Submit #563175: SourceCodester Stock Management System (SMS-PHP by oretnom23) 1.0 SQL Injection

Title SourceCodester Stock Management System (SMS-PHP by oretnom23) 1.0 SQL Injection

Description 1. Vulnerability Overview

Vulnerable Endpoint: /sms/classes/Login.php?f=login
Vulnerable Parameter: username
Issue Type: SQL Injection - Authentication Bypass
Severity: High (Critical) – Unauthorized access can be gained to the system, leading to potential unauthorized actions.
Software URL: https://www.sourcecodester.com/php/15023/stock-management-system-phpoop-source-code.html

2. Vulnerability Description
The Stock Management System software contains a SQL Injection vulnerability on the login page that leads to an authentication bypass. This vulnerability is triggered by the improper sanitization of user inputs, specifically the username parameter. Attackers can exploit this flaw to bypass the authentication mechanism and gain access to the system with admin privileges.

Source ⚠️ https://github.com/th3w0lf-1337/Vulnerabilities/blob/main/SMS-PHP/SQLi/Auth-Bypass/info.md

User Th3W0lf (UID 84351)

Submission 04/21/2025 08:03 PM (15 days ago)

Moderation 05/05/2025 01:33 PM (14 days later)

Status Accepted

VulDB Entry 307391 [SourceCodester/oretnom23 Stock Management System 1.0 Login.php?f=login Username 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