## 前端过滤

<script>

var obj = document.getElementById("file");

var array = new Array('gif','jpeg','png','jpg'); //allow type

if( obj.value == '' ){

alert("文件不能为空");

return false;

}

else{

var fileContentType = obj.value.match(/^(.\*)(\.)(.{1,8})$/)[3]; //get type

for( var i in array){

if(fileContentType.toLowerCase() == array[i].toLowerCase() )

return true;

}

alert("上传的图片类型只能为: gif, jpeg, png, jpg");

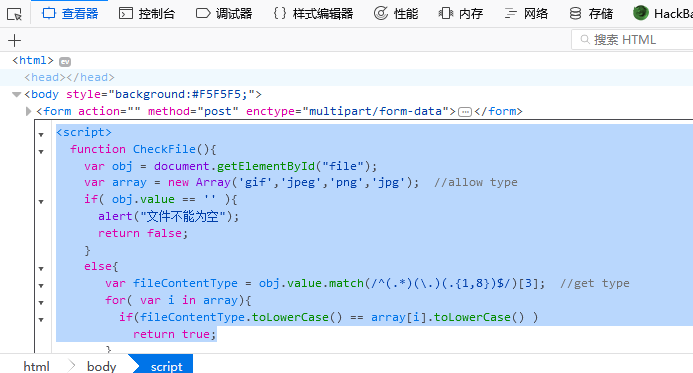
return false;

}

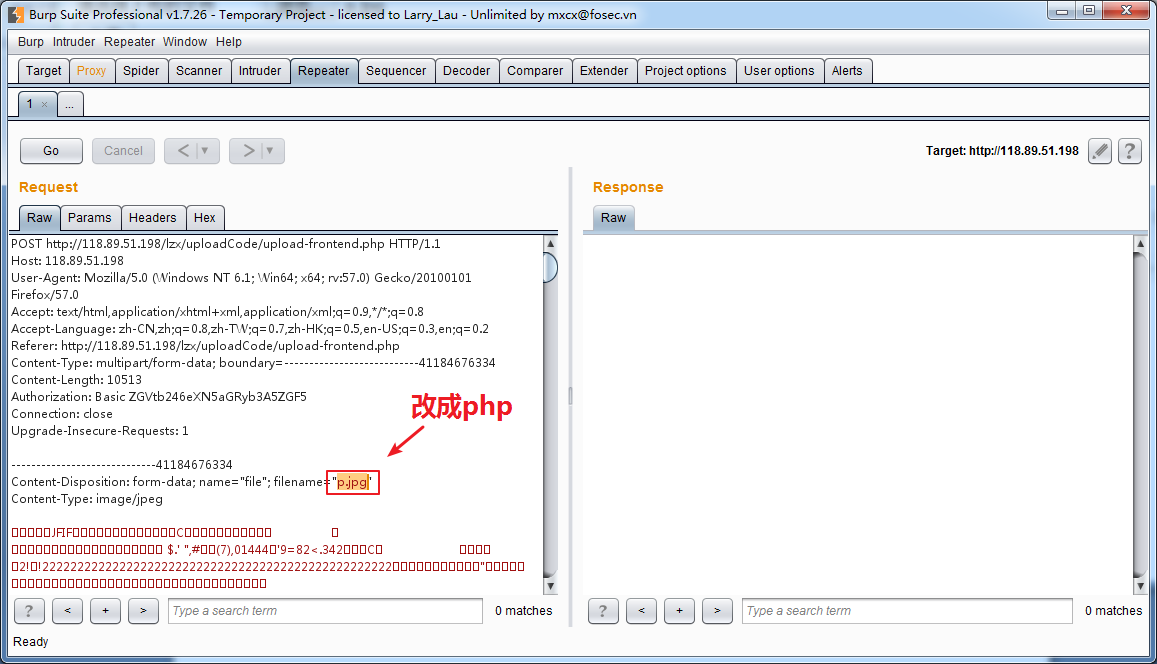
}

</script>

方法一，直接修改或者删除js代码



方法二，上传合法类型jpg，然后burp修改php类型



## 后台MIME类型过滤

<?php

$uploaddir = 'uploadfiles/';

if (isset($\_POST['submit'])) {

if (file\_exists($uploaddir)) {

if (($\_FILES['upfile']['type'] == 'image/gif') || ($\_FILES['upfile']['type'] == 'image/jpeg') ||

($\_FILES['upfile']['type'] == 'image/png') || ($\_FILES['upfile']['type'] == 'image/bmp')

) {

if (move\_uploaded\_file($\_FILES['upfile']['tmp\_name'], $uploaddir . '/' . $\_FILES['upfile']['name'])) {

echo '文件上传成功，保存于：' . $uploaddir . $\_FILES['upfile']['name'] . "\n";

}

} else {

echo '文件类型不正确，请重新上传！' . "\n";

}

} else {

exit($uploaddir . '文件夹不存在,请手工创建！');

}

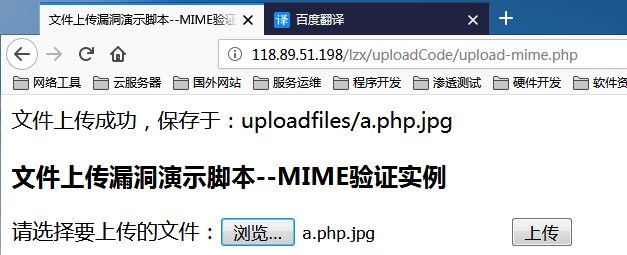
//print\_r($\_FILES);

}

?>

方法一：对于linux系统可以利用解析漏洞

上传a.php.jpg命名的木马文件



方法二：burp抓包修改mime类型application/octet-stream为img/jpeg

如果不是Linux系统，上面方法无效



## 后台后缀类型过滤

<?php

$uploaddir = 'uploadfiles/';

if (isset($\_POST['submit'])) {

if (file\_exists($uploaddir)) {

$deny\_ext = array('.asp', '.php', '.aspx', '.jsp');

$file\_ext = strrchr($\_FILES['upfile']['name'], '.');

if (!in\_array($file\_ext, $deny\_ext)) {

if (move\_uploaded\_file($\_FILES['upfile']['tmp\_name'], $uploaddir . '/' . $\_FILES['upfile']['name'])) {

echo '文件上传成功，保存于：' . $uploaddir . $\_FILES['upfile']['name'] . "\n";

}

} else {

echo '此文件不允许上传' . "\n";

}

} else {

exit($uploaddir . '文件夹不存在,请手工创建！');

}

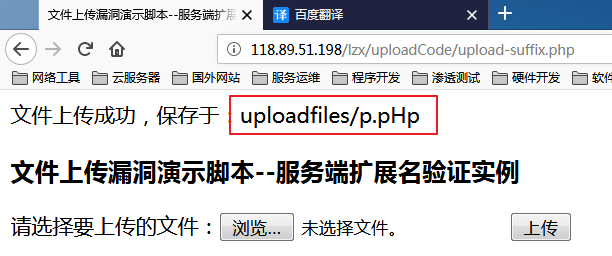
}

?>

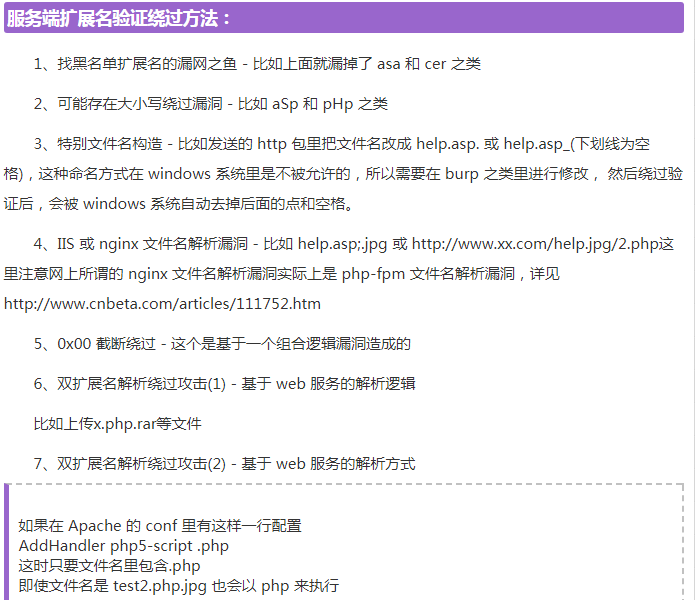
方法一：利用Linux的Apache解析漏洞

上传文件名为a.php.jpg就可以被解析成php文件

方法二：大小写混用，上传 p.pHP



其他绕过方法：



## 后台内容检测

<?php

$uploaddir = 'uploadfiles/';

if (isset($\_POST['submit'])) {

if (file\_exists($uploaddir)) {

$file\_name = $\_FILES['upfile']['tmp\_name'];

$allow\_ext = array('image/png', 'image/gif', 'image/jpeg', 'image/bmp');

$img\_arr = getimagesize($file\_name);

$file\_ext = $img\_arr['mime'];

if (in\_array($file\_ext, $allow\_ext)) {

if (move\_uploaded\_file($\_FILES['upfile']['tmp\_name'], $uploaddir . '/' . $\_FILES['upfile']['name'])) {

echo '文件上传成功，保存于：' . $uploaddir . $\_FILES['upfile']['name'] . "\n";

}

} else

echo '此文件不允许上传' . "\n";

} else

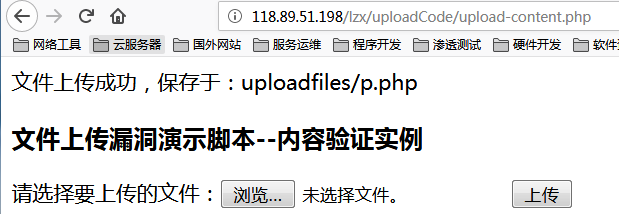
exit($uploaddir . '文件夹不存在,请手工创建！');

}

?>

这种只需要做图片木马，不用修改mime直接上传php文件即可

copy /b 1.php + 1.jpg p.php



00截断绕过

