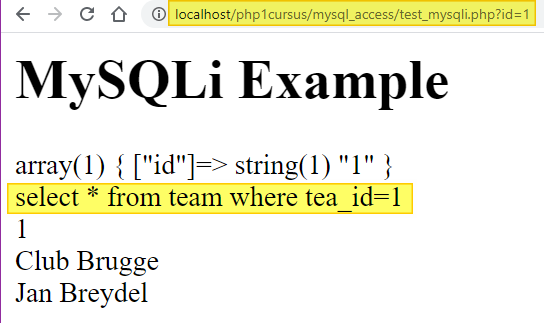
T 2.2 - SQL injection with GET parameters

# Voorbeeld

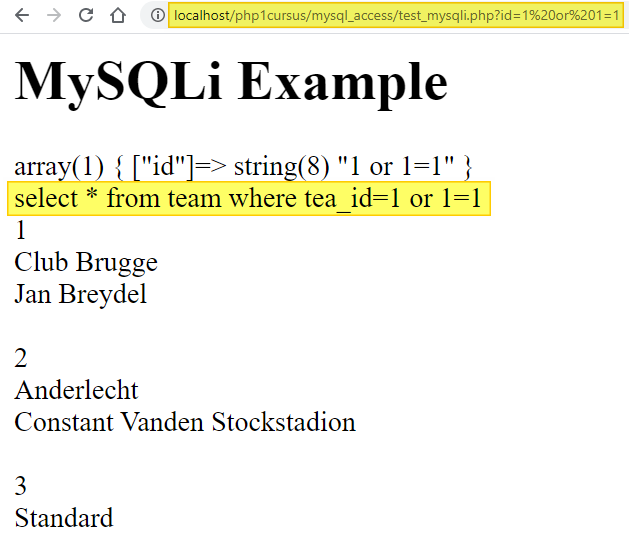
Stel dat we een script **test\_mysqli.php** gebruiken dat **één record** uit de databank haalt aan de hand van een **GET** parameter **id**:



Een slimme gebruiker verandert de parameter in ‘1 or 1=1’:



Het resultaat is dat we **alle records** uit de tabel te zien krijgen:

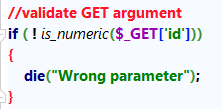


Wat zou deze gebruiker nog kunnen toevoegen aan ons SQL statement?

* **UNION …**
* **; drop schema products;**
* …

# Oplossing

* **Valideer** je GET parameters vooraleer je ze inbouwt in je SQL statements:



* Laat **nooit** toe dat de gebruiker **volledige SQL statements** kan doorsturen naar de databank
* Gebruik **prepared statements** met **parameter binding**: zie voorbeeld volgende pagina.   
    
  Bij prepared statements wordt de SQL gescheiden van de data. Zelfs als de data SQL instructies bevat, kunnen die nooit uitgevoerd worden, precies omdat ze als tekst behandeld worden.  
    
  Zie ook <https://www.programmerinterview.com/database-sql/example-of-prepared-statements-and-sql-injection-prevention/>

**<h1>MySQLi Prepared Statement Example</h1>  
  
<?php***error\_reporting***( *E\_ALL* )**;  
*ini\_set***( 'display\_errors',** 1 **)**;  
  
**require\_once "connection\_data.php"**;  
**require\_once "connection.php"**;  
  
**//validate GET argument  
if (** ! *is\_numeric***($\_GET['id']))  
{  
 die("Wrong parameter")**;  
**}  
  
//prepare statement  
$sql** = **"SELECT** *\** **FROM team WHERE tea\_id=?"**;  
**$stmt** = **$conn**->prepare**($sql)**;  
  
**if ( $stmt** == **false ){  
 die("Error preparing statement "** . **$sql)**;  
**}  
  
//bind parameters  
$stmt**->bind\_param**("i", $\_GET["id"])**; **//$\_GET['id'] must be convertable to int ("i")  
$stmt**->execute**()**;  
**$result** = **$stmt**->get\_result**()**; **// get the mysqli result  
  
//show result (if there is any)  
if ( $stmt**->**affected\_rows** > 0 **)  
{  
 // output data of each row  
 while( $row** = **$result**->fetch\_assoc**() )  
 {  
 echo $row["tea\_id"]** . **"<br>"**;  
 **echo $row["tea\_naam"]** . **"<br>"**;  
 **echo $row["tea\_stadion"]** . **"<br>"**;  
 **echo "<br>"**;  
 **}  
}  
else  
{  
 echo "No records found"**;  
**}  
  
$conn**->close**()**;  
**?>**