**SQL Injection**

select \* from users where name=‘admin’and password='1234';

imagine this is the correct username and password but we donot know the password.

* We can use this as username 🡪 admin' or '1'='1'
* This will make my query as   
  select \* from users where name='admin' or '1'='1' and password='1234';

2. Second method could be 🡪 admin’--

This will make my query: anything after -- is taken as comment  
select \* from users where name='admin’-- ’ and password='1234';

3. When we don’t know the username also

' or 1=1 --

(this works)

**How to prevent this??**

* **Use this**

If(isset($\_POST[‘submit’]))

{

$user=$\_POST[‘username’];

$user=mysqli\_real\_escape\_string($sonn,$user); //this will escape suspicious characters

}