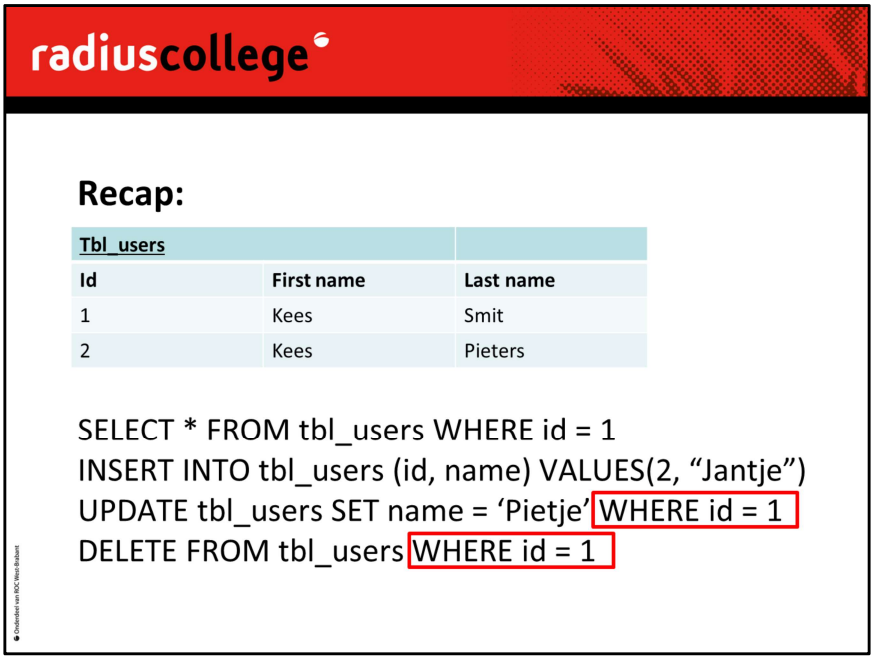
radiuscollege

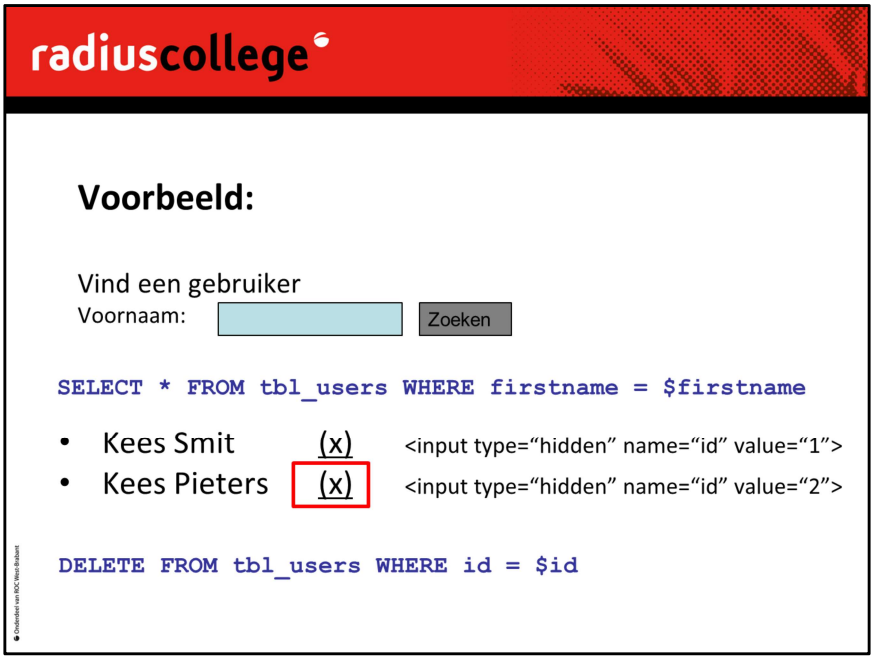
PR FIFA - HC 5

SQL Injection
Prepared statements



Gebruik in WHERE altijd id, dat is het enige unieke!

Anders loop je risico meerdere mensen met dezelfde naam te verwijderen

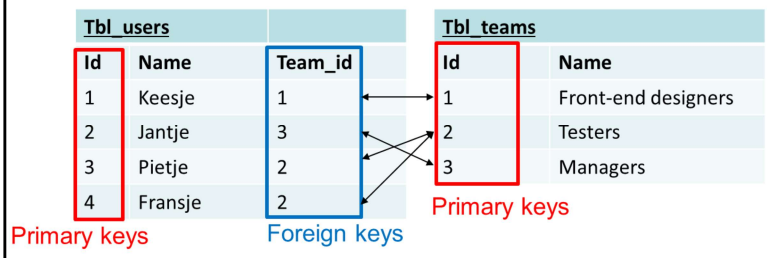


Gebruik in WHERE altijd id, dat is het enige unieke!

Anders loop je risico meerdere mensen met dezelfde naam te verwijderen

radiuscollege

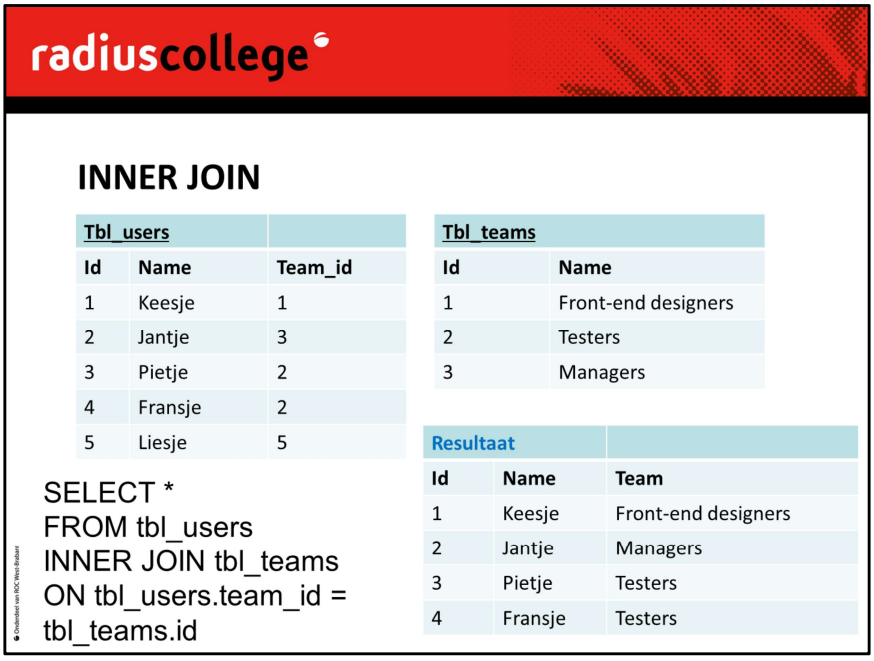
“Keys”



Je gebruikt dus nummers om tabellen te koppelen, we noemen dat “primary keys” of “foreign keys”.

Iedere tabel heeft een eigen primary key.

Een foreign key verwijst naar een andere tabel



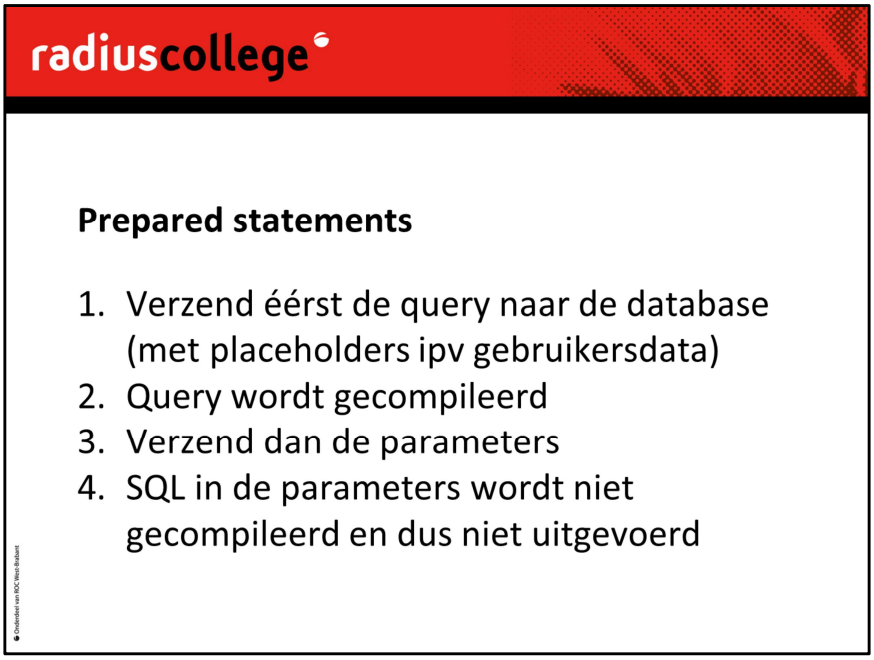
“Inner join”: krijgt alleen resultaat als in beide tabellen een overeenkomst is. Team 5 bestaat niet, dus je krijgt “Liesje” niet terug.

radiuscollege

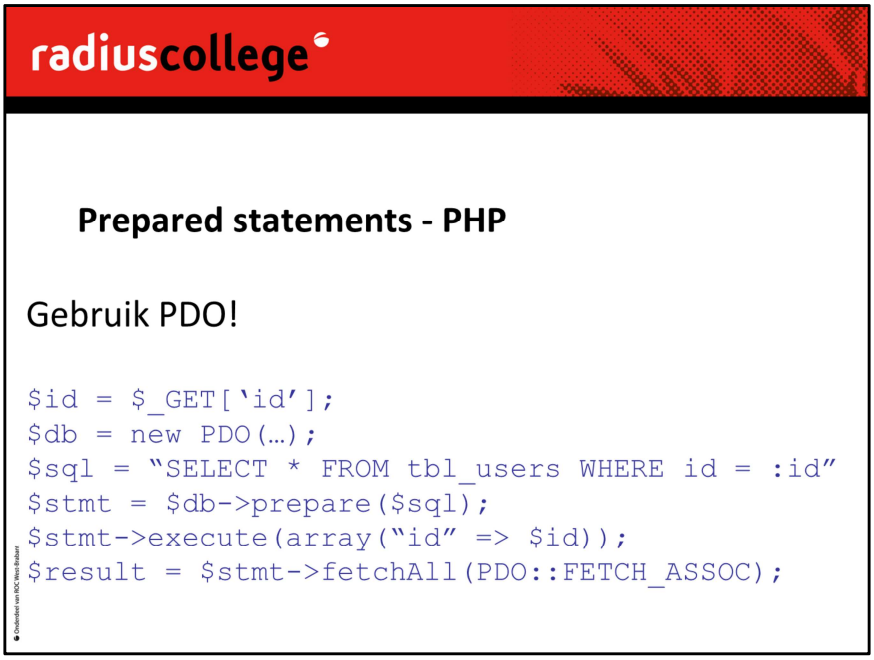
SQL Injection
Prepared statements

radiuscollege

Voorbeeld van SQL-injection

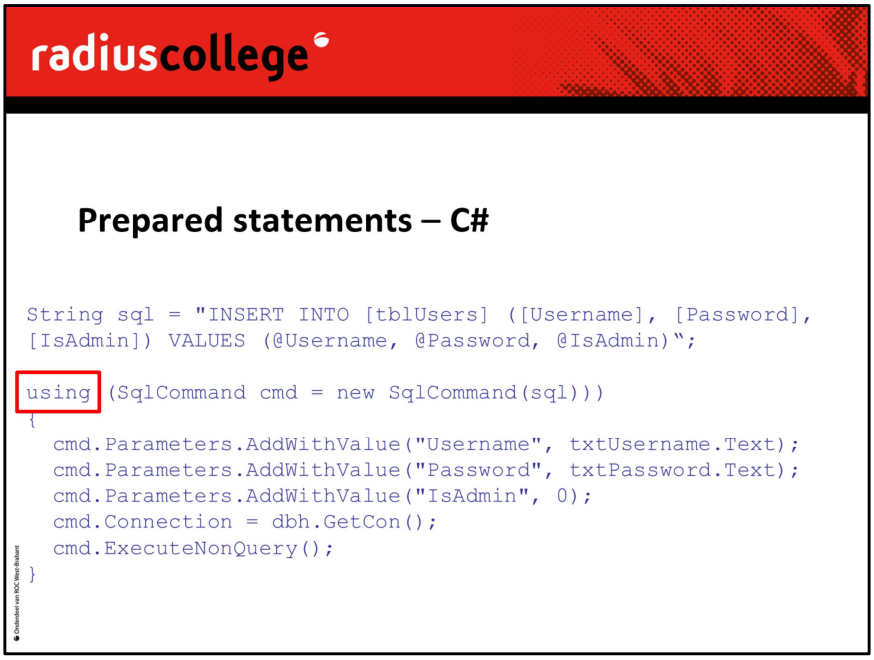


Hiermee voorkom je dus SQL-injection!



$stmt betekent dus “statement”!

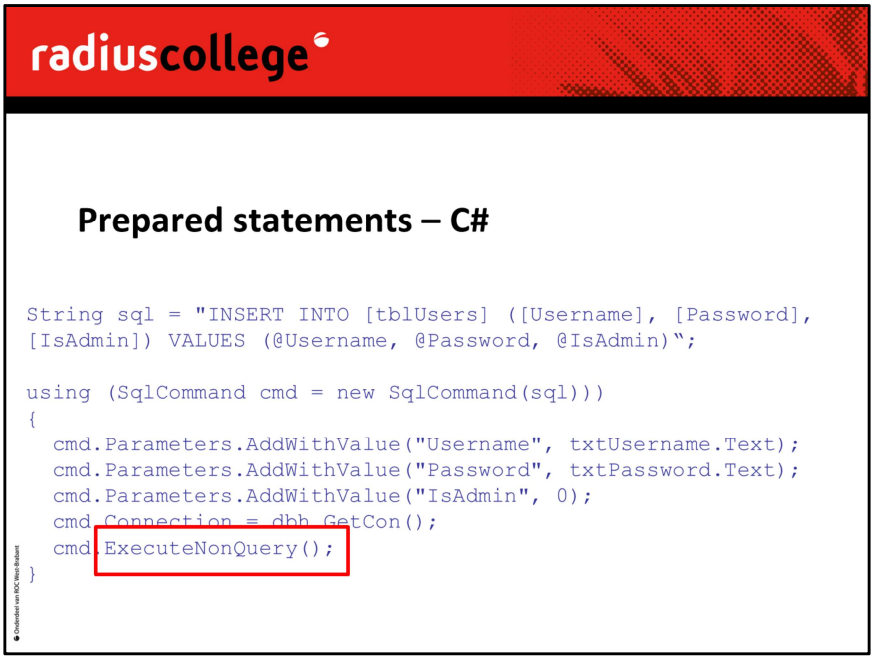
Ga dit niet onthouden, maar zoek het terug op mysite of elders op internet (“php pdo prepared statements”)



Wat is dat using-ding?

Zorgt ervoor dat het object na het blok netjes wordt weggegooid.

Je hebt het cmd-object immers niet meer nodig verderop in je code.



Wat is dat?

Gebruik je intellisense!