SQL Injection Attacks

• Web app code:
  
  txtUserId = getRequestString("UserId");
  txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;

• Fill out form with “anthony”
  
  SELECT * FROM Users WHERE UserId = anthony

• Fill out form with “admin OR 1=1”
  
  SELECT * FROM Users WHERE UserId = admin OR 1=1