Stored XSS in FastBee Syste

Stored XSS in FastBee System Notice

BUG_Author: Chengxin Xu
Affected Version: FastBee (1.2.1)
Vendor: FastBee GitHub Repository
Software: FastBee
Vulnerability Files:

- `springboot/fastbee-admin/src/main/java/com/fastbee/web/control`
- `springboot/fastbee-service/fastbee-system-service/src/main/resources/mapper/system/Sy`
- `vue/src/views/index.vue`

Description

FastBee contains a stored XSS vulnerability in the system no by the backend and stored in the database without HTML sar detail dialog, the frontend renders the stored notice content th JavaScript to execute in the victim's browser.

Stored XSS via System Notice Create/Edit

The vulnerability chain starts from the notice management en notice, the request body is persisted directly without XSS filte

Entry Point (SysNoticeController.java:67-86):

Code block

```
1  @PreAuthorize("@ss.hasPermi('system:notice:a
2  @PostMapping
3  public AjaxResult add(@Validated @RequestBod
```