Submit #567191: LmxCMS v1.41 SQL Injection

Title	LmxCMS v1.41 SQL Injection
Description	A critical SQL injection vulnerability exists in LmxCMS v1.41, located in the manageZt() method within c\admin\ZtAction.class.php. The vulnerability arises because user-supplied sortid parameters are directly concatenated into SQL queries without proper sanitization or parameter binding. This flaw allows attackers to inject arbitrary SQL code, which can lead to sensitive data exposure, privilege escalation, or complete compromise of the database. Exploitation can be achieved by sending a specially crafted POST request, allowing attackers to retrieve sensitive information, manipulate the database, or execute arbitrary SQL commands.
Source	⚠ https://github.com/xiaoyangsec/LmxCMS-SQL-Injection/blob/main/LmxCMS-SQL-Injection.md
User	xiaoyang (UID 84496)
Submission	04/29/2025 02:23 PM (12 days ago)
Moderation	05/10/2025 03:45 PM (11 days later)
Status	Accepted
VulDB Entry	308286 [LmxCMS 1.41 POST Request ZtAction.class.php manageZt sortid sql injection]
Points	20

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