ziyishen97 / CVE-2022-36255.md

Public Reference for CVE-2022-36255

CVE-2022-36255.md

Product: InvetoryManagementSystem

Vendor: https://github.com/sazanrjb

Affected Version(s): 1.0

CVE ID: CVE-2022-36255

Description: A SQL injection vulnerability in SupplierDAO.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via the parameters such as "searchTxt".

Vulnerability Type: SQL injection

Root Cause: Multiple methods and their parameters such as getSearchSuppliersQueryResult(String searchTxt) in source file SupplierDAO.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 "searchTxt" as '--.