## Brug af Prepared Statements

Dette sikre at en hacker ikke har mulighed for at ændrer på en Query, selv hvis SQL commands indsættes i forlængelse af den almindelige forespørgsel. Hvis en hacker tilføjer benjamin’ or 1 = 1; for at tilegne sig adgang, vil prepared statement søge efter det i databasen, i stedet for at return true.

## Escaping alt bruger tilføjet input.

Dette sikre sig at alt bruger input ikke er muligt at smide ind i en Query. Denne metode burde som udgangspunkt være et sidste resort når man har udtømt alle andre muligheder. At man validerer input vil i de fleste tilfælde være et bedre valg. Og som med alle andre metoder, kan man aldrig garantere at det er 100% sikkert mod alle injektions.

MySQL har en indbygget funktion: mysql.escape(userdata); som meget simpelt ignorer alt user data når det drejer sig om sql Querys.