ziyishen97 / CVE-2022-36257.md

Created 3 months ago

☆ Star

<> Code   Revisions 1

Public Reference for CVE-2022-36257

CVE-2022-36257.md

Product: InvetoryManagementSystem

Vendor: https://github.com/sazanrjb

Affected Version(s): 1.0

CVE ID: CVE-2022-36257

Description: A SQL injection vulnerability in UserDAO.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via the parameters such as "users", "pass", etc.

Vulnerability Type: SQL injection

Root Cause: Multiple methods and their parameters such as changePassword(String user, String pass), getUser(String user), etc. in source file UserDAO.java do not have user input sanitiazation.

Impact: An attacker is able to extract sensitive data from the database.

PoC:

1. Set value of parameter "user" as '--.