Security holes in Three-tier Applications: Architecture
SQL Injection

• **Why**
  - Different authentication mechanisms in Middle-Tier and Backend
    - **Middle-Tier**: Apache, MS Internet Information Server (IIS)
    - **Backend**: MS SQL Server, Oracle, IBM DB2

• **Security hole**
  - SQL Injection

• **Solution**
  - **Intranet**: Microsoft Windows Integrated Authentication
  - **Internet**: Use credentials entered on the Web to connect to Backend, if possible
  - **Internet**: Use a separate WEB_USER account with limited access
SQL Injection

• Main Idea
  ➢ Use Admin privileges to the backend to retrieve needed information

• Attack Example
  ➢ ASP.NET:
    SQL= 'select p.sum from paycheck as p
        where r.date='&str_date&' and p.employee = '&user_name
  ➢ Web form:
    ➢ First: enter &*(^&^%$^ instead of valid date
    ➢ Second: examine the query from the ODBC error
    ➢ Third: enter in the date field in the Web Form:
        ' or p.employee = p.employee --
    ➢ Forth: more destructive attack
        ' or p.employee = p.employee --%13%10% drop paycheck
msdn.microsoft.com/security