

Safe way to escape form variables to insert in sql (to oracle)

Source: <http://coding.derkeiler.com/Archive/PHP/alt.php/2005-05/msg00389.html>

- *From:* ATK <cifroes@xxxxxxxxxxx>
 - *Date:* Tue, 24 May 2005 22:44:49 +0100
-

Hi,

I'm connecting to a oracle db via ODBC (can't use native oracle functions) and i need to parse the input from a form to insert in a sql query.

I know the dangers of that so i want to be extra sure i "escape" all strange chars.

I would like to know if using placeholders is enough or should i do something else (maybe addslashes, htmlspecialcharsities, etc) to have safe queries without strange chars (maybe removing % and _ also, because they have special meaning in oracle).

The code i'm using right now is something like this:

```
$desc = $_POST['desc'];  
$sql = "select id from photo where desc LIKE '?'";  
$res = odbc_exec($conn, $sql, $desc);
```

Is this 100% safe or should i do anything more to secure it?

Thanks in advance,
ATK

.