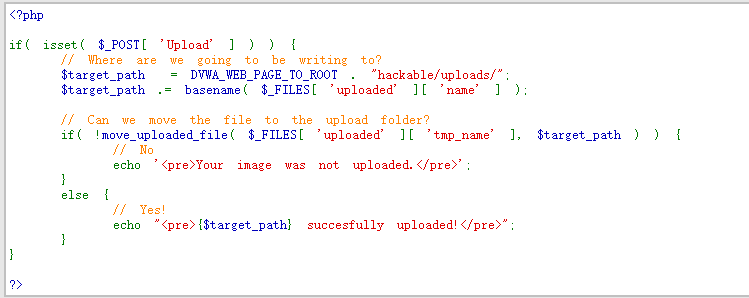
# File Upload文件上传

文件上传，顾名思义就是上传文件的功能行为，之所以会被发展为危害严重的漏洞，是程序没有对访客提交的数据进行检验或者过滤不严，可以直接提交修改过的数据绕过扩展名的检验。文件上传漏洞是漏洞中最为简单猖獗的利用形式，一般只要能上传获取地址，可执行文件被解析就可以获取系统WebShell

## 文件上传漏洞

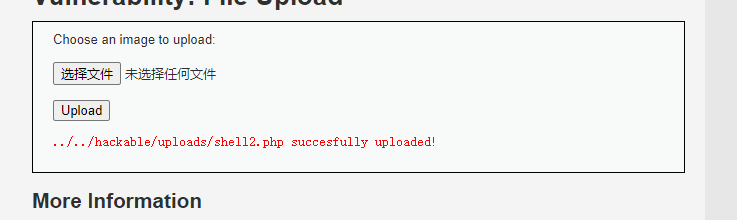
通常是由于对上传文件的类型、内容没有进行严格的过滤、检查，使得攻击者可以通过上传木马获取服务器的webshell权限，因此文件上传漏洞带来的危害常常是毁灭性的。

# Level：Low

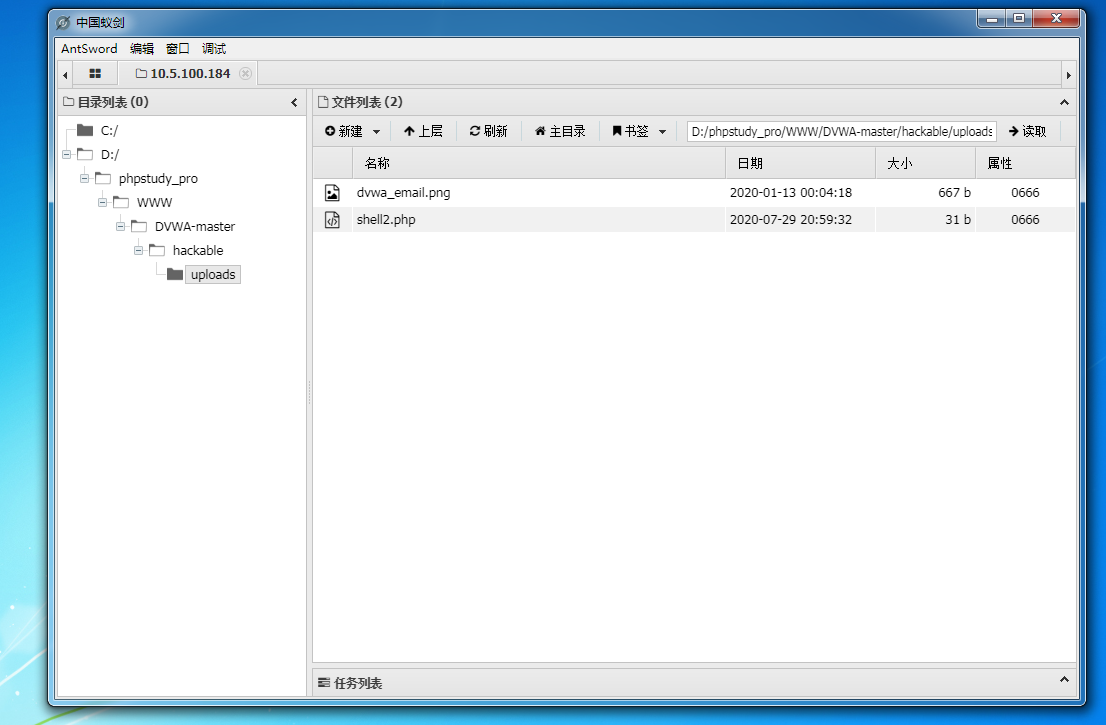


这段源码没有对上传的文件类型和内容没有过滤和检查，存在上传成功之后会返回路径信息

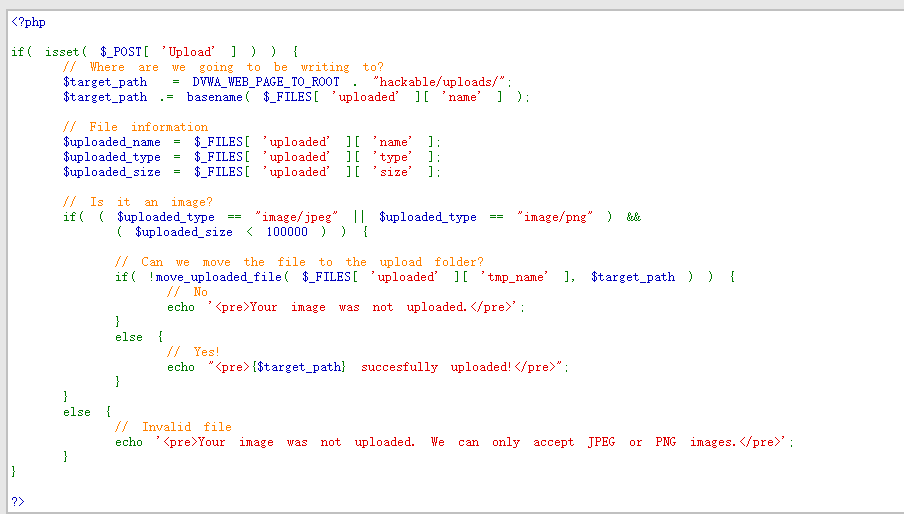
上传一个php文件用POST请求的一句话木马<?php @eval($\_POST[‘shell’])?>



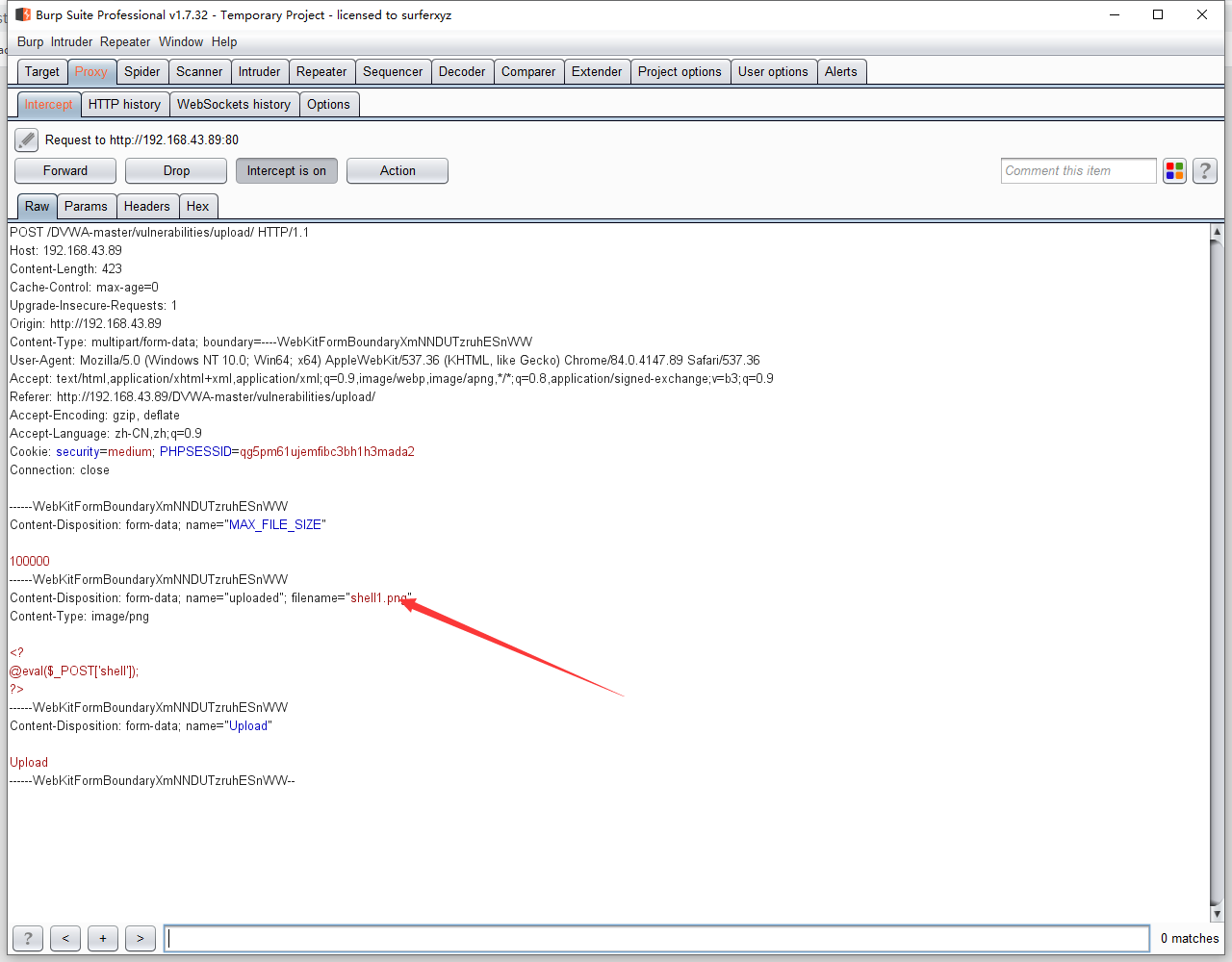
知道路径之后使用蚁剑进入

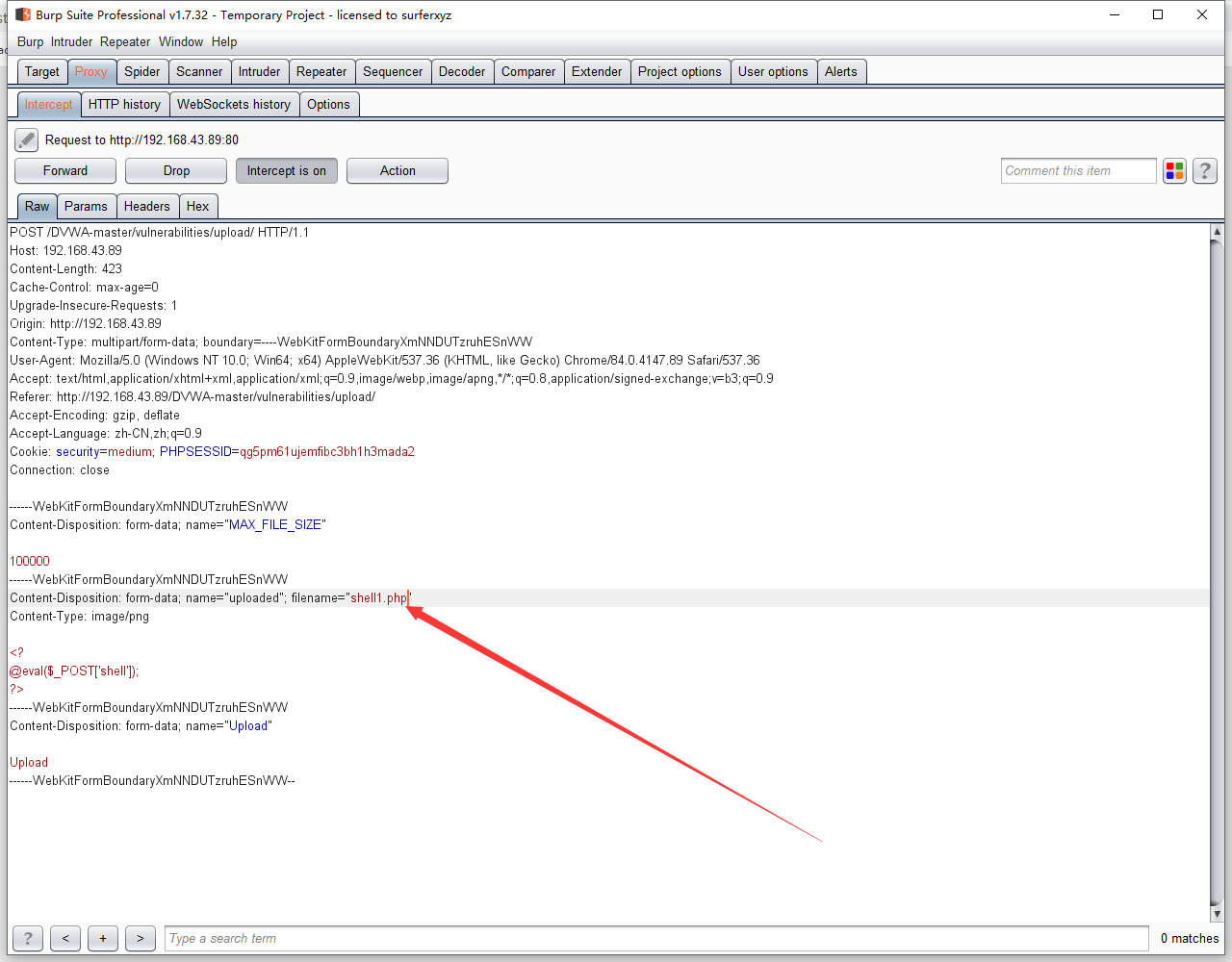


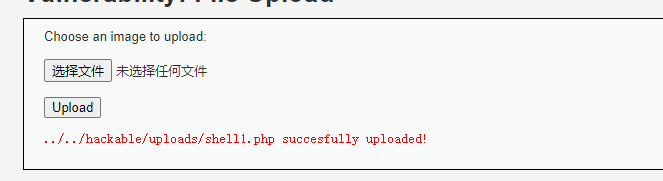
# Level:Medium



Medium等级的源码给上传的文件加了限制只能是image/jpeg或者iamage/png格式的文件，并且大小不能超过1M，这时候可以用BP抓包修改文件的后缀



改为php格式然后放包

成功绕过再用蚁剑来来激活

