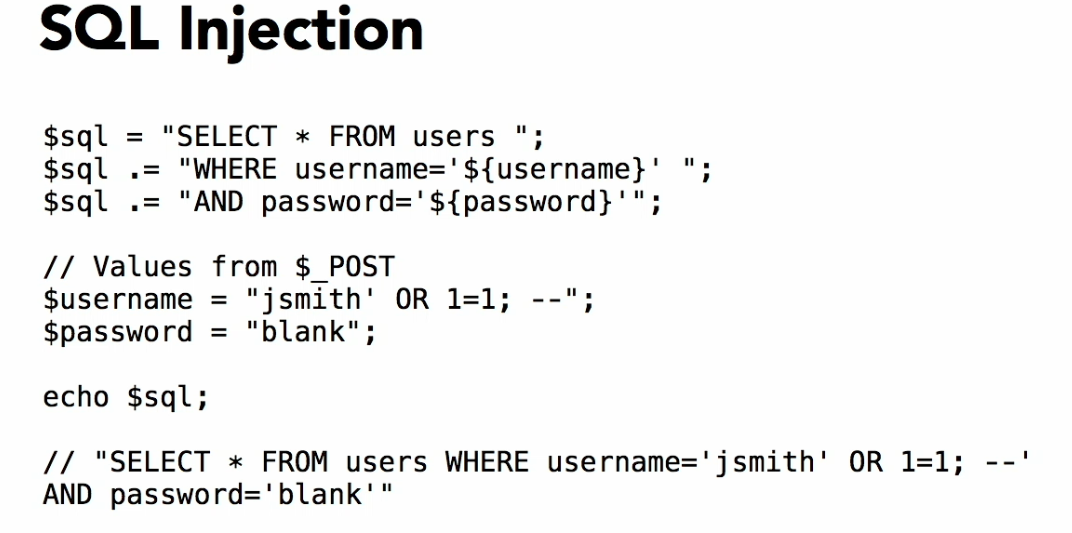
SQL Injection

* Hacker is able to execute arbitrary SQL requests
* Can be used to steal database data
* Can be used to add, delete, or change database data

Example



Keep in Mind

* In SQL syntax, text provided by the user should be always enclosed in single quotes like username = 'sabbir';
* The single quote character is part of the SQL language, not part of user’s input!
* Escaping strings for mysql

--Backslash before single-quote

Example --$menu\_name = “Today\’s widget Trivia”;

* For avoiding sql injection in mysql use mysqli\_real\_escape\_string($db,$string) designed for string
* Mysqli\_real\_escape\_string() -- escapes all strings.
* Mysqli\_real\_escape\_string() add a backslash before a single quote if the string contains before any single quote
* Mysqli understands oops it’s not ending quote of the string it’s the part of the string.
* What kind of things should be escaping those are following:
* We shouldn’t trust anything, anything means those are come from user whether from url string, form value, cookie value, even our database value which may have originated from somewhere else or some user we should escape
* When we use mysqli\_real\_escape\_string the query generate as like

INSERT INTO subjects (menu\_name, position, visible) VALUES (‘Today\'s new\'s item\'s', 1, 1)

* If we don’t escape the string then if the users give a malicious input then it will generate a valid sql as like

SELECT \* FROM users

WHERE username = 'sabbir' OR 1=1; -- ' AND password = '456';

SQL Injection Solutions

* In database Site,

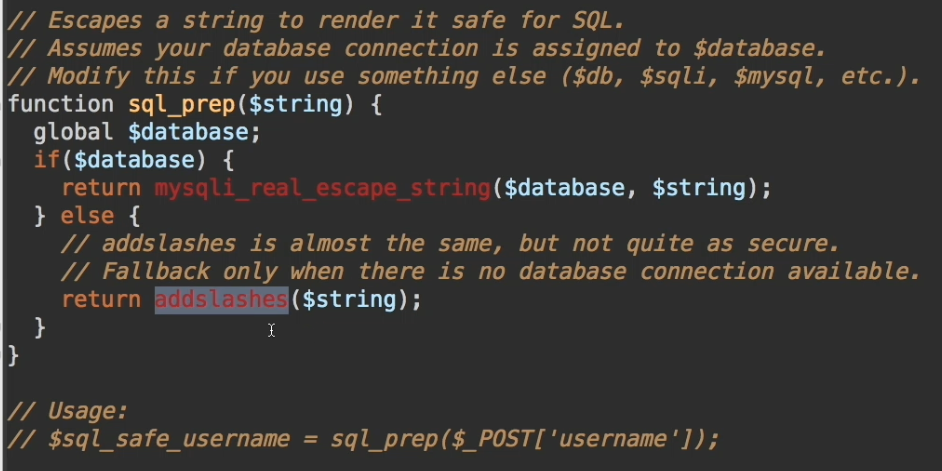
Give limited privileges to application’s database user

Users does not have the ability to drop table, truncate table

* In PHP Site,

1. Sanitize input for SQL
2. Prepared statements

One way for sanitizing input in mysqli



Mysqli\_real\_escape\_string

* The mysqli\_real\_escape\_string() function escapes special characters in a string for use in an SQL statement.

Register Globals

* register\_globals is an internal PHP setting which registers the $\_REQUEST array's elements as variables.
* If you submit a value in a form, via POST or GET, the value of that input will automatically be accessible via variable in the PHP script, named after the name of the input field.

Session Register

* Register one or more global variables with the current session.