



Home > Submit > 785867

# Submit #785867: Cyber-III Student-Management-System 1.0 XSS vulnerability

**Title** Cyber-III Student-Management-System 1.0 XSS vulnerability

**Description** A reflected Cross-Site Scripting (XSS) vulnerability exists in /admin/Add notice/batch-notice.php at line 190. 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/238>

**User** z3r0\_0 (UID 96582)

**Submission** 03/23/2026 03:57 AM (14 days ago)

**Moderation** 04/05/2026 10:36 PM (14 days later)

**Status** Verified

**VulDB entry** [\[Cyber-III Student-Management-System up to 1a938fa81e9f735078e9b291d2e6215b4942a13f batch-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](#)