

Instantly share code, notes, and snippets.

ziyishen97 / CVE-2022-36256.md

Created 3 months ago

☆ Star

<> Code - Revisions 1

Public Reference for CVE-2022-36256

 CVE-2022-36256.md

Product: InventoryManagementSystem

Vendor: <https://github.com/sazanrjb>

Affected Version(s): 1.0

CVE ID: CVE-2022-36256

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

Vulnerability Type: SQL injection

Root Cause: Multiple methods and their parameters such as checkStock(String productcode, Statement stmt) in source file Stocks.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 "productcode" as '--.