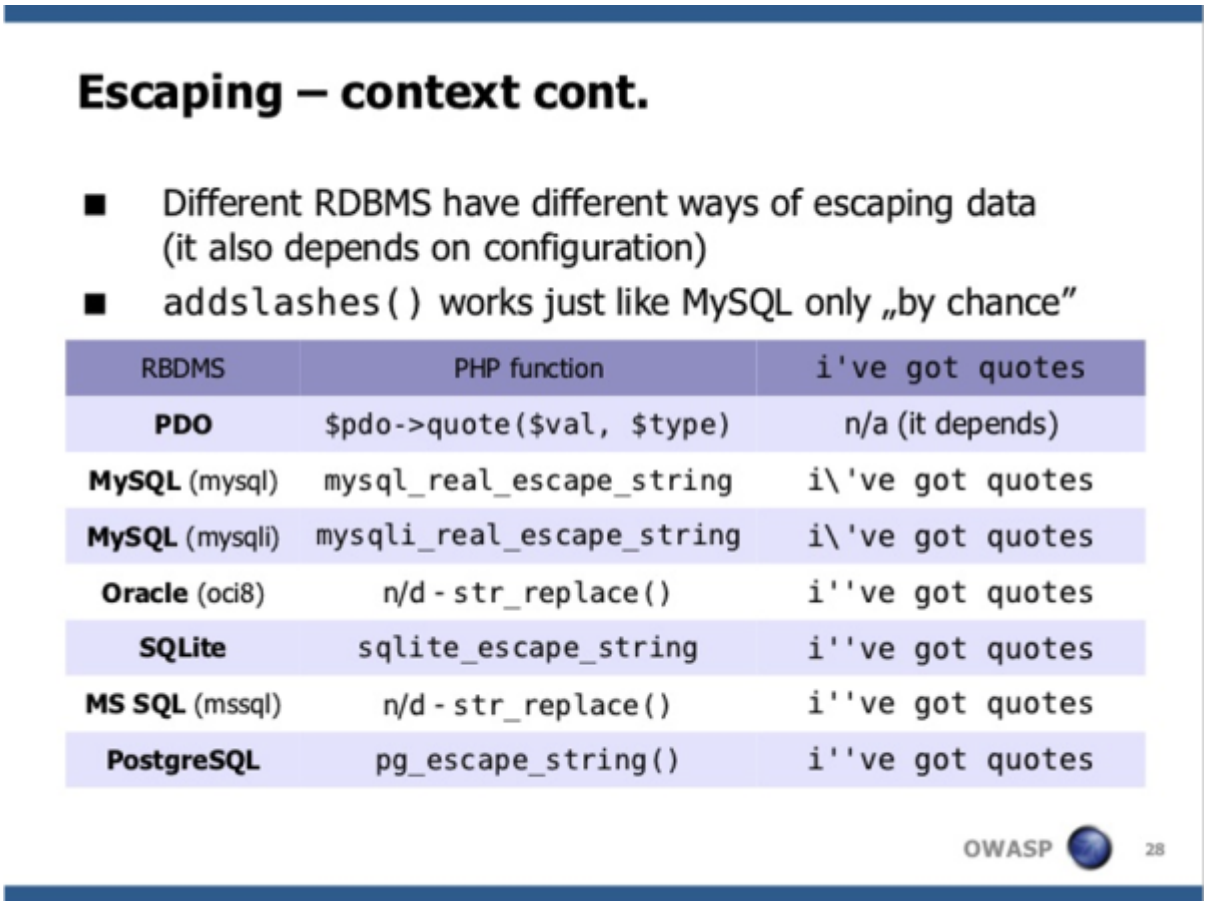
# LU10c - SQLi Gegenmassnahmen

Glücklicherweise gibt gegen alle SQLi-Varianten entsprechende Gegenmassnahmen. Die hier vorliegende Liste ist daher nur ein Ausschnitt mit den prominentesten.

## Escaping

Beim *escaping* werden Sonderzeichen nicht direkt in die Datenbank weitergeleitet. Die vom User eingegebenen Werte werden durch eine entsprechende Funktion/Methode, die es in vielen Programmiersprachen gibt vor der Weiterleitung gefiltert. Sonderzeichen, die den Angriffspunkt darstelle, werden von *gefährlichen* Steuerzeichen in *harmlose* Characters umgewandelt.Das „Escapen“ kann dabei auf der Client- und Serverseite geschehen.



### Escaping – context cont.

- Different RDBMS have different ways of escaping data (it also depends on configuration)
- addslashes() works just like MySQL only „by chance”

| RBDMS | PHP function | i've got quotes |
|---|---|---|
| **PDO** | $pdo->quote($val, $type) | n/a (it depends) |
| **MySQL** (mysql) | mysql_real_escape_string | i\'ve got quotes |
| **MySQL** (mysqli) | mysqli_real_escape_string | i\'ve got quotes |
| **Oracle** (oci8) | n/d - str_replace() | i''ve got quotes |
| **SQLite** | sqlite_escape_string | i''ve got quotes |
| **MS SQL** (mssql) | n/d - str_replace() | i''ve got quotes |
| **PostgreSQL** | pg_escape_string() | i''ve got quotes |

OWASP 28

---