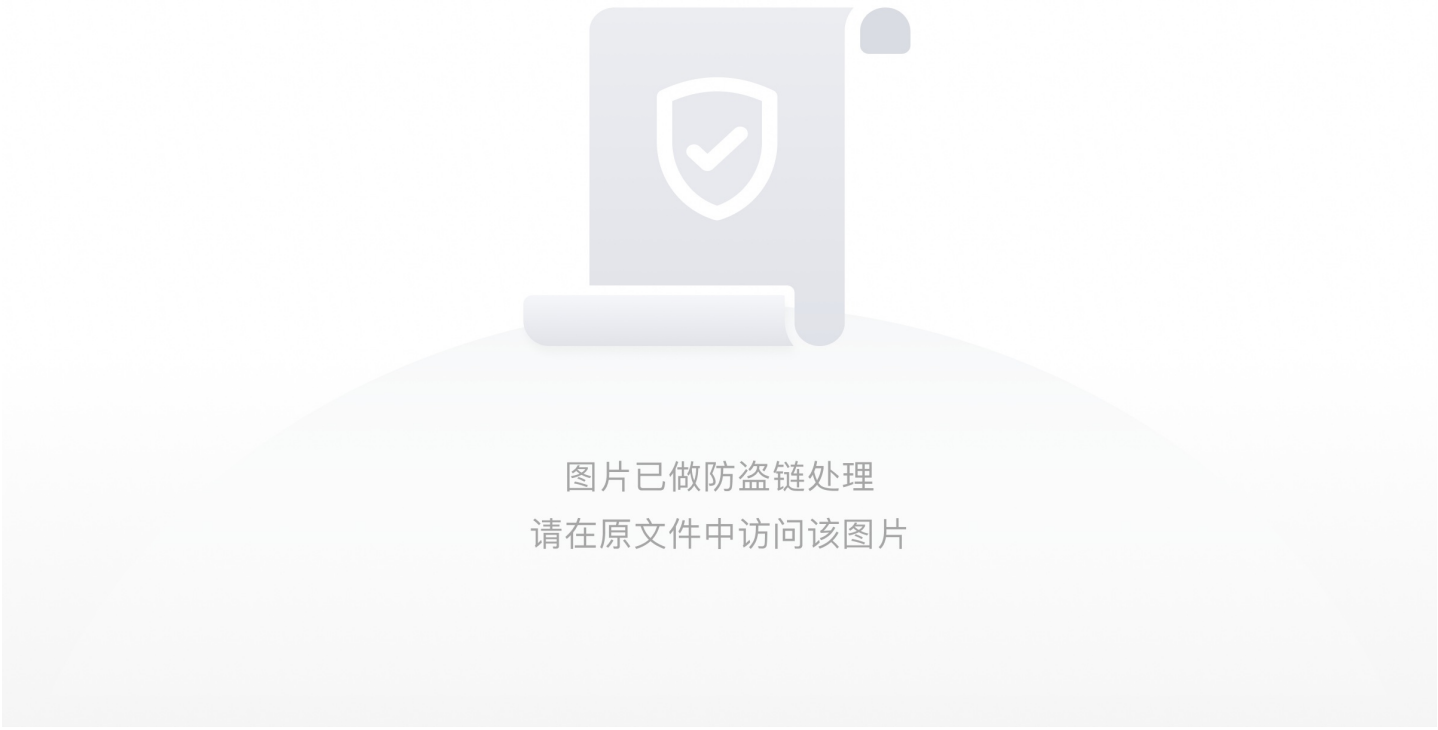


这边尝试了一下



发现1 9即可绕过。因为显然floatval($_GET[id]) !== '1’这是不等的，因为结果数据类型不同。然后最后一位为9.

然后本地数据库跑一下



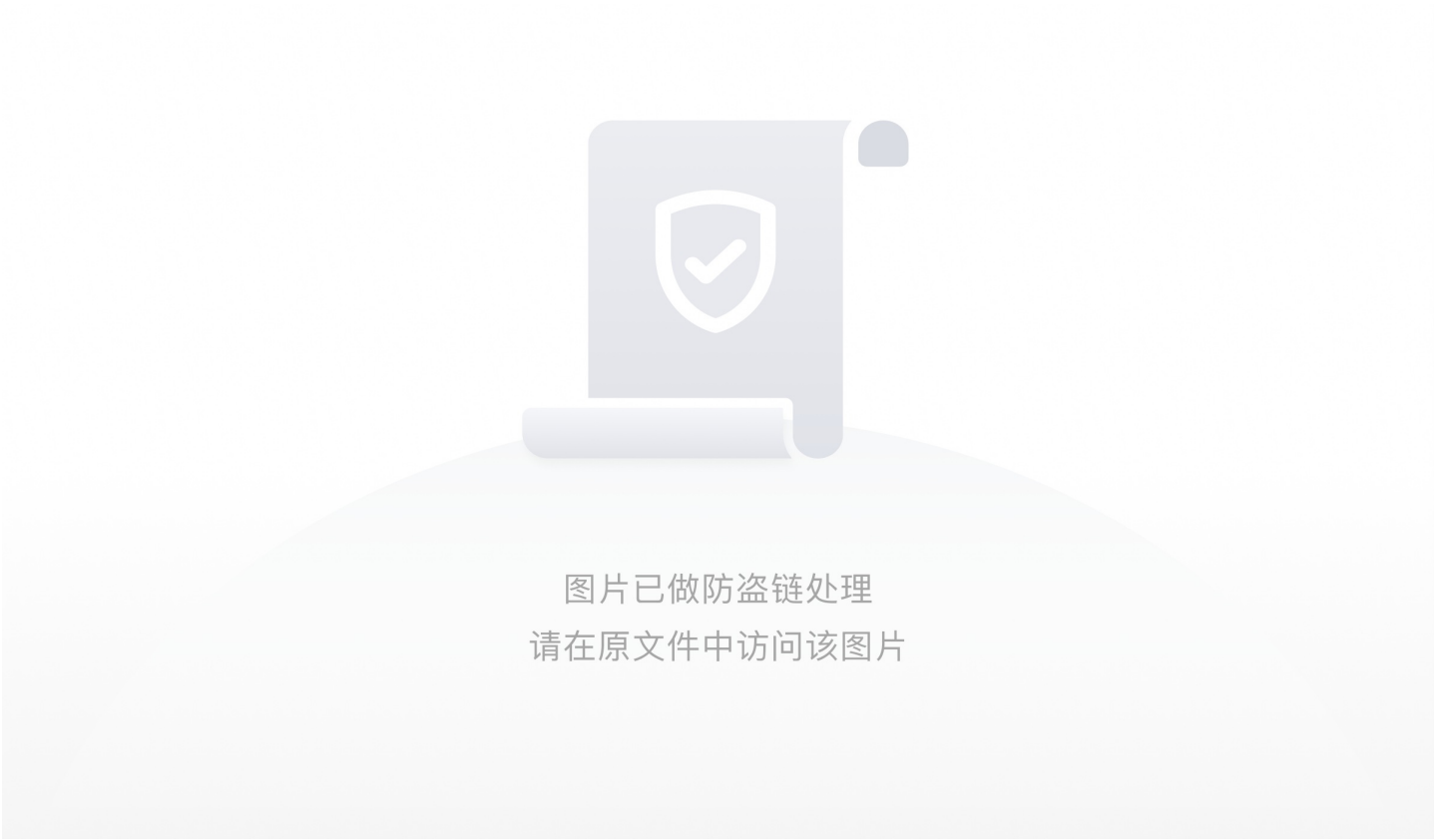
转为int类型直接就是1。所以直接能查出admin的那一条记录。

然后尝试去上传界面上传getshell

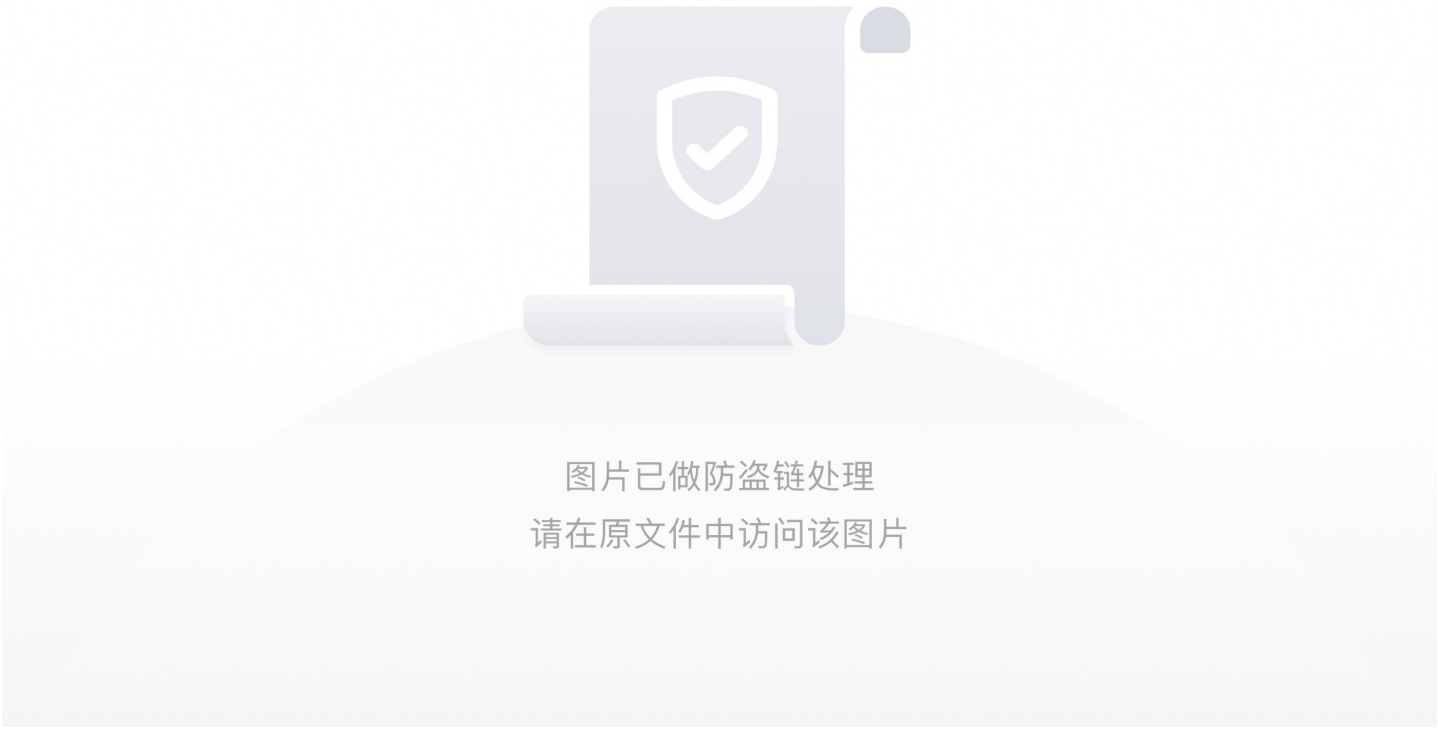
```
<?php if ($_SESSION['admin']) { $con = $_POST['con']; $file = $_POST['file']; $filename = "backup/".$file; if(preg_match('/.+\.ph(p[3457]?|t|tml)$/i', $filename)){ die("Bad file extension"); }else{ chdir('uploaded'); $f = fopen($filename, 'w'); fwrite($f, $con); fclose($f); } } ?>
```

可以发现post两个参数分别为con是文件内容，file为文件名。
然后尝试绕过正则

preg_match('/.+.ph(p[3457]?|t|tml)/i, filename)个人理解是。。这个需要绕过吗，直接上传配置文件，解析别的后缀名为php不就好了吗。

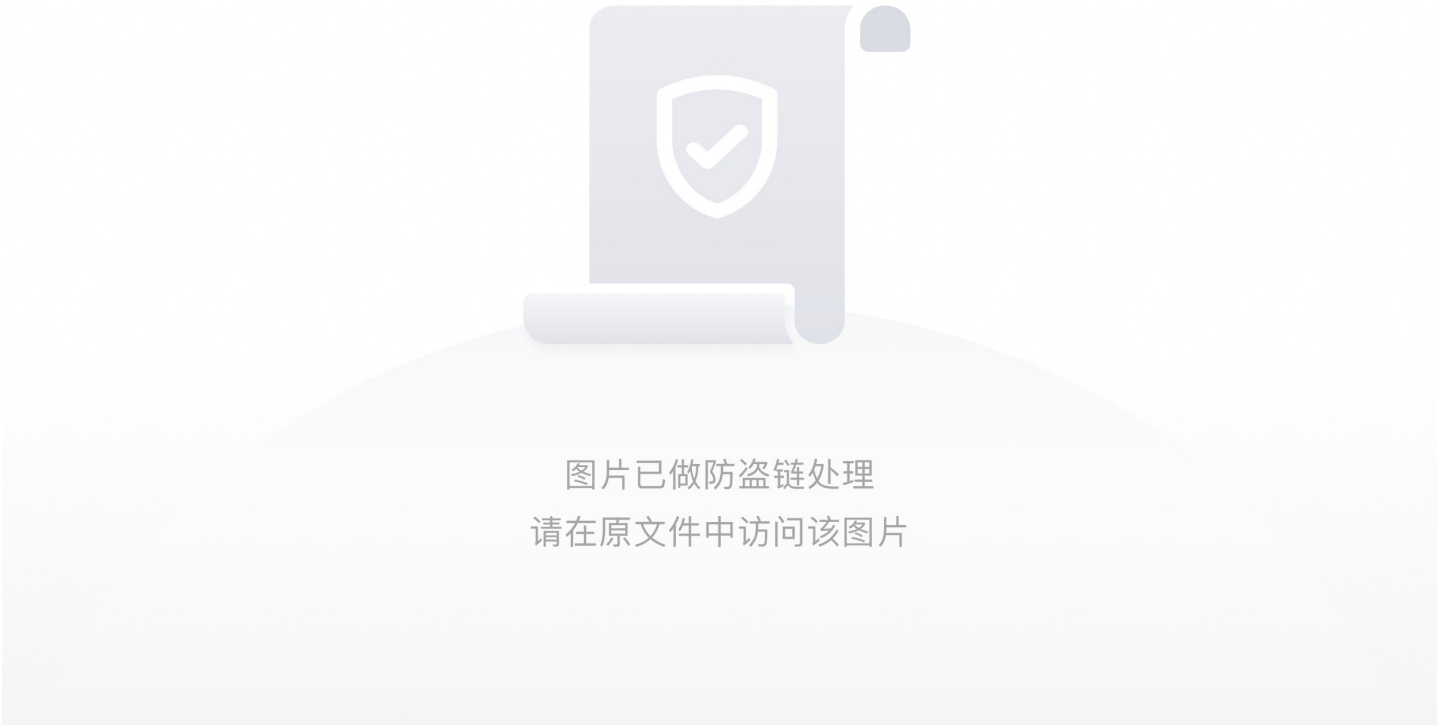


首先存在.htaccess文件

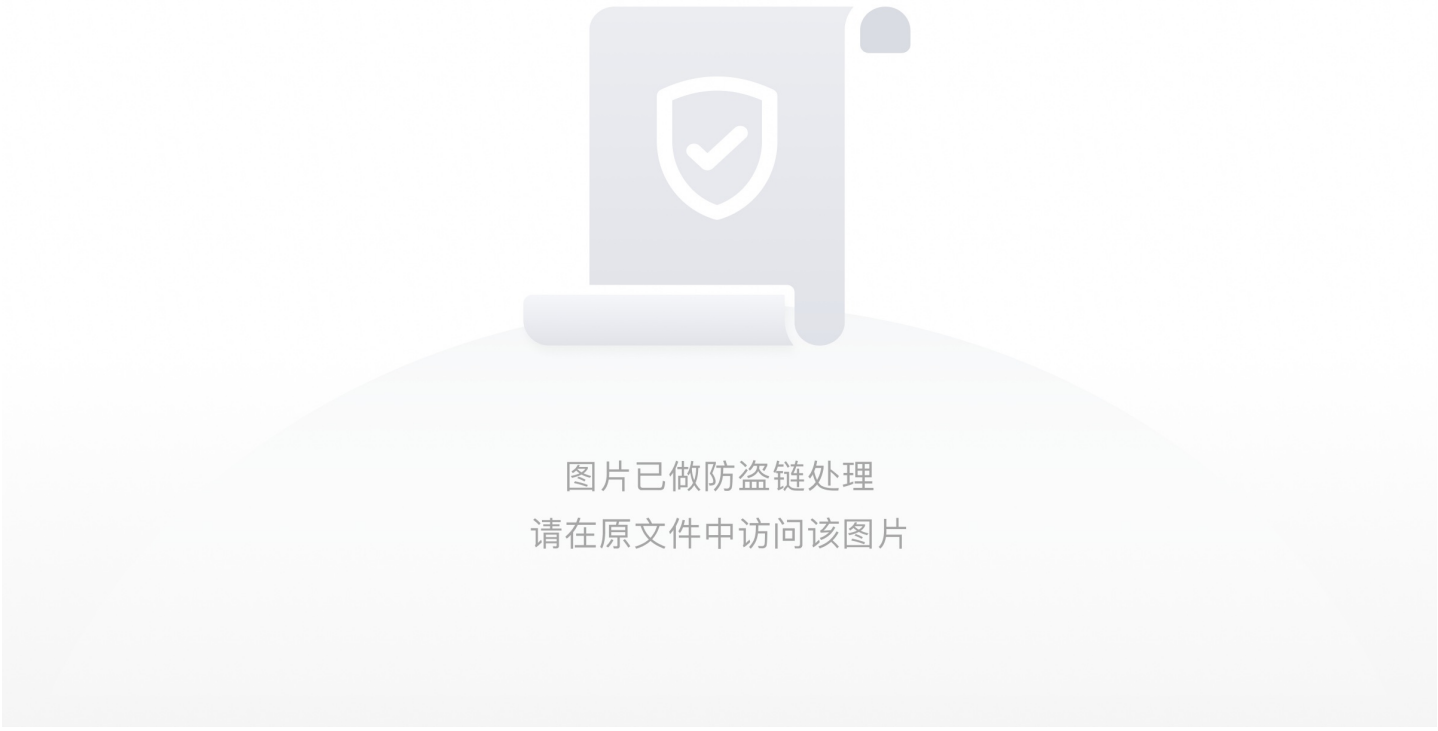


上传一句话木马。

上传覆盖.htaccess



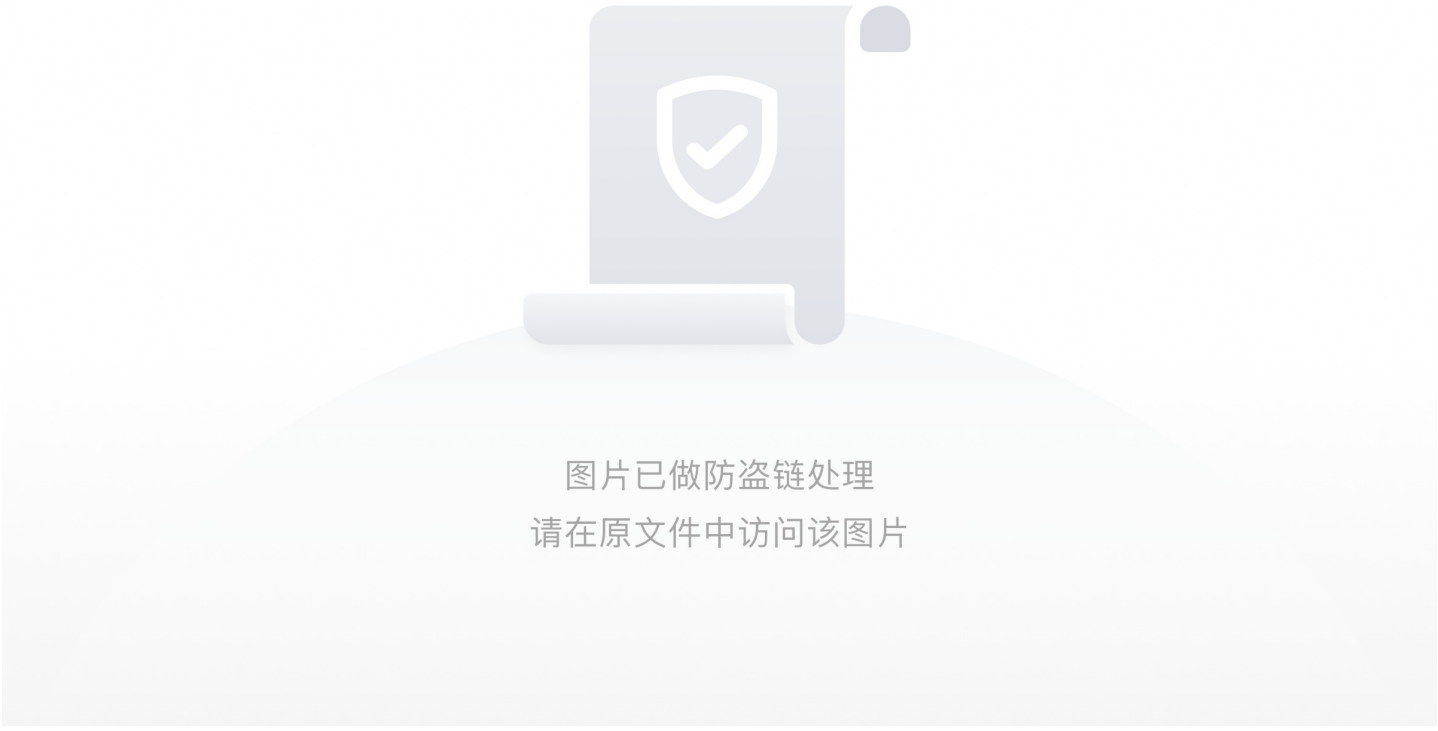
但是发现.jpg文件并没有被作为可执行文件执行



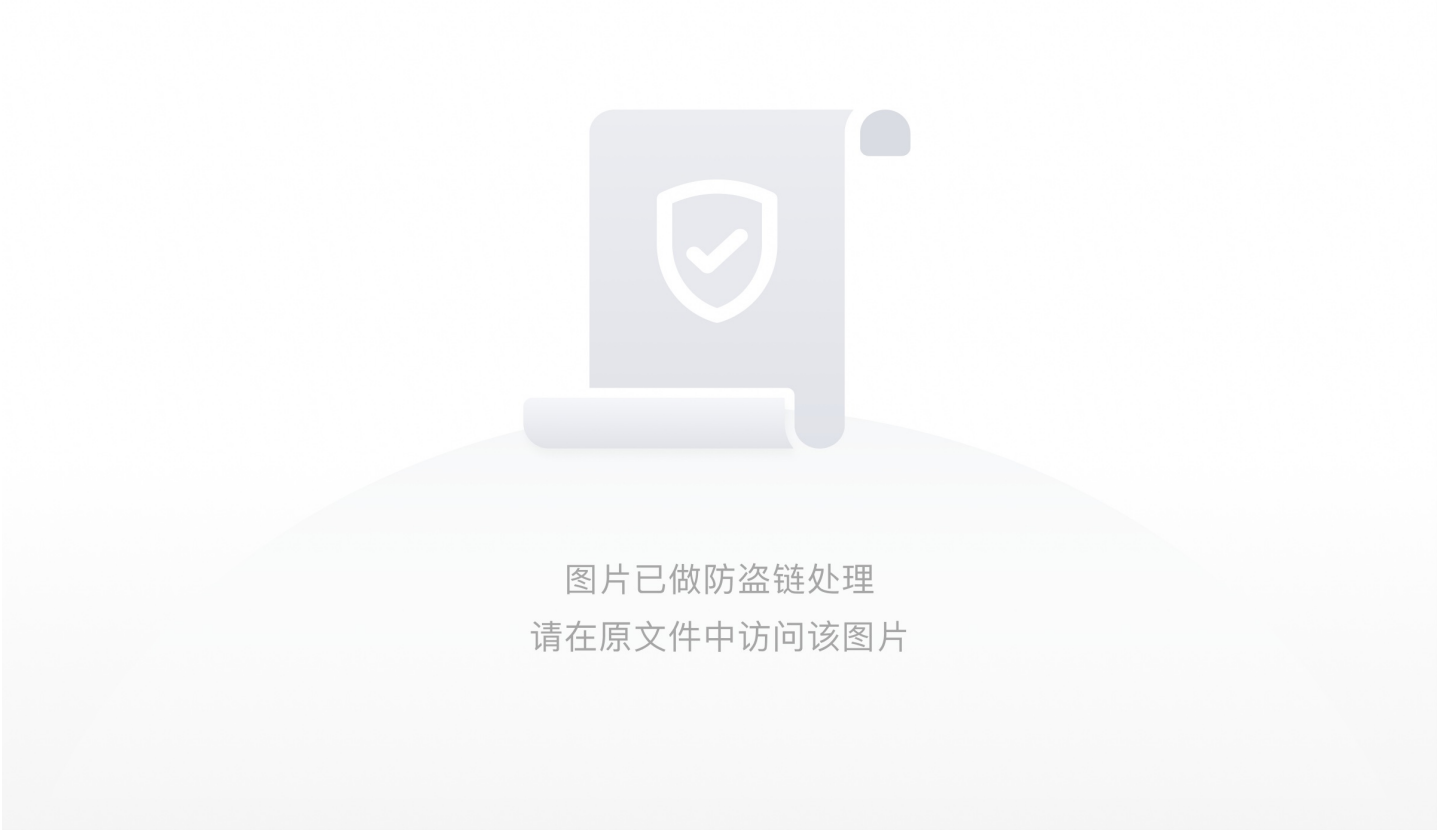
那应该是

.htaccess没有写权限吧。

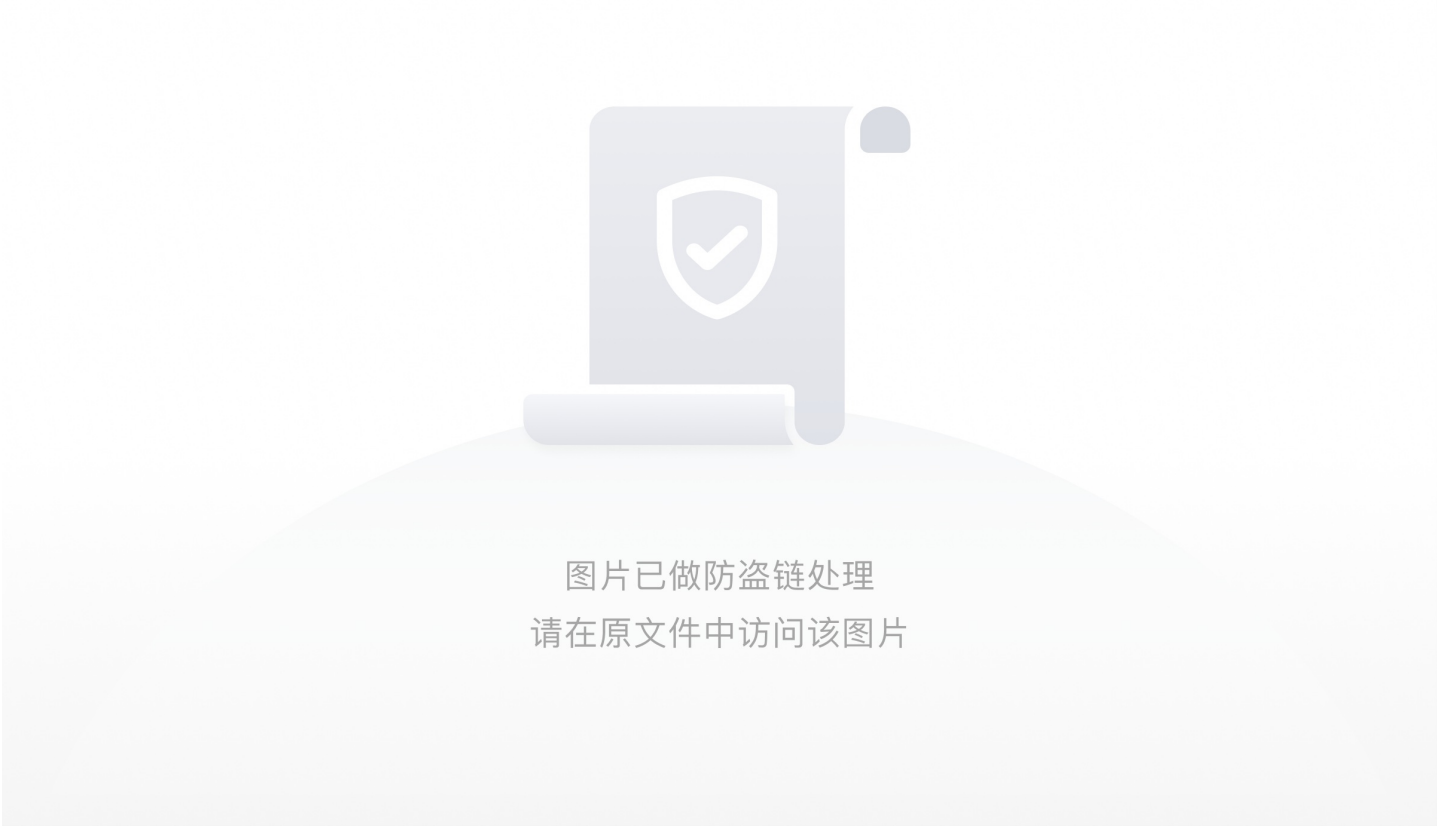
找先知上一些上传绕过的方法



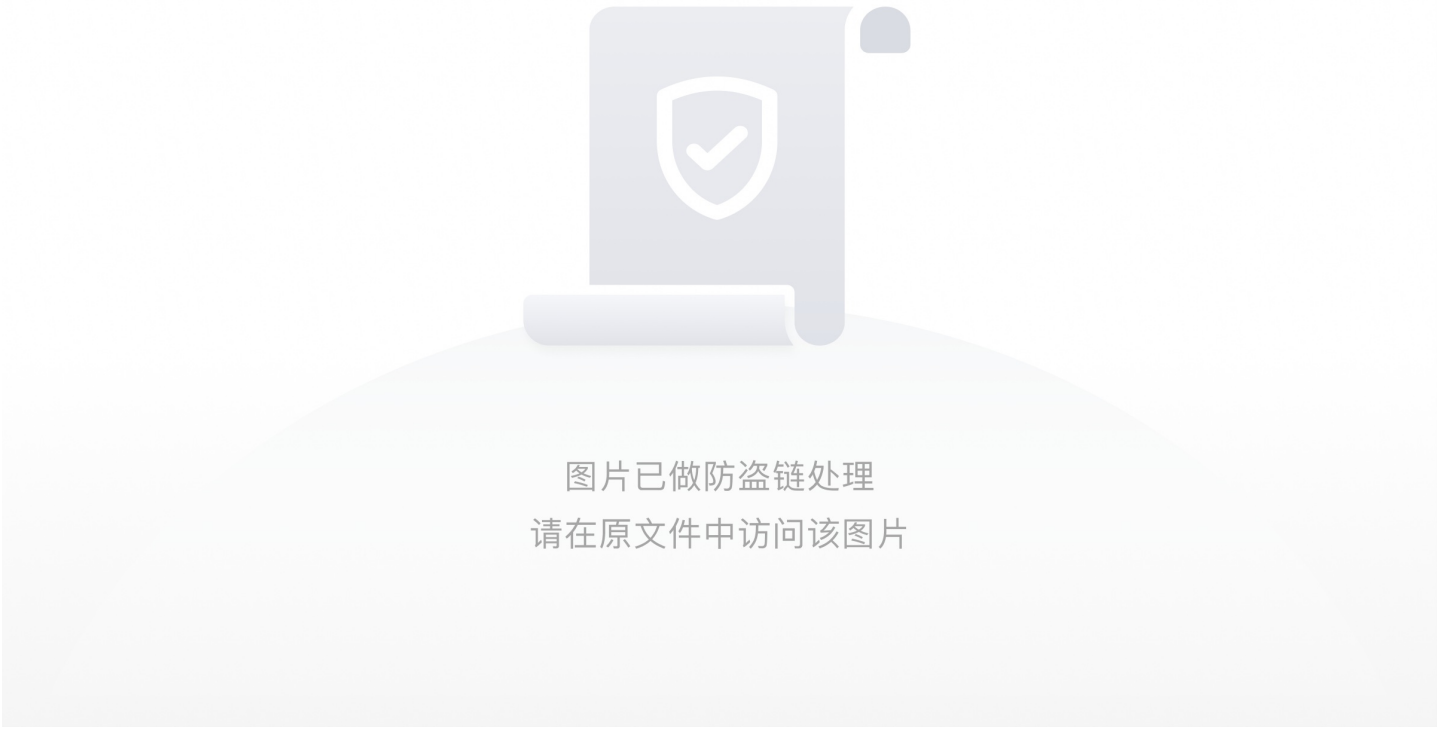
因为获取文件后缀进行正则匹配的时候，只会匹配最后一个.后的内容，所以通过php/.绕过



蚁剑连上去发现找到flag即可



神奇的是，发现成功上传了.htaccess文件，但是并没有能把jpg文件解析了emmm



望大佬告知~