New issue

Sql Injection Security Issues #14

⊙ **Open**   **ziyishen97** opened this issue on Jul 8 · 2 comments

---

ziyishen97 commented on Jul 8

Hey, I find few parameters are vulnerable to SQL injection vulnerability.
A list of affected files:
UserDAO.java
Stocks.java
SupplierDAO.java
ProductDAO.java
CustomerDAO.java
ConnectionFactory.java

---

ziyishen97 commented on Jul 8 · edited ▾   Author

In UserDAO.java, multiple parameters such as user, pass, etc. are vulnerable to SQL injection vulnerability.
PoC: Set value of parameter 'user' as ` ' `<SQL Query>--
In CustomerDAO.java, multiple parameters such as searchTxt, customercode, etc. are vulnerable to SQL injection vulnerability.
PoC: Set value of parameter 'searchTxt' as ` ' `<SQL Query>--
In Stocks.java, parameter productcode is vulnerable to SQL injection vulnerability.
PoC: Set value of parameter 'prductcodet' as ` ' `<SQL Query>--
In SupplierDAO.java, parameter searchTxt is vulnerable to SQL injection vulnerability.
PoC: Set value of parameter 'searchTxt' as ` ' `<SQL Query>--
In ProductDAO.java, parameter searchTxt is vulnerable to SQL injection vulnerability.
PoC: Set value of parameter 'searchTxt' as ` ' `<SQL Query>--
In ConnectionFactory.java, multiple parameters such as username, password, user, etc. are vulnerable to SQL injection vulnerability.
PoC: Set value of parameter 'username' as ` ' `<SQL Query>--

---

sazanrjb commented on Jul 9 · edited ▾   Owner

> Hey, I find few parameters are vulnerable to SQL injection vulnerability.
> A list of affected files:
> UserDAO.java
> Stocks.java
> SupplierDAO.java
> ProductDAO.java
> CustomerDAO.java
> ConnectionFactory.java

Hey, thanks for finding out time to read through and open the issue.

Since I do not maintain this project anymore, it would be great if you could open a pull request with necessary changes.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants