For at forhindre muligheden for SQL Angreb kan man lave server-side validering samt client-side validering.

På server-side kan man f.eks benytte sig af Regular Expressions (regex). Altså lave en metode som fjerner muligheden for at benytte 'Special characters' i input-felter.

Det er også en god ting at benytte sig af prepared statements, som er SQL Statements som bliver sendt og parsed af databasen uden påvirkelse af nogle parametre.

f.eks:

```
var sql = "SELECT * FROM twinships WHERE shipid = ?";

var inserts = [message.ship.id];

sql = mysql.format(sql, inserts);
```

Endnu en mulighed for at beskytte sig mod SQL injections er at lave stored procedures, som gør det muligt at brugere kun har adgang til den specifikke Stored Procedure uden at have adgang til tabeller.

På client-side kan du eksempelvis bruge JavaScript + HTML til at sørge for de rigtige input felter og info bliver benyttet som forventet.