Name:____ StudentID:_______________

W2D1 Quiz

CS472 WAP October 2016 – Prof. Zijlstra

1. Is the following code vulnerable to SQL injection? Please answer only with Yes or No

```
public boolean existsUser(Connection con, String name) throws SQLException {
    String sql = "SELECT * FROM user WHERE name ='" + name + "'";
    try (PreparedStatement ps = con.prepareStatement(sql)) {
        try (ResultSet rs = ps.executeQuery()) {
            if (rs.next()) {
                return true;
            }
        }
    }
    return false;
}
```

Yes

Because data is concatinated in → no separation between data and command

2. Please describe the similarities and differences between Session Hijacking and Session Fixation:

Similarity:
Attacker knows victim's sessionId and can therefore "be" the victim

Differences:
Hijacking: victim has a number and attacker finds what it is (sniffing)
Fixation: the attacker makes the victim start his session with the Id provided by the attacker