Instantly share code, notes, and snippets.

ziyishen97 / CVE-2022-36259.md

Created 3 months ago

☆ Star

Code Revisions 1

Public Reference for CVE-2022-36259

CVE-2022-36259.md

Product: InvetoryManagementSystem

Vendor: https://github.com/sazanrjb

Affected Version(s): 1.0

CVE ID: CVE-2022-36259

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

Vulnerability Type: SQL injection

Root Cause: Multiple methods and their parameters such as checkLogin(String username,String password, String user) in source file ConnectionFactory.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 "username" as '--.