SQL Injection in User List So boot

BUG_Author: Chengxin Xu
Affected Version: youlai-boot (v2.21.1)
Vendor: youlai-boot GitHub Repository
Software: youlai-boot
Vulnerability Files:

- `src/main/java/com/youlai/boot/system/contr`
- `src/main/java/com/youlai/boot/common/base/`
- `src/main/resources/mapper/system/UserMappe`

Description

youlai-boot contains a SQL injection vulnerability in the user l endpoint accepts user-controlled sorting parameters through whitelist validator, the `order` parameter is not validated and through MyBatis `${}` string interpolation.

This allows an authenticated attacker to inject arbitrary SQL f environment, the vulnerability was dynamically verified with a the injected SQL fragment was confirmed in the application lo

SQL Injection via User List Endpoint (/api/v1/us

The vulnerability chain starts from the `UserController.g` the user list, query parameters are bound into `UserQuery`

Entry Point (UserController.java:61-64):

Code block

```
1  @GetMapping
```