

&lt;&lt;

[SQL Injection in User List Sorti...](#)

Description

SQL Injection via User List End...

Proof of Concept:

Prerequisites:

Step 1: Prepare Authenticated ...

Step 2: Send Baseline Request

Step 3: Exploit SQL Injection in...

Step 4: Confirm with a Shorter ...

# 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 list endpoint accepts user-controlled sorting parameters through a whitelist validator, the `order` parameter is not validated and processed through MyBatis `${}` string interpolation.

This allows an authenticated attacker to inject arbitrary SQL fragments into the application environment, the vulnerability was dynamically verified with a proof of concept, the injected SQL fragment was confirmed in the application logs.

## SQL Injection via User List Endpoint (/api/v1/user)

The vulnerability chain starts from the `UserController.java` endpoint for getting the user list, query parameters are bound into `UserQuery` object.

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

Code block

```
1 @GetMapping
```