




Submit #562718: GitHub seccms v13.2 Cross Site Scripting

Title GitHub seccms v13.2 Cross Site Scripting

Description There is an XSS vulnerability in seacms, located at admin_cylog.php. The cause of the vulnerability is the lack of strict filtering of parameters passed by the client. Causing security threats to the system

Source  <https://github.com/seacms-net/CMS/issues/25>

User  zonesec (UID 74980)

Submission 04/20/2025 05:42 PM (15 days ago)

Moderation 05/04/2025 08:59 AM (14 days later)

Status Accepted

VulDB Entry 307360 [SeaCMS 13.2 /admin_paylog.php cstatus cross site scripting]

Points 17

Notice

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](#)