**通达OA任意用户登录和后台GetShell漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

通达OA任意用户登录漏洞可以登录到管理员，然后后台上传PHP文件导致远程命令执行。

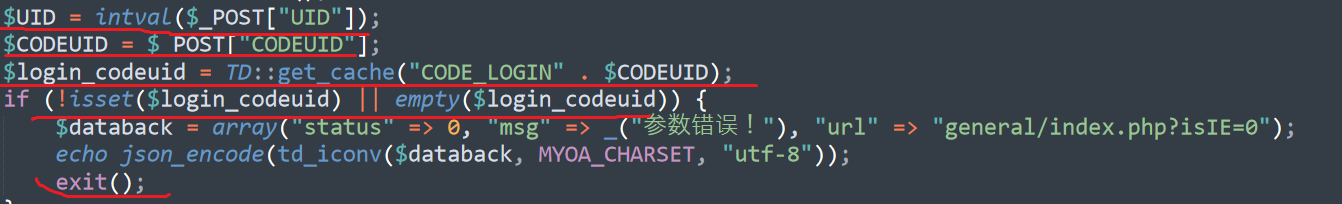
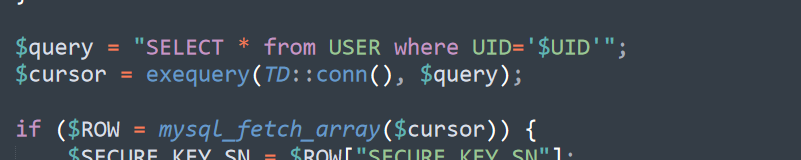
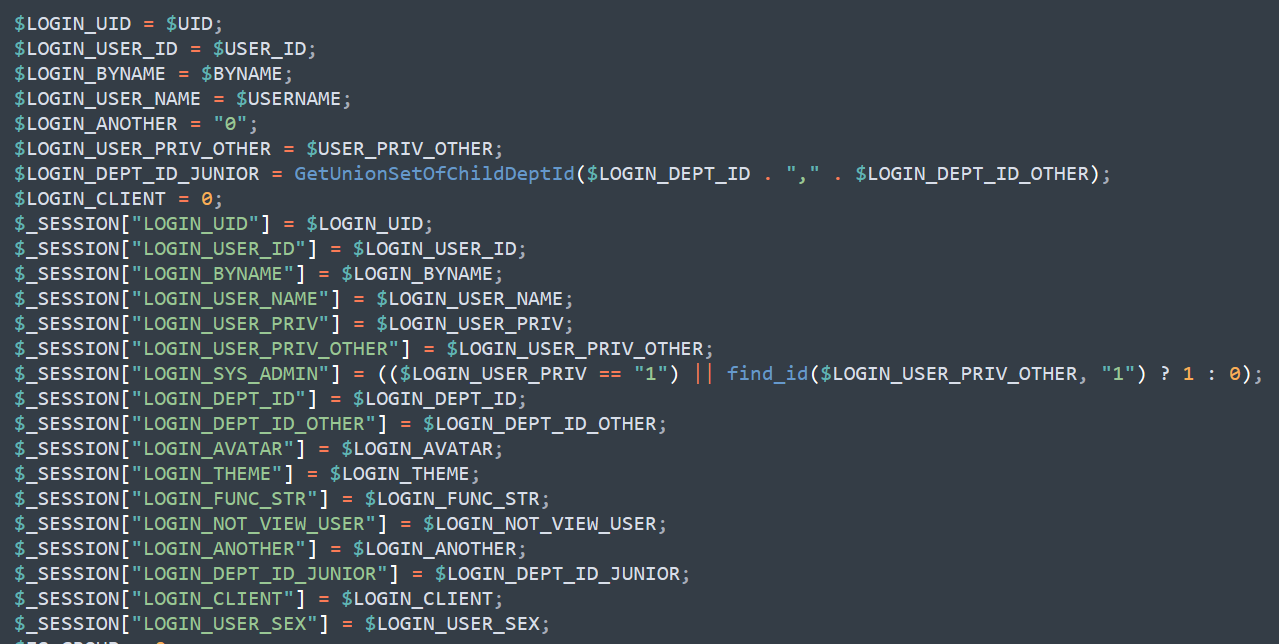
# 二、机理分析

## 1、任意用户登录漏洞

**影响版本：**通达OA-MYOA2017

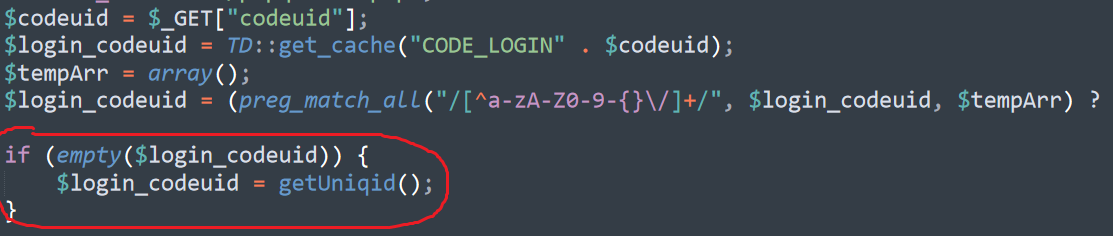
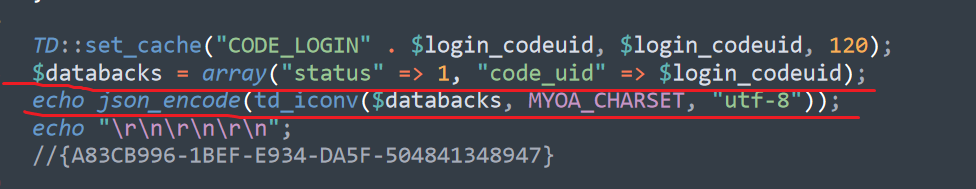
**漏洞编号：**无

1.分析一下存在漏洞文件 logincheck\_code.php

从代码中我们可以控制的有UID,CODEUID然后判断$login\_codeuid是否存在，不存在或者为空就退出，然后将获取的UID，带入到sql语句进行查询，后面会验证查询的结果，如果信息核对正确，则将个人信息放入到SESSION中，UID=1的时候默认是管理员，而UID我们可以输入一个1，就可以满足查询ql,而我们现在要绕过if (!isset($login\_codeuid) || empty($login\_codeuid)){exit();}，全局搜索一下$login\_codeuid可不可以控制

2.分析一下/general/login\_code.php，发现存在$login\_codeuid

如果$login\_codeuid为空，则给$login\_codeuid赋一个随机值，并且使用echo打印出来

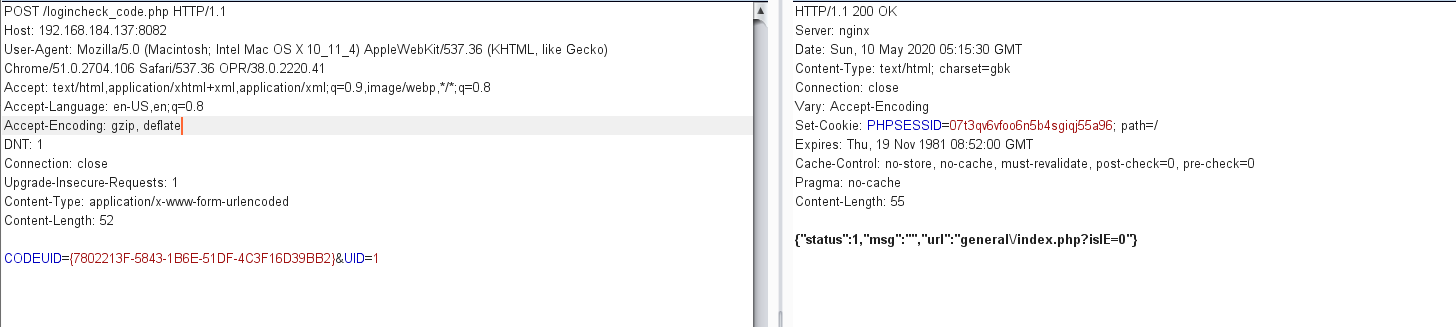
3.那我们的思路是:先去访问/general/login\_code.php,获得$login\_codeuid,再去访问logincheck\_code.php，同时POST传入获取的$login\_codeuid和UID=1,获得返回包的PHPSESSID,在使用火狐浏览器伪造COOKiE,登录后台

# 三、攻击路径

先去访问/general/login\_code.php,获得$login\_codeuid,再去访问logincheck\_code.php，同时POST传入获取的$login\_codeuid和UID=1,获得返回包的PHPSESSID,在使用火狐浏览器伪造COOKiE,登录后台



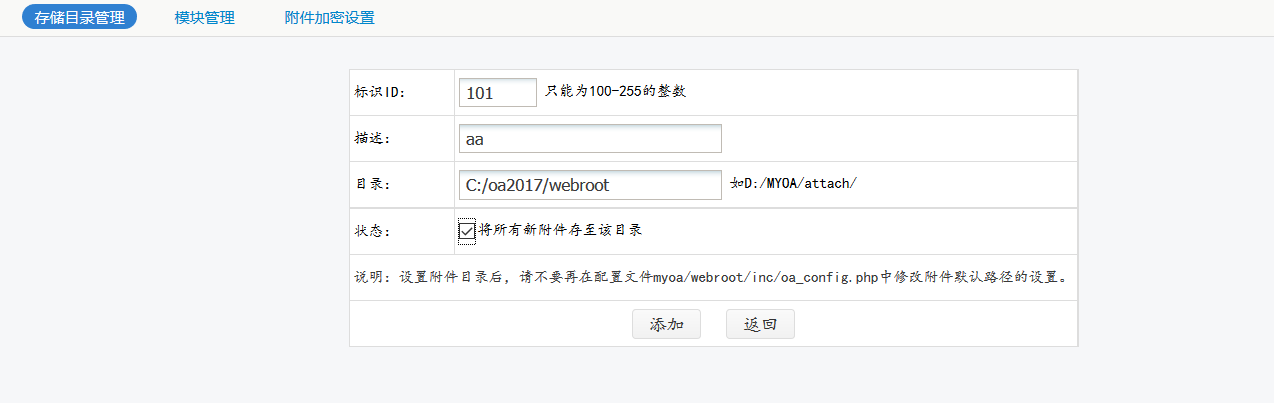
将获得的code\_uid保存下来，进行下一步



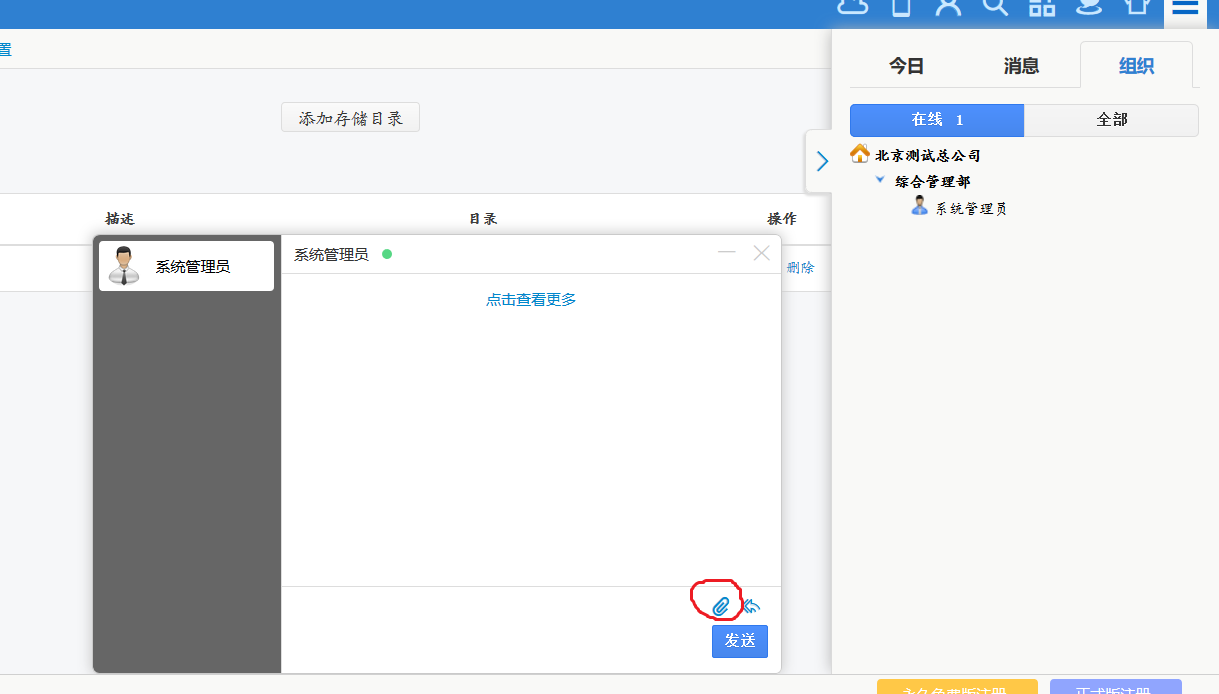
将获取的PHPSESSID保存下来，使用火狐浏览器伪造COOKIE，同时访问/general/index.php，便可以进入后台



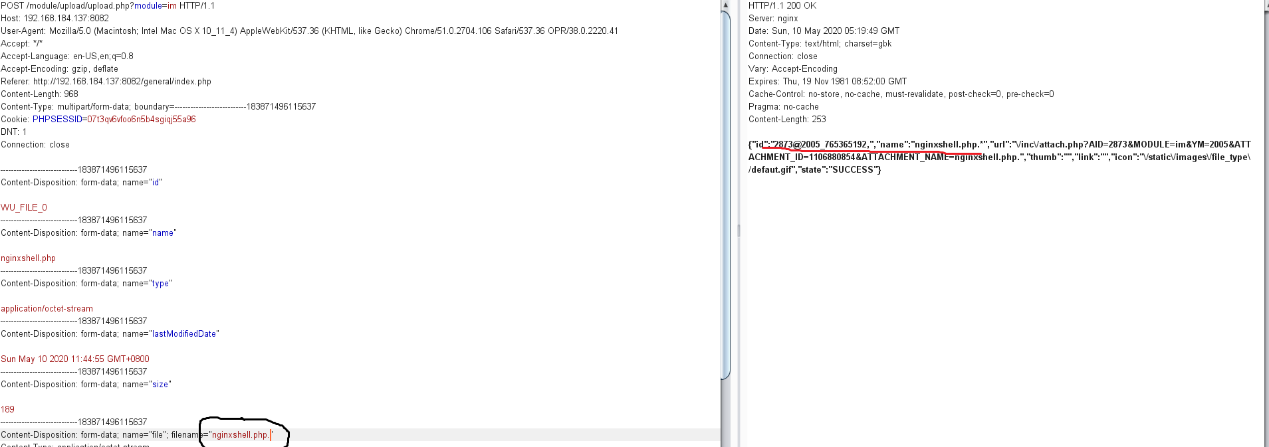
后台GetShell(靶机环境windows7 通道OA用的是MYOA2017)

依次点击系统管理-附件管理-添加存储目录，选择根目录  
  


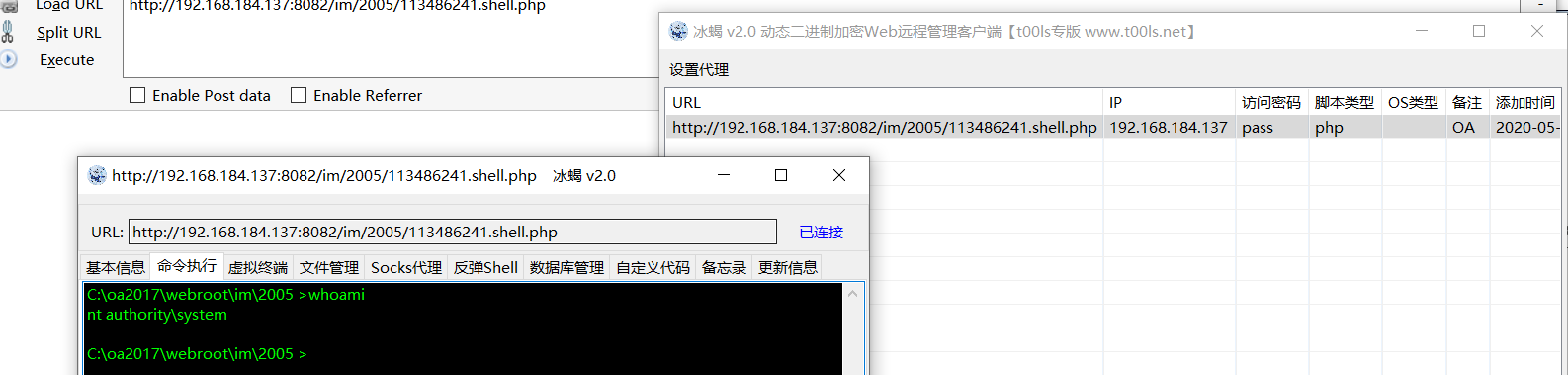
依次点击组织-系统管理员-附件(下图标注)



直接上传shell.php不能成功，开启抓包，上传shell.php.进行绕过，windows系统会自动去掉.，不符合windows的命名



使用冰蝎进行连接



实战(由以上的思路，进入到某站的OA后台管理系统)



# 四、防御方案

升级通达 OA 到最新版