COMMUNITY CONTENT

Home › Submit › 785859

Submit #785859: Cyber-III Student-Management-System 1.0 Insecure Direct Object Reference

Title	Cyber-III Student-Management-System 1.0 Insecure Direct Object Reference
Description	A reflected Cross-Site Scripting (XSS) vulnerability exists in /admin/Add notice/notice.php at line 128. The script uses the unsanitized $_SERVER['PHP_SELF'] variable as the form action attribute, allowing an attacker to inject arbitrary JavaScript code through a crafted URL.
Source	https://github.com/Cyber-III/Student-Management-System/issues/237
User	springbot (UID 96630)
Submission	03/23/2026 03:38 AM (14 days ago)
Moderation	04/05/2026 10:36 PM (14 days later)
Status	Approved
VulDB entry	[Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e62155b4942af3f Admin Add Endpoint notice.php $_SERVER['PHP_SELF'] cross site scripting]
Points	18

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