XSS = Cross site Scripting

XSS is quite similar to SQL injection except instead of using query, we use actual javascript code. We can trick the database to store this script as string. When there is a read request, this script together with other information is sent to the client browser. The browser upon spotted the javascript code will attempt to run it.

SQL injection : SQL Injection is a method that allows perpetrators to execute malicious SQL statements and bypass application security measures to retrieve or alter database contents.

Eg:

SELECT \* FROM users WHERE username='john' AND password='john123';

This statement will fetch the data of user whose useename is john and password is john123

SELECT \* FROM users WHERE username='hacker' AND password='hacker123' OR '1'='1'

This statement is used to trick database . here in or condition we have given true statement ‘1’ = ‘1’ ; this means the whatever is username or password is provided it is right and give access to database and fetch data . this is sql injection .

How to detect SQL Injection attacks

Creating a SQL Injection attack is not difficult, but even the best and good-intentioned developers make mistakes. The detection of SQL Injection is, therefore, an essential component of creating the risk of an SQL injection attack. Web Application Firewall can detect and block basic SQL injection attacks, but we should depend on it as the sole preventive measure.

Intrusion Detection System (IDS) is both network-based and host-based. It can be tuned to detect SQL injection attacks. Network-based IDSec can monitor all connections to our database server, and flags suspicious activities. The host-based IDS can monitor web server logs and alert when something strange happens.

## How to prevent SQL Injection attack

* We should use user authentication to validate input from the user by pre-defining length, input type, and the input field.
* Restricting the access privileges of users and defining the amount of data any outsider can access from the database. Generally, the user cannot be granted permission to access everything in the database.
* We should not use system administrator accounts.