# CVE Detail – CVE-2020-35666

Steedos Platform through 1.21.24 allows NoSQL injection because the /api/collection/findone implementation in server/packages/steedos\_base.js mishandles req.body validation, as demonstrated by MongoDB operator attacks such as an X-User-Id[$ne]=1 value.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.61148

## CVSS Scoring

CVSS v3.1 Score: 8.8

Severity: HIGH

## Mapped CWE(s)

* CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

## CAPEC(s)

* CAPEC-108: Command Line Execution through SQL Injection
* CAPEC-109: Object Relational Mapping Injection
* CAPEC-110: SQL Injection through SOAP Parameter Tampering
* CAPEC-470: Expanding Control over the Operating System from the Database
* CAPEC-66: SQL Injection
* CAPEC-7: Blind SQL Injection

## Affected Products

* cpe:2.3:a:steedos:steedos:\*:\*:\*:\*:\*:\*:\*:\*