* Give an example of a SQL inject which will give all users in a user table

SQL string: “SELECT \* FROM ‘user’ WHERE name = “+name+”;”

input: William‘ OR 1=1; --

* Explain how prepared statements prevent SQL injection

At i stedet for at man putter inputtet direkte ind i querien, så bliver inputet omdannet til en streng og derefter ind i querien, således at man ikke kan tilføje sql “harmful” sql kode til inputet.

* Explain how to use placeholders in cases where prepared statements cannot do the job
* keywords som er forventet af programmet, hvor det kun er de keywords der kan bruges
* Således kan der ikke laves injection da det ville give en fejl

* Explain how logging could be used to monitor injection attempts
* Man kan se hvordan et forsøgt hack har prøvet at fungere
* Man kan få idéer til at videreudvikle og forebygge injections
* Så kan man holde øje med hvordan en hacker har prøvet at tilgå ens database.