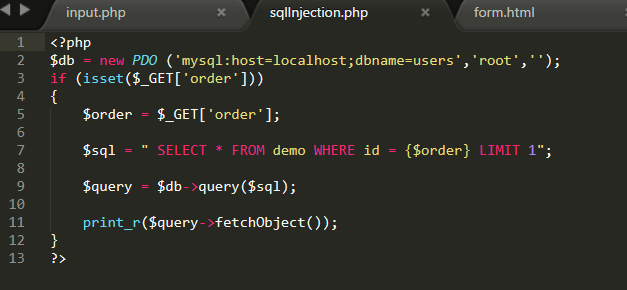
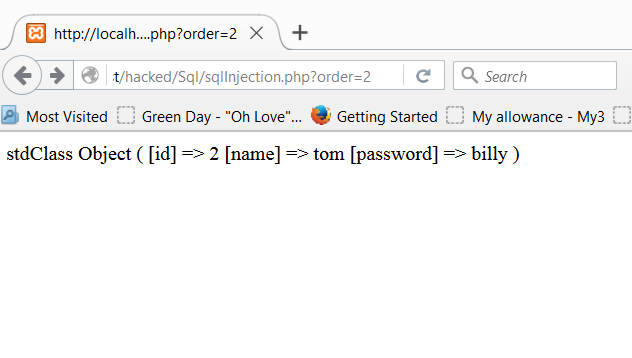
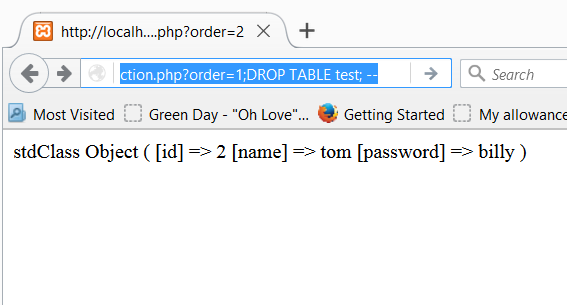
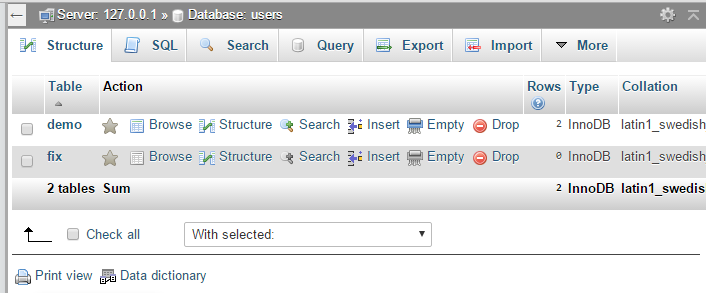
# SQL Injection

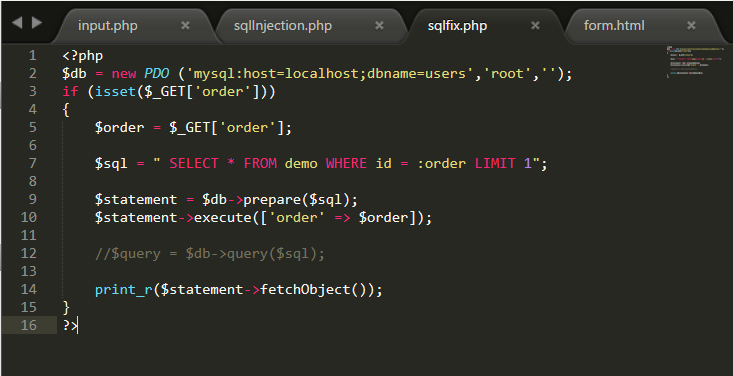


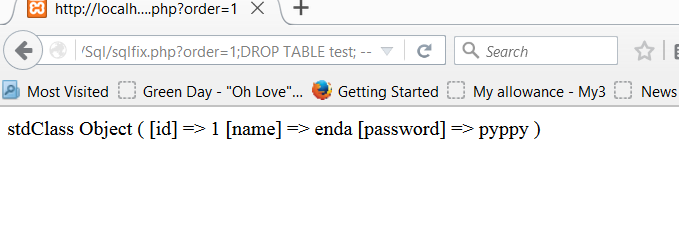


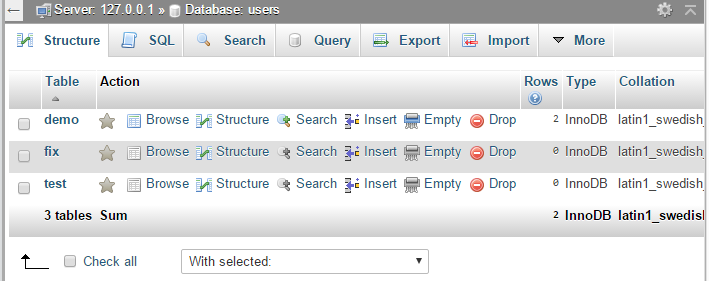




* Permissions should a user have access to drop tables
* But this still doesn’t fully fix the problem.
* Prepared statements does.
* If you cast cast to particular data type.







* Prepared statements are used to prevent SQL injection