COMMUNITY CONTENT

Submit #780614: bufanyun HotGo <= v2.0 Cross Site Scripting

Title	bufanyun HotGo <= v2.0 Cross Site Scripting
Description	A stored Cross-Site Scripting (XSS) vulnerability exists in HotGo ≤ v2.0 at the system notice functionality, where the /admin/notice/editNotice endpoint accepts user-supplied content field without sanitization or validation, stores it directly in the database, and the Vue.js frontend renders this content using v-html without sanitization or validation. As a result, authenticated attackers can inject arbitrary JavaScript that executes in the browsers of users viewing the system notice, potentially leading to session hijacking, credential theft, or malicious actions performed on behalf of victims. Mitigations include implementing HTML sanitization using libraries like DOMPurify, avoiding v-html in favor of safe Vue.js rendering, implementing Content Security Policy (CSP) headers, encoding output context-appropriately, and validating input against a whitelist of allowed HTML tags and attributes.
Source	https://github.com/CC-T-454455/Vulnerabilities/tree/master/hotgo/vulnerability-2
User	Anonymous User
Submission	03/16/2026 04:45 AM (16 days ago)
Moderation	03/31/2026 06:13 PM (15 days later)
Status	Accepted
VulDB entry	353975 [bufanyun HotGo 1.0/2.0 editNotice Endpoint MessageList.vue cross site scripting]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling