Problem Set 2

What are Injection Attacks and how does it work?

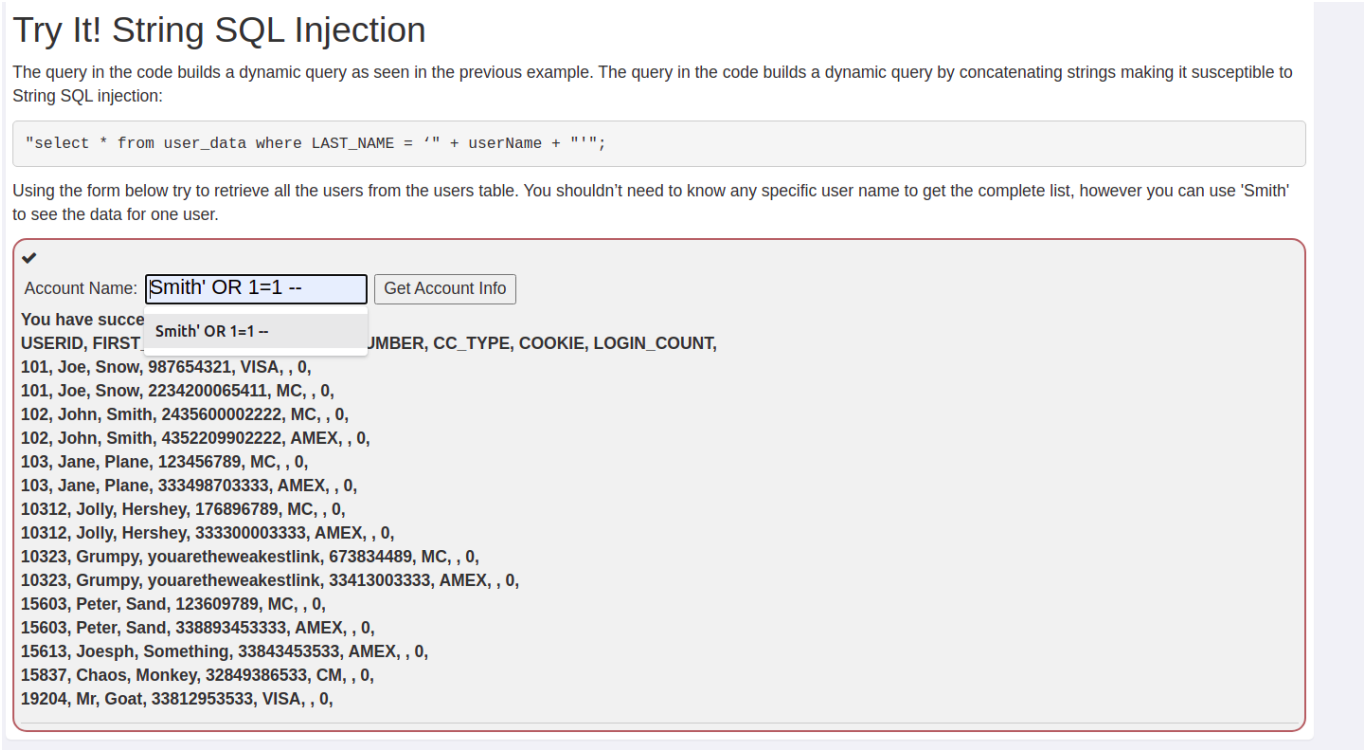
Injection attack is a form of injecting code through a vulnerability that is executed by the application.

This happens with untrusted or poor handled data, as allowed characters, data format and amount of expected data.

Why is it important to prevent Injection Attacks?

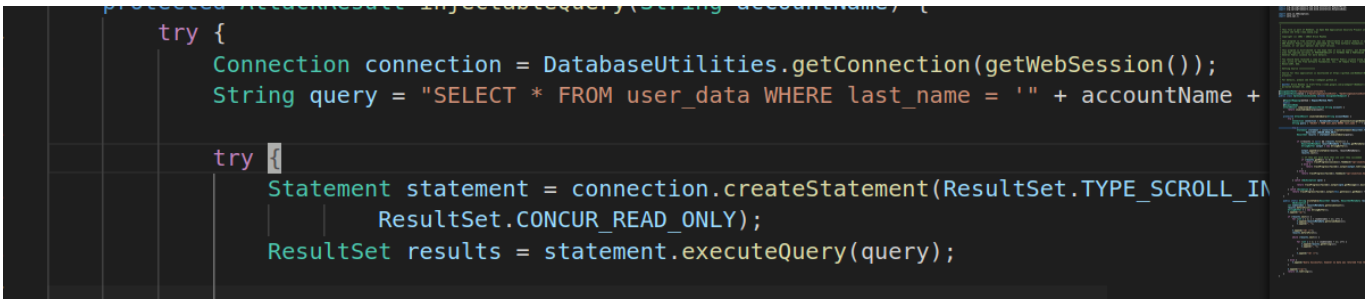
They could cause data loss, corruption (Integrality in CIA triad), disclosure to unauthorized parties (Confidentialy) or denial of access (Availability)

Try It! String SQL Injection

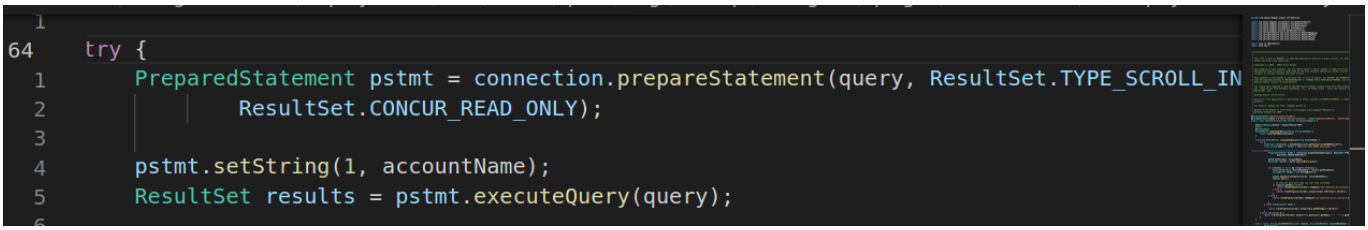


We can inject when we escape the input and select an always true condition, so we select * from table

Before patch



After Patch



```
64    try {
          PreparedStatement pstmt = connection.prepareStatement(query, ResultSet.TYPE_SCROLL_IN
                  ResultSet.CONCUR_READ_ONLY);

          pstmt.setString(1, accountName);
          ResultSet results = pstmt.executeQuery(query);
```