

A Hibernate mítosz

Terjeng egy mítosz a Hibernate HQL nyelvének "sebezhetetlenségéről"... vagyis az SQL injection elleni védettségéről. Pedig a HQL ugyanúgy sebezhet, mint az SQL: **ha rosszul használjuk**. Nézzünk miképp is [néz ki ez](#):

```
String goodParameter = "Raj lane";
Query badQuery = session.createQuery("from Address a where a.street='" + goodParameter + "'");
```

Látszik, hogy a paramétert hozzáfűzzük mezei szövegével, amely lehetőséget ad a HQL injection elvégzésére:

```
String badParameter = "la' or '1'='1";
Query reallyBadQuery = session.createQuery("from Address a where a.street='" + badParameter + "'");
```

Eredményül nem az utcára szkítést kapjuk, hanem a tábla teljes tartalmát, mivel a feltételhez odakerült egy **'1'='1'**, mégpedig VAGY kapcsolatban a többi feltétellel. Az HQL injection ellen a paraméterek átadásával tudunk védekezni:

```
String badParameter = "la' or '1'='1";
Query reallyBadQuery = session.createQuery("from Address a where a.street=:street");
reallyBadQuery.setParameter("street", badParameter);
```

Így a trükk semmit nem ér... :)