**SQL Injection**

An [SQL injection](https://www.owasp.org/index.php/SQL_injection) attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application. A successful SQL injection attack can read sensitive data from the database, modify database data (insert/update/delete), execute administration operations on the database (such as shutdown the DBMS)

**E.g.:** The Last Name should have field length 30 instead of 255. There may be some input fields where large data input is necessary, for such fields proper validation of input should be performed prior to saving that data in the application. Moreover, in such fields, any HTML tags or script tag input must be prohibited. In order to provoke XSS attacks, the application should discard script redirects from unknown or untrusted applications.

**How to test SQL Injection and XSS:** Tester must ensure that maximum lengths of all input fields are defined and implemented. (S)He should also ensure that defined length of input fields does not accommodate any script input as well as tag input. Both these can be easily tested

**E.g.:** If 20 is the maximum length specified for ‘Name’ field, and input string “<p>thequickbrownfoxjumpsoverthelazydog” can verify both these constraints. It should also be verified by the tester that application does not support anonymous access methods. In case any of these vulnerabilities exist, the application is in danger.