**通达OA11.6远程代码执行漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

通达OA11.6存在任意文件删除和任意文件上传，其中inc/auth.inc.php用于校验用户是否登录，所以在第一步任意文件删除时，删除了该文件导致未授权RCE。

# 二、机理分析

## 1、远程代码执行漏洞

**影响版本：**11.6

**漏洞编号：**无

### 1.任意文件删除

根据网传的Exploit，可以看到首先调用

/module/appbuilder/assets/print.php

接口，具体代码如下：

<?php  
$s\_tmp = \_\_DIR\_\_ . '/../../../../logs/appbuilder/logs';$s\_tmp .= '/' . $\_GET['guid'];if (file\_exists($s\_tmp)) { $arr\_data = unserialize(file\_get\_contents($s\_tmp)); unlink($s\_tmp); $s\_user = $arr\_data['user'];}

其实是将传入guid的值作为文件删除，当前操作路径为：D:/MYOA/logs/app/appbuilder/logs/所以想删除web文件，需要构造:

../../../../webroot/web文件名

### 2.任意文件上传

然后调用了/general/data\_center/utils/upload.php进行上传，看到代码如下：

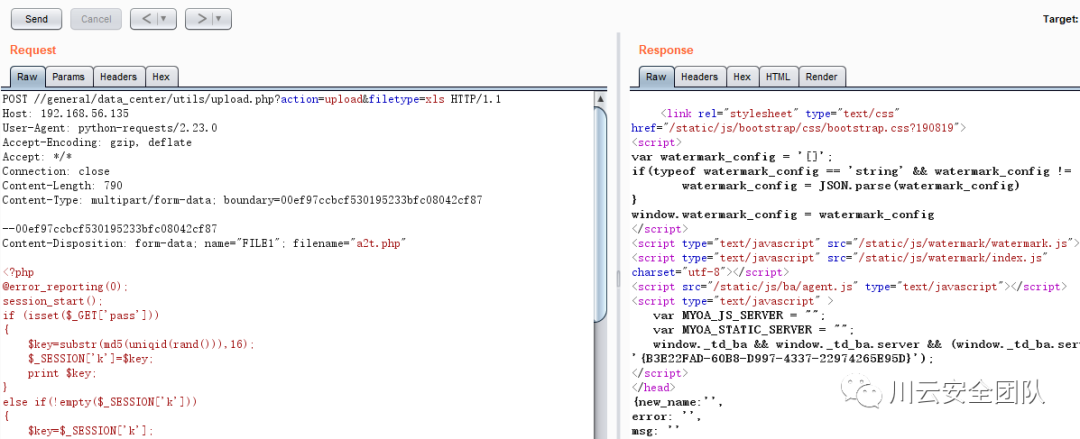
<?php  
include\_once 'inc/auth.inc.php';include\_once './utils.func.php';$HTML\_PAGE\_TITLE = \_('上传文件');include\_once 'inc/header.inc.php';

其中inc/auth.inc.php用于校验用户是否登录，所以在第一步任意文件删除时，删除了该文件导致未授权RCE。

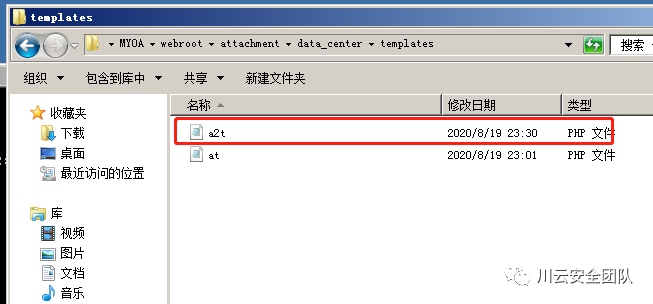
接着看代码：

<?php...if ($action == 'upload') { if ($filetype == 'xls') { $uploaddir = MYOA\_ATTACH\_PATH . '/data\_center/templates/'; if (!is\_dir(MYOA\_ATTACH\_PATH . '/data\_center/templates')) { if (!is\_dir(MYOA\_ATTACH\_PATH . '/data\_center')) { mkdir(MYOA\_ATTACH\_PATH . '/data\_center'); } mkdir(MYOA\_ATTACH\_PATH . '/data\_center/templates'); } if (move\_uploaded\_file($\_FILES['FILE1']['tmp\_name'], $uploaddir . $\_FILES['FILE1']['name'])) { } }

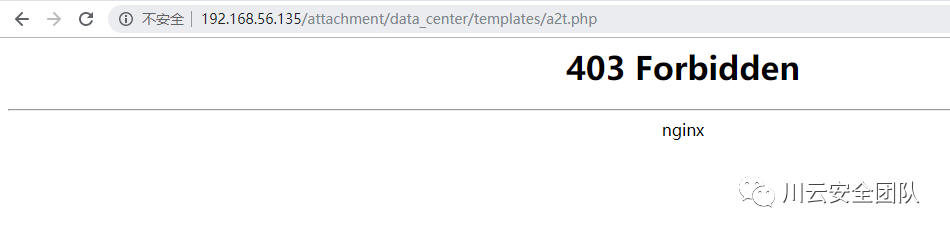
当$action为upload时，且filetype为xls时，也时可以任意文件上传的。其中MYOA\_ATTACH\_PATH 全局变量的值为：D:/MYOA/webroot/attachment/也在web目录下，尝试调用该点进行上传：



然后到服务器中查看：



访问shell：



发现D:/MYOA/webroot/attachment目录下默认没有执行权限，继续往下看逻辑：

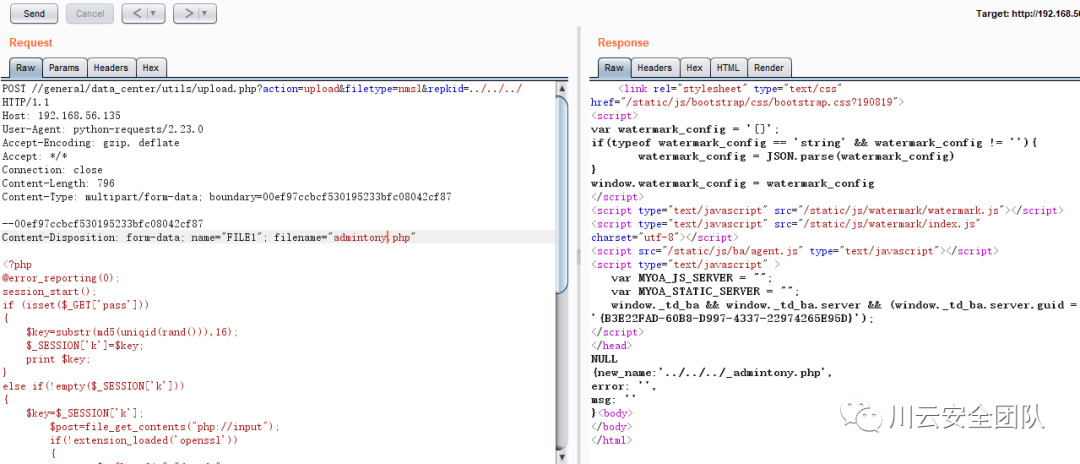
当filetype不为xls或img 时会执行以下代码：

// 46行开始if (isset($from\_rep)) { if ($from\_rep != '' && $from\_rep[0] == '{') { $repkid = GetRepKIDBySendId($from\_rep); if ($repkid != $to\_rep) { if (file\_exists($uploaddir . '/' . $repkid . '\_' . $filename)) { copy($uploaddir . '/' . $repkid . '\_' . $filename, $uploaddir . '/' . $to\_rep . '\_' . $filename); } } } else { $arr = explode(',', $from\_rep); for ($i = 0; $i < count($arr); $i++) { $p = strpos($arr[$i], '.'); $repno = substr($arr[$i], 0, $p); $repkid = GetRepKIDByNo($repno); if ($repkid != $to\_rep) { if (file\_exists($uploaddir . '/' . $repkid . '\_' . $filename)) { copy($uploaddir . '/' . $repkid . '\_' . $filename, $uploaddir . '/' . $to\_rep . '\_' . $filename); break; } } } }}else { $s\_n = $\_FILES['FILE1']['name']; if ($s\_n[0] != '{') { $s\_n = $repkid . '\_' . $s\_n; } if (move\_uploaded\_file($\_FILES['FILE1']['tmp\_name'], $uploaddir . $s\_n)) { }}

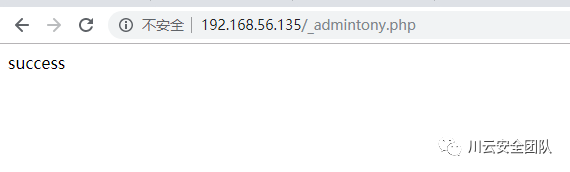
看到当from\_rep参数不存在时，会进入到另一个可以任意文件上传的else语句当中.

我们可以通过控制$repkid参数，达到控制文件目录的效果，如：传入repkid=../../../，则最终的$s\_n为：../../../\_filename

从而达到目录穿越，上传任意文件的效果。



最终shell地址为：http://192.168.56.135/\_admintony.php

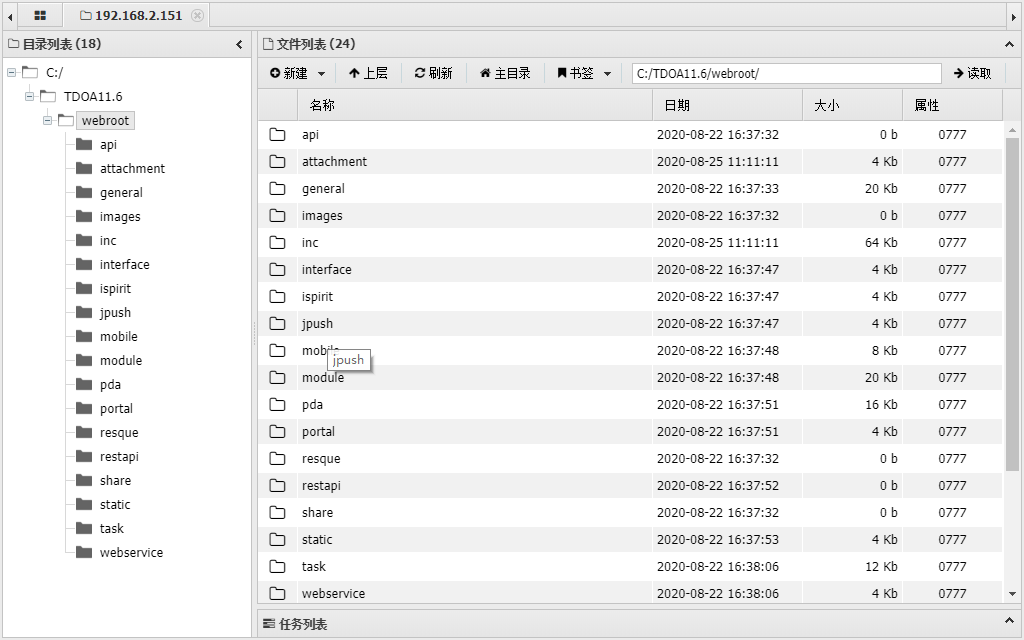


# 三、攻击路径

使用poc上传，得到一句话木马路径



然后蚁剑连接



# 四、防御方案

升级版本