

[Stored XSS in FastBee System...](#)[Stored XSS in FastBee System N...](#)[Description](#)[Stored XSS via System Notice ...](#)[Proof of Concept](#)[Prerequisites](#)[Step 1: Obtain an Authorized T...](#)[Step 2: Create a Notice with an...](#)[Step 3: Confirm the Payload W...](#)[Step 4: Trigger the Stored XSS](#)

Stored XSS in FastBee System

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 notice management interface. The vulnerability is caused by the backend and stored in the database without HTML sanitization. When the user clicks the detail dialog, the frontend renders the stored notice content through JavaScript to execute in the victim's browser.

Stored XSS via System Notice Create/Edit

The vulnerability chain starts from the notice management interface. When the user creates or edits a notice, the request body is persisted directly without XSS filtering.

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

Code block

```
1 @PreAuthorize("@ss.hasPermi('system:notice:admin')")
2 @PostMapping
3 public AjaxResult add(@Validated @RequestBody SysNotice notice)
```